Adviesraad
Internationale
Vraagstukken

# Regulering van online content

Naar een herijking van het Nederlandse internetbeleid

AIV-advies 113
24 juni 2020

## Adviesraad Internationale Vraagstukken

De Adviesraad Internationale Vraagstukken (AIV) is het adviescollege voor regering en parlement op het gebied van buitenlands beleid. De AIV adviseert gevraagd en ongevraagd over internationale vraagstukken. Het betreft in het bijzonder Europese samenwerking, mensenrechten, ontwikkelingssamenwerking en veiligheidsbeleid. De adviesraad richt zich op strategische dilemma's en op de agendering van nieuwe thema's met het oog op de langere termijn. De AIV beoogt met onafhankelijke, zorgvuldig beargumenteerde adviezen actuele internationale ontwikkelingen te analyseren en te duiden, aanbevelingen te doen voor het Nederlands buitenlands beleid en op deze manier bij te dragen aan het politieke en maatschappelijke debat over internationale kwesties.

### Samenstelling Adviesraad Internationale Vraagstukken

**Voorzitter**
Prof. mr. J.G. (Jaap) de Hoop Scheffer

**Vicevoorzitter**
Prof. dr. ir. J.J.C. (Joris) Voorhoeve

**Leden**
LGen b.d. G.J. (Jan) Broeks
Prof. mr. C.P.M. (Tineke) Cleiren
Prof. dr. E.M.H. (Ernst) Hirsch Ballin
Prof. dr. L.J. (Luuk) van Middelaar
Prof. dr. M.E.H. (Mirjam) van Reisen
Mr. J.N.M. (Koos) Richelle
Drs. M. (Monika) Sie Dhian Ho

**Secretaris**
Drs. M.E. (Marja) Kwast-van Duursen

### Leden gecombineerde commissie regulering online content

**Voorzitter**
Prof. mr. C.P.M. (Tineke) Cleiren

**Leden**
Prof. dr. E. (Edwin) Bakker
Prof. mr. J.H. (Janneke) Gerards
Mr. dr. B.W. (Bart) Schermer

**Secretarissen**
Drs. R.A.G. (Robert) Dekker MSc
Dr. M.M. (Marenne) Jansen

**Stagiairs**
N. (Nadine) Kops
M.A. (Jodie) in 't Groen LLM

De AIV heeft het advies **Regulering van online content: Naar een herijking van het Nederlandse internetbeleid** (AIV-advies 113) vastgesteld op 24 juni 2020.

# Inhoudsopgave

# Samenvatting

naar inhoud

Het internet is lange tijd bejubeld als forum van vrije informatie-uitwisseling, als aanjager van mensenrechten, emancipatie, diversiteit, democratie en als motor van innovatie en economische groei. Het is een hooggewaardeerd goed met een publieke kern. Het open en vrije karakter ervan is essentieel. Het is bovendien een instrument om fundamentele rechten te beschermen en te bevorderen, en het belang daarvan zichtbaar te maken en te houden. Het internet heeft mede hierdoor een centrale rol verworven in het dagelijks leven en het publieke debat, en het heeft zich met grote snelheid en op grote schaal ontwikkeld tot een vitale infrastructuur in grote delen van de wereld.

Het gepercipieerde karakter en de waarde van het internet hebben effect gehad op de manier waarop daarmee is omgegaan, zowel nationaal als internationaal en zowel in de publieke als in de private sector. Zo lag het zwaartepunt van beleidsvorming en regulering van het internet de afgelopen decennia bij het stimuleren van het vrije en open karakter van het internet. Naast deze perceptie en waardering hebben ook andere ontwikkelingen en motieven invloed gehad op de regulering en beleidsvorming rondom het internet, zoals economische ontwikkelingen (bijvoorbeeld de *new economy* van de jaren negentig) en (geo)politieke ontwikkelingen (zoals globalisering en de twitter-revoluties in het Midden-Oosten).

Het internet heeft de verspreiding van informatie een fundamenteel andere dynamiek gegeven. Content kan in zeer korte tijd wereldwijd met miljoenen internetgebruikers worden gedeeld. Met behulp van kunstmatige intelligentie en algoritmes kunnen heel gericht specifieke doelgroepen worden bereikt. Dit maakt van het internet een welhaast onweerstaanbaar instrument voor politiek-ideologische doeleinden. Daardoor is in toenemende mate duidelijk geworden dat het internet, ondanks zijn grote waarde, evenzeer kan worden ingezet om grote maatschappelijke schade aan te richten. Met behulp van het internet kunnen – letterlijk – levens worden verwoest.

Deze nadelige effecten van de snelle ontwikkeling van het internet en de daarmee samenhangende (potentiële) bedreigingen van mensenrechten hebben door allerlei omstandigheden relatief weinig aandacht gekregen. Voor overheden met een democratisch rechtsstatelijk fundament hebben de positieve effecten van het internet voor de grondrechten lange tijd prioriteit gehad, ook al werden uitwassen wel gezien. *Internet Service Providers* (ISPs) en digitale platformen waren en zijn vooral gericht op financiële belangen en een daarbij passend verdienmodel. Veel gebruikers laven zich aan de ongekende mogelijkheden en zijn nauwelijks kritisch over aantastingen van hun privacy, risico's van discriminatie of het gevaar voor beïnvloeding van hun opvattingen.

De nadelige effecten van het internet zijn in het bijzonder zichtbaar waar het gaat om de vele informatie die online wordt verspreid (online content). De AIV verstaat in dit advies onder online content uitingen gedaan door gebruikers (individuen, groepen, organisaties) via het internet, zoals het plaatsen van berichten op sociale media, online fora en websites. Deze online content beslaat een breed spectrum aan uitingen dat loopt van evident illegale uitingen tot en met uitingen die volledig onschuldig zijn. Tussen deze twee uitersten bevinden zich uitingen waarvan de strafbaarheid of onwenselijkheid afhankelijk is van tal van sociale, culturele en historische factoren en percepties. Binnen dit spectrum richt dit advies zich specifiek op de regulering van illegale, schadelijke of anderszins ongewenste content. Het gaat dan om content die de grondrechten van burgers aantast of een bedreiging vormt voor publieke waarden en de democratische rechtsorde.

Regulering van online content levert duivelse dilemma's op. Steeds moeten keuzes worden gemaakt tussen verschillende (mensen)rechten die als het ware tegenover elkaar komen te staan. Enerzijds kan

de introductie van zorgplichten voor internetplatformen of een grotere invloed van de overheid op het internet immers leiden tot een aantasting van de vrijheid van meningsuiting, het recht op toegang tot informatie, de bescherming van de persoonlijke levenssfeer en de vrijheid van ondernemerschap. Anderzijds kan niet-ingrijpen leiden tot discriminatie, aantasting van de veiligheid, en ondermijning van andere democratische en rechtsstatelijke beginselen. Bij de keuze voor regulering en de vorm daarvan zal steeds een balans moeten worden gevonden tussen verschillende rechten en belangen. Dit is een precair proces.

Bij de keuze van reguleringsopties is (technische) kennis van het internet als mondiaal, grensoverschrijdend netwerk van netwerken zonder centrale aansturing onontbeerlijk. Hetzelfde geldt voor kennis van de mogelijke consequenties van bepaalde technologische ingrepen. Met het tijdelijk geheel afsluiten van het internet, waartoe sommige overheden soms besluiten, kan bijvoorbeeld online content vergaand worden tegengehouden, maar het verlamt onmiddellijk de hele samenleving. Het gericht bestrijden van online content die door individuele gebruikers op internetplatformen en hun diensten wordt gedeeld is duidelijk minder ingrijpend – maar ook minder effectief. Daarnaast moet rekening worden gehouden met de diverse complicaties waarvoor de bijzondere aard van het internet ons stelt. Het sturend karakter van de technologie, de dominante positie van private internetbedrijven, de afwezige rechtsstaat, het fragmentarisch karakter van de bestaande regulering, en het ontbreken van grensoverschrijdende rechtsmacht brengen mee dat de aanpak van schadelijke online content uitermate complex is.

Bij het maken van reguleringskeuzes kiezen landen hun eigen weg, daarbij ook rekening houdend met hun eigen opvattingen over de onderliggende waarden en belangen. Autoritair geleide landen gebruiken het internet bijvoorbeeld als een overheidsinstrument om sociale cohesie, gewenst gedrag, politieke controle en nationale veiligheid te bewerkstelligen. Andere landen, waaronder de Verenigde Staten (VS), kijken door een bril van commerciële en individuele vrijheid naar het internet. Zij staan terughoudend tegenover overheidsingrijpen en geven de voorkeur aan zelfregulering door de techbedrijven. Europese landen als Duitsland, Frankrijk en het Verenigd Koninkrijk hebben al wetgeving aangenomen om schadelijke online content te bestrijden of hebben deze in voorbereiding. Ook de Europese Unie (EU) onderneemt initiatieven om illegale, schadelijke of terroristische online content op het internet tegen te gaan.

Binnen deze complexe context moet ook Nederland keuzes maken rondom het te voeren internetbeleid. Nederland heeft altijd grote waarde gehecht aan het internet als forum voor vrije informatie-uitwisseling, aanjager van mensenrechten en motor van innovatie en economische groei. Het Nederlandse beleid is van oudsher gericht op minimale regulering en het vrijlaten van de internetmarkt die grotendeels in private handen is. Waar regelgeving nodig is, stuurt Nederland traditioneel aan op zelfregulering door de techsector zelf. In het licht van de hierboven beschreven ontwikkelingen en factoren pleit de AIV voor een herijking van dit beleid.

## Uitgangspunten voor een herijkt internetbeleid

Uit de in dit advies gegeven analyse vloeien zeven uitgangspunten voort die volgens de AIV richtinggevend moeten zijn voor een herijkt internetbeleid en die de basis vormen voor een aantal – meer concrete – aanbevelingen.

**Een aanwezige rechtsstaat**

Bezien vanuit democratisch-rechtsstatelijk en mensenrechtenperspectief is een eenzijdige nadruk op het belang van innovatie en zelfregulering door de internetsector en van volledige internetvrijheid niet gerechtvaardigd. Om schadelijke online content effectief tegen te gaan moet de rechtsstaat nadrukkelijker aanwezig zijn, in die zin dat de overheid ervoor moet zorgen dat

rechtsstatelijke, democratische en grondrechtelijke waarborgen ook worden geboden waar het gaat om het internet. Bij de bestrijding van schadelijke content betekent dit dat de overheid haar verantwoordelijkheid moet nemen, zowel nationaal als internationaal. Zij moet op alle niveaus een politieke en maatschappelijke discussie entameren over de vraag welk soort uitingen nog acceptabel zijn binnen een open, democratische en rechtsstatelijke samenleving en welke niet, en welk soort handhaving hierbij passend is. Van de overheid mag bovendien worden verwacht dat zij naar aanleiding van een dergelijke discussie norm- en kaderstellend optreedt, toeziet op de handhaving van de gestelde regels, en voldoende rechtsbescherming biedt, dit alles met inachtneming van de basisbeginselen van een democratische rechtsstaat. Daarbij past bijvoorbeeld ook de betrokkenheid van onafhankelijke nationale expertorganisaties die toezien op de bescherming van mensenrechten. Daarbij valt te denken aan nationale mensenrechteninstituten, ombudspersonen en media-autoriteiten.

**Goede nationale en internationale coördinatie**

Inmiddels is bij alle betrokken spelers een groeiend bewustzijn van het belang van aanpak van schadelijke online content zichtbaar. De aard en omvang van de problematiek komen ook steeds beter in beeld, zowel nationaal als internationaal, en zowel bij publieke als private spelers. De in dit advies in kaart gebrachte activiteiten ten aanzien van schadelijke online content geven bovendien een beeld van een toenemend aantal initiatieven en beleids- en reguleringsinspanningen, zowel op nationaal als internationaal niveau. Tegelijkertijd moet worden geconstateerd dat deze initiatieven en inspanningen zich manifesteren op allerlei verschillende niveaus en tussen en binnen verschillende sectoren: nationaal, Europees, internationaal, publiek en privaat. Goede coördinatie en afstemming ontbreken. De wereldwijde, immense en groeiende impact van het internet op alle wereldburgers – en daarmee de potentiële schade aan mensenrechten die het gevolg kan zijn van schadelijke online content – noopt, gezien de governance en de eigenschappen van het internet, tot een goed gecoördineerd, gezamenlijk en gedeeld beleid van de diverse spelers in het veld, zowel publiek als privaat.

**Durf strategische en politieke keuzes te maken binnen rechtsstatelijke kaders**

Hoewel coördinatie en consensusvorming van groot belang zijn, mag de wens daartoe niet leiden tot besluiteloosheid. De (geo)politieke realiteit brengt onvermijdelijk mee dat strategische en politieke keuzes moeten worden gemaakt die op gespannen voet kunnen staan met de meest ideale oplossingen voor de aanpak van schadelijke online content. Wel moeten bij het maken van die politieke keuzes rechtsstatelijke kaders in acht worden genomen. Ten aanzien van bepaalde vormen van schadelijke online content bestaan zowel nationaal als internationaal heldere en kenbare normen, die worden gehandhaafd door instanties zoals het Europees Hof voor de Rechten van de Mens. Handelings- en reguleringsopties om schadelijke online content aan te pakken moeten uiteraard binnen de grenzen blijven zoals die door deze internationale en Europese normen zijn gedefinieerd. Ook waar er geen duidelijke (internationale) rechtspraak of juridische kaders zijn, waar consensus ontbreekt, of geopolitieke belangen niet in lijn met elkaar liggen, moet Nederland strategische en politieke keuzes durven maken die worden geïnformeerd door de rechtsstatelijke beginselen. Dat geldt zelfs als dit betekent dat het internet tot op zekere hoogte versnipperd raakt.

**Bijgesteld narratief: open en vrij internet binnen rechtsstatelijke en grondrechtelijke grenzen**

Het dominante narratief rondom internetvrijheid is geleidelijk aan het veranderen. Aanvankelijk was het uitgangspunt van het Nederlandse internetbeleid dat de vrijheid en openheid van het internet betekenden dat vrijwel iedere regulering van overheidswege moest worden vermeden. Inmiddels is duidelijk geworden dat het gebruik van het internet gepaard gaat met tal van vragen en dilemma's en dat ongehinderd gebruik van het internet inbreuken kan opleveren op mensenrechten van anderen en op rechtsstatelijke waarden. Dat betekent dat het tijd is dat de Nederlandse overheid het narratief bijstelt, namelijk naar dat van een open en vrij internet binnen rechtsstatelijke en grondrechtelijke grenzen. Die grenzen moeten gelden voor alle actoren die met het internet te maken hebben, van de overheid tot internetbedrijven en gebruikers.

Voor de overheid biedt dit bijgestelde narratief een zekere richting waar het gaat om de keuze voor handelings- een reguleringsopties. In het licht van het Nederlandse mensenrechtenperspectief en het bijgestelde narratief ligt de keuze voor minder absolute en verstrekkende reguleringsopties voor de hand, omdat die de mensenrechten in het algemeen het minst zwaar raken. Dat betekent dat moet worden vastgehouden aan de notie dat de publieke kern van het internet behouden moet blijven en dat daarin zo min mogelijk moet worden ingegrepen.[1] De handelingsopties liggen daardoor vooral op de andere niveaus, namelijk die van de digitale dienstverleners, de applicaties en de internetgebruikers. Dit betekent dat Nederland waakzaam moet zijn binnen internationale discussies over internettechnologieën en standaarden die de publieke kern aantasten en dat Nederland een actieve houding moet tonen waar het gaat om technologische innovaties die de publieke kern van het internet versterken. Daarnaast moet Nederland streven naar interventies in de contentlaag (websites, platformen, diensten en hun toepassingen of applicaties) van het internet die passen bij de rechtsstatelijke waarden en de grondrechten waar Nederland pal voor staat.

**Duidelijke kaderstelling rondom de verantwoordelijkheid van internetplatformen**

Internetplatformen dienen hun maatschappelijke verantwoordelijkheid te nemen bij het bestrijden van schadelijke en illegale content. Wanneer deze verantwoordelijkheid afgedwongen moet worden door wet- en regelgeving via het opleggen van een zorgplicht, dan is het van groot belang dat deze zorgplicht goed doordacht wordt. In het bijzonder moet er duidelijkheid zijn over wat schadelijke content is, met name in die gevallen waar het sterk van de context afhankelijk is. Ook waar duidelijkheid ontbreekt, mogen internetplatformen hun verantwoordelijkheid echter niet afschuiven. Op dat punt kunnen *good samaritan clauses* (behoud van aansprakelijkheidsvrijwaringen daar waar platformen zich bemoeien met de inhoud om schadelijke content te bestrijden) helpen om internetplatformen een meer proactieve rol aan te laten nemen. Hierbij is het van belang dat rekening wordt gehouden met ongewenste neveneffecten: internetplatformen mogen door dergelijke bepalingen niet nog meer controle en macht over het gebruik van hun platform krijgen. Bij de invulling van de juridische verantwoordelijkheid van internetplatformen is het ten slotte van belang om rekening te houden met de aard van de dienstverlening en de maatschappelijke positie van het internetplatform. In het bijzonder de marktmacht van partijen moet meegewogen worden bij de beoordeling van de aard en de omvang van hun zorgplicht.

**Onderkennen van het belang van alternatieve inrichting van technologieën en toepassingen**

Omdat de inrichting van een technologie of dienst de mogelijkheden en onmogelijkheden van het gebruik ervan bepaalt, is het van belang om bij het ontwerp van technologieën en diensten de impact daarvan op mensenrechten en maatschappelijke waarden nadrukkelijk mee te nemen. Het gebruik van *human rights impact assessments* en het ethisch ontwerp van systemen (*value sensitive design)* moet bevorderd worden. Verder moet de ontwikkeling van producten, diensten en toepassing die publieke waarden respecteren en het maatschappelijk belang dienen (*digital commons* en *open source*) ondersteund worden. Dit alles kan mede een tegenwicht vormen tegen de dominantie van commerciële, buitenlandse techbedrijven.

**Aandacht voor de internetgebruikers**

In de discussie over online content moeten de gebruikers niet uit het oog worden verloren. Internetgebruikers kunnen slachtoffer zijn van schadelijke online content, maar ook dader. Duidelijke normstelling, handhaving en voorlichting kunnen zowel bijdragen aan het leefbaar houden van het internet en aan bescherming van slachtoffers. In dit verband is het ook van belang dat gebruikers weerbaarder worden gemaakt. Onderwijs en voorlichting kunnen gebruikers helpen bij het herkennen en tegengaan van schadelijke content en *cyberbullying* en hen bewuster maken van privacyregels rondom opslaan en gebruik van hun persoonlijke data. Daarnaast moeten burgers in staat worden gesteld om actie te ondernemen tegen illegale en schadelijke content. Dit betekent dat zij content moeten kunnen melden bij de internetplatformen of specialistische meldpunten.
Tot slot moeten er effectieve mechanismen zijn voor de burger om content te (laten) verwijderen en om juridisch verhaal te halen bij degene die de schadelijke uitingen heeft gedaan of gefaciliteerd.

naar inhoud

# Aanbevelingen

naar inhoud

## ▸ Aanbeveling 1

**Herijk het Nederlandse internetbeleid**

Het huidige Nederlandse internetbeleid leunt traditioneel sterk op zelfregulering door de internetsector. Dit draagt het risico in zich dat internetplatforms een te grote zeggenschap krijgen over zowel regelgeving als handhaving en toezicht. De AIV meent dat in een democratische rechtsstaat de uiteindelijke zeggenschap in publieke handen dient te blijven, juist in een veld waar de private sector anders domineert. Hoewel samenspel met de private sector in multistakeholder governance de voorkeur geniet, moet de overheid dus nadrukkelijk aanwezig zijn als het gaat om het beschermen van mensenrechten en de rechtsstaat.

Het bestrijden van schadelijke online content kan volgens de AIV alleen effectief zijn in internationaal verband. Een herijking van het Nederlandse internetbeleid, waarbij een verschuiving plaatsvindt van zelfregulering naar vormen van co-regulering en een actieve rol voor de overheid, is daarvoor noodzakelijk. Een dergelijke aanpak moet zijn geworteld in een eenduidig en gecoördineerd nationaal beleid. Dat vereist dat op nationaal niveau de kennis en capaciteit, en de samenwerking en coördinatie tussen de vakministeries, lagere overheden, toezichthouders en bij het parlement wordt vergroot, zowel op het gebied van de werking van het internet als op het terrein van democratische en rechtsstatelijke waarden. Een goede nationale coördinatie is bovendien noodzakelijk om (bijvoorbeeld via onderwijs) de weerbaarheid van burgers ten aanzien van schadelijke online content te vergroten.

## ▸ Aanbeveling 2

**Verdedig en bevorder het open en vrije karakter van het internet op basis van democratische en rechtsstatelijke waarden**

Het open en vrije karakter van het internet staat onder druk door pogingen van landen om het nationale internet af te schermen of los te koppelen van de rest van de wereld. Nederland zou in moeten zetten op het verdedigen en bevorderen van het open en vrije karakter van het internet, maar dat moet wel plaatsvinden binnen de grenzen van democratische en rechtsstatelijke waarden (waaronder in het bijzonder de bescherming van mensenrechten). We moeten dus accepteren dat als er serieuze bedreigingen voor mensenrechten ontstaan of blijven bestaan door de inrichting van het internet, maatregelen moeten worden genomen om deze waarden te beschermen. Dit geldt zelfs als dit leidt tot enige regionale fragmentatie van het internet (versplintering).

