Rathenau Instituut

Reactie Rathenau Instituut op Consultatie AIV advies Regulering van online content

Het kabinet heeft in mei 2019 de Adviesraad Internationale Vraagstukken (AIV) gevraagd om internetreguleringsopties te onderzoeken. Dat heeft in juni 2020 geleid tot het AIV-advies *Regulering van online content: Naar een herijking van het Nederlandse internetbeleid*. Het Ministerie van Buitenlandse Zaken zal op basis van dit advies een reactie schrijven. Ter voorbereiding op die reactie consulteert het ministerie momenteel maatschappelijke organisaties, bedrijven, denktanks en onderzoekers en vraagt hun te reageren op de afzonderlijke aanbevelingen van de AIV. Door middel van deze brief geeft het Rathenau Instituut daar graag gehoor aan.

Aanbeveling 1: Herijk het Nederlandse internetbeleid

Het Rathenau Instituut is het eens met de constatering dat een nieuw vertoog over internetvrijheid noodzakelijk is. Reeds in 2012 liet de Rathenau studie *Voorgeprogrammeerd: Hoe het internet ons leven leidt* zien dat vanwege monopolisering en personalisatie van informatieaanbod online keuzevrijheid onder druk stond. In daaropvolgende studies, zoals *Opwaarderen*, werd het brede scala aan publieke waarden die door digitale technologie onder druk komen te staan in beeld gebracht.

De afgelopen jaren zijn de zorgen over online content flink gegroeid, onder meer als gevolg van pogingen tot het beïnvloeden van democratische verkiezingen, terroristische online content, *hate speech* en desinformatie. Het is daarom hoog tijd dat het vertoog van de overheid bijgesteld wordt van dat van zelfregulering van de internetsector naar dat van een open en vrij internet binnen rechtsstatelijke en grondrechtelijke grenzen. Daarbij is het zaak om voortdurend de juiste balans te zoeken tussen al dan niet dwingend overheidsingrijpen en de vrijheid om op het internet zonder censuur en overheidsinmenging actief te zijn. Bij het vinden van die balans, kan de rechtsstatelijkheid van het internet bewaakt worden. Overheidsingrijpen moeten leiden tot een *vrijer* én *democratischer* internet (zie ook aanbeveling 2).

We herkennen verder dat het kennisniveau op zowel nationaal als lager overheidsniveau moet worden versterkt (zie rapport *Raad weten met digitalisering*). Het internet wordt vaak als ongrijpbaar gezien of regulering als een op voorhand verloren strijd. Terwijl er wel degelijk bestuurlijke mogelijkheden zijn om te sturen op democratische en rechtsstatelijke waarden, waaronder het strikter reguleren van online platforms.

Ten slotte lijkt de aanbevolen inzet op co-regulering verstandig, omdat veel normen en standaarden nog moeten worden gevormd. Echter, niet het verdienmodel van internetdiensten, maar het belang van een open en vrij internet, moet daarbij voorop staan. Als internetbedrijven niet bereid zijn de nodige stappen te zetten, is het aan de overheid om de regie te nemen en zal co-regulering niet volstaan. Daar waar regulering meer verantwoordelijkheid legt bij internetbedrijven, zal de overheid ervoor moeten waken dat dit niet ten koste gaat van de vrijheid van meningsuiting en de persvrijheid.

<u>Bronnen:</u>

Voorgeprogrammeerd

Opwaarderen

Digitalisering van het nieuws

Digitale dreigingen voor de democratie

Raad weten met digitalisering

Aanbeveling 2: Verdedig en bevorder het open en vrije karakter van het internet op basis van democratische en rechtsstatelijke waarden

We erkennen de spanning tussen het beschermen van democratische en rechtsstatelijke waarden en het open en vrije karakter van het internet. Antidemocratische en antirechtsstatelijke actoren misbruiken het open internet om hun doelen ook in Nederland na te streven, en burgers schaden het vrije internet door diensten uit niet-democratische staten te gebruiken.

