

# Internationale principes van de Verenigde Naties voor informatie-integriteit

Aanbevelingen tot actie voor alle belanghebbenden

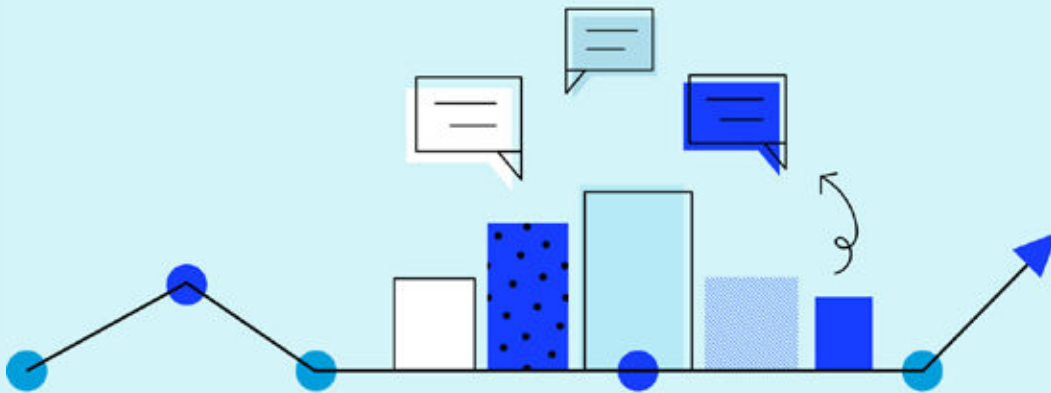


**Verenigde  
Naties**

# Inhoudstafel

<b>HET INFORMATIE-ECOSYSTEEM IN HET DIGITALE TIJDPERK</b>	<b>3</b>
Informatie-integriteit en Duurzame Ontwikkelingsdoelstellingen	<b>4</b>
Naar internationale principes van de Verenigde Naties voor informatie-integriteit	<b>5</b>
<b>INTERNATIONALE PRINCIPES VOOR INFORMATIE-INTEGRITEIT</b>	<b>7</b>
Maatschappelijk vertrouwen en veerkracht	<b>8</b>
Gezonde initiatieven	<b>10</b>
Burgeremancipatie	<b>12</b>
Vrije, onafhankelijke en pluralistische media	<b>14</b>
Transparantie en onderzoek	<b>16</b>
<b>OPROEPEN TOT ACTIE</b>	<b>18</b>
Technologische bedrijven	<b>19</b>
Actoren actief in artificiële intelligentie (AI)	<b>25</b>
Adverteerders	<b>27</b>
Andere actoren in de privésector	<b>29</b>
Nieuwsmedia	<b>30</b>
Onderzoekers en het maatschappelijk middenveld	<b>32</b>
Staten	<b>34</b>
De Verenigde Naties	<b>38</b>
<b>VOLGENDE STAPPEN</b>	<b>40</b>
<b>BIJLAGE</b>	<b>41</b>

# Het informatie-ecosysteem in het digitale tijdperk



In de laatste decennia heeft technologische vooruitgang communicatie ingrijpend veranderd, waardoor individuen en gemeenschappen op een voorheen ondenkbare schaal met elkaar in verbinding zijn komen te staan en ongekende mogelijkheden zijn ontstaan voor de verspreiding van kennis, culturele verrijking en duurzame ontwikkeling. In veel opzichten heeft die vooruitgang de lat hoger gelegd voor de integriteit van het informatie-ecosysteem. Daarin wordt vrijemeningsuiting immers volledig gerespecteerd en is nauwkeurige en betrouwbare informatie, vrij van discriminatie en haatspraak, voor iedereen beschikbaar in een open, inclusieve, veilige en beveiligde omgeving.

Hoewel die ontwikkelingen de massale verspreiding van informatie faciliteerden, bevorderden ze ook de verspreiding van onjuiste informatie, desinformatie en haatspraak door veel verschillende actoren met een niet eerder voorgekomen volume, snelheid en verspreidingsgraad. Hierdoor wordt de integriteit van het informatie-ecosysteem in gevaar gebracht. De risico's omvatten een reeks actuele, opkomende en toekomstige bedreigingen, in het kader van de snelle technologische inburgering van artificiële intelligentie.

De aantasting van de integriteit van informatieruimten kan ertoe leiden dat het vermogen van mensen om hun mensenrechten uit te oefenen in gevaar wordt gebracht en de inspanningen om vrede, welvaart en een leefbare toekomst op onze planeet te bereiken belemmerd worden. Een versterking van informatie-integriteit is daarom een van de meest urgente uitdagingen van onze tijd. Informatie-integriteit impliceert een pluralistische informatieruimte die mensenrechten, vreedzame samenlevingen en een duurzame toekomst verdedigt. Het bevat de belofte van een digitaal tijdperk dat vertrouwen, kennis en individuele keuze voor iedereen bevordert.

De bevordering van de informatie-integriteit houdt in dat mensen in staat worden gesteld om hun recht uit te oefenen om ongestoord informatie en ideeën van allerlei aard op te vragen, te ontvangen en door te geven en meningen te koesteren. In een steeds complexere digitale informatieomgeving betekent dit dat individuen in staat moeten worden gesteld om veilig door informatieruimten te navigeren en tegelijkertijd hun privacy en vrijheid te behouden.