## ▸ Aanbeveling 3

**Versterk de Nederlandse vertegenwoordiging in internationale internetorganisaties**

De toekomst van (de publieke kern van) het internet wordt bepaald in organisaties als de *Internet Corporation for Assigned Names and Numbers* (ICANN), de *Internet Engineering Task Force* (IETF), het *Internet Governance Forum* (IGF) en de *International Telecommunications Union* (ITU). Nederland moet gericht beleid voeren om de Nederlandse vertegenwoordiging in deze organisaties te vergroten en daarvoor mensen en middelen beschikbaar stellen. Als een van de belangrijkste internet-knooppunten ter wereld met een goed ontwikkelde internetinfrastructuur heeft Nederland hierbij een goede uitgangspositie.

naar inhoud

### ▸ Aanbeveling 4

**Stimuleer internationale normstelling voor de aanpak van schadelijke online content met een stevige verankering in bestaande mensenrechtenstandaarden**

Nederland moet een leidende rol nemen door in multistakeholder-organisaties internationale normstelling te stimuleren. Nederland kan in dit verband vooral op Europees niveau (Europese Unie) een betekenisvolle rol spelen. Concreet kan gedacht worden aan het initiëren van een Europese multistakeholder-taskforce die reguleringsopties van schadelijke online content in beeld brengt. Ook kan Nederland het lidmaatschap van de Raad van Europa en – op breder internationaal niveau – de VN-Mensenrechtenraad aangrijpen om met gelijkgezinde landen een internationale discussie te voeren over een op mensenrechten gestoelde aanpak van online content. Bestaande Europese mensenrechtenstandaarden onder meer op het gebied van kinderpornografie (Verdrag van Lanzarote) en het tegengaan van de verspreiding van racistisch en xenofobisch materiaal via computersystemen (Aanvullend Protocol bij het Verdrag van Boedapest) bieden handvatten om de internationale normstelling nader uit te werken.

### ▸ Aanbeveling 5

**Initieer maatregelen gericht op transparantie en toezicht**

Onafhankelijk toezicht op het identificeren en verwijderen van schadelijke content door internetplatformen draagt bij aan transparantie en rechtszekerheid voor internetgebruikers. Nederland moet zich in Europees verband inzetten om een Europees toezichtmechanisme te ontwikkelen. Een eerste stap in die richting is dat Nederland zich in Europees en in multistakeholder-verband hard maakt voor het transparant maken van het beleid van internetplatformen voor het identificeren en verwijderen van schadelijke content. De platformen moeten worden verplicht transparantierapporten te publiceren die voldoen aan eenduidige, op Europees niveau vastgestelde, criteria.

### ▸ Aanbeveling 6

**Stimuleer *value sensitive design* en *digital commons***

Het handelen van internetgebruikers wordt in hoge mate bepaald door de ruimte die de technologie van het internet hun biedt. Al bij het ontwerpen van nieuwe internettechnologieën en -toepassingen moet daarom rekening worden gehouden met mensenrechtelijke waarden zodat deze niet nadelig voor gebruikers uitpakken (*value sensitive design*). Nederland kan financiële middelen beschikbaar stellen voor onderzoeksprogramma's op dit gebied, zowel Europees als in multistakeholder-verband. Tevens kan Nederland bepleiten dat op Europees niveau kan worden geïnvesteerd in duurzame alternatieven voor bestaande internetdiensten met een publieke meerwaarde (*digital commons*).

### ▸ Aanbeveling 7

**Betrek onafhankelijke nationale expertorganen bij de beoordeling van schadelijke online content**

De beoordeling of content illegaal of schadelijk is, is sterk afhankelijk van de context. Bij het bepalen van de criteria voor de beoordeling en verwijdering van schadelijke content kunnen onafhankelijke nationale expertorganen een rol spelen. Daarbij kan gedacht worden aan nationale mensenrechteninstituten (zoals in Nederland het College voor de Rechten van de Mens), ombudspersonen en onafhankelijke media-autoriteiten. Zij kunnen voorts een actieve rol krijgen als *trusted flaggers* bij het toezicht op het beoordelen en verwijderen van schadelijke content in concrete gevallen.

## ▸ Aanbeveling 8

**Pleit voor een zorgplicht voor internetplatformen, onder duidelijke randvoorwaarden**

Europese wetgeving bepaalt dat internetplatformen – onder bepaalde voorwaarden – niet aansprakelijk zijn voor de informatie die gebruikers via het platform delen. Gezien de grote maatschappelijke verantwoordelijkheid die internetplatformen hebben bij het tegengaan van schadelijke online content is het van belang dat internetplatformen een zorgplicht krijgen, in het bijzonder wanneer zij zich bemoeien met de inhoud. Nederland moet zich inzetten om zo'n zorgplicht in Europese regelgeving tot uitdrukking te laten komen. Nederland moet hiertoe een voortrekkersrol nemen in de Europese discussie over de rol van internetplatformen, meer specifiek bij de onderhandelingen rondom de *Digital Services Act*. Een zorgplicht moet echter wel uitvoerbaar zijn voor de platformen. Dat vereist duidelijke criteria voor de beoordeling wat schadelijke content is, hoe en wanneer content verwijderd moet worden en hoe ver een zorgplicht reikt. Deze criteria kunnen met behulp van publiek-private samenwerking worden ontwikkeld en nader worden ingevuld, onder de randvoorwaarden gedefinieerd in aanbeveling 2 en met inachtneming van de in dit advies gedefinieerde uitgangspunten. Bij het opstellen van regels voor zorgplicht en aansprakelijkheid dient rekening te worden gehouden met de aard, omvang en marktmacht van internetplatformen. Ook dient nadrukkelijk rekening te worden gehouden met ongewenste neveneffecten die mensenrechten kunnen schaden, zoals zelfcensuur en het uitoefenen van meer controle over de inhoud.

## ▸ Aanbeveling 9

**Maak de gebruikersvoorwaarden van internetplatformen mensenrechten-inclusief**

Internetplatformen bepalen in belangrijke mate via hun gebruikersvoorwaarden in hoeverre en in welke situaties online content kan worden verwijderd, waarbij zij momenteel een ruime discretionaire bevoegdheid hebben. Nederland moet in de Europese Unie en de Raad van Europa bepleiten dat internetplatformen gehouden worden hun gebruikersvoorwaarden te baseren op internationaal erkende mensenrechtenstandaarden. In elk geval dienen zij de *UN Guiding Principles on Business en Human Rights* te onderschrijven.

## ▸ Aanbeveling 10

**Vergroot de digitale weerbaarheid van internetgebruikers**

Het is voor internetgebruikers niet altijd eenvoudig om schadelijke online content te herkennen of de gevolgen van (het plaatsen van) bepaalde content te overzien. Door middel van onderwijs en voorlichting moet Nederland nationaal en internationaal meer investeren in de digitale weerbaarheid van burgers, in het bijzonder voor groepen die minder internetvaardig zijn. Daarnaast moeten zij in staat gesteld worden om schadelijke content te melden en te (laten) verwijderen. Een Europees toezichtmechanisme als bepleit in aanbeveling 5 kan hierbij een rol spelen.

# Inleiding

Het internet werd lange tijd bejubeld als forum van vrije informatie-uitwisseling, als aanjager van mensenrechten, emancipatie, diversiteit, democratie en als motor van innovatie en economische groei. Internet kan evenzeer worden ingezet om grote maatschappelijke schade aan te richten.

Op vrijdagochtend 15 maart 2019 plaatst een 28-jarige Australische inwoner van de Nieuw-Zeelandse stad Dunedin een manifest van tientallen pagina's op 8chan, een online discussieplatform waarop gebruikers anoniem rechts-extremistische inhoud en kinderpornografie kunnen uitwisselen. In het document waarschuwt de man dat de Westerse samenleving en het blanke ras worden bedreigd door immigratie van moslims. Gewapend met semiautomatische vuurwapens rijdt hij vervolgens naar de stad Christchurch.
Daar aangekomen dringt hij de Al Noor-moskee binnen en begint om zich heen te schieten. Hij doodt 42 mensen. Via een hoofdcamera filmt de schutter de eerste 17 minuten van de aanslag en streamt hij die beelden via Facebook Live. Bij een tweede schietpartij, vijf kilometer verderop in het *Linwood Islamic Centre*, maakt hij 7 dodelijke slachtoffers. In totaal raken 49 mensen gewond. De man wordt 21 minuten na de eerste noodoproep gearresteerd.

Volgens Facebook[2] kijken tijdens de aanslag minder dan 200 mensen naar de livestream. Geen van hen rapporteert de video bij Facebook. De eerste melding komt pas 12 minuten na het einde van de livestream bij Facebook binnen. Facebook verwijdert daarop de originele video, maar die is dan al ongeveer 4000 keer bekeken. De beelden zijn dan bovendien inmiddels gedeeld via andere platformen zoals Liveleak, Youtube, Reddit en Twitter en als een downloadbestand op verschillende filesharing sites. In de eerste 24 uur na de aanslag verwijdert Facebook wereldwijd zo'n 1,5 miljoen video's van de aanslag en voorkomt naar eigen zeggen 1,2 miljoen uploads. Ook Youtube en Twitter proberen de video te verwijderen maar kunnen moeilijk op tegen de snelheid waarmee gebruikers nieuwe kopieën en links delen.[3]

De aanslagen maken internationaal veel reacties los. In mei 2019 maken 18 landen, waaronder Nederland, de Europese Commissie en acht techbedrijven in Parijs afspraken om de verspreiding van terroristische en extremistische online content tegen te gaan. In september sluiten nog eens 31 landen, de Raad van Europa en de UNESCO zich aan bij deze *Christchurch Call to Action*. Wel zijn degemaakte afspraken breed geformuleerd en vrijwillig. De Verenigde Staten zeggen de doelstellingen van de verklaring te steunen maar doen zelf niet mee, omdat dit mogelijk strijdig wordt geacht met grondwettelijke bepalingen over de bescherming van de vrijheid van meningsuiting.

Maanden later zijn het manifest van de dader – inmiddels in meerdere talen vertaald – en beelden van de aanslag nog altijd vindbaar op het internet.[4]

## 1.1 Focus, context en leeswijzer

De minister van Buitenlandse Zaken heeft – mede in het licht van de aanslagen in Christchurch – de Adviesraad Internationale Vraagstukken (AIV) gevraagd om beleidsaanbevelingen te doen voor een 'rechtsstatelijke mensenrechten-inclusieve benadering van regulering van online content'.
De adviesaanvraag van de minister sluit naadloos aan op de vraag of het traditionele internetbeleid

van Nederland – dat is gestoeld op het initiële optimisme over de werking en de effecten van het internet uit de jaren'90 en '00– nog wel past bij de huidige tijd. Niemand voorzag de snelheid waarmee het internet zich ontwikkelde tot een vitale infrastructuur in grote delen van de wereld en de schaal waarop dat is gebeurd, noch de nadelige effecten ervan zoals die worden geïllustreerd door het in het kader gegeven voorbeeld. Ook de focus van overheden en de techsector op innovatie, economische ontwikkeling en gebruikersgemak leidde ertoe dat de ogen lang gesloten bleven voor de mensenrechtelijke en bredere geopolitieke gevolgen van het internet. De voordelen van het internet, maar ook de complexiteit van de werking daarvan susten gebruikers in slaap: zij blijken zich vaak nauwelijks bewust van de bedreigingen van hun privacy, van beïnvloeding van hun meningen door desinformatie of de beperkingen van toegang tot informatie. Deze stand van zaken wordt weerspiegeld in de beperkte en fragmentarische regelgeving ten aanzien van schadelijke online content.

Toch is langzaam een kentering zichtbaar geworden en is er sprake van een groeiend bewustzijn van de schaduwkanten van het internet. Zelfs Facebookoprichter Mark Zuckerberg pleit al enige tijd voor wettelijke kaders waarbinnen schadelijke content kan worden aangepakt. Ook maakte Facebook in mei 2020 de oprichting bekend van een eigen onafhankelijke toezichthouder.[5] De internationale discussie die dergelijke ontwikkelingen teweegbrengen laat zien dat het vinden van oplossingen voor de aanpak van schadelijke online content urgent is, maar ook dat dit geen vanzelfsprekend of eenvoudig proces is. Het is binnen deze complexe context dat dit rapport moet worden gepositioneerd.

In deze inleiding wordt het in de adviesaanvraag voorgelegde vraagstuk nader in kaart gebracht. Het spanningsveld tussen het belang van het internet voor de mensenrechten en de risico's van het internet voor de mensenrechten wordt zichtbaar gemaakt. Ook wordt het internationale krachtenveld, de context waarbinnen het vraagstuk moet worden geplaatst, in de inleiding beschreven. Daarnaast wordt geduid wat onder schadelijke online content wordt begrepen. Hoofdstukken 2 en 3 beschrijven vervolgens respectievelijk de technische werking van het internet en de huidige stand van multilaterale reguleringsmodaliteiten. In hoofdstuk 4 worden de beperkingen en randvoorwaarden die eigen zijn aan het internet nader besproken en geplaatst in het perspectief van een effectief en mensenrechten-inclusief internetbeleid. Tot slot worden in het afsluitende hoofdstuk 5 de risico's en dilemma's van het reguleren van online content voor de mensenrechten geduid en wordt een aantal oplossingsrichtingen besproken. Deze analyse mondt uit in de in de samenvatting neergelegde zeven uitgangspunten die de basis vormen voor de tien – meer concrete – aanbevelingen van de AIV.

## 1.2 Mensenrechten en internet: positieve en negatieve kanten

De in het kader geschetste gebeurtenissen in Christchurch hebben pijnlijk duidelijk gemaakt dat het internet zijn onschuld heeft verloren. Met behulp van het internet kunnen – letterlijk – levens worden verwoest. Opruiende pamfletten en beelden van gewelddadigheden zijn op zichzelf niet nieuw en ook niet per se verbonden met het internet. Het internet heeft de verspreiding van informatie echter een fundamenteel andere dynamiek gegeven. Allereerst kan content in zeer korte tijd wereldwijd met miljoenen internetgebruikers worden gedeeld. Tegelijkertijd kunnen met behulp van kunstmatige intelligentie en algoritmes heel gericht specifieke doelgroepen worden bereikt. Dit maakt het internet tot een welhaast onweerstaanbaar instrument voor politiek-ideologische doeleinden. Het internet verbindt, maar kan mensen ook uit elkaar drijven.

Deze ontwikkelingen staan niet op zichzelf. Online desinformatiecampagnes waarmee Russische internettrollen de Amerikaanse presidentsverkiezingen probeerden te beïnvloeden, IS-propaganda-video's op Youtube, Chinese berichtgeving rondom het coronavirus, of grof taalgebruik op sociale media en in Whatsapp-groepen. De onoverzichtelijke grens tussen openbaarheid en vertrouwelijkheid

van communicatie via het internet kan risico's met zich meebrengen voor de privacy. Twitter bijvoorbeeld is openbare communicatie maar wordt door velen gebruikt alsof het besloten communicatie in een groep zou zijn. Al deze voorbeelden laten zien dat het internet negatieve effecten kan hebben op mensenrechten en op andere publieke waarden. Dit heeft geleid tot een groeiende politiek-maatschappelijke discussie over de vraag of elke uitlating op het internet moet zijn toegestaan. Er wordt daarbij al snel naar de overheid gekeken, die door middel van wetgeving paal en perk zou moeten stellen aan de verspreiding van dit soort online content. Ook vinden velen dat techbedrijven (meer in het bijzonder *Internet Service Providers* (ISPs) en sociale-mediaplatformen (SMPs) moeten worden gedwongen tot een actievere zorgplicht waar het gaat om het monitoren van de content die gebruikers op het internet delen.

De reacties op 'Christchurch' tonen aan hoezeer ook de techbedrijven worstelen met deze problematiek. Ondanks de technologische middelen waarover SMPs beschikken, zijn zij niet altijd in staat om effectief op te treden tegen schadelijke content die de gebruikers van het platform plaatsen. Overheden zijn eveneens zoekende. Gezien het grensoverschrijdende karakter van het internet kan schadelijke online content alleen zinvol via een internationale aanpak worden ingedamd. Het ontbreekt echter aan internationale consensus over wat precies onder dergelijke content moet worden begrepen en wat de juiste aanpak daarvan zou moeten zijn. Wellicht nog belangrijker is dat iedere inperking van de vrije informatiestroom op het internet op gespannen voet staat met de vrijheid van meningsuiting en het recht op informatie. In liberale democratieën zijn het juist deze belangrijke mensenrechten die niet simpelweg kunnen worden ingeperkt.

In dit internationale vacuüm kiezen landen hun eigen weg. Landen als Duitsland, Frankrijk en het Verenigd Koninkrijk hebben al wetgeving aangenomen om schadelijke online content te bestrijden of hebben deze in voorbereiding. Ook de EU onderneemt initiatieven om illegale, schadelijke of terroristische online content op het internet tegen te gaan. Andere landen, waaronder de Verenigde Staten, staan terughoudend tegenover overheidsingrijpen en geven de voorkeur aan zelfregulering door de techbedrijven.

## Het internet verbindt, maar wordt ook ingezet om grote maatschappelijke schade aan te richten.

Nederland heeft altijd grote waarde gehecht aan het internet als forum voor vrije informatie-uitwisseling, aanjager van mensenrechtenbescherming en motor van innovatie en economische groei. De adviesaanvraag (zie bijlage 1) benadrukt dat het Nederlandse internetbeleid zich richt op het verdedigen en stimuleren van een open, vrij en veilig internet vanuit de gedachte dat mensenrechten ook op het internet onverminderd van kracht zijn. Uitgangspunt is tegelijkertijd dat Nederland veiligheid en vrijheid niet als tegengestelde, maar als fundamenteel complementaire belangen beschouwt. Het stimuleren van zowel de vrijheid van meningsuiting als de internetvrijheid is een van de prioriteiten in het Nederlandse mensenrechtenbeleid. De universele rechten van de mens gelden, aldus het kabinet, zowel offline als online. Bijzondere aandacht gaat daarbij uit naar vrijheid van meningsuiting, vrije informatievergaring, privacy en bescherming van persoonsgegevens.[6] Met betrekking tot de regulering van het internet is het Nederlandse beleid tot dusver gericht op minimale regulering en het vrijlaten van de internetmarkt die grotendeels in private handen is. Waar regelgeving nodig is, stuurt Nederland traditioneel aan op zelfregulering door de techsector zelf. Bij dit beleid past van oudsher een terughoudende rol van de overheid.

## 1.3 Het internationale krachtenveld

De adviesvraag van de minister van Buitenlandse Zaken gaat specifiek over de regulering van online content. Het is dan verleidelijk om onmiddellijk in te zoomen op dit specifieke thema. Het onderwerp kan echter niet los worden gezien van de bredere maatschappelijke discussie rondom de governance van het internet. De reden hiervoor is dat het succes van maatregelen om schadelijke online content te bestrijden sterk afhankelijk is van de technische en organisatorische inrichting van het internet. Deze inrichting is niet enkel het domein van nationale overheden, maar vormt een transnationale aangelegenheid waarbinnen overheden, bedrijven, technische experts en civil society in gezamenlijkheid besluiten over de vormgeving van het internet. Er wordt in dit rapport dan ook geen wezenlijk onderscheid aangebracht tussen binnenlands en buitenlands internetbeleid. Dit rapport van de AIV begint daarom met een schets van de geopolitieke context waarbinnen deze internet governance plaatsvindt.

**Het toenemend belang van het internet**

Binnen enkele decennia is het internet van een grenzeloze ruimte waarin gebruikers vrijelijk kennis en ideeën met elkaar kunnen uitwisselen, uitgegroeid tot de ruggengraat van internationale handel en wereldwijde communicatie. In een groot deel van de wereld drijft de dienstverlening van de overheid en van bedrijven inmiddels op informatie- en communicatietechnologie (ICT), waaronder het internet. Ook ondersteunende technologieën als het *Internet of Things*, waarbij apparaten online met elkaar in verbinding staan (denk aan de slimme energiemeter of een espressoapparaat dat via een app op de smartphone kan worden ingeschakeld), maken dat het internet tot in de haarvaten van de samenleving is doorgedrongen. Dat heeft grote waarde, maar het maakt samenlevingen ook kwetsbaar, met name in technologisch hoogontwikkelde – veelal Westerse – landen met een hoge internetpenetratie.[7] Dat geldt zeker voor Nederland dat een groot aantal datacentra huisvest en met de *Amsterdam Internet Exchange* een van de grootste internetknooppunten ter wereld binnen de landsgrenzen heeft. Een goed gerichte hack kan leiden tot grote maatschappelijke ontwrichting.