Internetdiensten zullen, net als alle andere producten en diensten binnen de Europese interne markt, moeten voldoen aan bepaalde standaarden. De Europese General Data Protection Regulation (GDPR) is een voorbeeld van dergelijke regulering. Om regionale fragmentatie te voorkomen, is het zaak op Europese regulering in te blijven zetten. Evengoed kunnen Europese verordeningen op wereldniveau leiden tot verschillen in de omgang met het internet (versplintering). Dit zullen we moeten accepteren.

Verder zijn nieuwe kaders nodig voor het vaststellen en erkennen van het strategische belang van bepaalde kennis- en internettechnologie. De traditionele kaders voor dual-use-technologie volstaan niet. Het is onwenselijk als onbetrouwbare, autoritaire staten beslag leggen op technologie die van groot belang is voor de veiligheid van Nederland en de EU. Bovendien is het van belang om geen technologie te verhandelen met autoritaire staten, die gebruikt kan worden om het vrije internet verder te ondermijnen. Het zal nodig zijn om, op basis van nieuwe kaders, technologie af te schermen, bijvoorbeeld op het gebied van dataversleuteling, biometrie en kunstmatige intelligentie.

Tenslotte zijn op het internet machtsconcentraties zichtbaar rond bepaalde dienstverlening. Zodra één actor een bepaalde dienst domineert, bestaat het risico dat een staat grote invloed kan uitoefenen op de aanbieder, en daarmee de content en de manier waarop deze kan worden verspreid bepaalt.

<u>Bronnen:</u>

Opwaarderen

Kennis in vizier

Cyberweerbaar met nieuwe technologie

Aanbeveling 3: Versterk de Nederlandse vertegenwoordiging in internationale internetorganisaties

In zijn advies beschrijft de AIV dat Nederland sterker kan worden vertegenwoordigd bij 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). Het Rathenau Instituut onderschrijft deze aanbeveling.

Al eerder beschreef het Rathenau Instituut in het rapport *Cyberspace zonder conflict* het gebrek aan internationale normen en standaarden op onderdelen van internet governance. Er is internationaal onvoldoende overeenstemming over welke vormen van beïnvloeding van content, en daarmee bijvoorbeeld beïnvloeding van het maatschappelijke debat, ongewenst zijn. Diplomatie en deelname aan internationale fora zijn noodzakelijk om tot internationaal gedeelde normen te komen. Tegelijkertijd zal dit gepaard moeten gaan met een maatschappelijke dialoog op nationaal niveau over de regulering van het internet, zodat de diplomatieke inzet voldoende draagvlak heeft in de samenleving.

Bron:

Cyberspace zonder conflict

Aanbeveling 4: Stimuleer internationale normstelling voor de aanpak van schadelijke online content met een stevige verankering in bestaande mensenrechtenstandaarden

Bij het aanpakken van schadelijke online content is het van groot belang om een onderscheid te maken tussen de regulering van de inhoud van content en de verspreiding van content. Beide raken aan de vrijheid van meningsuiting: het recht een mening te hebben en de vrijheid kennis te nemen en te geven van informatie of ideeën. Regulering van de inhoud van berichten raakt de vrijheid van meningsuiting in vrijwel alle gevallen direct en zichtbaar. Bij de regulering van de verspreiding van content spelen algoritmen van internetdiensten vaak een cruciale rol. De regulering van de verspreiding van content is daarmee minder zichtbaar. Transparantie over de werking van de algoritmen, eventuele voorwaarden waar algoritmen aan moeten voldoen en het afleggen van verantwoording aan een toezichthouder zijn van belang om de rechten te borgen.

De bestaande internationale verdragen en normen over kinderpornografie, racistisch en xenofoob materiaal bieden uitgangspunten voor verdere regulering, met name als het gaat om onrechtmatige content. Het Rathenau Instituut erkent het belang van het stellen van normen en standaarden. De geschiedenis van internetregulering laat wel zien dat zodra een bepaalde standaard is vastgesteld, het heel lastig is om daar later nog verandering in te brengen. Het is dus van belang dat de overheid proactief deelneemt aan het ontwikkelen van normen en dit niet alleen aan commerciële partijen overlaat.