# Informatie-integriteit en Duurzame Ontwikkelingsdoelstellingen

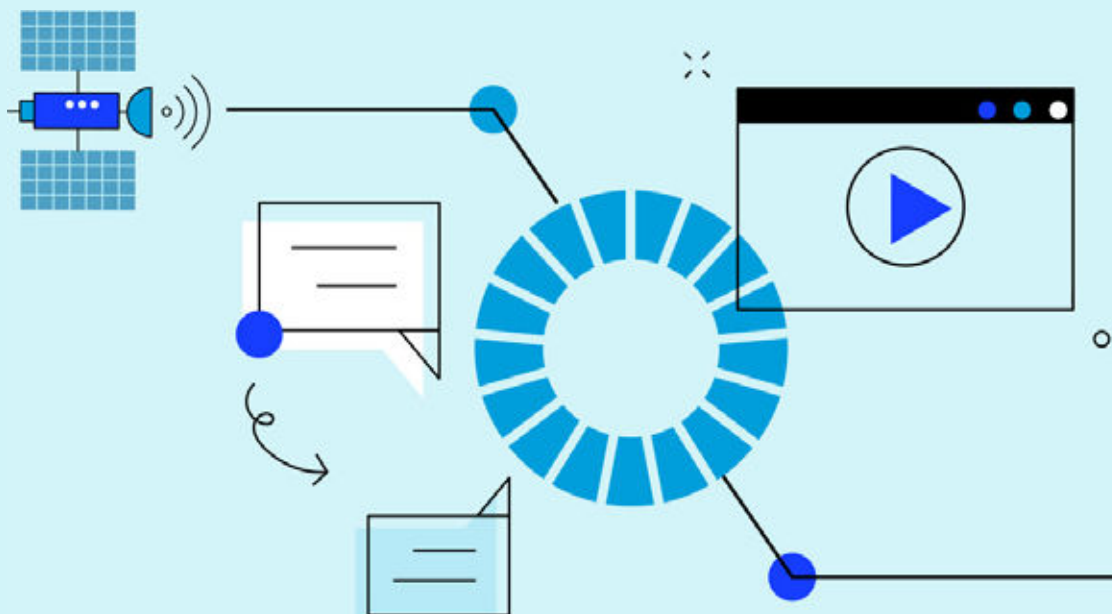
Inspanningen om de informatie-integriteit te versterken zijn essentieel om de Duurzame Ontwikkelingsdoelstellingen te beschermen en vooruit te helpen. De aantasting van de integriteit van het informatie-ecosysteem kan (de) bestaande kwetsbaarheden van deze doelen verergeren wanneer deze behaald worden, voornamelijk in landen in het Mondiale Zuiden.

Kwetsbare en gemarginaliseerde groepen worden onevenredig getroffen door dat fenomeen. Zo is een grotere deelname van vrouwen aan de wereldwijde arbeidsmarkt cruciaal om de Duurzame Ontwikkelingsdoelstellingen te behalen. Naast de bestaande discriminerende wetten en beleidsmaatregelen in veel landen worden haatspraak, desinformatie en gendergerelateerd geweld echter systematisch ingezet om vrouwen het zwijgen op te leggen en hen uit de publieke ruimte te weren. Dat kan verwoestende en langdurige gevolgen hebben voor hun deelname, door hun stem te onderdrukken en zelfcensuur in de hand te werken, hun professionele en persoonlijke reputatie te schaden en de moeizaam behaalde vooruitgang in gendergelijkheid in gevaar te brengen.

Daarnaast benadrukken de inspanningen om de informatieruimte te misbruiken om klimaatactie te ondermijnen de urgentie van die uitdaging. Gecoördineerde desinformatiecampagnes, die vaak aangestuurd worden door commerciële belangen, proberen twijfel te zaaien over de wetenschappelijke basis van door de mens veroorzaakte klimaatverandering, de oorzaken en de gevolgen ervan. Hun doel: klimaatactie vertragen of saboteren.

Publieke figuren zoals activisten, wetenschappers en journalisten worden steeds vaker het doelwit van haat, bedreigingen en intimidatie vanwege hun inzet om feitelijke informatie over de klimaatcrisis te verspreiden en oplossingen aan te dragen.

In alle domeinen die onder de Duurzame Ontwikkelingsdoelstellingen vallen – van gezondheid en het uitbannen van honger tot vrede, gerechtigheid, onderwijs en de minimalisering van ongelijkheden – zullen maatregelen ter bevordering van informatie-integriteit bijdragen aan een duurzamere toekomst waarin niemand achterblijft.



# Naar internationale principes van de Verenigde Naties voor informatie-integriteit

De Verenigde Naties hebben in alle regio's uitgebreid overlegd over de informatie-integriteit met de lidstaten, het maatschappelijk middenveld waaronder jongerenorganisaties, de media, academici en de vertegenwoordigers van de privésector. De belanghebbenden hebben gesprekken gevoerd op nationaal niveau, tijdens virtuele sessies, bilaterale vergaderingen en via een wereldwijd verspreid webformulier.

Uit deze raadplegingen is gebleken dat er behoefte is aan uniforme aanbevelingen die in alle regio's en contexten toepasbaar zijn en die beantwoorden aan de behoeften van alle individuen, met name van kwetsbare en gemarginaliseerde groepen.

Daarom bieden de internationale principes van de Verenigde Naties voor informatie-integriteit een holistisch kader om verschillende belanghebbenden te begeleiden naar een gezonder informatie-ecosysteem. Dat kader bestaat uit vijf principes om de informatie-integriteit te versterken, waarbij elk principe aanbevelingen bevat voor de belangrijkste groepen belanghebbenden.

Die principes luiden als volgt: maatschappelijk vertrouwen en veerkracht, onafhankelijke, vrije en pluralistische media, transparantie en onderzoek, burgeremancipatie en gezonde initiatieven. Ze staan allemaal in het teken van mensenrechten.

De internationale principes erkennen en bouwen voort op de aanzienlijke inspanningen en de al geboekte vooruitgang van staten, het maatschappelijk middenveld, de privésector en andere belanghebbenden. Ze bieden een uniform uitgangspunt voor de bescherming en bevordering van de informatie-integriteit in alle aspecten van het leven en in alle talen en contexten. Ze erkennen de wereldwijde solidariteit en de omvang van

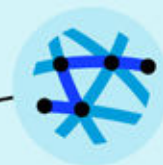
de antwoorden die op een ongekeerde schaal, snelheid en intensiteit nodig zijn.