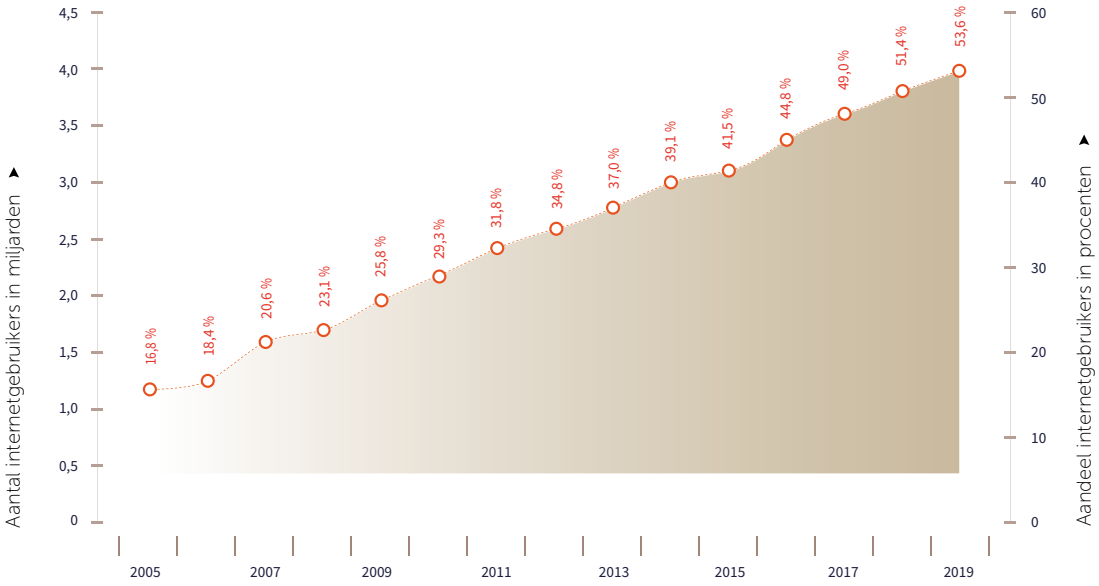
**Internet als geopolitiek instrument**

In zijn internationale cyberstrategie (2017) schrijft het kabinet dat verschillende kwaadwillende actoren steeds meer gebruik maken van het internet (cyberdomein) om hun belangen na te streven, bijvoorbeeld voor geldelijk gewin, het verwerven van informatie of politiek-militaire doeleinden.[8] Het internet wordt in toenemende mate gebruikt door criminelen die bijvoorbeeld door middel van hacks, het digitaal gijzelen van netwerken en *phishingmails* economische schade toebrengen aan bedrijven, instellingen en burgers. Ook voor staten is het internet een aantrekkelijk geopolitiek machtsinstrument geworden. Via het internet wordt gespioneerd en met behulp van desinformatiecampagnes in andere landen kunnen politieke processen worden verstoord of maatschappelijke groepen tegen elkaar worden opgezet. Landen als Rusland, Iran en Noord-Korea, gebruiken het internet als instrument van hybride oorlogvoering om tegen relatief lage kosten andere landen te destabiliseren.[9]

Deze ontwikkelingen leveren continue bedreigingen op voor de vrijheid en veiligheid in de samenleving. Tegelijkertijd maakt het decentrale, grensoverschrijdende en anonieme karakter van het internet dat het voor overheden steeds moeilijker wordt om tegen cyberagressie – zowel statelijk als niet-statelijk – op te treden. Opsporings- en inlichtingendiensten vinden bijvoorbeeld IP-adressen in plaats van aanwijsbare burgers die op basis van strafrecht kunnen worden vervolgd. Klassieke veiligheidsconcepten gebaseerd op nationale soevereiniteit, de inzet van militaire middelen en bondgenootschappelijke afspraken over collectieve verdediging voldoen in dit nieuwe schemergebied niet meer. Op termijn kan dit zelfs de internationale rechtsorde ondermijnen. Operaties via internet vinden bovendien veelal plaats buiten het zicht van de samenleving en de politiek. Daardoor is er – anders dan over de inzet van conventionele of nucleaire militaire middelen – geen maatschappelijk debat over de wenselijkheid van dergelijke acties. Zolang landen geen verantwoordelijkheid erkennen

## Wereldwijde internetpenetratie in procenten

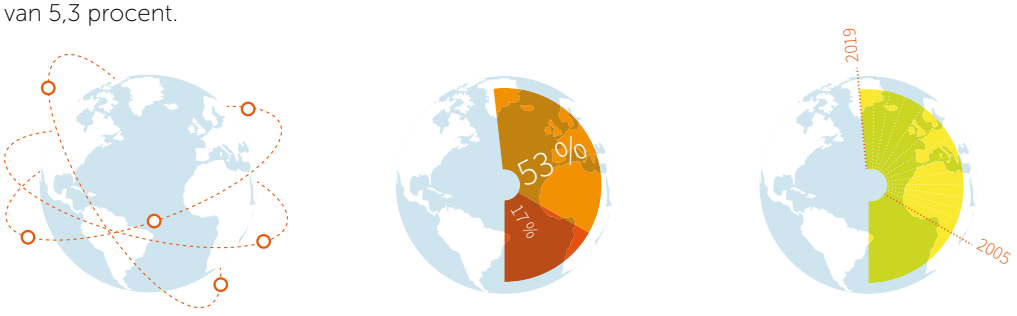
naar inhoud




In 2019 maakten naar schatting 4,1 miljard mensen gebruik van internet; vergeleken met 2018 is dit een toename van 5,3 procent.

De wereldwijde internetpenetratie steeg van bijna 17 procent in 2005 tot ruim 53 procent in 2019.

Tussen 2005 en 2019 steeg het aantal internetgebruikers met gemiddeld 10 procent per jaar.




**Figuur 1:** Wereldwijd internetgebruik. Gebaseerd op ITU, Measuring digital development. Feiten en cijfers 2019.

voor hun cyberactiviteiten is het ook niet mogelijk om internationale afspraken te maken en daar wederzijdse controle op uit te oefenen.

**Data: de nieuwe olie?**

Een andere belangrijke ontwikkeling die de uitvinders van het internet niet hadden kunnen voorzien, is die van exponentiële groei van de data die bedrijven en overheden verzamelen van internetgebruikers. Het bezit van en de zeggenschap over data zijn politiek en economisch van onschatbare waarde geworden.[10] Met behulp van persoonlijke gegevens die internetgebruikers actief afstaan (door in te stemmen met gebruikersvoorwaarden) of passief achterlaten (door hun surfgedrag) kunnen bedrijven en overheden gedetailleerde profielen samenstellen en die gebruiken voor commerciële of politieke doelen. Dit roept vragen op met betrekking tot verantwoordelijkheid, aansprakelijkheid en controleerbaarheid van het verzamelen en gebruiken van data en daarmee in wezen over democratische rechtsstatelijkheid.

## Een wereldwijde, geharmoniseerde en mensenrechteninclusieve benadering van online content is nog ver weg.

**Wie heeft de macht over het internet?**

Omdat het internet zo belangrijk is geworden, is ook de controle over het internationale beheer van het internet inzet van geopolitieke strijd. Achterliggende waarden en belangen bepalen de inzet van staten ten aanzien van het internet en het gebruik van data.[11] Aan de ene kant van het spectrum staan autoritair geleide landen die het internet als een instrument voor de overheid zien om sociale cohesie, controle en nationale veiligheid te bewerkstelligen. Zij bestrijden criminaliteit en terrorisme, maar ook politieke opponenten, door internetgebruikers met behulp van cybersurveillance in de gaten gehouden. In hun visie horen niet private partijen, maar de overheid de controle te voeren over het internet en behoren data toe aan de staat. China is het meest in het oog springende voorbeeld van een dergelijk op overheidsregulering gericht land (zie ook AIV-advies 111, *China en de strategische opdracht voor Nederland in Europa*, 2019). Aan de andere kant van het spectrum staan landen als de Verenigde Staten, die enerzijds door een bril van commerciële en individuele vrijheid naar het internet kijken en anderzijds een bijna absolute (constitutionele) invulling geven aan de vrijheid van meningsuiting. Dat vertaalt zich in minimale overheidsregulering, privaat eigendom van de internetinfrastructuur, nadruk op innovatie en commerciële exploitatie van persoonsgegevens. Daarnaast steunt de Amerikaanse overheid in haar handelsbeleid de grote Amerikaanse techbedrijven die het internet domineren. Zij zijn in staat om nieuwkomers buiten de deur te houden, onder meer door succesvolle startups op te kopen en zo potentiële concurrentie te neutraliseren. Door tussen nationale rechtsregels door te laveren, betalen deze techbedrijvenbovendien nauwelijks belasting in de andere landen waarin zij actief zijn.

Een derde model van omgang met het internet, dat zich ergens in het midden van het spectrum positioneert, is te vinden in Europa.[12] Net als de Verenigde Staten onderschrijft Europa waarden als vrijheid van meningsuiting en online vrijheid van informatie. Privaat beheer van het internet wordt gezien als voorwaarde voor economische ontwikkeling en innovatie. Tegelijkertijd lijken de opvattingen in Europa en ook Nederland in het laatste decennium weer enigszins te verschuiven in de richting van een sterkere rol voor de overheid, juist om bepaalde rechtsstatelijke en grondrechtelijke waarden te kunnen beschermen. Een verschil met de VS is bijvoorbeeld dat er in Europa een grotere bereidheid bestaat om burgers te beschermen door middel van strenge regelgeving op het gebied van

privacy en door regulering van online content. Een aansprekend voorbeeld is de Algemene verordening gegevensbescherming (AVG), waarmee de EU eigenstandig een wereldwijd relevante standaard heeft gecreëerd. Tegelijkertijd laat dit zien hoezeer de Europese benadering verschilt van de Chinese: mensenrechten als privacy en vrijheid van meningsuiting staan hier bij het vormgeven van overheidsregulering hoog in het vaandel. Anders dan de VS en China heeft Europa bovendien vrijwel geen grote internetplatformen.[13]

Bovenstaande laat zien dat er in velerlei (groepen van) landen een sterk verschillende aanpak van de bijzondere kansen en bedreigingen van het internet bestaat, die wordt bepaald door hun (rechts) cultuur en hun eigen, achterliggende waarden. Een wereldwijde, geharmoniseerde en mensenrechten-inclusieve benadering van online content is dan ook nog ver weg.

**Multistakeholder-model**

Voor zover er al sprake is van een zekere wereldwijde governance van het internet, is die tot nu toe gebaseerd op het zogenaamde multistakeholder-model. Dit betekent dat alle betrokken partijen – bedrijfsleven, overheden, maatschappelijke organisaties, toezichthouders, kennis- en onderzoeksinstellingen – in gezamenlijkheid besluiten over het bestuur en de ontwikkeling van het internet. Een voorbeeld is de *Internet Corporation for Assigned Names and Numbers* (ICANN). De ICANN is een private non-profitorganisatie die een aantal internet-gerelateerde taken uitvoert, zoals het toekennen en specifiëren van topleveldomeinen, het toewijzen van domeinnamen en de distributie van IP-nummers (zie hoofdstuk 2). De ICANN heeft daarmee een grote invloed op de vormgeving van het internet. Naast ICANN zijn technische gremia relevant waar over de technische inrichting van het internet wordt besloten. Het gaat dan in het bijzonder om de *Internet Engineering Taskforce* (IETF) en de *Internet Architecture Board* (IAB). Naast de technische gremia zijn er de meer politieke gremia zoals het *Internet Governance Forum* (IGF) en het *Global Network Initiative* (GNI). Daar waar het binnen de technische gremia gaat over de technische werking van het internet gaat het binnen het IGF en de GNI meer over het gebruik van het internet. Toch kunnen techniek en gebruik niet los van elkaar worden gezien, omdat de inrichting van de technologie de mogelijkheden van het gebruik bepalen (zie hoofdstuk 2).

Het multistakeholder-model is kwetsbaar. Een kleine groep goed ingevoerde experts of (door nationale overheden ondersteunde) techbedrijven kan disproportioneel veel invloed op de besluitvorming uitoefenen. Maatschappelijke organisaties zijn ondervertegenwoordigd en hebben niet de financiële middelen om een krachtig tegengeluid te laten horen. Vanuit mensenrechtenperspectief bezien biedt het multistakeholder-model daardoor te weinig waarborgen. Tegelijkertijd biedt het multistakeholder-model wel de belangrijke waarborg dat (autoritaire) staten geen dominante rol kunnen spelen in de besluitvorming over de werking van het internet. Om die reden hebben China, Rusland en andere landen[14] bijvoorbeeld al eerder pogingen gedaan om het multistakeholder-model te ondermijnen en intergouvernementele organisaties zoals de *International Telecommunications Union* (ITU) (en daarmee nationale overheden) een grotere rol te geven bij de besluitvorming over het internet. Die pogingen waren niet succesvol, onder andere door weerstand vanuit de Verenigde Staten, daarin gesteund door Nederland. Toch is er inmiddels groeiende invloed van sommige landen op de governance van het internet. Dat geldt in het bijzonder voor de Verenigde Staten, waar het internet in belangrijke mate is ontwikkeld en waar 's werelds grootste internetbedrijven zijn gehuisvest. Als onderdeel van de bredere machtsstrijd tussen beide landen zoekt ook China naar wegen om de governance van het internet te beïnvloeden. China doet dit bijvoorbeeld door via strategisch personeelsbeleid landgenoten te benoemen op invloedrijke posities in internationale VN-organisaties die ook een rol spelen in de governance van het internet. Recent kwam de benoeming van een Chinese kandidaat als Directeur-Generaal van de Wereldorganisatie voor Intellectueel Eigendom (WIPO) na Amerikaanse inspanningen niet tot stand.[15] Als lid van de Veiligheidsraad en als grote geldschieter van de VN heeft China de nodige invloed binnen deze organisatie. Daarnaast bouwt China aan een informele machtsbasis in multilaterale instellingen door een groot aantal landen aan

zich te binden, onder meer door het geven van financiële en technische steun in het kader van de Nieuwe Zijderoute. China wordt daarbij in de kaart gespeeld door de huidige Amerikaanse regering, die multilaterale samenwerking juist de rug toekeert en minder bereid is om op basis van gemeenschappelijke waarden internationale coalities te bouwen. China springt behendig in het gat dat de VS achterlaten, ook op het gebied van internet-governance.[16]

**Uiteenvallen van het wereldwijde internet**

De kracht van het internet is gelegen in het decentrale en grensoverschrijdende karakter ervan. Tegen de achtergrond van de bredere geopolitieke machtsstrijd op het wereldtoneel dreigt echter voortdurend het gevaar van het uiteenvallen van het wereldwijde internet in meerdere regionale of nationale internetten. Rusland werkt al aan het ontwikkelen van een gesloten, eigen internet. Ook China doet dit door bijvoorbeeld Google, Facebook, Twitter en Wikipedia niet toe te laten ten gunste van Chinese, door de eigen overheid gesponsorde, alternatieven. In dit verband wordt ten aanzien van China ook wel gesproken van de *Great Firewall*, een systeem van internetcensuur. Vanuit mensenrechtenperspectief is deze ontkoppeling van internetsystemen een zorgwekkend vooruitzicht. Als landen en regio's zich opsluiten achter digitale dijken, wordt het voor hun inwoners steeds moeilijker om met elkaar in gesprek te gaan en informatie uit te wisselen, waardoor er weinig overblijft van de oorspronkelijke openheid en vrijheid van het internet.

Als landen en regio's zich opsluiten achter digitale dijken, verliest het internet de oorspronkelijke vrijheid.

## 1.4 Schadelijke online content: waar hebben we het over?

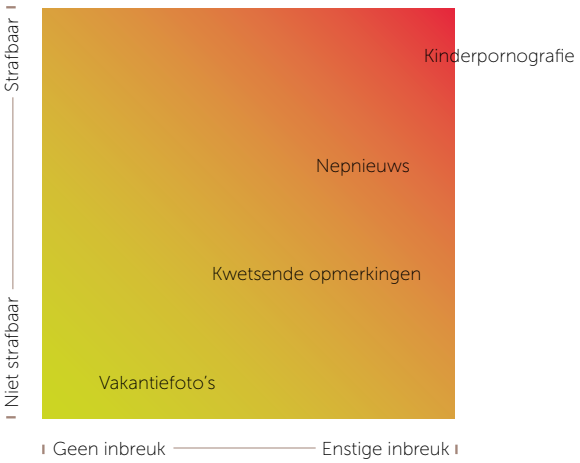
De AIV verstaat in dit advies onder 'online content' uitingen gedaan door gebruikers (individuen, groepen, organisaties) via het internet, zoals het plaatsen van berichten op sociale media, online fora en websites. Online content beslaat een breed spectrum aan uitingen dat loopt van evident illegale uitingen (bijvoorbeeld beelden van kindermisbruik) tot en met uitingen die volledig onschuldig zijn (bijvoorbeeld het plaatsen van vakantiefoto's). Tussen deze twee uitersten bevinden zich uitingen waarvan de strafbaarheid of onwenselijkheid afhankelijk is van tal van sociale, culturele en historische factoren en percepties. Binnen dit spectrum richt dit advies zich specifiek op de regulering van illegale, schadelijke of anderszins ongewenste content. Het gaat dan om content die de grondrechten van burgers aantast of een bedreiging vormt voor publieke waarden en onze democratische rechtsorde.

De context waarin een uiting wordt gedaan speelt een belangrijke rol bij de beoordeling of content illegaal of schadelijk is. Deze context wordt onder meer bepaald door de concrete situatie waarin een uiting is gedaan, de intentie van de afzender, de bedoelde ontvanger, de maatschappelijke en politieke omstandigheden of het tijdgewricht. De uiting 'ik hak je kop eraf' kan binnen de context van twee vrienden die bijvoorbeeld een online spel spelen bijvoorbeeld volledig onschuldig zijn, maar kan worden gezien als een strafbare bedreiging wanneer de tekst via Twitter aan een politicus wordt gericht. Daar komt bij dat er wereldwijd tussen mensen zeer verschillende ideeën leven over wat schadelijk en illegaal is; wat voor de één een milde belediging is, kan door de ander worden gezien als een feitelijke oproep tot haat of geweldpleging. Dit maakt de beoordeling of er sprake is van problematische content niet alleen in hoge mate contextueel, maar tot op zekere hoogte ook subjectief.

Omdat het moeilijk is om vooraf te definiëren welke uitingen schadelijk of ongewenst zijn, wordt in dit advies niet enkel naar de eigenlijke content en de vorm ervan gekeken, maar ook naar het effect ervan, dat wil zeggen de ernst van de aantasting van collectieve waarden of mensenrechten die het gevolg is van het verspreiden van deze content. Zo kan het verspreiden van discriminerende beelden, opruiend taalgebruik of haatzaaiende uitingen de menselijke waardigheid, de autonomie van individuele burgers en de rechten en belangen van minderheden of andere groepen in de samenleving aantasten. Ook kan het functioneren van de maatschappij als geheel worden verstoord wanneer mensen en groepen tegen elkaar worden opgezet. De democratische rechtsstaat wordt bijvoorbeeld bedreigd wanneer online activiteiten ingezet worden om het stemgedrag van burgers te beïnvloeden of maatschappelijke verhoudingen te polariseren. Wanneer deze activiteiten ondersteund worden door buitenlandse mogendheden is bovendien de nationale soevereiniteit in het geding. Ten slotte kan door online content de nationale en internationale vrede en veiligheid in gevaar komen. Hierbij valt te denken aan de verspreiding van content met een terroristisch oogmerk of aan technische of tactische aanwijzingen voor het plegen van aanslagen. Ook deze effecten kunnen bovendien weer zeer ernstig en rechtstreeks zijn, maar ook indirect of mild.

> De uiting 'ik hak je kop eraf' kan tussen twee gamende vrienden onschuldig zijn, maar geuit via Twitter aan een politicus strafbaar.

Samenvattend is er niet alleen sprake van een spectrum dat loopt van illegale tot onschuldige content, maar ook om een oplopend spectrum als het gaat om de ernst van de aantasting van maatschappelijke waarden als gevolg van deze content. Bij de vraag naar regulering van het internet, is het steeds zaak om rekening te houden met dit dubbele spectrum. Grafisch kan dit als een figuur met twee assen worden weergegeven.




**Figuur 2:** Spectrum illegale en onschuldige content

Hoofdstuk 2

# Hoe werkt het internet?

Om overwogen beleidsaanbevelingen te kunnen doen voor de regulering van online content is een gedegen begrip noodzakelijk van de techniek achter het internet en het ecosysteem van partijen die een rol spelen bij het creëren van het internet.

Begrip van de technische werking van het internet is van belang omdat de mogelijkheden van de technologie in overwegende mate het handelen van de gebruikers bepalen. Wanneer een internetdienst bijvoorbeeld geen mogelijkheid biedt om filmpjes te uploaden, dan kan de gebruiker geen filmpjes delen via dit platform. Deze sturende betekenis van technologie wordt ook wel aangeduid met de benaming *code as code* of *code as law*.[17]

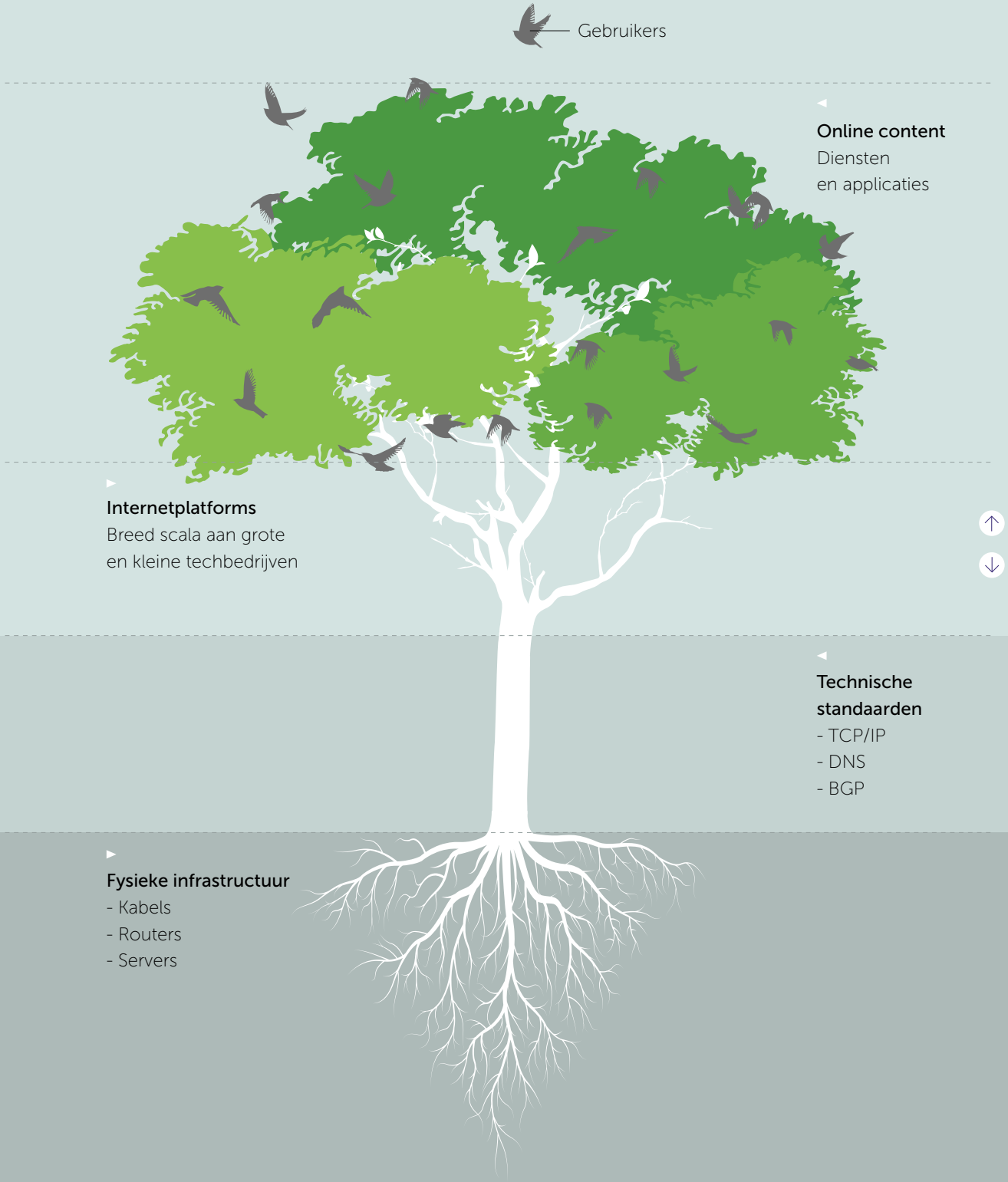
Deze sturende werking van de technologie is van belang voor het maken van reguleringskeuzes. Het kan voor het tegengaan van schadelijke online content bijvoorbeeld effectiever zijn om in te zetten op het verbieden van zo'n uploadmogelijkheid dan om een systeem van monitoring van de inhoud van de filmpjes in het leven te roepen. Tegelijkertijd legt dit meteen ook de dilemma's bloot die in het vorige hoofdstuk zijn geschetst: weliswaar is het tegengaan van zo'n uploadmogelijkheid een effectief instrument, maar het levert meteen ook een belangrijke inbreuk op de vrijheid van meningsuiting op. Met de wisselwerking tussen de technologische mogelijkheden en de geschetste uitgangspunten moet bij het maken van beleid dan ook steeds rekening worden gehouden.