De huidige aanbeveling legt echter de nadruk enkel op de inhoud van de content, en dreigt daarmee een aantal belangrijke schadelijke elementen in de onlineomgeving buiten beeld te houden. De schadelijkheid van internetgebruik hangt ook samen met de psychologische effecten van het gebruik van content (zoals het verslavende karakter van internetdiensten), het type interacties (zoals likes, retweets, duets, pins, et cetera), het systeem van aanbevelingen

(zoals aanbevolen kanalen/groepen, trending topics, et cetera) en de alomtegenwoordige surveillance.

Bovendien zien we dat door data-extractie en profilering content meer en meer polariseert. De inhoud van (advertentie)berichten past zich aan op basis van het profiel van de ontvanger, wat stigmatisering, discriminatie, uitsluiting en manipulatie in de hand werkt. Het volstaat dus niet om enkel uit te gaan van statische content die eenmalig zal moeten worden getoetst.

Ook zal voldoende rekening moeten worden gehouden met de opkomst van multimedia content (zoals audio of video en statische AR/VR-omgevingen) en live/directe vormen van interactie (zoals video/audio-streaming, chatbots, spraakassistenten en interactieve games of AR/VR-omgevingen). In een recent manifest stelt het Rathenau Instituut 10 ontwerpeisen aan dit soort 'immersieve' technologie.

Ten slotte is het zaak het consumentenperspectief centraal te stellen. De rechten van consumenten dienen beschermd te worden, zoals het recht contact te kunnen hebben met een platformbedrijf.

<u>Bronnen:</u>

Verantwoord virtueel

Hoor wie het zegt

Nep echt

Manifest

Digitale dreigingen voor de democratie

Online platformen, offline impact

Aanbeveling 5: Initieer maatregelen gericht op transparantie en toezicht

De AIV stelt in zijn advies dat online platformen verplicht moeten worden om transparantierapporten op te stellen.

Het Rathenau Instituut mist echter de analyse die hieraan vooraf gaat, want: *waarom* moeten zij hiertoe verplicht worden? Het is zaak als samenleving vast te stellen dat private platformen zo'n essentiële en impactvolle maatschappelijke functie zijn gaan vervullen, dat ze een publieke verantwoordelijkheid moeten dragen – en ook door de overheid als zodanig aangesproken en gereguleerd moeten worden.

Bovendien is het transparant maken van het beleid voor het identificeren en verwijderen van schadelijke content onvoldoende. De huidige transparantie en standaarden schieten ook tekort op diverse andere terreinen, namelijk transparantie over onder andere:

- Productie van onrechtmatige en schadelijke content

    - Inzicht in de manier waarop misbruik van productietechnieken die platformen aanbieden (videofilters, stories, et cetera) wordt voorkomen;
    - Inzicht in welke actoren welke schadelijke of onrechtmatige content produceren;
    - Inzicht in de preventieve maatregelen die worden getroffen om actoren te beoordelen, in plaats van de content die zij produceren.
- Verspreiding van onrechtmatige en schadelijke content
    - Inzicht in de rol van aanbevelingsalgoritme voor content, maar bijvoorbeeld ook voor de aanbeveling voor het volgen van profielen, groepen, kanalen, trending topics et cetera en deelname aan live interactieve content als videostreams en VR-omgevingen;
    - Inzicht in de manier waarop besloten en/of versleutelde verspreiding wordt gefaciliteerd en hoe content bijvoorbeeld kan worden gemeld of aangemerkt.
- Advertentiesystemen
    - Inzicht in de manier waarop de klanten worden gescreend;
    - Inzicht in de manier waarop het (mis)bruik van de systemen wordt gemonitord;
    - Inzicht in welke data worden gebruikt om advertenties te maken en te verspreiden, en inzicht in de herkomst van die data;
    - Inzicht in de criteria die beschikbaar worden gesteld aan adverteerders om hun doelgroepen te selecteren en hoeverre die schadelijk zijn (bijvoorbeeld selectie op extremisme of manipuleerbaarheid).
- Procedures voor gebruikers
    - Inzicht in hoe gebruikers schadelijke content kunnen melden;
    - Inzicht in hoe beoordelingsprocedures verlopen.
- Inspanning die platformen doen om schadelijke content te voorkomen of verwijderen
    - Inzicht in alle inspanningen die platformen op lidstaatniveau verrichten op het gebied van onrechtmatige of schadelijke content.