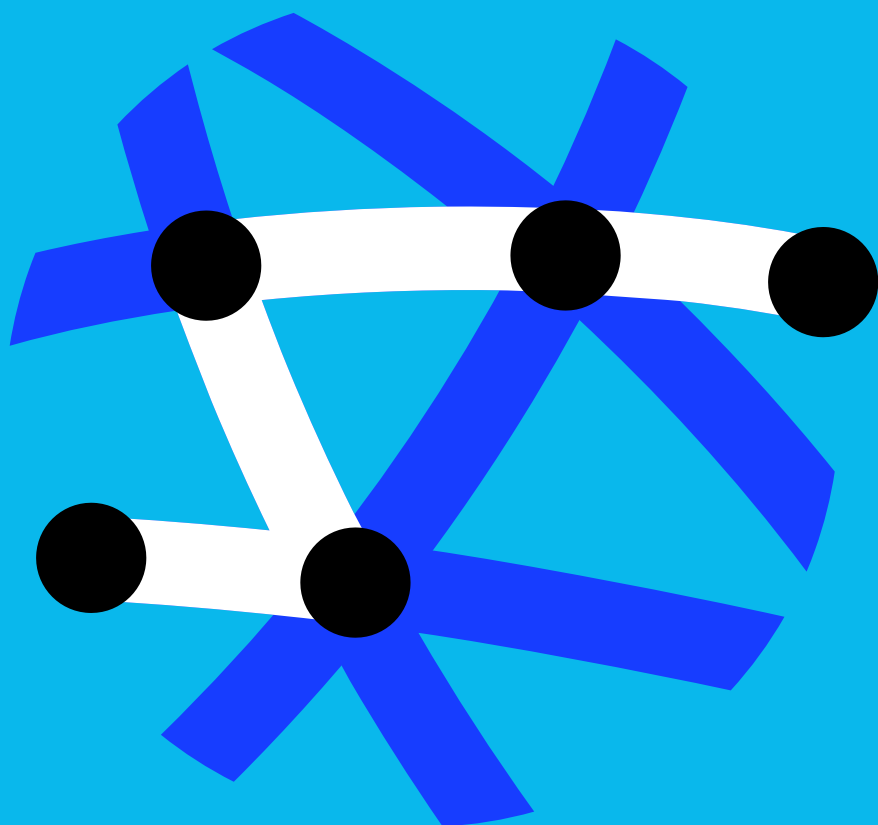
Met de internationale principes kunnen individuen, particuliere- en overheidsinstanties, inclusief het systeem van de Verenigde Naties, regeringen, de media, de organisaties van het maatschappelijk middenveld en bedrijven met winstoogmerk in de technologie-, reclame- en PR-sectoren zich aansluiten bij de rechten en vrijheden die zijn vastgelegd in de internationale wetgeving, alsook brede coalities vormen om de informatie-integriteit te ondersteunen.

De internationale principes zijn gebaseerd op de ideeën uit Onze Gemeenschappelijke Agenda en uit beleidsnota nr. 8 van de Secretaris-Generaal van de Verenigde Naties over informatie-integriteit op digitale platforms.

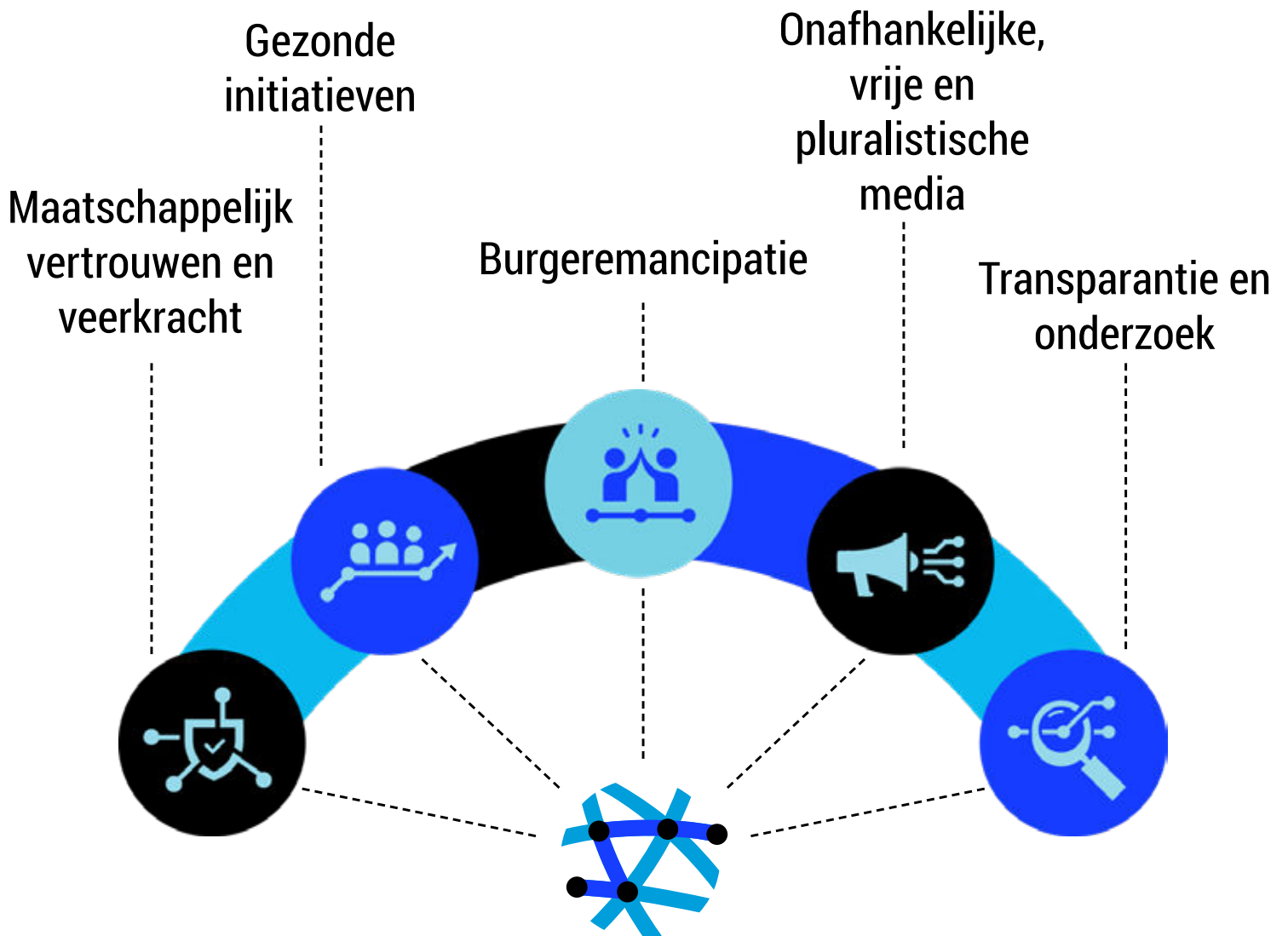
De internationale principes berusten niet alleen op het internationaal recht en de internationale wetgeving inzake mensenrechten, maar zijn ook een aanvulling op de VN-richtlijnen voor het bedrijfsleven en de mensenrechten, de richtlijnen van UNESCO voor de regulering van digitale platforms, het actieplan van de VN inzake de veiligheid van journalisten en de kwestie van strafeloosheid, de UNESCO-Aanbeveling over de ethiek van artificiële intelligentie (AI) en de Strategie en het Actieplan van de Verenigde Naties inzake aanzetten tot haat. De internationale principes vormen een hulpmiddel voor VN-lidstaten bij hun overwegingen over een Pact voor de Toekomst en het Mondiaal Digitaal Pact.