Voor het identificeren van reguleringsopties is het verder relevant om te beseffen dat het internet een mondiaal, grensoverschrijdend netwerk van netwerken is dat geen centrale aansturing kent. Zowel publieke als private partijen spelen daardoor een rol in het reguleren van het internet. Met name ISPs en digitale platformen zoals SMPs hebben veel invloed op het gedrag van gebruikers.

## 2.1 Het internet is gelaagd opgebouwd: een boom als metafoor

In dit advies wordt de opbouw van het internet visueel inzichtelijk gemaakt met een metafoor van een boom.[18] Deze metafoor wordt gebruikt om inzicht te geven in de elementaire structuur van het internet, al sluit zij naar haar aard niet aan op alle kenmerken van het internet en daarbij behorende nuances. De wortels van de boom zijn in deze metafoor de harde internetinfrastructuur (kabels, routers, etc.). De stam wordt gevormd door de kernprotocollen – de programmataal waarmee computers met elkaar kunnen communiceren – die uitmondt in een aantal dikke takken: techbedrijven als Alphabet (Google), Apple, Amazon, Facebook en Microsoft die de belangrijkste internetplatformen uitbaten.De diensten en applicaties die zij aanbieden, zijn de bladeren van de boom. Rondom de boom cirkelen de internetgebruikers als vogels die geregeld op de takken en bladeren zitten en die dus gebruik maken van de diverse onlinediensten en -toepassingen.

In het algemeen geldt dat hoe lager in de boom wordt ingegrepen (in de wortels of de stam), hoe effectiever de maatregelen zijn om illegale, schadelijke of ongewenst online content te weren. Alle communicatie in de dikke takken en de kruin is immers afhankelijk van de wortels en het transport via de stam. Dit betekent echter ook dat ingrijpen op deze niveaus het meest verstrekkend is vanuit zowel technisch als mensenrechtenperspectief. Door internet tijdelijk af te sluiten (het doorzagen




**Figuur 3:** Een boom als metafoor. Vrij naar Van Dijck (2019).

van de wortels of stam), waartoe sommige overheden soms besluiten, kan online content vergaand worden tegengehouden. Tegelijkertijd verlamt dat onmiddellijk de hele samenleving. Het gericht bestrijden van door individuele gebruikers geplaatste online content is minder ingrijpend, maar ook minder effectief.

naar inhoud

## 2.2 De wortels: fysieke infrastructuur

De wortels van de internetboom worden gevormd door de fysieke netwerkinfrastructuur, zoals het geheel van kabels, routers en servers waarop het internet draait. Deze infrastructuur is, zeker in de westerse wereld, grotendeels in handen van private partijen zoals telecomaanbieders, hostingpartijen en de grote techbedrijven. Omdat de netwerken van eindgebruikers doorgaans geen autonoom systeem zijn, kunnen zij niet zomaar verbonden worden met het internet. Om dit mogelijk te maken, zijn ISPs nodig. ISPs kunnen toegang tot het internet verschaffen (dan zijn het *access providers*) of informatie opslaan en toegankelijk maken voor gebruikers (dan zijn het *hosting providers*).

## 2.3 De stam: kernprotocollen en gecentraliseerde beheersfuncties

Het internet kent geen centrale aansturing. Het is organisch gegroeid tot een relatief los georganiseerd wereldomspannend netwerk van netwerken dat werkt op basis van het gebruik van specifieke communicatieprotocollen.[19] Naast de protocollen die communicatie via het internet mogelijk maken zijn er twee beheersfuncties: nummering en het domeinnaamsysteem. Deze functies kennen wel een centrale aansturing.

**Communicatieprotocollen**

Alle apparaten en toepassingen die op het internet zijn aangesloten communiceren op basis van een aantal gestandaardiseerde communicatieprotocollen. De belangrijkste protocollen zijn *Transmission Control Protocol* (TCP), *Internet Protocol* (IP) en het *Border Gateway Protocol* (BGP).

- TCP en IP
  Het *Transmission Control Protocol* en het *Internet Protocol* (kortweg TCP/IP) zijn communicatie protocollen die worden gebruikt om betrouwbare en robuuste verbindingen op te zetten tussen op het internet aangesloten apparaten (*nodes*).[20] Daarbij wordt gebruik gemaakt van *packet switching*. In *packet-switched*-netwerken wordt de communicatie opgedeeld in kleine pakketjes die vervolgens de meest efficiënte route door het netwerk zoeken naar de eindbestemming. Bij de ontvanger worden de losse pakketjes vervolgens weer samengevoegd tot het oorspronkelijke bericht.[21] Wanneer er een blokkade in de verbinding ontstaat (bijvoorbeeld omdat een netwerk-*node* uitvalt) dan kan TCP/IP de pakketjes via een nieuwe route door het netwerk bezorgen.

- BGP
  Hoewel het internet een netwerk van netwerken is, kan niet ieder netwerk zomaar verbonden raken met het internet. Een netwerk kan alleen onderdeel worden van het internet als het een zogenaamd autonoom systeem is. Een autonoom systeem is een netwerk (of netwerken) met een duidelijk intern routeringsbeleid dat wordt aangestuurd door een beheerder en dat valt onder een administratieve entiteit (bijvoorbeeld een bedrijf of een universiteit). Met dit interne routeringsbeleid kunnen alle computers binnen het netwerk elkaar vinden en informatie uitwisselen. Het BGP zorgt voor de koppeling tussen de autonome systemen (AS) die samen het internet vormen. Daar waar TCP/IP zich richt op het opstellen van verbindingen tussen op het internet aangesloten apparaten, maakt BGP het mogelijk om verkeer te routeren van netwerk naar netwerk.

- Overige protocollen
  Naast de hierboven genoemde protocollen draaien meer specifieke communicatieprotocollen voor allerlei toepassingen. Zo zorgt het *Hypertext Transfer Protocol* (HTTP) voor het verzenden en ontvangen van webpagina's, het *File Transfer Protocol* (FTP) voor het versturen van bestanden en het *Internet Message Access Protocol* (IMAP) voor het beheer van e-mail.

**Gecentraliseerde beheersfuncties**

Dankzij TCP/IP en BGP is het mogelijk om computers en netwerken overal ter wereld met elkaar te verbinden zonder dat daarvoor centrale aansturing of controle nodig is. Er is dan ook geen eigenaar van het internet. Echter, om het internet op een wereldwijde schaal efficiënt te laten functioneren zijn er twee cruciale beheersfuncties die centraal georganiseerd zijn, namelijk die ten aanzien van nummering en domeinnamen.

- Nummering
  Wil een apparaat op het internet gevonden kunnen worden, dan heeft het een adres nodig: het IP-adres. Om tot een uniforme adressering te komen en te voorkomen dat meerdere apparaten hetzelfde adres gebruiken, is de uitgifte van internetadressen (IP-nummers) centraal belegd bij de *Internet Assigned Numbers Authority* (IANA). Deze instantie zorgt ervoor dat de nummers wereldwijd gedistribueerd worden via vijf regionale *Internet Registries*. De *Registry* voor Europa, Rusland en het Midden-Oosten is het in Nederland gevestigde *RIPE Network Coordination Centre* (RIPE NCC). Samen met onder meer de *Amsterdam Internet Exchange* (AIE) draagt dit bij aan de prominente positie die ons land internationaal inneemt op het gebied van internet governance.[22] De IANA geeft ook zogenaamde AS-nummers uit; dit zijn nummers die worden toegekend aan autonome systemen zodat deze elkaar kunnen vinden.

- Domeinnaamsysteem
  Omdat mensen minder goed lange getallenreeksen dan namen onthouden is een domeinnaam systeem ontwikkeld. Het domeinnaamsysteem (DNS) vertaalt alfanumerieke adressen naar het bij dat adres behorende IP-adres. Het bijhouden van het officiële wereldwijde adresboek (de DNS-*rootzone*) is een taak van IANA, evenals het beheer van topleveldomeinen zoals .com, .org en .net.

- IANA
  De functies van de IANA en het beheer van de DNS-rootzone zijn belegd bij de *Internet Corporation for Assigned Names and Numbers* (ICANN). ICANN, een private non-profit-organisatie,[23] is daarmee de belangrijkste partij voor het functioneren van het wereldwijde internet. ICANN is gevestigd in de Verenigde Staten. ICANN heeft een eigen multistakeholder-governancemodel, zoals in hoofdstuk 1 al aan de orde kwam.[24] De bestuursraad (*board of directors)* bepaalt de koers van ICANN. De bestuursraad bestaat uit experts die zijn afgevaardigd vanuit de achterban van ICANN (regionale *registries*, nationale *registries*, bedrijfsleven en maatschappelijk middenveld). Opvallend is dat overheden geen stemrecht hebben binnen de bestuursraad. Wel is er een *Governmental Advisory Committee* (GAC), waarin 111 landen zijn vertegenwoordigd. De GAC heeft echter geen stemrecht.

## 2.4 De takken en de bladeren: digitale dienstverleners en hun toepassingen

Daar waar de wortels en de stam van de boommetafoor de communicatie op het internet symboliseren, verbeelden de takken en de bladeren (kruin) van de boom alle websites, platformen, diensten en hun toepassingen of applicaties. Dit niveau wordt in technische termen vaak de contentlaag genoemd.

**De grote techbedrijven**

Hoewel het landschap aan platformen en diensten divers is, kan worden vastgesteld dat de voor gebruikers meest relevante platformen en diensten in handen zijn van een beperkte groep aanbieders. Zij domineren de internetbeleving van de meeste gebruikers. Dit zijn primair de Amerikaanse techreuzen (Facebook, Alphabet (Google), Apple, Amazon en Microsoft), maar in toenemende mate ook de Chinese techgiganten (denk aan Alibaba, Tencent, Baidu en Xiaomi).

Gelet op het feit dat deze grote techbedrijven samen een groot aantal platformdiensten en toepassingen aanbieden, zijn ze voor het doel van dit rapport te beschrijven als de hoofdtakken van de boom, waaruit kleinere takken en blaadjes voortkomen. Dit kan worden begrepen als een breder ecosysteem van diensten en producten, waarbij er sprake is van interactie tussen de diensten en producten van één groot techbedrijf. Te denken is bijvoorbeeld aan de integratie tussen de diensten en producten van Apple: de iPhones en iPads, het daarvoor gehanteerde besturingssysteem (iOS) en de applicaties (Appstore, Apple Music, Apple Pay) maken allemaal deel uit van hetzelfde ecosysteem.

**Internetplatformen**

Platformen, diensten en toepassingen maken het mogelijk om online content te delen tussen groepen gebruikers. Het businessmodel van een digitaal platform bestaat uit het bijeenbrengen van gebruikers. Hierbij kan worden gedacht aan het samenbrengen van aanbieders van vakantiewoningen en toeristen (Booking.com, Airbnb), of van taxichauffeurs en reizigers (Uber, Lyft). Wellicht het populairst zijn de platformen die mensen in staat stellen om met elkaar te communiceren. Zo zijn er sociale-mediaplatformen (Facebook, Twitter, Instagram, TikTok), videodiensten (YouTube, Vimeo), streamingdiensten (Twitch, Mixer), berichtendiensten (WhatsApp, WeChat, Telegram, Signal), diensten voor videoconferenties (Zoom, Starleaf, Microsoft Teams) en diensten gericht op het delen van bestanden (WeTransfer, Dropbox). Deze diensten stellen gebruikers in staat content te delen. Hoewel de meerderheid van deze content goedaardig is wordt ook illegale, schadelijke en ongewenste content gedeeld via de platformen.

## 2.5 De vogels: internetgebruikers

De internetgebruikers ten slotte zijn te zien als de vogels die rond de boom vliegen en er soms in landen om gebruik te kunnen maken van de digitale platformen en de onlinediensten die via het internet worden aangeboden. In het kader van de regulering van online content zijn de gebruikers belangrijke spelers. Niet alleen zijn zij de afnemers van online content, in veel gevallen zijn zij ook de producent of distributeur daarvan, bijvoorbeeld door het creëren en delen van boodschappen en video's via de genoemde platformen. Evenzeer van belang voor reguleringskwesties is dat de vrijheid van de gebruikers niet altijd zo groot is als het beeld van de vogels doet veronderstellen. Zo kan de onderlinge afhankelijkheid binnen een ecosysteem dat door één techbedrijf is gecreëerd het voor een gebruiker lastig maken om over te stappen naar een concurrent. Hierdoor wordt de individuele keuzevrijheid van de gebruiker beperkt.

# Multilaterale initiatieven

naar inhoud

Om te komen tot handelings- en reguleringsopties voor het Nederlands beleid ten aanzien van regulering van online content is een overzicht van bestaande multilaterale initiatieven van de Verenigde Naties, de Raad van Europa en van de Europese Unie behulpzaam. Dit overzicht geeft aanknopingspunten om te bepalen langs welke wegen regulering tot uitvoering kan worden gebracht en bij welke bestaande initiatieven kan worden aangesloten.

## 3.1 De Verenigde Naties

**Mensenrechtenraad**

De Mensenrechtenraad van de Verenigde Naties heeft zich sinds 2012 in een viertal resoluties[25] uitgesproken over 'het bevorderen, beschermen en genieten van mensenrechten op internet'.[26] De Mensenrechtenraad benadrukt in deze resoluties dat de rechten die burgers offline hebben ook online beschermd moeten worden, in het bijzonder de vrijheid van meningsuiting. De Mensenrechtenraad verwijst daarbij naar artikel 19 van de Universele Verklaring van de Rechten van de Mens (UVRM) en naar artikel 19 van het Internationaal Verdrag inzake burgerrechten en politieke rechten (IVBPR).[27] Dit laatste verdrag is door 170 landen geratificeerd. Terwijl de Mensenrechtenraad in zijn eerste resoluties vooral de positieve kanten van het wereldwijde en open internet heeft belicht, onder meer als instrument voor ontwikkeling en het uitoefenen van mensenrechten, heeft hij in de latere resoluties ook opgeroepen om de negatieve aspecten tegen te gaan, waaronder *advocacy of hatred*, de verspreiding van online informatie *'that may be deliberately misleading or false'* en propaganda via het internet, onwettig gebruik van persoonsgegevens en online aanvallen op vrouwen.[28] De Mensenrechtenraad doet in de resoluties geen expliciete oproep tot (internationale) regulering van online content. In 2018 heeft de Mensenrechtenraad wel gewezen op de verantwoordelijkheid van het bedrijfsleven om mensenrechten te respecteren, zoals uiteengezet in de *Guiding Principles on Business and Human Rights*.[29]

**Mensenrechtencomité**

Het Mensenrechtencomité van de Verenigde Naties, dat toezicht houdt op de naleving door staten van het IVBPR, heeft zich in een *General Comment* uit 2011 uitgelaten over meningsuiting online.[30] Het Comité benadrukt hierin dat online uitingen ook binnen de vrijheid van meningsuiting vallen en dat staten de onafhankelijkheid van online media en de toegang van individuen daartoe moeten beschermen. Dezelfde voorwaarden die Artikel 19 IVBPR stelt aan beperkingen van de vrijheid van meningsuiting gelden ook voor online uitingen. Beperkingen moeten specifiek zijn; generieke, brede verboden op complete websites of platformen zijn in principe niet toegestaan. Evenmin mag volgens het *General Comment* een verbod op een website of platform puur zijn gebaseerd op het tegengaan van kritiek op een regering of een heersend politiek-sociaal systeem.

**Speciale Rapporteur voor de bevordering en bescherming van de vrijheid van meningsuiting**

De Speciale Rapporteur van de Verenigde Naties voor de bevordering en bescherming van de vrijheid van meningsuiting, David Kaye, heeft onder meer in 2018 en 2019 gerapporteerd over de regulering van respectievelijk online content die door gebruikers zelf is gegenereerd en van *hate speech*.[31] Beide rapporten bevatten gerichte aanbevelingen voor zowel overheden (staten) als bedrijven in de ICT-sector.

De Speciale Rapporteur onderstreept het belang van de vrijheid van meningsuiting zoals die is vastgelegd in de genoemde bepalingen van de UVRM en het IVBPR. De vrijheid van meningsuiting is fundamenteel voor het genieten van alle mensenrechten, zo stelt hij. Overheden hebben de plicht om de uitoefening van de vrijheid van meningsuiting voor hun burgers mogelijk te maken en te beschermen. Daartoe dienen zij onder meer de diversiteit van onafhankelijke media en de toegang tot informatie te bevorderen. Overheden hebben bovendien de verplichting om ervoor te zorgen dat private ondernemingen de vrijheid van meningsuiting niet belemmeren.

De Speciale Rapporteur benadrukt dat de vrijheid van meningsuiting alleen in uitzonderlijke gevallen mag worden beperkt. Deze beperkingsmogelijkheden, vastgelegd in artikel 19 lid 3 IVBPR, zijn het belang van de rechten of de goede naam van anderen of in het belang van de nationale veiligheid ter bescherming van de openbare orde, de volksgezondheid of de goede zeden. De Speciale Rapporteur wijst er verder op dat artikel 20 lid 1 IVBPR oorlogspropaganda verbiedt en dat artikel 20 lid 2 IVBPR een verbod bevat op 'het propageren van op nationale afkomst, ras of godsdienst gebaseerde haatgevoelens die aanzetten tot discriminatie, vijandigheid of geweld'.[32]

De Speciale Rapporteur benadrukt verder dat beperkingen van de vrijheid van meningsuiting moeten voldoen aan een drietal voorwaarden. Ten eerste moeten beperkingen een geldige en voldoende duidelijke rechtsbasis hebben. Dat betekent dat ze tot stand komen via een deugdelijk wetgevingsproces en dat ze getoetst kunnen worden door een onafhankelijke rechterlijke instantie. Ten tweede moeten beperkingen van de vrijheid van meningsuiting legitiem zijn, in die zin dat moet worden aangetoond dat ze dienen tot bescherming van de belangen die in artikel 19 lid 3 of eventueel artikel 20 worden genoemd. Ten derde dienen beperkingen noodzakelijk en proportioneel te zijn met het oog op de bescherming van deze legitieme belangen.

Volgens de Speciale Rapporteur voldoet nationale regelgeving om schadelijke online content tegen te gaan, in de praktijk vaak onvoldoende aan de genoemde voorwaarden. Zij vertrouwen bijvoorbeeld op zware maatregelen als censuur of strafbaarstelling of verbieden uitingen die feitelijk legitiem zijn met behulp van niet nader gedefinieerde termen als extremisme, blasfemie, *fake news* en propaganda. Sommige wetgeving staat bovendien op gespannen voet met het recht op online privacy.

De Speciale Rapporteur zet ook vraagtekens bij wetgeving waarvan de intentie op zichzelf goed is, maar die vanuit mensenrechtenperspectief verkeerd uitwerkt. Als voorbeeld noemt hij het gebruik van uploadfilters die volgens hem leiden tot feitelijke censuur. Een tweede voorbeeld is de *notice-and-take-down*-wetgeving van sommige landen die bedrijven dwingt om schadelijke of illegale content binnen een bepaalde termijn offline te halen. Vaak ontbreekt het in de wetgeving aan duidelijke criteria waarmee kan worden vastgesteld welke content schadelijk of illegaal is, zodat niet wordt voldaan aan het vereiste van een geldige en voldoende duidelijke rechtsbasis. Overheden maken volgens de Speciale Rapporteur weinig gebruik van een onafhankelijke rechterlijke of toezichthoudende instantie en leggen de verantwoordelijkheid grotendeels bij de internetplatformen om te beoordelen welke online content ontoelaatbaar is.

Internetplatformen leggen regels voor het plaatsen en eventueel verwijderen van online content meestal vast in gebruikersvoorwaarden. Gebruikers moeten hiermee akkoord gaan wanneer zij gebruik willen maken van een bepaalde applicatie of dienst. De Speciale Rapporteur stelt vast dat deze gebruiksvoorwaarden niet of nauwelijks zijn gebaseerd op nationale of internationale wetgeving met betrekking tot de vrijheid van meningsuiting. Zo kennen internetplatformen zichzelf een ruime discretionaire bevoegdheid toe om te bepalen welke online content kan worden verwijderd. Hij spreekt van het ontstaan van *'platform law in which clarity, consistency, accountability and remedy are elusive'*.[33] Onduidelijke definities van welke online content kan worden verwijderd, gebrek aan transparantie en de beperkte mogelijkheid voor gebruikers om bezwaar te maken tegen verwijderde online content worden door de Speciale Rapporteur als bezwaarlijk gezien. Hij bepleit dat relevante mensen-

rechtenprincipes direct worden opgenomen in de gebruikersvoorwaarden zodat voor regulering van online content door sociale platformen dezelfde maatstaven gaan gelden als van toepassing zijn bij de beperking van vrijheid van meningsuiting door overheden. Dat betekent dat er een geldige en voldoende duidelijke rechtsbasis moet zijn, een legitiem doel moet bestaan en de restricties noodzakelijk en proportioneel moeten zijn in het licht van dat doel.