Wat betreft een eventuele toezichthouder is niet duidelijk of er wordt gedoeld op een publieke toezichthouder of private auditing. Een keuze tussen één van beide leidt tot verschillende toezichtsystemen. Andere vraagstukken zijn:

- Krijgen toezichthouders inzicht in het mechaniek en de algoritmen van platformen of alleen de uitkomsten?
- Krijgen toezichthouders inzicht in data en datastromen?
- Welke handhavingsmiddelen krijgen de toezichthouders?
- Kunnen gebruikers zich ook rechtstreeks wenden tot een toezichthouder, en zo ja, op welke wijze?
    - Bijvoorbeeld om onrechtmatige of schadelijke content te melden?
    - Kunnen gebruikers bezwaar maken tegen de beoordeling of verwijdering van content bij een onafhankelijke toezichthouder?

Het is in elk geval duidelijk dat er behoefte is aan eenduidige rapportage, en deze zal moeten plaatsvinden op het niveau van lidstaten. Anders is het voor Nederland niet mogelijk om te bepalen of maatregelen effectief zijn.

Bron:

Digitale dreigingen voor de democratie

Aanbeveling 6: Stimuleer value sensitive design en digital commons

De AIV stelt in zijn advies voor om gelden beschikbaar te stellen voor onderzoek naar value sensitive design en te investeren in alternatieven voor internetdiensten.

Het Rathenau Instituut ziet naast het bieden van subsidies nog meer stimulatiemogelijkheden. Het gaat bijvoorbeeld ook om het creëren van een eerlijk speelveld, waardoor alternatieve internetdiensten kunnen concurreren met de al bestaande spelers. De alternatieven voor gangbare internetdiensten bestaan immers vaak al, maar kunnen lastig concurreren met het verdienmodel van gangbare internetdiensten (die vaak gratis zijn voor gebruikers, dankzij opbrengsten door middel van datahandel, profilering en advertenties).

De overheid kan zelf als launching customer en grote afnemer van internetdiensten een verschil maken, bijvoorbeeld door value sensitive design en digital commons onderdeel te maken van inkoopvoorwaarden.

Bron:

Cyberweerbaar met nieuwe technologie

Aanbeveling 7: Betrek onafhankelijke nationale expertorganen bij de beoordeling van schadelijke online content

De AIV stelt in zijn advies voor om illegale of schadelijke content door onafhankelijke, nationale experts te laten beoordelen.

Maar voor onrechtmatige content ligt het allereerst voor de hand dat de internetdiensten zélf meer invulling geven aan hun verantwoordelijkheid om die te bestrijden. Dat kan door middel van transparante en adequate procedures, bijvoorbeeld door maximale doorlooptijd vast te stellen. De bestaande partijen die onrechtmatige zaken beoordelen, zoals de rechtsinstituten en media-autoriteiten, moeten daarop toezien en eveneens adequaat zijn uitgerust om in te grijpen.

Bij schadelijke, maar niet onrechtmatige content, zoals mogelijk schadelijke, misleidende informatie, is een oordeel vellen alleen onvoldoende. Een onafhankelijke beoordelaar moet deze content niet alleen beoordelen, maar ook invloed hebben op de gevolgen van diens oordeel. Alleen zo kan een expertorgaan volledig invulling geven aan de verantwoordelijkheid die het krijgt. Beoordelingen hebben immers consequenties. Denk aan het labelen, de-ranken of verwijderen van content. De onafhankelijke beoordelaars moeten ook invloed hebben op deze consequenties, en bepalen of deze proportioneel en subsidiair zijn.
Vanuit een rechtenperspectief is het van belang dat de beoordeling niet in private handen ligt, om zo onafhankelijkheid te waarborgen. Tevens moeten gebruikers van de internetdiensten voldoende mogelijkheden hebben om bezwaar te kunnen maken tegen beoordelingen en de consequenties.

Aanbeveling 8: Pleit voor een zorgplicht voor internetplatformen, onder duidelijke randvoorwaarden

De AIV stelt in zijn advies voor dat Nederland zich inspant om duidelijke criteria ten aanzien van schadelijke content en een zorgplicht te ontwikkelen in samenwerking met platformen. Hierbij moet nadrukkelijk rekening worden gehouden met (zelf)censuur.