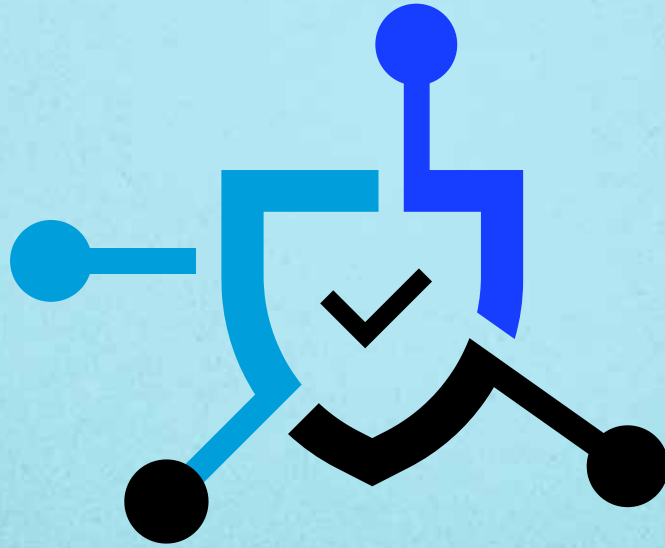
Zo weerspiegelen ze de standvastige inzet van de Verenigde Naties om de informatie-integriteit te versterken en zijn ze bedoeld als leidraad voor het werk van de organisatie in de toekomst.





# INTERNATIONALE PRINCIPES VOOR INFORMATIE-INTEGRITEIT





# Maatschappelijk vertrouwen en veerkracht

Vertrouwen en veerkracht binnen samenlevingen zijn essentiële pijlers van informatie-integriteit. Vertrouwen verwijst in deze context naar het geloof dat mensen hechten aan officiële bronnen en de betrouwbaarheid van informatie waartoe zij toegang hebben, evenals aan de mechanismen die de circulatie van informatie binnen het ecosysteem mogelijk maken. Veerkracht wijst op het maatschappelijke vermogen om met ontwrichting of manipulatie om te gaan binnen het informatie-ecosysteem.

Vertrouwen en veerkracht zijn kwetsbaar voor de acties van statelijke en niet-statale actoren die het informatie-ecosysteem proberen uit te buiten voor strategische, politieke of financiële doeleinden. Die acties, die soms op grote schaal worden gecoördineerd, kunnen leiden tot aanzienlijke schade en kunnen ervoor zorgen dat mensen feiten en wetenschap niet meer kritisch kunnen beoordelen. Grote technologiebedrijven hebben veel macht in het informatie-eco-

systeem en oefenen een enorme invloed uit op de manier waarop belanghebbenden, waaronder andere bedrijven, adverteerders, nieuwsmedia en individuele gebruikers, omgaan met en toegang hebben tot informatie.

De vooruitgang in artificiële intelligentie (AI) technologieën zoals generatieve AI heeft tegen minimale kosten grootschalige risico's veroorzaakt in het informatiesysteem. AI-gegenereerde of -gestuurde inhoud die als echt of origineel wordt voorgesteld, kan uiterst geloofwaardig overkomen, een emotionele impact hebben, lastig te herkennen zijn en zich razendsnel verspreiden via algoritmegestuurde media en platforms. Dat kan het vertrouwen schaden en het wantrouwen verder aanwakkeren. Om de risico's aan te pakken die de informatie-integriteit aantasten, zijn sterke, innovatieve en toekomstgerichte digitale vertrouwens- en beveiligingspraktijken nodig die consequent worden toegepast in alle talen en contexten.

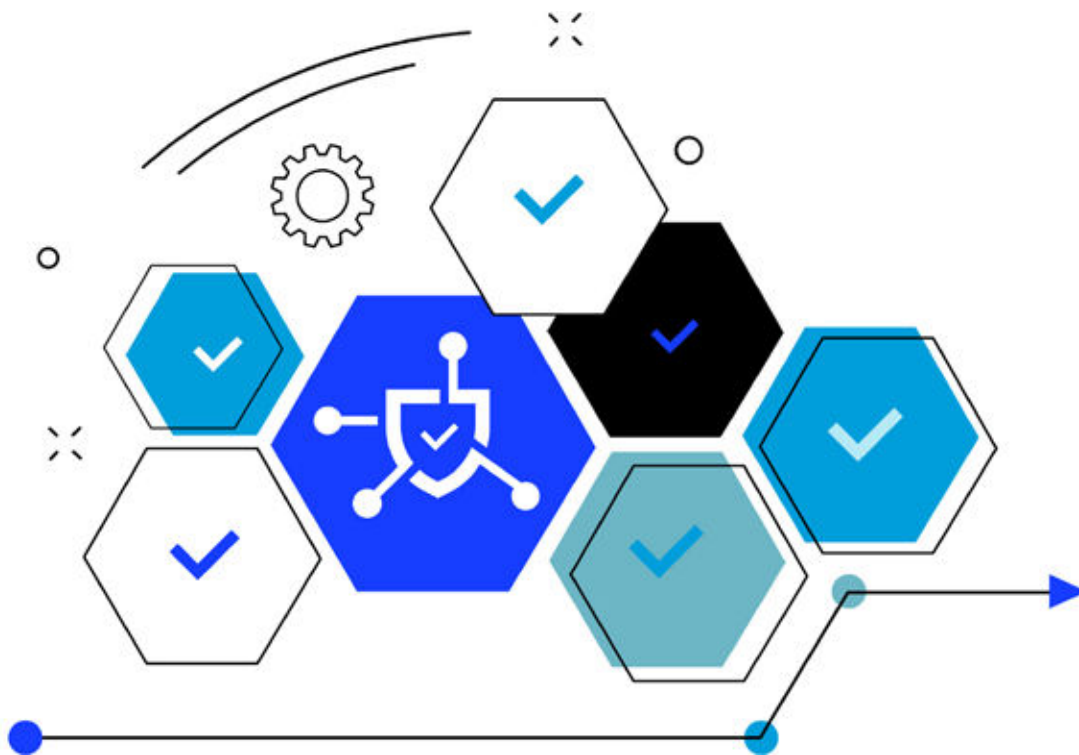
Die praktijken moeten de inzichten weerspiegelen van kwetsbare en gemarginaliseerde groepen die onevenredig worden blootgesteld aan potentiële schade.