De aanbevelingen die de Speciale Rapporteur in beide rapporten aan zowel overheden als bedrijven doet zijn er daarmee op gericht om de regulering van online content (door wetgeving of via gebruikersvoorwaarden) goed in te passen in het mensenrechtelijk kader en bovendien te laten voldoen aan de genoemde beperkingsvoorwaarden. Zo moeten overheden en internetbedrijven onder meer duidelijk omschrijven welke online content niet is toegestaan, mag monitoring alleen achteraf plaatsvinden, dient er onafhankelijk toezicht te zijn door een rechterlijke instantie of door een *Social Media Council* en moeten er bezwaarmogelijkheden voor internetgebruikers worden gecreëerd. Daarnaast moeten overheden en bedrijven veel transparanter zijn over hoe de regelgeving wordt vormgegeven en hoe deze wordt toegepast. Internetbedrijven zouden moeten erkennen dat internationale mensenrechtenstandaarden de basis zijn voor de vrijheid van meningsuiting op hun platformen. Deze bedrijven zouden ook de *UN Guiding Principles on Business and Human Rights* moeten onderschrijven.

## 3.2 De Raad van Europa

**Europees Hof voor de Rechten van de Mens**[34]

De Speciale VN-Rapporteur baseert zich in zijn rapporten op multilaterale mensenrechtenverdragen. Op Europees niveau is die normstelling in het bijzonder geconcretiseerd in de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) van de Raad van Europa. Bij het EHRM kunnen landen, non-gouvernementele organisaties, rechtspersonen, groepen en individuele burgers een klacht indienen tegen een van de 47 lidstaten van de Raad van Europa, waarin zij een beroep kunnen doen op het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele Vrijheden (EVRM).

**Vrijheid van meningsuiting**

Het recht op vrijheid van meningsuiting is vastgelegd in artikel 10 (1) van het EVRM. Uit de rechtspraak van het Hof blijkt dat de vrijheid van meningsuiting ruim moet worden geïnterpreteerd. Zo vallen onder andere kunstuitingen, films, interviews en commerciële informatie onder de vrijheid van meningsuiting, net als de mogelijkheid om deze informatie te verspreiden of te ontvangen. Bovendien moet in een democratie ruimte zijn voor uitlatingen die kwetsen, choqueren of verontrusten. Tegelijkertijd heeft het EHRM – afhankelijk van de gebruikte bewoordingen – geoordeeld dat bepaalde racistische, antisemitische, islamofobe uitlatingen, het rechtvaardigen van oorlogsmisdaden en terroristische propaganda buiten de bescherming van Artikel 10 EVRM vallen.[35]

Net als het IVBPR biedt het EVRM in het tweede lid van artikel 10 de mogelijkheid om beperkingen te stellen op de uitoefening van de vrijheid van meningsuiting. Het gaat dan om beperkingen 'die bij de wet zijn voorzien en die in een democratische samenleving noodzakelijk zijn in het belang van de nationale veiligheid, territoriale integriteit of openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden, de bescherming van de goede naam of de rechten van anderen, om de verspreiding van vertrouwelijke mededelingen te voorkomen of om het gezag en de onpartijdigheid van de rechterlijke macht te waarborgen'.

Nationale autoriteiten hebben een zekere beoordelingsvrijheid om vast te stellen of sprake is van dergelijke beperkingsgronden. In algemene zin geldt dat die beoordelingsvrijheid beperkter is naarmate uitingen een groter belang hebben voor democratische en rechtsstatelijke discussies of als

ze betrekking hebben op onderwerpen van algemeen belang. In die gevallen moet er sprake zijn van zwaarwegende argumenten en de maatregelen met de nodige waarborgen zijn omkleed. Het EHRM toetst in dergelijke gevallen zorgvuldig of de vrijheid van meningsuiting niet verdergaand is ingeperkt dan strikt noodzakelijk is om een zwaarwegend doel te kunnen bereiken, en of er een redelijk evenwicht bestaat tussen het belang van dit doel en het recht dat door de beperking is aangetast.

Anders dan de Speciale Rapporteur van de Verenigde Naties bepleit, is het voorafgaand aan het verspreiden of publiceren van bepaalde content verbieden daarvan volgens het EHRM niet per definitie verboden. Omdat de vrijheid van meningsuiting echter een fundamenteel en essentieel grondrecht is voor de democratische samenleving, hebben staten hier een minimale beoordelingsvrijheid. Opnieuw geldt dat het EHRM nauwkeurig zal onderzoeken of de voorafgaande beperkingen noodzakelijk en proportioneel waren ten opzichte van een zwaarwegende doelstelling van algemeen belang.

Het voorgaande laat zien dat ook het EHRM aan een drietal vereisten toetst om vast te kunnen stellen of een beperking van het recht op vrijheid van meningsuiting is toegestaan, die in hoge mate overeenkomen met de voorwaarden die hiervoor voor de VN-context al zijn besproken:

1. Bij wet voorzien: een beperking dient volgens het EHRM toegankelijk en voorzienbaar te zijn, zodat de burger weet waar zij aan toe is.
2. Legitiem doel: aangetoond moet worden dat met de beperking een van de in artikel 10(2) EVRM genoemde doelstellingen wordt nagestreefd.
3. Noodzakelijk in een democratische samenleving (noodzakelijk en proportioneel): de beperking dient noodzakelijk te zijn om het gestelde doel, een 'dwingende maatschappelijke behoefte', te bereiken, de voor de beperking gegeven redenen moeten relevant en voldoende zijn en er moet een redelijk evenwicht bestaan tussen het nagestreefde doel en het aangetaste recht.

**Internetplatformen en andere internettussenpersonen**

In diverse arresten heeft het EHRM vastgesteld dat ook uitingen die worden gedaan via sociale media en andere digitale platformen binnen het bereik van artikel 10 EVRM vallen. Deze platformen maken immers de uitwisseling mogelijk van informatie en ideeën en bieden een podium voor het doorgeven en ontvangen van informatie door anderen, of het creëren en delen van informatie binnen een groep.[36] Internetplatformen kunnen onder het EVRM niet rechtstreeks worden aangesproken op uitingen die op hun fora of platformen worden gedaan: klachten bij het EHRM kunnen alleen tegen de staat worden gericht. Wel heeft het EHRM geoordeeld dat het niet in strijd is met de vrijheid van meningsuiting als een nationale rechter een internetplatform aansprakelijk stelt voor het plaatsen of niet verwijderen van online content op het platform wanneer deze duidelijk onwettig is, zoals het geval kan zijn bij haat zaaien en het aanzetten tot geweld. In dat geval kan het platform op nationaal niveau redelijkerwijze de plicht worden opgelegd de content te verwijderen. Het EHRM kijkt daarbij onder meer naar de context waarin een uiting is gedaan, de aard en de mogelijke gevolgen van de *comments*, naar de maatregelen die het platform zelf al heeft genomen om de uitingen te verwijderen, de mogelijkheid om de oorspronkelijke auteurs van de uiting aansprakelijk te stellen, en gevolgen die het niet-verwijderen van de uiting heeft voor het platform.[37] Het EHRM heeft onderkend dat een verplichting voor een internetplatform om zelf onrechtmatige uitingen te verwijderen ertoe kan leiden dat deze platformen de online content automatisch gaan filteren, bijvoorbeeld met behulp van algoritmes. Anders dan de Speciale VN-Rapporteur is het EHRM daar niet per se op tegen, omdat dit de enige manier kan zijn om de legitieme belangen en rechten van anderen te beschermen tegen onrechtmatige uitingen.

**Relevante verdragen van de Raad van Europa**

In oktober 2007 sloten de lidstaten van de Raad van Europa het Verdrag inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik (Verdrag van Lanzarote), voor het Europese

deel van het Koninkrijk der Nederlanden in werking getreden op 1 juli 2010.[38] De totstandkoming van dit verdrag was een direct gevolg van het toenemend gebruik van het internet door zowel kinderen als daders, waardoor kinderpornografie zich eenvoudig over landsgrenzen kon verspreiden en die verspreiding ook steeds grotere proporties aannam. Met dit verdrag streven de aangesloten staten naar nauwere samenwerking om seksueel misbruik van kinderen te voorkomen en te bestrijden.

Het Verdrag van Lanzarote biedt handvatten voor de regulering van online content omdat het in breed Europees verband overeengekomen definities geeft van onder meer seksueel misbruik, kinderprostitutie en kinderpornografie. Ook geeft het verdrag een overzicht van relevante strafbare feiten. Zo wordt het vervaardigen, aanbieden, verspreiden, verwerven en het zich door middel van ICT-technologie toegang verschaffen tot kinderpornografie strafbaar gesteld.

Begin 2003 kwamen de lidstaten van de Raad van Europa een aanvullend protocol overeen bij het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Verdrag van Boedapest, 2001), dat voor het Koninkrijk der Nederlanden in werking is sinds 1 november 2010.[39] De staten die dit protocol[40] aanvaarden verplichten zich om nationale wetgeving aan te nemen die de verspreiding van racistisch en xenofobisch materiaal via computersystemen strafbaar maakt 'wanneer deze opzettelijk en onrechtmatig plaatsvinden', net als bedreiging en belediging met een racistische en xenofobische motivering, en ontkenning, grove bagatellisering, goedkeuring of rechtvaardigheid van volkerenmoord of misdaden tegen de menselijkheid. Bij de aanvaarding van het protocol is namens het Koninkrijk der Nederlanden een verklaring afgelegd, luidende; *'The Kingdom of the Netherlands will comply with the obligation to criminalize the denial, gross minimisation, approval or justification of genocide or crimes against humanity laid down in Article 6, paragraph 1, of the Protocol where such conduct incites hatred, discrimination or violence on the grounds of race or religion.'* Een ander voorbeeld van bestaande Europese mensenrechtenstandaarden over het tegengaan van de verspreiding van racistisch en xenofobisch materiaal, kan worden gevonden in artikel 19, lid 1 van het Europees Sociaal Handvest, dat staten oproept om misleidende propaganda en valse informatie betrekking hebbende op migratie tegen te gaan.

**Comité van Ministers**

Het Comité van Ministers van de Raad van Europa heeft sinds de jaren vijftig van de vorige eeuw een omvangrijk stelsel opgebouwd van (niet-bindende) aanbevelingen, verklaringen en resoluties op het gebied van media en de informatiemaatschappij.[41] In 1997 nam het Comité een aanbeveling aan over *'the gratuitous portrayal of violence in the various electronic media at national and transfrontier level'*,[42] waarin ook de rol van het internet genoemd werd. Sindsdien heeft het Comité zich meermaals uitgesproken over onder meer de regulering van het internet en van online content, mensenrechten van internetgebruikers, en de rol en verantwoordelijkheden van internettussenpersonen.[43] Voor dit advies is vooral relevant dat het Comité van Ministers de rechtspraak van het EHRM volgt en een centrale positie toekent aan de vrijheid van meningsuiting en het recht van internetgebruikers om alle gewenste informatie en ideeën op te zoeken, te ontvangen en te communiceren. Het Comité volgt de lijn van het EHRM dat online content onder artikel 10 van het EVRM valt, en dat overheden in overeenstemming met de beperkingsvoorwaarden van artikel 10 lid 2 EVRM beperkingen kunnen stellen aan online content die aanzet tot discriminatie, haat of geweld. Het Comité geeft op een aantal punten ook concrete aanknopingspunten die in de EHRM-rechtspraak nog niet zo duidelijk tot uitdrukking zijn gekomen. Zo heeft het Comité vermeld dat internetgebruikers ervoor moeten kunnen kiezen hun identiteit op het internet niet bekend te maken, maar dat zij er rekening mee moeten houden dat nationale autoriteiten maatregelen kunnen nemen waardoor hun identiteit bekend wordt, bijvoorbeeld voor de bestrijding van criminaliteit.

Mensenrechten en de daarmee verband houdende normen hebben volgens het Comité voorrang boven de algemene voorwaarden die internetbedrijven formuleren en waarmee internetgebruikers moeten instemmen om bepaalde diensten of applicaties te kunnen gebruiken. Tegelijkertijd is het

volgens het Comité wel aanvaardbaar dat internetproviders en aanbieders van onlinediensten op basis van hun eigen beleid bepaalde content beperken. Zij moeten daarbij specifiek omschrijven wat zij als onrechtmatige of ongepaste inhoud beschouwen en hoe zij daarmee omgaan. Ook moeten zij voor klachtenprocedures zorgen.

Ten aanzien van internettussenpersonen heeft het Comité van Ministers aanbevolen dat zij niet aansprakelijk gesteld kunnen worden voor door derde partijen geplaatste content wanneer de tussenpersoon deze content slechts doorgeeft of opslaat. Wanneer de internettussenpersoon echter een grotere rol speelt, en bijvoorbeeld zelf content produceert of cureert, kan deze mede aansprakelijk worden gesteld voor illegale content. In dat geval draagt de tussenpersoon dus een grotere verantwoordelijkheid voor het verwijderen van dergelijke content. Het Comité heeft de lidstaten van de Raad van Europa opgeroepen om met de internetsector samen te werken en zo ten aanzien van online content een systeem van zelfregulering of co-regulering te ontwikkelen dat is gestoeld op de eisen van rechtmatigheid, noodzakelijkheid en proportionaliteit. Internetbedrijven zouden zich voorts moeten houden aan de *UN Guiding Principles on Business and Human Rights.*

## 3.3 Europese Unie

De Europese Unie heeft verschillende instrumenten die relevant zijn voor het tegengaan van schadelijke online content. Het mensenrechtelijke kader daarvan wordt gevormd door het Handvest van de grondrechten van de Europese Unie. Daarin is naast de vrijheid van meningsuiting en van informatie (artikel 11) en de vrijheid van kunsten en wetenschappen (artikel 13) de aanspraak op non-discriminatie (artikel 21) en de bescherming van kinderen (artikel 24) van belang. Hoewel het in 2000 opgestelde Handvest behoort tot de meest actuele documenten op het gebied van de fundamentele rechten, kon daarin nog geen rekening worden gehouden met de ontwikkeling van het internet in deze eeuw. Een groep deskundigen heeft op uitnodiging van de *ZEIT-Stiftung Ebelin und Gerd Bucerius* wel een voorstel ontwikkeld voor een – anders dan het Handvest juridisch niet bindend – *Charter of Fundamental Digital Rights of the European Union*,[44] dat als richtsnoer voor de rechtsontwikkeling op dit terrein kan dienen.

> Het EU-beleid staat ervoor dat internettussenpersonen maatregelen nemen om de verspreiding van schadelijke online content tegen te gaan. Anderzijds wil de EU deze tussenpersonen niet aansprakelijk stellen wanneer dergelijke content via hun platformen wordt gedeeld.

De EU lijkt in haar beleid op dit terrein op twee gedachten te hinken. Enerzijds staat het EU-beleid ervoor dat internettussenpersonen vanuit hun maatschappelijke verantwoordelijkheid proactief maatregelen nemen om de verspreiding van schadelijke en illegale online content tegen te gaan. Anderzijds wil de EU deze tussenpersonen niet aansprakelijk stellen wanneer dergelijke content via hun platformen wordt gedeeld.[45]

Dit leidt ertoe dat de EU heeft gekozen voor een afzonderlijke aanpak voor de verspreiding van drie verschillende typen schadelijke content: illegale online content (waaronder *hate speech*), online terroristische content, en online desinformatie. Een aantal van deze instrumenten is juridisch bindend terwijl andere instrumenten vooral zijn bedoeld om vrijwillige zelfregulering door internetplatformen te stimuleren. Daarnaast publiceerde de Europese Commissie in februari 2020 een Witboek over kunstmatige intelligentie[46] en een Mededeling over een Europese datastrategie, waarin nadere beleidsvoorstellen worden aangekondigd.[47]

**EU-wetgeving**

*Richtlijn: Elektronische handel*

In juni 2000 namen het Europees Parlement en de Raad van de Europese Unie de Richtlijn inzake elektronische handel aan.[48] In deze Richtlijn is vastgelegd dat een internetserviceprovider of internetdienst die informatie van gebruikers doorgeeft of opslaat, niet aansprakelijk is voor de inhoud van deze informatie als is voldaan aan een aantal voorwaarden. Voor *access providers* geldt de aansprakelijkheidsvrijwaring wanneer zij niet het initiatief nemen tot de doorgifte, niet de ontvangers bepalen en de gegevens niet selecteren of wijzigen. Voldoen zij aan deze randvoorwaarden dan zijn zij als doorgeefluik (*mere conduit)* niet aansprakelijk.

Een *hosting provider* is niet aansprakelijk voor de informatie die is opgeslagen op zijn servers wanneer hij geen weet heeft van het onrechtmatige karakter van de informatie en dit ook niet redelijkerwijs behoeft te weten. Wanneer de provider wel weet heeft van de informatie (bijvoorbeeld omdat hij daarvan op de hoogte wordt gesteld), dan moet de provider prompt de onrechtmatige informatie verwijderen of ontoegankelijk maken. De aansprakelijkheidsvrijwaring voor *hosting providers* is relevant, omdat ook internetplatformen vallen onder het bereik van deze bepaling en aldus gebruik kunnen maken van deze vrijwaring.

De Richtlijn inzake elektronische handel bepaalt tevens dat de lidstaten internetdiensten geen algemene verplichting mogen opleggen om toe te zien op de informatie die zij doorgeven of opslaan, of om actief te zoeken naar 'feiten of omstandigheden die op onwettige activiteiten duiden'.[49] Deze EU-regels over de aansprakelijkheid van internetdiensten sluiten aan bij de aanbevelingen van het Comité van Ministers van de Raad van Europa op dit gebied.

De Richtlijn inzake elektronische handel biedt lidstaten ook de mogelijkheid om beperkingen aan informatiediensten te stellen. Deze maatregelen moeten noodzakelijk zijn voor de bescherming van de openbare orde, de bescherming van minderjarigen, de bestrijding van het aanzetten tot haat wegens ras, geslacht, godsdienst of nationaliteit of de bestrijding van schendingen van de menselijke waardigheid ten aanzien van individuen. Ook de bescherming van de volksgezondheid, de openbare veiligheid en consumenten zijn geldige redenen voor beperking.

*Richtlijn: audiovisuele mediadiensten*

De hierboven genoemde aansprakelijkheidsbepalingen zijn ook onderdeel van de Richtlijn audiovisuele mediadiensten (2010).[50] Deze Richtlijn is in 2018 herzien, waarbij videoplatformdiensten aan de reikwijdte van de Richtlijn zijn toegevoegd.[51] Daarbij kan gedacht worden aan platformen als Netflix en YouTube, of aan Facebook wanneer daarop video's worden gedeeld. Ook deze Richtlijn bevat mogelijkheden om audiovisuele mediadiensten beperkingen op te leggen, vergelijkbaar met datgene dat daarover in de Richtlijn inzake elektronische handel is vastgelegd.[52]

*Overig*

Het Kaderbesluit van 28 november 2008 betreffende de bestrijding van bepaalde vormen en uitingen van racisme en vreemdelingenhaat door middel van het strafrecht van 28 november 2008 verplicht de lidstaten tot strafbaarstelling. Die betreft het publiekelijk aanzetten tot geweld of haat jegens een groep personen, of een lid van die groep, die op basis van ras, huidskleur, godsdienst, afstamming, dan

wel nationale of etnische afkomst wordt gedefinieerd, van zulke gedragingen door het publiekelijk verspreiden of uitdelen van geschriften, afbeeldingen of ander materiaal, en van het publiekelijk vergoelijken, ontkennen of verregaand bagatelliseren van genocide en andere internationale misdrijven, misdaden tegen de menselijkheid en oorlogsmisdaden. Volgens artikel 9 van het Kaderbesluit dient elke lidstaat ervoor te zorgen dat zijn rechtsmacht zich uitstrekt tot gevallen waarin de gedraging via een informatiesysteem is begaan en de dader dan wel het informatiesysteem zich op zijn grondgebied bevindt.[53] De Richtlijn ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie van 13 december 2011[54] en de Richtlijn inzake terrorismebestrijding van 15 maart 2017[55] verbieden de distributie, verspreiding of uitzending, online zowel als offline, van respectievelijk kinderpornografie en van materiaal dat aanzet tot terroristische misdrijven.

**Gedragscode: online haatzaaien**

De Europese Commissie kwam in mei 2016 met Facebook, Microsoft, Twitter en YouTube een *Code of conduct on countering illegal hate speech online* overeen.[56] In 2018 sloten ook Instagram, Google+, Snapchat en Dailymotion zich bij deze gedragscode aan. Deze gedragscode schrijft voor om minstens de helft van de meldingen van haatzaaiende content binnen 24 uur te beoordelen en deze zo nodig van hun platform te verwijderen. De platformen bepalen zelf op basis van hun gebruikersvoorwaarden of hiertoe aanleiding is. Onder haatzaaiende berichten verstaat de gedragscode berichten die aanzetten tot haat of geweld tegen een persoon of groep van personen op grond van ras, huidskleur, religie, nationaliteit of etnische afkomst.[57] Daarnaast beloven de platformen om te investeren in bewustwording van internetgebruikers over wat voor soort content niet is toegestaan.

De *Code of conduct on countering illegal hate speech online* is niet juridisch bindend, maar is een vorm van zelfregulering door de internetplatformen. Zij werken daarbij samen met een netwerk van zogenaamde *trusted flaggers.* Dit zijn (maatschappelijke) organisaties die op basis van hun expertise de platformen wijzen op mogelijk illegale content. Volgens de Europese Commissie slaagden de internetplatformen er in 2016 in om 40 procent van het aantal meldingen van haatzaaiende content binnen 24 uur te beoordelen. In 2019 was dat 89 procent. De content die daarop daadwerkelijk verwijderd werd steeg van 28 procent in 2016 naar 72 procent in 2019.

De voortgangsrapportage van de Commissie besteedt geen aandacht aan de bewustwordingsdoelstellingen die in de Gedragscode zijn vastgelegd, waardoor niet duidelijk is hoe en in hoeverre die worden gerealiseerd.[58]

**Mededeling: illegale online content**

In september 2017 heeft de Europese Commissie een Mededeling gepubliceerd over de bestrijding van illegale online content.[59] De Europese Commissie stelt in de Mededeling dat wat illegaal is in de fysieke wereld, dat ook online is. Daarbij kan worden gedacht aan het aanzetten tot terrorisme, haatzaaien en kinderpornografie. Volgens de EC hebben de online platformen een belangrijke maatschappelijke verantwoordelijkheid om internetgebruikers en de samenleving als geheel hiertegen te beschermen. Tegelijkertijd wijst de Europese Commissie erop dat het nemen van vrijwillige, proactieve maatregelen er niet automatisch toe leidt dat het online platform het voordeel verliest dat voortvloeit uit de vrijstelling van aansprakelijkheid die is vastgelegd in de bovengenoemde Richtlijn inzake elektronische handel.