Wat betreft onrechtmatige content moeten internetplatformen inderdaad een zorgplicht krijgen. Zij dragen een verantwoordelijkheid als het gaat om het faciliteren van de productie van onrechtmatige content (bijvoorbeeld door de middelen die zij aanreiken voor het bewerken van video's) en het faciliteren van de verspreiding door keuzes die worden gemaakt in hun algoritmen. Aan de zorgplicht moeten adequate handhavingsinstrumenten worden gekoppeld.

Aanbeveling 9: Maak de gebruikersvoorwaarden van internetplatformen mensenrechten-inclusief

Het Rathenau Instituut erkent deze aanbeveling. Nu al maken de UN Guiding Principles on Business and Human Rights, de OESO-richtlijnen voor Multinationale Ondernemingen, en de OESO Due Diligence Guidance duidelijk dat internetplatformen een verantwoordelijkheid hebben om mensenrechten te respecteren. Deze normen voor maatschappelijk verantwoord ondernemen roepen internetplatformen op om gepaste zorgvuldigheid (due diligence) te betrachten om maatschappelijke schade te voorkomen of te repareren. Hier kunnen ze onder andere via hun gebruikersvoorwaarden invulling aan geven.

Het Rathenau Instituut constateert verder dat internetdiensten meer inspanningen moeten verrichten om de digitale samenleving inclusief te maken. Internetdiensten moeten niet discrimineren of discriminatie faciliteren. Er zijn nu voorbeelden in de praktijk waarbij dit wel gebeurt. Sommige spraakgestuurde systemen verstaan bijvoorbeeld vrouwen minder goed dan mannen. En er zijn filters die videostreams voorzien van virtuele achtergronden die slechter werken als er een persoon met een donkere huidskleur in beeld is. De bedrijven en ontwikkelaars zetten nog vaak de technologische mogelijkheden voorop, in plaats van waarden als gelijkheid en inclusie. De overheid kan bedrijven hier, door op de al bestaande (internationale) richtlijnen te wijzen, op aanspreken.

Bron:

Manifest

Aanbeveling 10: Vergroot de digitale weerbaarheid van internetgebruikers

De AIV wijst terecht ook op het versterken van de positie van burgers op het internet. Zij moeten bewust worden van regelgeving en in staat worden gesteld om actie te ondernemen. Bij digitale weerbaarheid wordt dan vaak gedacht aan het kunnen weren of bestrijden van schadelijke content of desinformatie. Het Rathenau Instituut hanteert echter een breder begrip van weerbaarheid: dat van technologisch burgerschap. Burgerschap verwijst naar het democratisch opeisen, vastleggen en implementeren van rechten en plichten. De Britse

socioloog Marshall ziet burgerschap als een ‘developing institution’. Drie processen spelen daarbij een rol: het opeisen van burgerrechten, het formeel vastleggen daarvan in grondrechten en wet- en regelgeving, en de implementatie van wetgeving en beleid. Het claimen van rechten door middel van maatschappelijke strijd is een cruciaal onderdeel van burgerschap. Op dit moment strijden burgers in de digitale wereld al voor verschillende rechten, zoals hun recht op menswaardigheid, veiligheid, autonomie, emancipatie en menselijk contact. Het is cruciaal dat de overheid deze strijd omarmt en steunt, en burgers betrekt bij het debat over de toekomst van het internet.

Technologisch burgerschap houdt in dat Nederlanders de vaardigheden hebben om de mogelijkheden van digitalisering te begrijpen, de kennis hebben om met de risico’s van digitale technologie om te gaan, en kunnen deelnemen aan het democratisch debat en de politieke besluitvorming over nieuwe digitale technologie. Internetvaardigheden en mediawijsheid – verstandig omgaan met media en het herkennen en omgaan met schadelijke content - zijn hier een essentieel onderdeel van. Ze vormen alleen niet het geheel van digitale weerbaarheid. Naast het vergroten van de digitale weerbaarheid van internetgebruikers, is het Rathenau Instituut daarom voorstander van het versterken van het technologisch burgerschap.

<u>Bronnen:</u>

Technologisch burgerschap

Digitale vaardigheden voor technologisch burgerschap

Desinformatie bestrijden, censuur vermijden