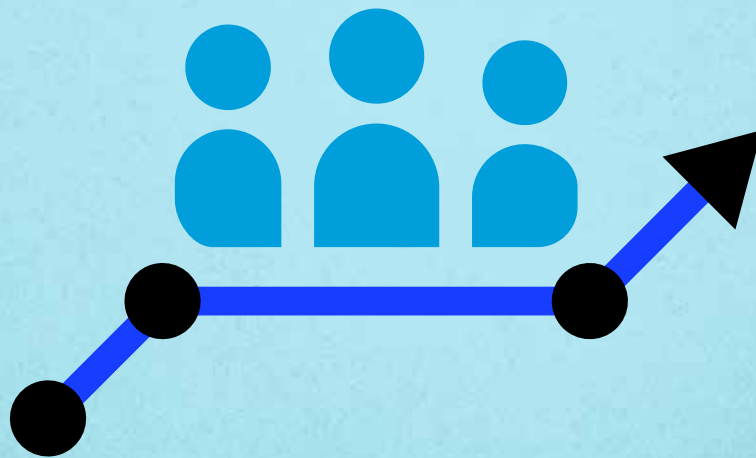
Er moet vooral rekening worden gehouden met vrouwen, ouderen, kinderen, jongeren, personen met een handicap, autochtonen, vluchtelingen en staatlozen, de LGBTIQ+ gemeenschap en etnische of religieuze minderheidsgroepen. Veel jongeren en kinderen brengen een groot deel van hun leven online door en ontvangen veel informatie via digitale kanalen. Zij zijn nu al de dupe van de risico's in informatiesystemen en zullen het meest worden getroffen door opkomende technologieën en mediatrends.

Mensen zijn over het algemeen veerkrachtiger en beter in staat om met die risico's om te gaan en ze te voorkomen wanneer ze toegang hebben tot tal van informatiebronnen en ze zich betrokken, gelijkwaardig, socio-economische veilig en politiek geëmancipeerd voelen. Mocht dat niet zo zijn, kunnen die risico's vaak een vruchtbare voedingsbodem vinden om zich verder te verspreiden. Bij het zoeken naar oplossingen moet er daarom rekening worden gehouden met de onder-

liggende maatschappelijke behoeften om de veerkracht op lange termijn te versterken. Alle betrokkenen die zich inzetten voor het algemeen belang moeten zich aanpassen aan het voortdurend veranderende communicatielandschap door de informatiesystemen te benutten voor het welzijn van iedereen. Dat is vooral belangrijk op cruciale maatschappelijke momenten, zoals verkiezingen, natuurrampen en door de mens veroorzaakte crises. Wanneer de risico's voor informatiesystemen groot zijn, kunnen ze de sociale polarisatie verergeren, de deelname van mensen aan het publieke leven ondermijnen en in extreme gevallen gebruikt worden om geweld aan te wakkeren.

Activisten, journalisten, hulpverleners en VN-personeel waaronder vredeshandhavers, verkiezingswerknemers, wetenschappers, zorgverleners en andere betrokkenen kunnen een doelwit worden, met alle desastreuze gevolgen van dien. Cyberpesten en andere sluwe tactieken kunnen mensen het zwijgen opleggen en de ruimte voor de burgers verkleinen. Daarom is het essentieel om gezamenlijke inspanningen te leveren om deze mensen te beschermen.





## Gezonde initiatieven

Om gezonde initiatieven te creëren moeten we de kritieke gevolgen aanpakken voor de integriteit van het informatie-ecosysteem van de huidige bedrijfsmodellen, die afhankelijk zijn van gerichte reclame en andere vormen van contentmonetisering als voornaamste manier om inkomsten te genereren.

Die modellen hebben gezorgd voor ongekennde groei-mogelijkheden voor allerlei bedrijven, van kmo's tot multinationals, met name technologiebedrijven die digitale platforms bezitten en exploiteren, en hebben een creatieve economie ontwikkeld die wordt aangedreven door talloze mensen en waarvan zij ook profiteren. Die modellen hebben ook financiële stimulansen en opportuniteiten gecreëerd voor verspreiders van desinformatie en haatspraak. Zij maken gebruik van de aandachtseconomie waarin technologiebedrijven gebruikersgedrag surveilleren om gegevens te verza-

melen die algoritmes aanvoeren die de betrokkenheid prioriteren om de potentiële inkomsten voor adverteerders en ontwikkelaars te maximaliseren. Boodschappen die zijn gemaakt om te polariseren en sterke emoties op te roepen, wekken vaak de meeste betrokkenheid op, waardoor algoritmes ertoe hebben geleid dat schadelijke inhoud wordt beloond en versterkt.

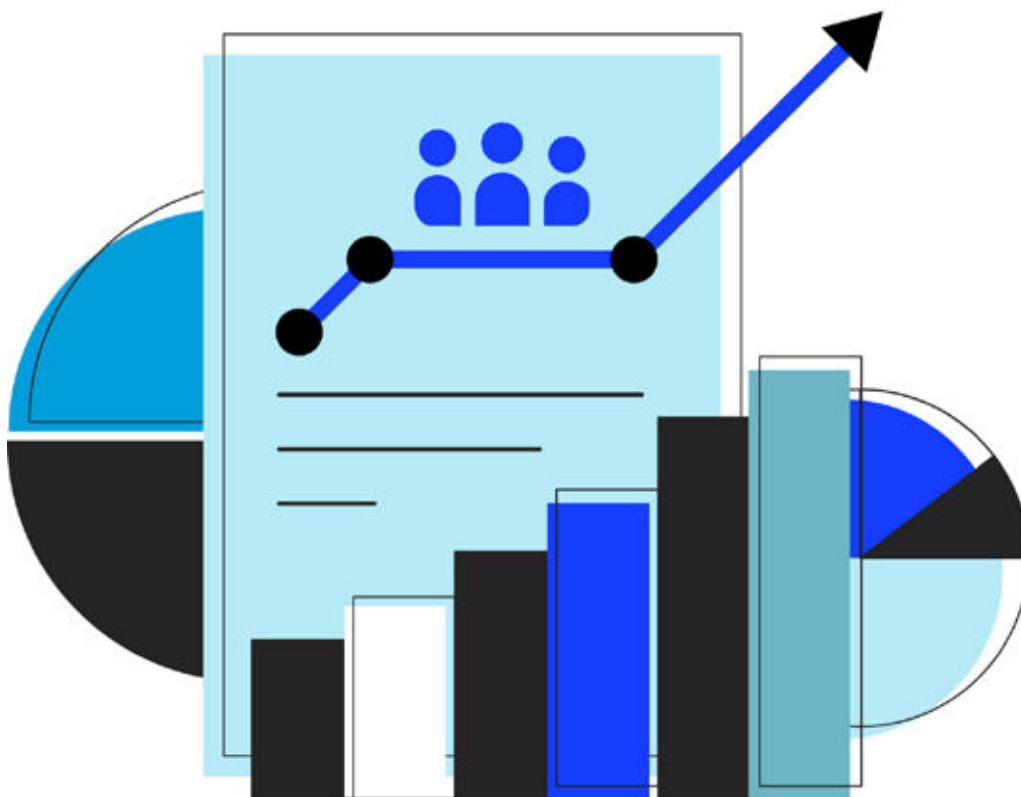
De actoren die deze bedrijfsmodellen exploiteren zijn onder andere informatiemanipulators en traditionele pr-bedrijven die door overheden, politieke figuren en entiteiten uit de privésector worden ingehuurd om georkestreerde manipulatiecampagnes uit te voeren, soms op transnationale schaal. De technologiesector heeft complexe en ondoorzichtige digitale advertentieprocessen ontwikkeld met minimale menselijke supervisie.