In de Mededeling schetst de Europese Commissie verder enkele richtsnoeren en beginselen voor internetplatformen om in samenwerking met nationale autoriteiten in de lidstaten de verspreiding van illegale content beter tegen te gaan. Daarnaast moeten online platformen in hun gebruiksvoorwaarden op een begrijpelijke manier uitleg geven over hun contentbeleid en moeten zij transparantieverslagen publiceren over de aard van de ontvangen meldingen en ondernomen acties. Om overmatige verwijdering van online content tegen te gaan moeten de platformen duidelijke bezwaarprocedures inrichten.

Op deze Mededeling volgde in maart 2018 een (niet bindende) Aanbeveling voor een effectieve aanpak van illegale online content[60] waarin bovenstaande richtsnoeren nader worden uitgewerkt in operationele maatregelen die de lidstaten en internetplatformen moeten nemen om illegale inhoud op te sporen en te verwijderen.

**Wetgevingsvoorstel: terroristische online content**

De Europese Commissie presenteerde in 2018 een voorstel voor een Verordening ter voorkoming van de verspreiding van terroristische online content.[61] Het Europees Parlement stemde in april 2019 in met het voorstel voor de verordening en het is momenteel voorwerp van onderhandeling tussen de lidstaten. Dit voorstel heeft betrekking op aanbieders van hostingdiensten en beoogt een aantal nieuwe maatregelen te introduceren. Zo moeten bevoegde (rechterlijke) autoriteiten in een lidstaat een aanbieder kunnen bevelen om binnen één uur illegale terroristische online content te verwijderen. Daarnaast harmoniseert het voorstel de minimumvereisten die door aanbieders van hostingdiensten in acht moeten worden genomen bij het beoordelen van online content die mogelijke van terroristische aard is.[62] Verder zal de aanbieders in bepaalde gevallen een zorgplicht worden opgelegd om proactief 'passende, redelijke en evenredige maatregelen'[63] te nemen tegen terroristische online content op hun diensten. Tegelijkertijd stelt dit voorstel dat de Verordening geen afbreuk mag doen aan de vrijstelling (onder voorwaarden) van aansprakelijkheid die in de Richtlijn inzake elektronische handel is vastgelegd.[64] Om te voorkomen dat legale online content ten onrechte wordt verwijderd dienen de aanbieders van hostingdiensten onder meer een klachtenprocedure te hebben en moeten zij jaarlijks verslag uitbrengen van de maatregelen die zij hebben genomen.

**Beleidsmaatregelen: online desinformatie**

De EU heeft verschillende beleidsmaatregelen aangenomen om online desinformatie tegen te gaan. In april 2018 omschreef de Europese Commissie in een Mededeling desinformatie als 'aantoonbare onjuiste of misleidende informatie die wordt opgesteld, weergegeven en verspreid om winst te maken of om het publiek opzettelijk te bedriegen, en die schade in het publieke domein kan veroorzaken'.[65] De Europese Commissie stelde de volgende maatregelen voor om online desinformatie aan te pakken:[66]

- Aannemen van een praktijkcode voor internetplatformen.
- Inrichting van een onafhankelijk Europees netwerk van *fact checkers.*
- Oprichting van een Europees online platform met EU-brede gegevens over desinformatie, ter ondersteuning van het netwerk van *fact checkers.*
- Ondersteuning van lidstaten om ervoor te zorgen dat hun verkiezingen bestand zijn tegen steeds complexere cyberdreigingen, waaronder online desinformatie en cyberaanvallen.
- Sterkere bewustwording (mediageletterdheid) van internetgebruikers.
- Bevordering van vrijwillige online identificatie om de traceerbaarheid van aanbieders van informatie te vergroten.
- Stimulering van kwaliteitsjournalistiek om zodoende 'een pluralistisch, gevarieerd en duurzaam medialandschap' te waarborgen.
- Inrichting van een gecoördineerd Europees strategisch communicatiebeleid.

In oktober 2018 ondertekenden Facebook, Google, Twitter, Mozilla, brancheorganisaties van de reclamesector en adverteerders de *EU Code of Practice on Disinformation*.[67] Microsoft sloot zich in mei 2019 hierbij aan.[68] Deze praktijkcode bevat een groot aantal afspraken om (online) desinformatie tegen te gaan, waaronder het bieden van meer transparantie over politieke advertenties, het sluiten van nep-accounts, samenwerking met *fact checkers*, en het beter zichtbaar maken van informatie die op waarheid is gecontroleerd. Hoewel de Europese Commissie in de hiervoor genoemde Mededeling ook inzette op meer duidelijkheid over de werking van algoritmes en controle daarop door derden, is dit punt in de praktijkcode nauwelijks uitgewerkt.

In twee rapportages over de naleving van deze praktijkcode heeft de Commissie geconcludeerd dat de praktijkcode een goed instrument is voor dialoog met de internetplatformen en dat zij de transparantie over hun beleid ten aanzien van desinformatie heeft vergroot. Tegelijkertijd meent de Commissie dat de samenwerking met *fact checkers* kan worden verbeterd en dat de platformen meer data toegankelijk moeten maken voor wetenschappelijke onderzoeken. Ook wordt volgens deze rapportages nog onvoldoende invulling gegeven aan de toezeggingen om het bewustzijn van desinformatie onder internetgebruikers te vergroten.[69]

De Praktijkcode is ten slotte een van de elementen die worden benoemd in het Europese Actieplan tegen desinformatie[70] dat de Europese Commissie en de Hoge Vertegenwoordiger voor buitenlandse zaken en veiligheidsbeleid in december 2018 presenteerden. Het doel van dit actieplan is om de capaciteit van de EU-instellingen en de coördinatie tussen de lidstaten te versterken om desinformatie door actoren binnen de Unie en vanuit derde landen op te sporen en tegen te gaan. In lijn met de Mededeling van de Commissie op dit terrein zet het actieplan ook in op het verbeteren van de bewustwording van burgers.

**Europese datastrategie**

In februari 2020 presenteerde de nieuwe Europese Commissie haar plannen voor een 'Europese Data Strategie'.[72] De strategie is gericht op het omvormen van Europa tot een leidende data gedreven samenleving. Vanuit het perspectief van content regulering zijn twee elementen uit de datastrategie van belang. Het gaat om: 1) het herzien van de regels voor de aansprakelijkheid van internettussenpersonen en 2) de regels voor het gebruik van kunstmatige intelligentie.

*Herziening aansprakelijkheidsregels internettussenpersonen*

De voorzitter van de Europese Commissie Von der Leyen heeft in haar *political guidelines* uiteengezet dat zij de bestaande regels voor aansprakelijkheid wil upgraden.[72] De richtlijn elektronische handel zal hiertoe vervangen worden door een *Digital Services Act.* Hoewel op het moment van schrijven nog geen concrete voorstellen openbaar zijn gemaakt is de algemene verwachting dat er een strenger aansprakelijkheidsregime komt voor internettussenpersonen met een focus op de zorgplicht die de tussenpersonen hebben.[73]

*Regels voor het gebruik van kunstmatige intelligentie*

De Europese Commissie wil ook regels formuleren voor de toepassing van kunstmatige intelligentie. Hiertoe heeft de Europese Commissie een witboek over het gebruik van kunstmatige intelligentie uitgebracht.[74] Het witboek onderstreept het belang van transparantie en uitlegbaarheid van algoritmische besluitvorming en bouwt daarmee voort op de *Ethical guidelines for trustworthy AI* van de *EU High Level Expert Group on Artifical Intelligence.*[75]

Hoofdstuk 4

# Complicaties bij het reguleren van online content

Het effectief en mensenrechten-inclusief reguleren van schadelijke online content is complex. Prangende vraagstukken betreffen commercialisering, het ontbreken van rechtsmacht, de afwezige rechtsstaat, het sturende karakter van technologie, het gebruik van algoritmes, de anonimiteit van gebruikers en de gebrekkige coördinatie.

## 4.1 Commercialisering en privaat karakter van het internet

Het internet is vanaf de jaren zeventig van de vorige eeuw ontwikkeld door publiek gefinancierde Amerikaanse overheidsinstellingen en onderzoeksinstituten. De betrokken technologie-experts waren veelal idealistisch gemotiveerd en streefden met het bouwen van het internet naar de creatie van een vrijplaatsvan ideeën en kennisuitwisseling zonder overheidsbemoeienis. Vanuit deze gedachte was de kennis van de internettechnologie en -protocollen voor iedereen beschikbaar. Vanaf de jaren tachtig werd de rest van de wereld aangesloten op het internet. De uitvinding van het *World Wide Web* maakte het internet vervolgens gemakkelijk toegankelijk voor burgers, waardoor het vanaf begin jaren negentig een enorme groei doormaakte. Deze groei vormde tevens het begin van de commercialisering van het internet. De notie van een openen vrij internet vertaalde zich in praktijk in de gedachte dat internetdiensten en online informatie gratis toegankelijk moesten zijn. Dit doel bleek echter alleen economisch haalbaar door middel van reclame in combinatie met het verzamelen van data van internetgebruikers. Zoals in hoofdstuk 2 uiteen is gezet zijn als gevolg van dit verdienmodel enkele grote techbedrijven ontstaan die het internet inmiddels domineren.

De missiestatements van de dominante techbedrijven zijn veelal idealistisch geformuleerd en staan ten dienste van de internetgebruiker. Ze spreken onder meer over het organiseren en universeel toegankelijk maken van informatie (Google), het bouwen van gemeenschappen en het dichterbij elkaar brengen van de wereld (Facebook), en *empowerment* van elke persoon en organisatie op de wereld (Microsoft). Deze bedrijven zijn echter beursgenoteerd en winst maken is voor de aandeelhouders een belangrijke, zo niet de belangrijkste, doelstelling. Het verdienmodel van techbedrijven is veelal afhankelijk van aantallen *clicks* en *likes*, van een grootschalig verzamelen en verwerken van data en van het gepersonaliseerd aanbieden van advertenties, informatie en diensten. Dit verdienmodel lokt steeds aantrekkelijkere en sensationelere content uit. In tegenstelling tot traditionele nieuwsmedia is waarheidsvinding en betrouwbaarheid daarbij geen leidend principe. Dit lijkt er bovendien toe te leiden dat online andere normen en waarden zijn gaan gelden dan in de fysieke, offline wereld. De commercialisering van het internet werkt daardoor verspreiding van schadelijke online content in de hand.

Technologische wereldkaart, volgens de cijfers van 2020

naar inhoud

### Verenigde Staten

| | | |
|---|---|---|
| Apple | $ 1,4 | biljoen |
| Microsoft | $ 1,3 | biljoen |
| Amazon | $ 1,0 | biljoen |
| Alphabet | $ 988,7 | miljard |
| Facebook | $ 575,5 | miljard |
| Salesforce | $ 161,7 | miljard |
| Netflix | $ 151,4 | miljard |
| PayPal | $ 133,6 | miljard |
| Uber | $ 61,9 | miljard |
| Airbnb | $ 35,0 | miljard |
| Twitter | $ 25,2 | miljard |

### Azië

| | | |
|---|---|---|
| Alibaba | $ 554,2 | miljard |
| Tencent | $ 458,8 | miljard |
| Samsung | $ 281,2 | miljard |
| Meituan | $ 74,4 | miljard |
| JD.com | $ 55,05 | miljard |
| Baidu | $ 42,8 | miljard |
| Pinduoduo | $ 40,9 | miljard |

### Europa

| | | |
|---|---|---|
| SAP SE | $ 160,1 | miljard |
| Spotify | $ 26,0 | miljard |

### Afrika

| | | |
|---|---|---|
| Naspers | $ 73,1 | miljard |

### Nederland

| | | |
|---|---|---|
| BBP | $ 913,7 | miljard |

**Figuur 4:** Technologische wereldkaart. Gebaseerd op The Economist (2020).

## 4.2 Rechtsmacht over het internet

De soevereiniteit van nationale overheden wordt per definitie begrensd door de landsgrenzen, terwijl het internet juist sterk grensoverschrijdend is. In de begindagen van het internet werd het open en vrije karakter sterk bejubeld. De nadruk lag op de vrije ruimte en de staat had ten aanzien daarvan geen rol. Inmiddels is duidelijk dat vanuit het perspectief van bescherming van mensenrechten vormen van rechtsmacht op het internet van belang worden.[76] De concepties van territorialiteit en rechtsmacht komen daarmee in een ander daglicht te staan en verdienen hernieuwde aandacht.

Gezien het grensoverschrijdend karakter van het internet is bij de keuze van reguleringsopties (technische) kennis van het internet als mondiaal, grensoverschrijdend netwerk van netwerken zonder centrale aansturing onontbeerlijk. Hetzelfde geldt voor kennis van de mogelijke consequenties van bepaalde technologische ingrepen. Met het tijdelijk geheel afsluiten van het internet, waartoe sommige overheden soms besluiten, kan bijvoorbeeld online content vergaand worden tegengehouden, maar het verlamt onmiddellijk de hele samenleving.

In dit advies is vastgesteld dat het internet weliswaar een mondiaal publiek goed is, maar wel één dat grotendeels in handen is van private partijen. De private sector heeft dus een dominante positie op het internet. Dit brengt mee dat commerciële techbedrijven regels kunnen maken, vastgelegd in lange, vaak bijna onleesbare gebruikersvoorwaarden waar vrijwel niemand écht kennis van neemt. Die regels kunnen zij bovendien zelf uitvoeren en zij kunnen ook zelf toezicht houden op de naleving, zowel voor wat betreft de technische infrastructuur als de contentlaag van het internet. Commerciële spelers zijn zodoende wetgever, politie en rechter ineen geworden. In een democratische en rechtsstatelijke samenleving zijn deze drie functies juist welbewust gescheiden.

Hier komt bij dat de grote techbedrijven gemakkelijk over landsgrenzen heen kunnen opereren, terwijl statelijke overheden voor regulering van grensoverschrijdende onderwerpen zijn aangewezen op verdeling van rechtsmacht (jurisdictie), op bilaterale en multilaterale onderhandelingen en op de functionaliteit van internationale organisaties. Het wereldwijde en open karakter van het internet bevordert die grensoverschrijdende positie van de techbedrijven. Daardoor zijn vooral grote techbedrijven bij de governance van het internet momenteel dominant.

In beginsel kunnen staten de discussie over de regulering van online content wel aangrijpen om de controle over het internet en over de grote techbedrijven te vergroten. Zodra nationale regelgeving wordt toegepast op het internet leidt dit echter tot fragmentatie en tot een 'splinternet'. De spanning tussen de publieke en de private sfeer is in het geval van het internet dus ook een spanning tussen nationale soevereiniteit en het mondiale, niet aan rechtsmacht gebonden karakter van het internet.

Het reguleren van de private internetsector biedt een bijzondere uitdaging. Zo'n regulering vindt immers veelal plaats ex post, wanneer private ondernemingen zich reeds (geruime tijd) een aanzienlijke feitelijke machtspositie hebben verworven. Als wordt beoogd via regulering die machtspositie in te perken of de wijze van werken van die ondernemingen te veranderen kan dat het best geschieden in een proces van samenwerking en coördinatie. Dit geldt in het bijzonder wanneer bedrijven vanuit het buitenland opereren, omdat dan de mogelijkheden om wet- en regelgeving effectief af te dwingen beperkter zijn.

Content die in ons land illegaal is of schadelijk wordt geacht, kan via buitenlandse servers daardoor alsnog de weg naar de Nederlandse samenleving vinden. Ook kunnen buitenlandse mogendheden zonder al te veel moeite via het internet invloed uitoefenen op onze democratische rechtsstaat. Internationale organisaties hebben geen wereldwijde macht om tegen dergelijke beïnvloeding of schadelijke online content op te treden.

## 4.3 De afwezige rechtsstaat

In de offlinewereld kan gedrag dat schadelijk is voor mensenrechten, de nationale veiligheid en rechtsstatelijke waarden worden aangepakt met behulp van de structuren waarop onze democratische rechtsstaat is gebouwd. De normen en waarden zijn democratisch bepaald, openbaar en toegankelijk en kunnen op een rechtsstatelijke verantwoorde wijze worden gehandhaafd. Online schadelijk gedrag dat onmiskenbaar in strijd is met de nationale rechtsregels, zoals kinderpornografie, kan daarbij eveneens worden aangepakt. In hoofdstuk 1 is al gebleken dat het bij online content die minder duidelijk illegaal is, lastiger is om handhavend op te treden in overeenstemming met rechtsstatelijke waarden. Zo is de vraag wie bepaalt wat de gedragsnormen zijn op het internet (zeker nu online content vaak in andere landen wordt geplaatst), wie de positie of de macht heeft om te beoordelen of deze normen zijn geschonden, en wie in de positie is om deze normen te handhaven en zo nodig in te grijpen. Daarnaast kent de onlinewereld door zijn mondiale en overwegend private karakter geen eenduidig normenstelsel en ontbeert zij zo goed als alle processuele waarborgen die in een democratische rechtsstaat voorhanden zijn. Mechanismen die in de offlinewereld goed werken voor de rechtshandhaving (bijvoorbeeld de opsporingsbevoegdheden onder gezag van het Openbaar Ministerie of de signaleringsfunctie van een wijkagent), werken in de online context vaak ook minder goed. Een en ander betekent dat de overheid bij het bestrijden van de negatieve effecten van het internet voor de mensenrechten en democratische rechtsstatelijke waarden niet kan terugvallen op de klassieke instrumenten en waarborgen die haar in de offlinewereld ter beschikking staan. In zekere zin is de rechtsstaat bij de regulering van het internet momenteel afwezig.

## 4.4 Het sturend karakter van technologie

Bij de regulering van online content is het van belang te onderkennen dat de technologie zelf ook gebruikt kan worden als instrument om het gedrag van gebruikers te beïnvloeden. Zoals aangegeven in hoofdstuk 2 bepalen technologische mogelijkheden en ontwerpkeuzes welke online content gebruikers kunnen plaatsen en waar zij dat kunnen doen. Gedacht kan bijvoorbeeld worden aan de *retweet*- of *like*-functies of aan de algoritmes die bepalen welke informatie aan welke gebruiker wordt aangeraden. Dergelijke ontwerpkeuzes kunnen vanuit mensenrechten- en rechtsstatelijk perspectief onverwachte neveneffecten hebben. Zo heeft de *retweet*-functie het mogelijk gemaakt dat choquerende en beledigende content zich razendsnel over de wereld kan verspreiden,zonder dat dit de bedoeling van de ontwerper was. Voormalig Twitter-ontwikkelaar Chris Wetherell zei daarover: 'We hebben een geladen wapen aan een vier jaar oud kind gegeven.'[77]

> We hebben een geladen wapen aan een vier jaar oud kind gegeven.
>
> Voormalig Twitter-ontwikkelaar Chris Wetherell

Op de gemaakte technologische keuzes bestaat lang niet altijd democratische controle en van transparantie en verantwoording is zelden sprake. Wordt ertoe besloten om dit te voorkomen door van overheidswege invloed uit te oefenen, dan heeft dit grote gevolgen. Weliswaar kunnen sommige mensenrechten daardoor soms beter worden beschermd, maar tegelijkertijd komen de openheid en vrijheid van het internet hierdoor onder druk te staan.

## 4.5 Algoritmes als katalysator én oplossing

Voor vraagstukken rondom regulering van online content is het belangrijk te wijzen op het gebruik van algoritmes door vrijwel alle internetplatformen en -toepassingen om (onder meer) op basis van *big data* bepaalde groepen te bereiken met een (op hen) toegespitste boodschap. Dat kan een commerciële, maar ook een politiek geladen boodschap betreffen. Algoritmes en *big data*-analyses worden zo gebruikt voor het personaliseren van informatie en microtargeting. Dit betekent dat zij een gerichte informatiestroom kunnen genereren die sterke invloed kan hebben op iemands persoonlijke mening.

Bezien in het licht van mensenrechten en van internetgovernance verdient dit gebruik van algoritmes en *big data*-analyses aandacht. De grote techbedrijven weten hierdoor inmiddels meer van het persoonlijke leven van hun gebruikers dan de overheid van haar burgers. Bovendien kunnen internetplatformen en -toepassingen door de inzet van hun algoritmes invloed uitoefenen op de aard en inhoud van informatie die wordt verspreid en op de manier waarop mensen toegang hebben tot die informatie. De vraag rijst in hoeverre burgers nog in vrijheid afgewogen keuzes kunnen maken als hun gedrag wordt beïnvloed door gepersonaliseerde boodschappen die zij ongemerkt tijdens het internetgebruik krijgen voorgeschoteld.

Vooralsnog is de regulering van het algoritmegebruik door private ondernemingen beperkt en richt zij zich met name op databescherming. Veel algoritmes worden bovendien door het bedrijfsgeheim beschermd zodat techbedrijven weinig transparant zijn over de inhoud en werking van de algoritmes. Dit is tot op zekere hoogte begrijpelijk omdat de algoritmes tot het verdienmodel van platformen en techbedrijven behoren en er veel wordt geïnvesteerd in de ontwikkeling en verdere verbetering van die algoritmes. Tegelijkertijd laat dit zien dat er een hiaat is in de bescherming van mensenrechten in de moderne internetsamenleving. Die bescherming richt zich immers nog steeds vooral op overheidshandelen en biedt nauwelijks nog een antwoord op de vraag hoe het (commerciële) handelen van techbedrijven en platformen kan worden verenigd met de mensenrechten.

Techbedrijven zetten algoritmes eveneens in voor de zelfregulering van schadelijke online content. Hoewel de ontwikkelingen snel gaan, kunnen dergelijke algoritmes (vooralsnog) onvoldoende onderscheid maken als het gaat om de vraag welke informatie ontoelaatbaar is en daarom moet worden verwijderd. Bovendien kunnen algoritmes de context waarin de uitingen zijn gedaan niet begrijpen, terwijl deze zeer relevant is. Gevolg is dat automatische selectie van te verwijderen content, bijvoorbeeld door filtering, veel fouten kan bevatten. Dit kan als consequentie hebben dat de vrijheid om ideeën en informatie via het internet te delen op onterechte gronden wordt ingeperkt.