Die situatie is gunstig voor veel spelers in de toeleveringsketen van advertentietechnologie, waarin de grote technologiebedrijven het meest profiteren. Dergelijke onopvallendheid kan ertoe leiden dat reclamebudgetten onbedoeld mensen, entiteiten of ideeën financieren die adverteerders niet van plan waren te steunen, wat een belangrijk risico voor merken kan zijn. Die advertentieplaatsingen kunnen ook een negatieve invloed hebben op de effectiviteit van reclamecampagnes en op de veiligheid van merken.

De handvol bedrijven die de reclametechnologie domineren zijn tegelijkertijd verantwoordelijk voor de introductie van reclamestandaarden op de platformen waarvan zij de eigenaar zijn, waarbij de toepassing van deze standaarden ongelijk en inconsistent kan zijn. Dat de integriteit van het informatie-ecosysteem zo wordt aangepast, onderstreept de noodzaak van een fundamentele verandering in de stimuleringsstruc-

turen. Dat kan worden gedaan met bedrijfsmodellen die worden geleid door mensenrechten en die niet zijn gebaseerd op algoritmegestuurde programmatische reclame, die online gedrag en persoonlijke gegevens opvolgt.

Adverteerders kunnen profiteren van het informatie-ecosysteem op een manier die de integriteit van de informatie versterkt en verstandig is vanuit zakelijk oogpunt. Het is niet erg waarschijnlijk dat technologiebedrijven de huidige bedrijfsmodellen zomaar zullen opgeven. Toch kunnen er gezondere initiatieven worden ingevoerd door meer transparantie van de kant van adverteerders in het advertentieproces en de naleving van een advertentiebeleid dat de mensenrechten respecteert. Door meer controle te krijgen over een transparante toeleveringsketen kunnen adverteerders ook een beter rendement op hun investering behalen.





# Burgeremancipatie

Burgeremancipatie bij individuen die door het informatie-ecosysteem navigeren, vereist dat het publiek controle heeft over hun online ervaring, dat ze verstandige beslissingen kunnen nemen over de media die ze kiezen te consumeren en dat ze zich vrij kunnen uiten. Burgeremancipatie vereist voortdurende toegang tot diverse en betrouwbare informatiebronnen. Digitale ruimtes hebben op veel manieren gewerkt als katalysatoren voor inclusieve deelname aan het openbare leven, door mensen over geografische grenzen heen met elkaar in contact te brengen met gedeelde verlangens naar vooruitgang. Als ze welbewust worden gebruikt, kunnen deze ruimtes bijdragen aan de burgeremancipatie en macht geven aan mensen die vaak worden uitgesloten en gemarginaliseerd.

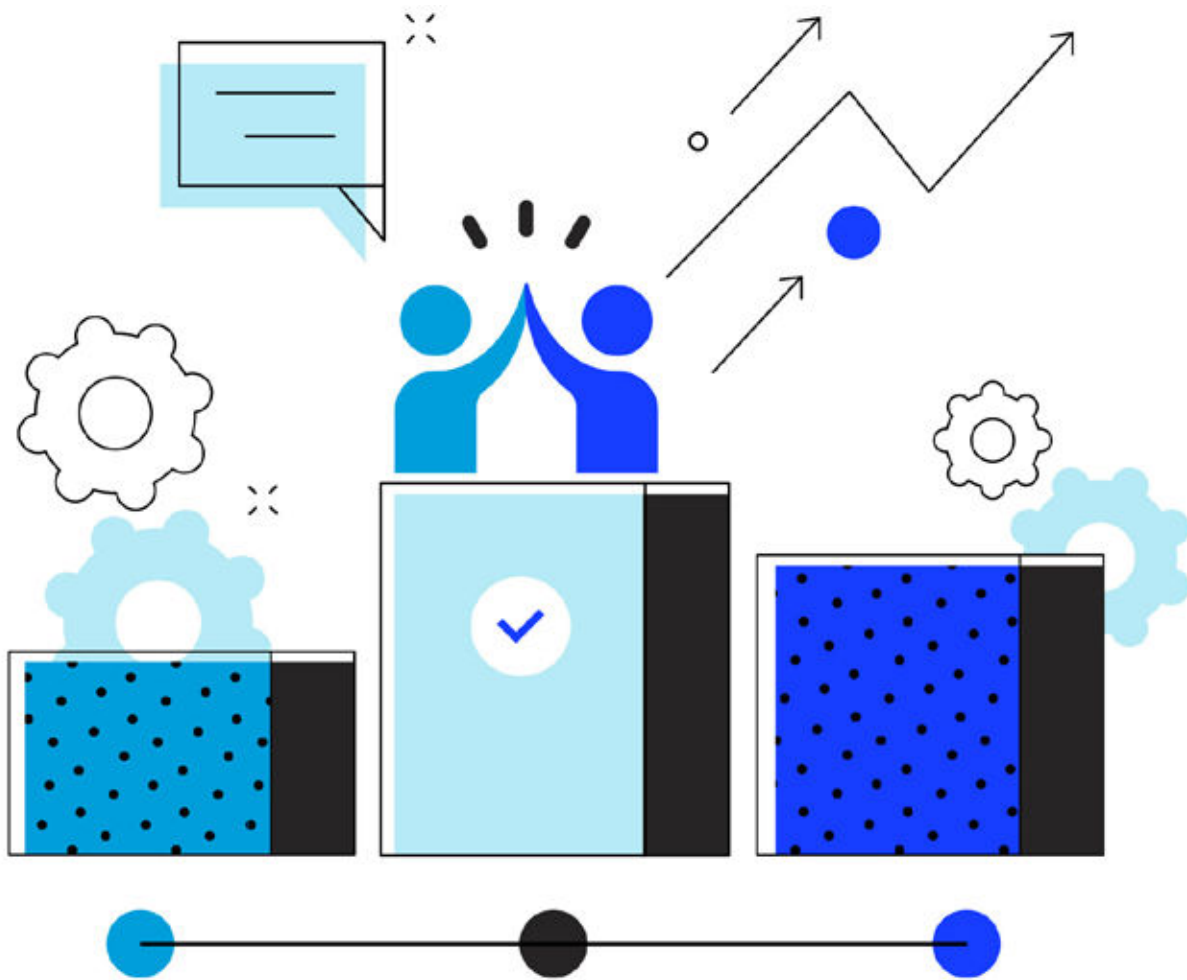
Tegelijkertijd kunnen digitale technologieën echte burgeremancipatie ook belemmeren. Individuen hebben vaak slechts weinig controle over het gebruik van hun persoonlijke gegevens of over de gepersonaliseerde algoritmes door grote technologiebedrijven. Daarbij beperken informatieleveranciers het inzicht in en de toegang tot de criteria en mechanismen die ze gebruiken om bepaalde soorten inhoud voorrang te geven en te promoten.

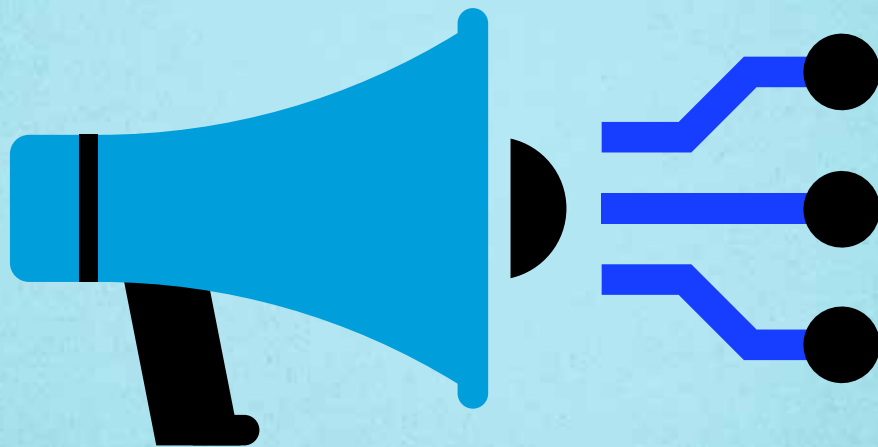
Technologiebedrijven moeten gebruikers de kans geven om informatie en commentaar te geven over alle aspecten van vertrouwen en veiligheid, privacybeleid en gegevensgebruik, waarbij de privacyrechten van gebruikers worden erkend. Ze moeten de controle en keuze van de gebruiker versterken, waaronder

interoperabiliteit met een reeks diensten van verschillende aanbieders. Initiatieven op het gebied van media, informatie en digitale vaardigheden moeten gericht zijn op de burgeremancipatie van iedereen, in het bijzonder op de specifieke uitdagingen waarmee vrouwen, ouderen, kinderen, jongeren, mensen met een handicap en kwetsbare en gemarginaliseerde groepen worden geconfronteerd.

Hoewel de internetconnectiviteit toeneemt, blijft een derde van de wereld offline. Zelfs voor mensen die online zijn, kan onvoldoende toegang ervoor zorgen dat ze de internetbronnen niet volledig kunnen be-

nutten, waardoor ze kwetsbaar blijven voor risico's in informatieruimtes – digitale omgevingen waarin informatie wordt gedeeld en gecreëerd zoals websites en sociale media. Hoewel de barrières voor connectiviteit – factoren die de toegang tot en het gebruik van het internet belemmeren – snel afnemen, moeten er initiatieven worden genomen om nieuwe internetgebruikers meer macht te geven en degenen die geen toegang hebben te voorzien van de digitale vaardigheden die nodig zijn voor veilige en productieve online ervaringen.





## Vrije, onafhankelijke en pluralistische media

Informatie-integriteit kan alleen maar gegarandeerd worden dankzij vrije, onafhankelijke en pluralistische media.

Een vrije pers vormt de basis van de rechtsstaat en ligt ten grondslag aan democratische maatschappijen, waarin een helder burgerlijk discours kan bestaan, het leiderschap tot verantwoording wordt gedwongen en de mensenrechten worden beschermd. De pers kan als vrij beschouwd worden wanneer journalisten en mediaprofessionals, waaronder vrouwen en gemar-

ginaliseerde en kwetsbare personen, steeds in alle vrijheid informatie kunnen verstrekken en openlijk en in alle veiligheid kunnen werken, en iedereen te allen tijde toegang heeft tot pluralistische en betrouwbare informatiebronnen.