## 4.6 Anonimiteit van gebruikers en verantwoordelijkheid

Anonimiteit van gebruikers vormt een belangrijk kenmerk van het internet. Dit neemt niet weg dat gebruikers ook hun eigen verantwoordelijkheden hebben. Anonimiteit zorgt ervoor dat gebruikers minder snel de consequenties van hun gedragingen hoeven te ervaren: zij kunnen vrijelijk alles online zetten. De tussenkomst van derde partijen, zoals digitale platformen, leidt bovendien tot een attributie- en verantwoordelijkheidsprobleem dat weer doorwerkt in de keuze van reguleringsopties voor het internet en het daarbij passende juridische instrumentarium. Zo is het moeilijk te bepalen of bij een onrechtmatige uiting alleen de gebruiker daarop kan worden aangesproken, of ook het platform of webforum dat de uitingen faciliteert. In dit verband is de ontwikkeling binnen de EU over het aannemen van een grotere zorgplicht voor hostingpartijen en internetplatformen relevant. Vooralsnog wordt door internetplatforms echter slechts in beperkte mate aanvaard dat de overheid een taak heeft om te bepalen binnen welke kaders en in welke mate die zorgplicht moet worden uitgeoefend.

## 4.7 Gebrekkige (nationale) coördinatie

De regulering van online content is een relatief nieuw vraagstuk. In de inleiding van dit advies werd al aangegeven dat het niet eenvoudig is om tot internationale afspraken te komen en dat veel landen daarom hun eigen weg kiezen. Uit de diverse consultaties die de AIV voor dit advies hield, bleek dat ook binnen de Nederlandse overheid verschillend wordt gedacht over de regulering van online content en dat er nog nauwelijks overlegstructuren bestaan om tot een nationale standpuntbepaling te komen. De verschillende ministeries benaderen het onderwerp veelal onafhankelijk van elkaar en kijken daarbij weinig voorbij de grenzen van de eigen beleidsbevoegdheid waardoor een integrale nationale benadering ontbreekt. Door deze gebrekkige nationale beleidscoördinatie laat ook de inzet voor een internationale benadering te wensen over.

naar inhoud

# Regulering van online content: een duivels dilemma

Vanuit mensenrechtenperspectief bezien is het moeilijk om te komen tot passende regulering. Actieve interventie ten aanzien van online content kan op gespannen voet staan met mensenrechten en met democratische en rechtsstatelijke waarden. Hetzelfde geldt voor niét reguleren of passief zijn ten aanzien van content op het internet.

## 5.1 Risico's en dilemma's bij actief reguleren

Bij het maken van keuzes rondom de governance van het internet op nationaal, regionaal of internationaal niveau moeten de duivelse dilemma's en de daarmee verbonden risico's van regulering van online content onder ogen worden gezien. Om die reden worden deze dilemma's en risico's hieronder in kaart gebracht.

- **Inperking vrijheid van meningsuiting en informatiegaring**
  Regulering van online content met het oog op bescherming van mensenrechten levert onvermijdelijk een spanning op met andere mensenrechten en rechtsstatelijke waarden. Een beledigende, aanstootgevende of bedreigende uiting kan vanuit het perspectief van de vrijheid van meningsuiting door de beugel, maar tegelijkertijd kan zo'n uiting leiden tot discriminatie, reputatieschade of aantastingen van de menselijke waardigheid, integriteit of identiteit. Op een vergelijkbare manier kan nepnieuws vanuit het perspectief van de vrijheid van meningsuiting niet eenvoudig worden afgekeurd, maar het kan wel de grondwaarden van de democratische rechtsstaat aantasten wanneer het tot gevolg heeft dat de meningsvorming eenzijdig wordt beïnvloed en gestuurd. Bij het beschermen van het ene mensenrecht door middel van regulering ontstaat daardoor het risico dat een ander mensenrecht of een bepaalde rechtsstatelijke waarde minder goed wordt beschermd.

- **Ondermijning individuele autonomie door regulering en handhaving**
  Actieve regulering en de daarmee noodzakelijkerwijs gepaard gaande handhaving (al dan niet afgedwongen door de technologie) betekent doorgaans meer machtsuitoefening door de overheid. Dit heeft al snel een negatief effect op de persoonlijke autonomie en de bescherming van de mensenrechten. Een blik op de regulering van het internet in landen als China en Rusland laat een beeld zien van een overheid die een stevige greep heeft op het gedrag van haar burgers en het maatschappelijk debat online.

- **Verlies van de publieke kern en het mondiale karakter van het internet**
  (Nationale) regulering van online content die wordt afgedwongen door de technologie kan de publieke, vrije kern van het internet raken. Hierdoor ontstaat het risico op een uiteen gevallen en gefragmenteerd 'splinternet'. Een dergelijke 'cyberbalkanisering' zorgt voor een onvermijdelijke aantasting van het internet als grensoverschrijdend medium voor vrije expressie en toegang tot informatie.

- **Ondermijning innovatie en economische welvaart**
  De huidige regulering van online content is doorgaans gericht op internetplatformen en tussenpersonen. Deze (mede) aansprakelijk maken voor online content, een zorgplicht opleggen of beperken in de vrijheid om te ondernemen brengt voor deze actoren aanzienlijke risico's en kosten met zich. Investeringen door ondernemingen en het klimaat voor nieuwe *startups* zullen mogelijk minder aantrekkelijk worden als overheden besluiten tot een verdergaande regulering van het internet.

- **Risico voor averechtse effecten**
  Een actieve, restrictieve nationale of regionale regulering van het eigen internet kan buitenlandse regimes met een dubieus mensenrechtenklimaat legitimeren om hetzelfde te doen, met vergelijkbare middelen, maar dan met een doel dat niet goed past bij het Nederlandse mensenrechtenbeleid of bij rechtsstatelijke waarden.

## 5.2 Risico's en dilemma's bij niet actief reguleren

Een passieve rol van de (Nederlandse) overheid brengt minstens zozeer risico's en dilemma's mee:

- **Aantasting individuele rechten**
  Het is de taak van de staat om zijn burgers te beschermen. Wanneer de staat niet effectief kan of wil optreden tegen illegale, schadelijke of ongewenste content, dan komen rechten van burgers in het gedrang. In het bijzonder moet hierbij gedacht worden aan aantastingen van de menselijke waardigheid, zoals door discriminatie en bedreiging of belediging van individuen en (kwetsbare) groepen.

- **Aantasting van publieke waarden en ondermijning van de democratische rechtsstaat**
  Bij een passieve houding ten opzichte van illegale, schadelijke of ongewenste content kunnen publieke waarden zoals sociale cohesie en democratische besluitvorming onder druk komen te staan. Dit kan onder meer teweeg worden gebracht door een verharding en polarisatie van het maatschappelijk debat, maar ook door bewuste desinformatiecampagnes, al dan niet vanuit vreemde mogendheden die een belang hebben bij de ondermijning of destabilisatie van de democratische rechtsstaat.[78]

- **Vrij spel geven aan vreemde mogendheden**
  Terughoudendheid van de Nederlandse overheid in het reguleren van online content zowel nationaal als internationaal, weerhoudt andere staten er niet van die delen van het internet die binnen hun invloedssfeer liggen te reguleren. In bijvoorbeeld China, Saudi-Arabië en Iran is het blokkeren van bepaalde websites of het tijdelijk geheel afsluiten van het internet (de publieke kern van het internet) altijd gangbaar beleid geweest. In die zin is de eerdergenoemde 'balkanisering' van het internet al een feit. Terughoudendheid bij de regulering maakt het voor staten tegelijkertijd moeilijker het eigen internet te beschermen en om de eigen waarden in het debat krachtig te positioneren tegenover die van andere mogendheden.

- **Risico's voor veiligheid en de openbare orde**
  Het internet kan niet los worden gezien van de fysieke wereld. Dat betekent dat online uitingen en gedragingen ook een effect kunnen hebben in de fysieke wereld. Dit geldt bijvoorbeeld voor online opruiing, bedreiging of aanzetten tot haat, maar ook voor het digitaal uitwisselen van beelden van kindermisbruik of het op het *dark web*[79] voorbereiden van criminele of terroristische activiteiten. Niet ingrijpen in deze onlinewereld betekent dan ook al snel dat in de offlinewereld onvoldoende bescherming wordt geboden aan mensenrechten en rechtsstatelijke waarden.

- **Oneerlijke verdeling van kosten en baten**
  Het verdienmodel van internetplatformen is gebaseerd op het bij elkaar brengen van mensen en hen in staat te stellen om informatie met elkaar te delen. Wanneer illegale, schadelijke of ongewenste content wordt gedeeld, heeft dit een negatief effect op individuen, groepen en de maatschappij als geheel. De kosten van deze negatieve effecten worden niet gedragen door de internetplatformen zelf, maar door de slachtoffers en de samenleving. Je kan daarmee stellen dat door het uitoefenen van hun economische activiteit de internet platformen negatieve externaliteiten creëren, vergelijkbaar met een vervuilende industrie. Professionele internetplatformen nemen doorgaans hun maatschappelijke verantwoordelijkheid voor het voorkomen of beperken van deze effecten wel, maar hun commerciële verdienmodellen blijven sturend als het gaat om de mate waarin en de manier waarop zij invulling geven aan hun verantwoordelijkheid. Wanneer er sprake is van negatieve externaliteiten en de overheid neemt geen maatregelen om deze effecten te adresseren, kan er een oneerlijke verdeling van kosten en baten tussen de internetplatformen en de samenleving ontstaan.

## 5.3 Balanceren van mensenrechten in context

**Een open, vrij en veilig internet is een illusie**

Een mensenrechten-inclusieve benadering vergt dat meer aandacht wordt gegeven aan de negatieve impact van het internet op democratisch-rechtsstatelijke waarden, waaronder de grondrechten. De inherente spanning tussen de bescherming van mensenrechten in concrete gevallen, zoals de mogelijke spanning tussen vrijheid van meningsuiting en het discriminatieverbod, kan en mag niet worden veronachtzaamd.[80] Ook als het uitgangspunt blijft dat het internet zo open, vrij en veilig mogelijk moet zijn, moet tegelijkertijd buiten kijf staan dat het op en via het internet toebrengen van schade aan mensenrechten en democratische rechtsstatelijke waarden moet worden bestreden. De overheid kan niet meer ontkomen aan het ontwikkelen van vormen van regulering met het oog op bescherming tegen schadelijke online content.

Dat dit niet eenvoudig is, maakt dit advies op verschillende punten duidelijk. De in hoofdstuk 4 beschreven complicaties bij het reguleren van online content bepalen en beperken de handelingsopties en de hierboven besproken risico's en dilemma's van reguleren of niet-reguleren, mogen niet worden veronachtzaamd. Ongeacht welk vorm(en) van reguleren ook wordt gekozen, vaak zullen belangrijke verworvenheden en waarden onder spanning komen te staan. Ook zullen er keuzes moeten worden gemaakt tussen verschillende (mensen)rechten die bij de verspreiding van schadelijke online content tegenover elkaar komen te staan. Enerzijds kan de introductie van zorgplicht voor internetplatformen of een grotere invloed van de overheid op het internet immers leiden tot een aantasting van de vrijheid van meningsuiting, het recht op toegang tot informatie, de bescherming van de persoonlijke levenssfeer en de vrijheid van ondernemerschap. Anderzijds kan niet-ingrijpen leiden tot discriminatie, aantasting van de veiligheid en ondermijning van andere democratische en rechtsstatelijke beginselen. Bij het zoeken naar vormen van regulering zal dus steeds een balans moeten worden gevonden tussen verschillende rechten en belangen – een precair proces.

**Een route met hindernissen**

Hoewel veel mensen het internet nog steeds kritiekloos gebruiken, is via media, belangenbehartigers en educatie bij veel gebruikers het besef doorgedrongen van de risico's voor het verspreiden van schadelijke content en desinformatie en van personalisering. Ook overheden en internationale instituties zijn inmiddels alert en actief geworden. Er is een politieke en maatschappelijke roep om meer overheidsregulering van online content en een actievere zorgplicht voor het bedrijfsleven (meer in ISPs en internetplatformen) waar het gaat om het monitoren van de inhoud die eindgebruikers op het internet delen.[81] Die roep is er bovendien niet alleen in Nederland; ook traditionele (westerse) bondgenoten zoals Duitsland, het Verenigd Koninkrijk en Frankrijk dringen aan op wetgeving

en/of hebben dergelijke wetgeving zelf al ingevoerd. Het besef van de noodzaak van actie is ook op EU en breder Europees en internationaal niveau aanwezig. Actie is inmiddels in allerlei vormen te zien, variërend van het doen van aanbevelingen voor (zelf)regulering en het formuleren van gedragscodes tot het reguleren van specifieke toepassingen van het internet of het beschermen van specifieke grondrechten (zoals de bescherming van persoonsgegevens). Het bewustzijn van de risico's van het internet is daarnaast te herkennen in diverse acties en reacties van grote techbedrijven die steeds meer investeren in het identificeren en verwijderen van schadelijke online content en in verschillende vormen van zelfregulering.

Deze activiteiten zijn allemaal van vrij recente datum, mede als gevolg van het pas relatief laat onderkennen van de risico's en nadelen van internet. In het voorgaande is bovendien geconstateerd dat er weliswaar allerlei beleids- en reguleringsinspanningen zijn, maar dat die zich op allerlei verschillende niveaus en binnen verschillende sectoren manifesteren – nationaal, Europees, internationaal, publiek en privaat. Goede coördinatie en afstemming ontbreekt. Als gevolg daarvan is de bescherming van grondrechten en rechtsstatelijke waarden tegen aantastingen door schadelijke online content versnipperd en onvolledig. Er zijn weinig heldere internationale regels en voorschriften om schadelijke online content te kunnen bestrijden. Weliswaar zijn in rechtspraak van Europese hoven als het EHRM algemene vereisten en voorwaarden ontwikkeld, maar ook die bieden in de praktijk niet altijd evenveel houvast. Veel schadelijke online content wordt bovendien niet exclusief beheerst door EU- en/of nationale wetgeving en valt niet onder de rechtsmacht van individuele staten. Handhaving en sanctionering noch daarbij passende bevoegdheden zijn duidelijk vastgelegd. Zelfregulering en zorgplichten zijn er wel, maar de vormgeving daarvan verschilt nogal eens per staat, per sector of zelfs per bedrijf. Deze lappendeken van regulering heeft ook voor internetbedrijven tot gevolg dat zij met conflicterende regelgeving of onduidelijke verplichtingen worden geconfronteerd. Daarnaast sluiten handelings- en reguleringsmogelijkheden die nationaal en internationaal gebruikelijk zijn om maatschappelijk ongewenste activiteiten aan te pakken (verdragen, richtlijnen, bindende afspraken en resoluties) niet als vanzelf – en in de kern helemaal niet – aan op de governance en de bijzondere eigenschappen van het internet, zoals die in het voorgaande uitgebreid aan bod zijn geweest.

> Internetregulering speelt zich niet af in een nationale cocon. Oplossingen zullen in internationaal verband moeten worden ontwikkeld.

Deze bevindingen illustreren dat overgaan tot regulering niet alleen leidt tot inhoudelijke dilemma's, maar ook tot de vraag op welke wijze het proces van regulering vorm zou moeten en kunnen krijgen. Daarbij moet bovendien rekening worden gehouden met de diverse uitdagingen waarvoor het internet ons stelt en die in hoofdstuk 4 in beeld zijn gebracht. Het sturend karakter van de technologie, de dominante positie van private actoren, de afwezige rechtsstaat, het fragmentarisch karakter van de bestaande regulering en het ontbreken van grensoverschrijdende rechtsmacht brengen mee dat de aanpak van schadelijke online content uitermate complex is. Deze uitdagingen bij het reguleren van het internet in het algemeen en van online content in het bijzonder zijn bepalend voor de te kiezen vormen van regulering. Om enkele voorbeelden te noemen: met welke private en/of publieke partners moet het proces van regulering worden aangegaan? In welk tempo en in welke volgorde moet dat gebeuren? En op welk niveau van het internet moet regulering worden ingezet?

Daar komt bij dat internetregulering zich niet afspeelt in een nationale cocon. Op basis van nationale wet- en regelgeving kunnen wellicht beperkingen worden opgelegd aan het gebruik van het internet, maar daarmee wordt de aantasting van mensenrechten en democratisch rechtsstatelijke waarden door schadelijke online content op internationaal niveau of vanuit het buitenland niet voorkomen. Het ligt daarom in de rede om zoveel mogelijk in internationaal verband te zoeken naar oplossingen, ook al is het zoeken naar internationale consensus lastig en tijdrovend. Nederland kan met name op Europees niveau een betekenisvolle rol spelen. In Europa zijn de opvattingen over schadelijke content homogener dan op internationaal niveau en bestaan er meer mogelijkheden om tot gezamenlijke normstelling, toezicht en handhaving te komen. Daarnaast kan ons land via Europa een krachtiger geluid laten horen in internationale discussies over de regulering van online content. Mensenrechtenstandaarden die in relevante Europese verdragen als het Verdrag van Lanzarote en het Verdrag van Boedapest met aanvullend Protocol zijn vastgelegd en de ervaringen die met de uitvoering zijn opgedaan, kunnen gebruikt worden om op het niveau van de Verenigde Naties soortgelijke verdragen in relatie tot online regulering tot stand te brengen. Nederland zou daartoe initiatieven kunnen nemen in samenwerking met gelijkgezinde landen.

De in dit advies gepresenteerde analyse overziend, moet worden geconcludeerd dat een herijking van het mensenrechtenbeleid inzake schadelijke online content noodzakelijk is. Tegelijkertijd zijn de discussies over normstelling en regulering zowel nationaal als internationaal nog niet voldoende uitgekristalliseerd, hetgeen consequenties heeft voor de concreetheid van de aanbevelingen die in dit verband kunnen worden gedaan. Wil de Nederlandse overheid tot een mensenrechten-inclusieve benadering van de aanpak van schadelijke online content komen, dan is het noodzakelijk dat zij ook in het nationaal beleid ten aanzien van internet een aantal stevige stappen zet. Zonder eenduidig en gecoördineerd beleid op nationaal niveau zal regulering van het internet in het belang van de mensenrechten op internationaal niveau nog complexer zijn dan het toch al is. Het nationale en het buitenlands beleid moeten in elkaars verlengde liggen en samenvallen. Het in acht nemen van de in de samenvatting weergegeven uitgangspunten en het opvolgen van de aanbevelingen in dit advies kunnen hieraan in belangrijke mate bijdragen.


naar inhoud

# Eindnoten

naar inhoud

1 De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) heeft eerder al gesignaleerd in *De publieke kern van het internet. Naar een buitenlands internetbeleid* (2015) dat het internet alleen als publiek goed functioneert als het de kernwaarden universaliteit, interoperabiliteit en toegankelijkheid garandeert en als het de kerndoelen van informatieveiligheid ondersteunt, te weten vertrouwelijkheid, integriteit en beschikbaarheid. Nederland moet zich in internationaal perspectief dan ook hardmaken voor het behoud en het versterken van deze publieke kern, die met name wordt gevormd door de kernprotocollen en technische standaarden.

2 Facebook (2019) Update on New Zealand.

3 The Guardian (2019) Social media firms fight to delete Christchurch shooting footage.

4 NRC (2019) Hoe het Christchurch-manifest in alle talen de wereld over gaat.

5 Zie onder meer: Washington Post (2019) The internet needs new rules; Financial Times (2019) Mark Zuckerberg: Big Tech needs more regulation en NRC (2020) Facebook maakt werk van toezicht op moderatiebeleid.

6 Zie: Ministerie van Buitenlandse Zaken, Mensenrechtenrapportage 2018.

7 Zie: NCSC, Cybersecuritybeeld Nederland CSBN 2019.

8 Kamerstuk 26643-447 (2016 -2017).

9 Zie in dit kader ook: AIV-briefadvies 31 (2017) Rusland en de Nederlandse defensie-inspanningen,.

10 Zie: The Economist (2017) The world's most valuable resource is no longer oil, but data.

11 O'Hara, Kieren en Hall, Wendy (2018) *Four Internets. The Geopolitics of Digital Governance*. CIGI Papers No. 206.

12 Zie: Van Reisen, Mirjam (2018) Dutch National Data Policy.

13 Zie in dit verband ook de Mededeling van de Europese Commissie over een Europese datastrategie (COM(2020) 66 final) en het Witboek over kunstmatige intelligentie (COM(2020) 65 final).

14 Zie: Welch, Chris (2012) Russia, China, and other nations draft proposal to give ITU greater influence over the internet. Zie ook: Nye, Jr., Joseph S. (2016) *'The regime complex for managing global cyber activities', in GCIC, Who runs the internet. The global multistakeholder model of internet governance,* Chatham House, p. 8.

15 Lynch, Colum (2019) China Bids to Lead World Agency Protecting Intellectual Property' in *Foreign Policy.*

16 Zie: Negro, Gianluigi (2019) A history of Chinese global internet governance and its relations with ITU and ICANN, in Chinese Journal of Communication en Financial Times (2020) Inside China's controversial mission to reinvent the internet.

17 Lessig, L. (2006), Code v2, New York: Basic Books.

18 Deze metafoor is losjes gebaseerd op het werk van Van Dijck, José (2019) Europa moet zorgen voor een diverse digitale infrastructuur, *Financieel Dagblad*; Van Dijck, José (in voorbereiding) *Visualizing platform power: the platformization tree.* De boommetafoor van Van Dijck heeft daarbij wel een andere functie, namelijk die van het specifiek inzichtelijk maken van de rol van grote internetbedrijven en SMPs op onze samenleving. In dit rapport is de metafoor vooral bedoeld om de verschillende spelers in de wereld van het internet in beeld te brengen, waardoor de boom een iets andere vorm heeft gekregen.

19 Zie: Request for Comments 1602.

20 TCP/IP refereert doorgaans aan een *stack* (stapel) protocollen. Voor de leesbaarheid beperken wij ons tot de bespreking van TCP en IP.

21 Schermer, Bart W., Lodder, Arno (2014) Internet Governance in *Recht & Computer* (6e druk), Deventer: Kluwer.

22 Andere factoren die hieraan bijdragen zijn de goede (hosting)infrastructuur in Nederland en de aanwezigheid van instituten als SURF dat via een computernetwerk wereldwijd hogescholen, universiteiten, academische ziekenhuizen, onderzoeksinstituten en andere wetenschappelijke

organisaties met elkaar verbindt.

23 ICANN stond tot 1 oktober 2016 onder toezicht van het Amerikaanse ministerie van Handel.

24 Zie: ICANN.

25 Resoluties zijn politiek bindende besluiten die met consensus of na stemming door de Mensenrechtenraad kunnen worden aangenomen.

26 Zie: A/HRC/RES/20/8; A/HRC/RES/26/13; A/HRC/RES/32/13 en A/HRC/RES/38/7.

27 Het Internationaal Verdrag inzake burgerrechten en politieke rechten is door 170 landen geratificeerd. Artikel 19 luidt: '1. Een ieder heeft het recht zonder inmenging een mening te koesteren. 2. Een ieder heeft het recht op vrijheid van meningsuiting; dit recht omvat mede de vrijheid inlichtingen en denkbeelden van welke aard ook op te sporen, te ontvangen en door te geven, ongeacht grenzen, hetzij mondeling, hetzij in geschreven of gedrukte vorm, in de vorm van kunst, of met behulp van andere media naar zijn keuze. 3. Aan de uitoefening van de in het tweede lid van dit artikel bedoelde rechten zijn bijzondere plichten en verantwoordelijkheden verbonden. Deze kan derhalve aan bepaalde beperkingen worden gebonden, doch alleen beperkingen die bij de wet worden voorzien en nodig zijn: a) in het belang van de rechten of de goede naam van anderen; b) in het belang van de nationale veiligheid of ter bescherming van de openbare orde, de volksgezondheid of de goede zeden'.

28 Ibid.

29 Ibid.

30 CCPR/C/GC/34, UN Human Rights Committee, General Comment No, 34: Article 19: Freedoms of Opinion and Expression, 12 september 2011, paras. 12, 15 en 43.

31 A/HRC/38/35 en A/HRC/74/486. In 2017 berichtte de Speciale Rapporteur tevens over de rol van 'private actors engaged in the provision of internet and telecommunications access' (A/HRC/35/22).

32 Deze laatste bepaling moet ook worden gelezen in het licht van het Internationaal Verdrag inzake de uitbanning van alle vormen van rassendiscriminatie. In artikel 4 veroordelen de Staten die partij zijn bij dit Verdrag 'alle propaganda en alle organisaties die berusten op denkbeelden of theorieën die uitgaan van de superioriteit van een bepaald ras of een groep personen van een bepaalde huidskleur of etnische afstamming, of die trachten rassenhaat en rassendiscriminatie in enige vorm te rechtvaardigen of te bevorderen, en nemen de verplichting op zich onverwijld positieve maatregelen te nemen die erop zijn gericht aan elke vorm van aanzetting tot of aan elke uiting van een zodanige discriminatie een einde te maken (...)'. In artikel 5 nemen de Staten die partij zijn bij het Verdrag 'de verplichting op zich rassendiscriminatie in al haar vormen te verbieden en uit te bannen en het recht van een ieder, zonder onderscheid naar ras, huidskleur of nationale of etnische afstamming, op gelijkheid voor de wet te verzekeren (...).'

33 A/HRC/38/35, para 1.

34 Voor deze paragraaf is onder meer gebruik gemaakt van: A.L.J. Janssens en A.J Nieuwenhuis (2019) *Uitingsdelicten*, vierde druk, Studiepockets Strafrecht nr. 36, Wolters Kluwer, Hoofdstuk 2; J.H. Gerards, 'Artikel 10 EVRM. Vrijheid van meningsuiting', in: J.H. Gerards e.a. (red.), *Sdu Commentaar EVRM*, Den Haag: Sdu 2020; J.H. Gerards, *General principles of the European Convention on Human Rights,* Cambridge University Press (2019); M.M. Julicher, 'Red het censuurverbod: schaf het af!', in: Tijdschrift voor Constitutioneel Recht, juli 2019, pp. 184-210.

35 Het EHRM baseert zich hierbij vaak (maar niet altijd) op artikel 17 EVRM, dat bepaalt dat het uitoefenen van bepaalde vrijheden zoals de vrijheid van meningsuiting niet grondrechtelijk wordt beschermd als het doel is om de rechten en vrijheden die in het EVMR zijn vastgelegd, te ondermijnen of te vernietigen. Zie hierover nader o.m. P.E. de Morree, *Rights and wrongs under the ECHR. The prohibition of abuse of rights in Article 17 of the European Convention of Human Rights,* Antwerpen: Intersentia, 2016.

36 Zie: *Tamiz t. het Verenigd Koninkrijk,* EHRM 19 september 2017, nr. 3877/14; *Cengiz en anderen t. Turkije,* EHRM1 december 2015, nr. 48226/10 en 14027/11; *Ahmet Yildirim t. Turkije,* EHRM 18 december 2012, nr. 3111/10; *Einarsson t. IJsland,* EHRM 7 november 2017, nr. 24703/15; *Kablis t.*

*Rusland,* EHRM 30 apri 2019, nr. 48310/16 en 59663/17; *Magyar Tartalomszolgáltatók Egyesülete en Index.hu Zrt t. Hongarije,* EHRM 2 mei 2016, nr. 22947/13.

37 *Delfi AS t. Estland,* EHRM 16 juni 2015, nr. 64569/09.

38 Trb. 2008, 58.

39 Trb. 2002, 18.

40 Trb. 2003, 60.

41 Zie: Council of Europe, *Recommendations and declarations of the Commmittee of Ministers of the Council of Europe in the field of media and information society,* Strasbourg (2016).

42 Recommendation No. R (97) 19.

43 Zie onder meer: Recommendation Rec (2001) 8; Recommendation CM/Rec (2007) 11; Recommendation CM/Rec (2008) 6; Recommendation CM/Rec (2011) 8; Recommendation CM/Rec (2014) 6 ; Recommendation CM/Rec (2018) 2; Declaration on freedom of communication on the internet (28 May 2003).

44 Digital Charter (2019).

45 Ook de Nederlandse regering laveert tussen de opties van 'vrijwillige- doch geen vrijblijvende samenwerking tussen overheid en IT-platformen' en bindende Europese of nationale wetgeving. Zie kamerstuk 30950, nr. 158 (2018).

46 COM(2020) 65 final.

47 COM(2020) 66 final.

48 Richtlijn 2000/31/EG. Een EU-richtlijn is een juridisch bindend instrument en legt het eindresultaat vast dat alle EU-lidstaten moeten bereiken. De lidstaten kunnen vervolgens zelf bepalen welke nationale wetgeving daartoe moet worden vastgesteld.

49 Ibid., artikel 15.

50 Richtlijn 2010/13/EU, artikel 4.

51 Richtlijn (EU) 2018/1808, artikel 1.

52 Ibid., artikel 6.

53 Kaderbesluit 2008/913/JBZ.

54 Richtlijn 2011/92/EU.

55 Richtlijn (EU) 2017/541.

56 Zie: The EU Code of Conduct (2018).

57 Zie ook het eerder genoemde Kaderbesluit 2008/913/JBZ betreffende de bestrijding van bepaalde vormen en uitingen van racisme en vreemdelingenhaat door middel van het strafrecht.

58 European Commission (2019) *Assessment of the Code of Conduct on Hate Speech online. State of Play* (12522/19).

59 COM(2017) 555 final.

60 C(2018) 1177 final.

61 COM(2018) 640 final; 2018/0331 (COD). Een EU-Verordening is rechtstreeks van toepassing in alle lidstaten. Anders dan bij een Richtlijn hoeft een Verordening dus niet te worden omgezet in nationale regelgeving.

62 'Terroristische inhoud' wordt in artikel 2 van het voorstel gedefinieerd als: 'informatie die aan een of meer van de volgende voorwaarden voldoet: (a) het aanzetten tot of het verdedigen van het plegen van terroristische misdrijven, onder meer door ze te verheerlijken, waardoor het gevaar ontstaat dat dergelijke daden worden gepleegd; (b) het aanmoedigen van het bijdragen aan terroristische misdrijven; (c) het bevorderen van de activiteiten van een terroristische groepering, met name door aanmoediging van het deelnemen aan of het ondersteunen van een terroristische groepering in de zin van artikel 2, lid 3, van Richtlijn (EU) 2017/541; (d) het instrueren over methoden of technieken voor het plegen van terroristische misdrijven.'

63 Ibid., artikel 3.

64 2018/0331 (COD), overweging 5.

65 COM(2018) 236 final.

66 De Mededeling van de Europese Commissie is onder meer gebaseerd op het advies van de

*High Level Expert Group on Fake News* die in 2017 is opgericht door de Commissie. Zie: Europese Commissie (2018) Final report of the High Level Expert Group on Fake News and Online Disinformation.

67 Zie: Europese Commissie (2018) Code of Practice on Disinformation.

68 Zie: Europese Commissie (2018) Roadmaps to implement the Code of Practice on disinformation.

69 Zie: Europese Commissie (2019) Last intermediate results of the EU Code of Practice against disinformation en Europese Commissie (2019) Annual self-assessment reports of signatories to the Code of Practice on Disinformation 2019.

70 JOIN(2018) 36 final.

71 COM(2020) 65 final.

72 Zie: Von der Leyen, Ursula (2019) A Union that strives for more . My agenda for Europe.

73 Zie: Financial Times (2019) EU draws up sweeping rules to curb illegal online content.

74 COM(2020) 66 final.

75 Europese Commissie (2019) Ethics guidelines for trustworthy AI.

76 Zie voor een fundamentele benadering van deze problematiek Lianne Boer en Wouter Werner, Concepties van territorialiteit in het internationaal recht in: De Grenzen voorbij, De actualiteit van territorialiteit en jurisdictie, Preadviezen Nederlandse Juristen-Vereniging 2019, Wolters Kluwer, p. 15-58.

77 Volkskrant (2019) Techbedrijven moeten steeds vaker aanzien hoe hun creaties door kwaadwilligen worden gebruikt.

78 Zie in dit kader ook AIV-advies 104 (2017) De wil van het volk? Erosie van de Democratische Rechtsstaat in Europa.

79 Het *dark web* is het deel van het *world wibe* web dat niet rechtstreeks vindbaar is voor zoekmachines. Het *dark web* wordt niet alleen gebruikt voor illegale handel in goederen en diensten. Journalisten, mensenrechtenactivisten, dissidenten en klokkenluiders kunnen op het *dark web* anoniem gevoelige informatie uitwisselen.

80 Een spanning die bij de aanpak van ongewenst gedrag, zoals in het strafrecht (zowel materieelrechtelijk als procedureel) voortdurend aan de orde is en nimmer kan of mag worden ontkend.

81 Denk onder andere aan de strafbaarstelling van wraakporno en de wens van de kamer om de privacy in horizontale verhoudingen beter te beschermen (Initiatiefnota Koopmans Onderlinge Privacy). Zie: Kamerstukken II, 2017/2018, 34926 nrs. 1-2.

# Adviesaanvraag

naar inhoud

Ministerie van Buitenlandse Zaken

Aan de Voorzitter van de Adviesraad Internationale Vraagstukken
Mr. J.G. de Hoop Scheffer
Postbus 20061
2500 EB
DEN HAAG

Rijnstraat 8
2515 XP Den Haag
Postbus 20061
2500 EB Den Haag
Nederland
www.rijksoverheid.nl
Nederland
www.nederlandwereldwijd.nl

Datum 27 mei 2019
Betreft Aanvraag voor AIV-advies over regulering van online content

Geachte voorzitter,

Nederlands internetbeleid, zowel binnenlands als buitenlands, richt zich op het verdedigen en stimuleren van het open, vrije en veilige internet. Het internet is een plek waar mensenrechten, zoals het recht op vrijheid van meningsuiting en het recht op bescherming tegen willekeurige of onwettige inmenging in privéleven, onverminderd van kracht zijn. Inperking van deze rechten online dient te voldoen aan de internationaal vastgestelde voorwaarden. Nederland zet zich hier stevig voor in.

In de Nederlandse digitaliseringsstrategie van juni 2018 wordt de Nederlandse voortrekkersrol onder meer gekenmerkt door het versterken van weerbaarheid van burgers en organisaties en bescherming van grondrechten en ethiek in de digitale tijd[1]. De Nederlandse Cyber Security Agenda[2] van april 2018 benoemt het beschermen van waarden en grondrechten in het digitale domein als belangrijk onderdeel van cybersecurity. De Internationale Cyberstrategie[3] van februari 2017 stelt dat Nederland baat heeft bij een wereldwijde bescherming van mensenrechten online en de actualisering van het mensenrechtenbeleid[4] van mei 2018 benadrukt de inzet op respect voor universele rechten van de mens offline en online en identificeert vrijheid van meningsuiting offline en online als een van de prioriteiten van het Nederlands buitenlands mensenrechtenbeleid.

De laatste tijd groeien echter de zorgen over *online content* (datgene wat door gebruikers op het internet gedeeld wordt) waar een dreiging van uitgaat – van bijvoorbeeld kwetsbare groepen in de samenleving, democratische processen of de zittende macht – en de verspreiding ervan.

Veel landen beschouwen het bestaan en verspreiden van deze *online content* als veiligheidsvraagstuk en ontwerpen regelgeving met inperking van de ruimte voor uitoefening van mensenrechten online en impact op de functionaliteit van het wereldwijde internet.

[1] Kamerstuk 26643-541, tevens in lijn met motie 26643-566 over nadruk op grondrechten en ethiek in de Digitaliseringsstrategie.
[2] Kamerstuk 26643-536
[3] Kamerstuk 26643-447
[4] Kamerstuk 26643-447

Pagina 1 van 2

Regulering van het internet is een uitdagend vraagstuk omdat Nederland gericht is op de minimale regulering en het vrijlaten van de internetmarkt. Zowel de infrastructuur als de *content*laag van het internet is in private handen. Op deze wijze wordt volgens Nederland het beste het vrije, open en veilige karakter van het internet behouden. In veel democratische landen wordt door overheden met name verwezen naar de verantwoordelijkheid van deze bedrijven om zelfregulering toe te passen om verspreiding van ongewenste *online content* tegen te gaan.

De roep om internationale regulering door overheden van *online content* wordt echter steeds sterker. De verwachting is dat internationale en nationale regulering in andere landen implicaties kan hebben voor het wereldwijde open en vrije internet en de ruimte voor internetgebruikers in Nederland. Het is van belang dat Nederland hierop anticipeert door reguleringsopties te onderzoeken zonder de terughoudendheid ten aanzien van regulering van online content te veronachtzamen.

Nederland heeft de potentie om binnen de EU en in internationale gremia een voortrekker te zijn als pleitbezorger van een rechtsstatelijke, mensenrechteninclusieve benadering van regulering van *online content*. Dit zou een aanvulling vormen op de reeds gezaghebbende internationale positie van Nederland op het gebied van de toepassing en implementatie van internationaal recht, inclusief mensenrechten, in cyberspace. Gezien de nauwe verwevenheid tussen binnen- en buitenlands beleid ten aanzien van het internet, is een herkenbare Nederlandse visie en praktijk noodzakelijk om internationaal effectief te zijn.

Een spoedig AIV-advies met richtinggevende beleidsaanbevelingen op dit onderwerp heeft toegevoegde waarde voor de internationale inzet van Nederland en kan complementair zijn aan nationale beleidstrajecten. Het advies kan voortbouwen op AIV-advies 'Het internet; een wereldwijde vrije ruimte met begrensde staatsmacht' door met name aanbeveling 8 uit dit advies omtrent de omgang met internetbedrijven nader uit te werken voor de specifieke uitdaging omtrent regulering van ongewenste *online content*.

Het kabinet wil de volgende vragen aan de AIV voorleggen:

1. Op welke internationale ontwikkelingen omtrent regulering van online content en verspreiding ervan, inclusief in het multilaterale domein, moet Nederland waakzaam zijn? Welke handelingsopties heeft Nederland? Wat kan Nederland het beste doen om internationale ontwikkelingen te beïnvloeden in multi- en bilateraal verband?
2. In het licht van de antwoorden op bovenstaande vragen: wat zijn reguleringsopties van online content door overheden? Hoe kan regulering mensenrechteninclusief worden vormgegeven zodat democratische waarden en mensenrechten gewaarborgd worden op het internet? Wat zijn de keerzijden van regulering? Wat past bij de Nederlandse rechtspraktijk en de traditionele Nederlandse houding van terughoudendheid?
3. Op welke manieren kan richting en sturing worden gegeven aan private internetbedrijven als belangrijke actor bij het uitvoeren van regulering?

Ik zie uw advies graag voor het einde van het jaar tegemoet.

Stef Blok
Minister van Buitenlandse Zaken

Pagina 2 van 2

# Geraadpleegde personen

Ter voorbereiding van het advies heeft de commissie gesproken met een groot aantal deskundigen. De AIV is hen zeer erkentelijk voor hun inzichten en hun inbreng.

- **Drs. E.S.M. *(Erik)* Akerboom**
  Korpschef van de Nationale Politie (tot 29 april 2020)
- **P.J. *(Pieter-Jaap)* Aalbersberg EMPM**
  Nationaal Coördinator Terrorismebestrijding en Veiligheid
- **Mr. A. *(Arie)* van Bellen**
  Directeur van Platform ECP
- **Mr. G.W. *(Gerrit)* van der Burg MPA**
  Voorzitter College van Procureurs-Generaal
- **Ms. S. *(Siobhan)* Cummiskey LLM**
  Director of Public Policy, Campaigns and Programs, Facebook
- **A. *(Astrid)* van Engen MSc**
  Coördinerend adviseur bij Nationaal Coördinator Terrorismebestrijding en Veiligheid
- **Drs. E. *(Edo)* Haveman**
  Hoofd Public Policy BENELUX, Facebook
- **Drs. A. *(Arjan)* El Fassed**
  Hoofd Public Policy Google in Nederland
- **P. *(Puck)* Gorrissen MA**
  Beleidsmedewerker Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- **J. *(Jochem)* de Groot MSc**
  Directeur Corporate Affairs voor Microsoft in Nederland
- **L.A. *(Lauren)* Heida MA**
  Beleidsmedewerker Ministerie van Defensie
- **Prof. dr. ir. E. *(Erik)* Huizer**
  CEO van GÉANT
- **A. *(Alex)* de Joode LLM**
  Public Affairs Manager bij NLdigital (tot mei 2020)
- **M. *(Marisa)* Jimenez Martin**
  Director and Deputy Head of EU Affairs at Facebook
- **P. *(Pieter)* van Koetsveld MA**
  Sr. beleidsmedewerker Ministerie van Onderwijs Cultuur en Wetenschap
- **Drs. M. *(Merel)* Koning**
  Sr. beleidsmedewerker, Amnesty International Nederland
- **R. *(Ruth)* Kronenburg**
  Operationeel directeur van Free Press Unlimited
- **Mr. L.W. *(Lousewies)* van der Laan**
  Director ICANN (tot 2018)
- **Drs. H. *(Hans)* van Leeuwe**
  Hoofd, Directoraat General of Policy Ministerie van Defensie
- **Dhr. Dr. T. *(Tarlach)* McGonagle**
  Bijzonder hoogleraar Mediarecht & Informatiesamenleving, Universiteit van Leiden
- **A. *(Arienne)* Mulder**
  Legal Specialist, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- **M. *(Martinus)* Oosterbaan**
  Nationaal Coördinator Terrorismebestrijding en Veiligheid
- **A. *(Auke)* Pals BSc**
  Voorzitter ECP Digiraad

- **A. (*Arnold*) van Rhijn LLM**
  Sr. beleidsmedewerker, Ministerie van Economische Zaken en Klimaat
- **Mr J.J. (*Just*) Stam**
  Raadadviseur Ministerie van Justitie en Veiligheid
- **Drs. G.P.M.H. (*Gerard*) Steeghs**
  Directeur Multilaterale Organisaties en Mensenrechten, Ministerie van Buitenlandse Zaken
- **M. (*Michiel*) Steltman**
  Directeur DINL
- **S. (*Sam*) Stevens MA**
  Public Policy Manager at Facebook
- **M. (*Marleen*) Stikker**
  Directeur Waag Technology & Society
- **Drs. L. (*Lisa*) Vermeer**
  Sr. beleidsadviseur, Ministerie van Buitenlandse Zaken (tot okt 2019)
- **L. (*Lisa*) van de Voort LLM MSc**
  Sr. beleidsmedewerker Mediabeleid, Ministerie van Onderwijs Cultuur en Wetenschap
- **M. (*Michael*) Vos MSc**
  Government Affairs Consultant, Microsoft NL
- **M. (*Maarten*) van Waveren LLM**
  Sr. beleidsadviseur, Ministerie van Economische Zaken en Klimaat
- **Drs. B.T. (*Bastiaan*) Winkel**
  Beleidsadviseur Criminaliteit en Veiligheid, Ministerie van Justitie en Veiligheid
- **G. (*Guus*) van Zwoll MA**
  Sr. beleidsadviseur, Ministerie van Buitenlandse Zaken
- **H. (*Hans*) de Zwart**
  Directeur van Bits of Freedom (tot oktokber 2019)

naar inhoud

# Lijst met afkortingen

| | |
|---|---|
| **AIV** | Adviesraad Internationale Vraagstukken |
| **AVG** | Algemene verordening gegevensbescherming |
| **EC** | Europese Commissie |
| **EHRM** | Europees Hof voor de Rechten van de Mens |
| **EU** | Europese Unie |
| **EVRM** | Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden |
| **FTP** | File Transfer Protocol |
| **HTTP** | Hypertext Transfer Protocol |
| **IANA** | Internet Assigned Numbers Authority |
| **ICANN** | Internet Corporation for Assigned Names and Numbers |
| **ICT** | Informatie- en communicatietechnologie |
| **IETF** | Internet Engineering Task Force |
| **IGF** | Internet Governance Forum |
| **IMAP** | Internet Message Access Protocol |
| **ISP** | Internet Service Providers |
| **ITU** | International Telecommunications Union |
| **IP** | Internet Protocol |
| **IVBPR** | Internationaal Verdrag inzake burgerrechten en politieke rechten |
| **SMPs** | Sociale mediaplatformen |
| **UVRM** | Universele Verklaring van de Rechten van de Mens |
| **VN** | Verenigde Naties |
| **VS** | Verenigde Staten |
| **WIPO** | Wereldorganisatie voor de Intellectuele Eigendom |
| **WRR** | Wetenschappelijke Raad voor het Regeringsbeleid |

naar inhoud