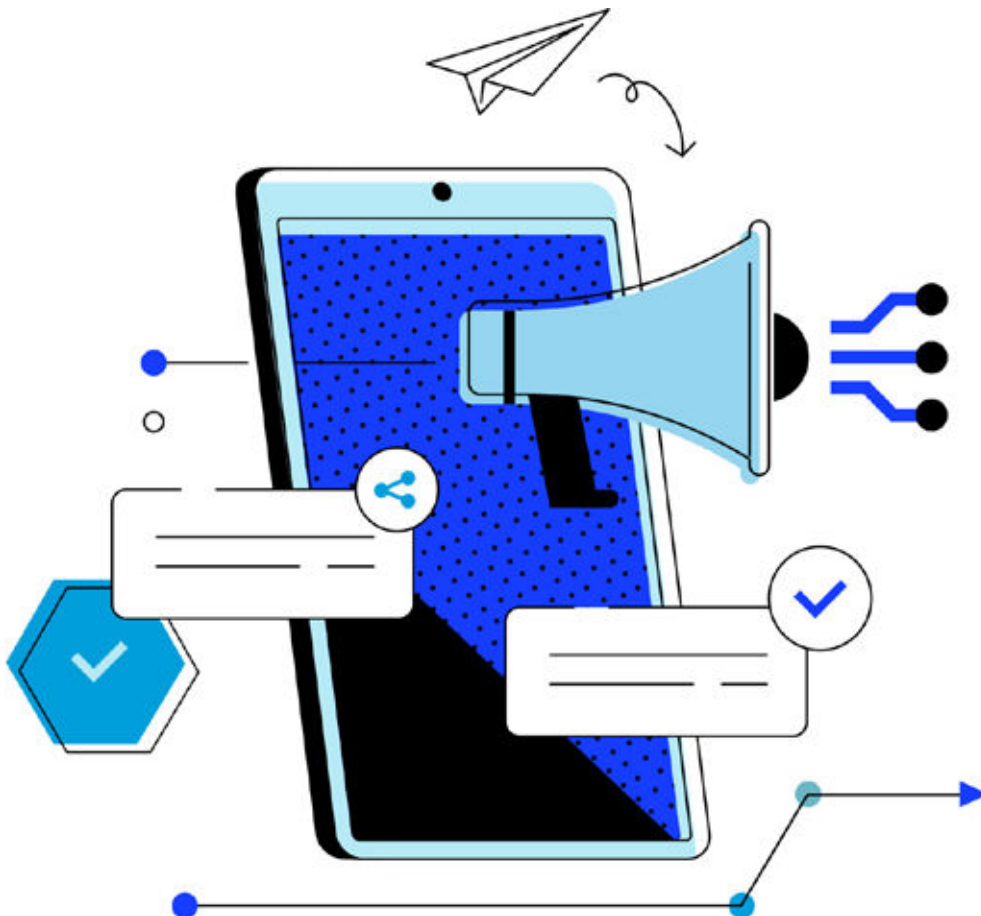
De media beschikken over een bepaalde rol en verantwoordelijkheid om duidelijke en betrouwbare informatie te verstrekken en risico's te formuleren die gerelateerd worden aan informatiekkanalen. Toch krijgt de persvrijheid te maken met grote en langdurige

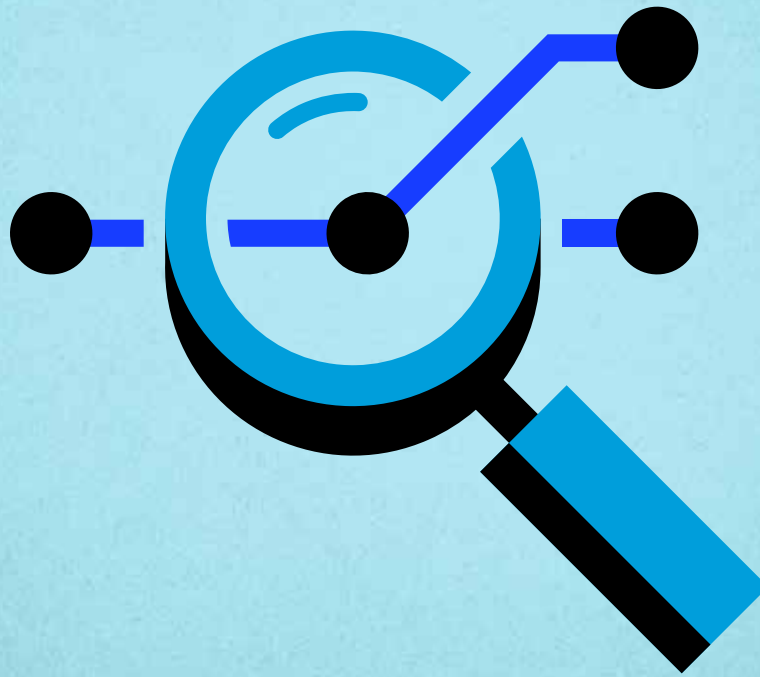
dreigingen, ondanks het recht op de vrijheid van meningsuiting, waartoe de pers en andere vrije, ongecensureerde en onbelemmerde media behoren. Media-professionals worden geconfronteerd met intimidatie, dreigingen en on- en offline geweld, wat leidt tot zelfcensuur en arbeidsrisico's verhoogt.

Tegelijkertijd heeft de informatie-industrie geleden onder de overgang van reclame-inkomsten naar de digitale wereld, die gedomineerd wordt door grote technologiebedrijven. Door die factoren kunnen dergelijke bedrijven de media in handen nemen, waardoor de mediadiversiteit verkleint en de kleine onafhankelijke journalistiek verdwijnt die net belangrijk is voor de publieke belangen. Wanneer uitgavenormen niet strikt gerespecteerd worden, zullen op die manier de risico's van informatie-integriteit in de hand gewerkt en uitvergroot worden bij de media, die zich kunnen kruisen met de on- en offline wereld.

Er is nood aan duidelijke antwoorden om de informatiekanalen te verdedigen die instaan voor het publieke belang, alsook de journalisten en mediaprofessionals. Hierbij wordt rekening gehouden met de contexten waar media-infrastructuur gelimiteerd is en waar burgerjournalisten een vitale dienst bieden aan lokale kiezers. Dergelijke antwoorden kunnen zich uiten in de vorm van betrouwbare steun voor de ontwikkeling van media, waarbij er een beroep wordt gedaan op lokale uitvoerders.

De Staten en technologiebedrijven oefenen een belangrijke invloed uit op de informatieflex en de politiek. Ze zouden hun inzet moeten verhogen om de persvrijheid en onherroepelijke veiligheid van journalisten te verzekeren.





## Transparantie en onderzoek

Een grotere transparantie van technologiebedrijven en andere informatiekanalen kan leiden tot een betere kennis over hoe informatie verspreid wordt, hoe persoonlijke gegevens gebruikt worden en hoe de risico's op informatie-integriteit behandeld worden.

Hoe dan ook leidt een wankelend machtsevenwicht tot moeilijkheden voor transparantie. Een handvol technologiebedrijven hebben toegang tot een ongeziene hoeveelheid gegevens en samen met media-eigenaars oefenen ze veel controle uit over het informatie-ecosysteem. Dat gebeurt soms in een rechtstreekse relatie met de Staten en politieke en economische actoren. Bovendien hebben de reglementaire keuzes betreffende de transparantie die wordt uitgevoerd in

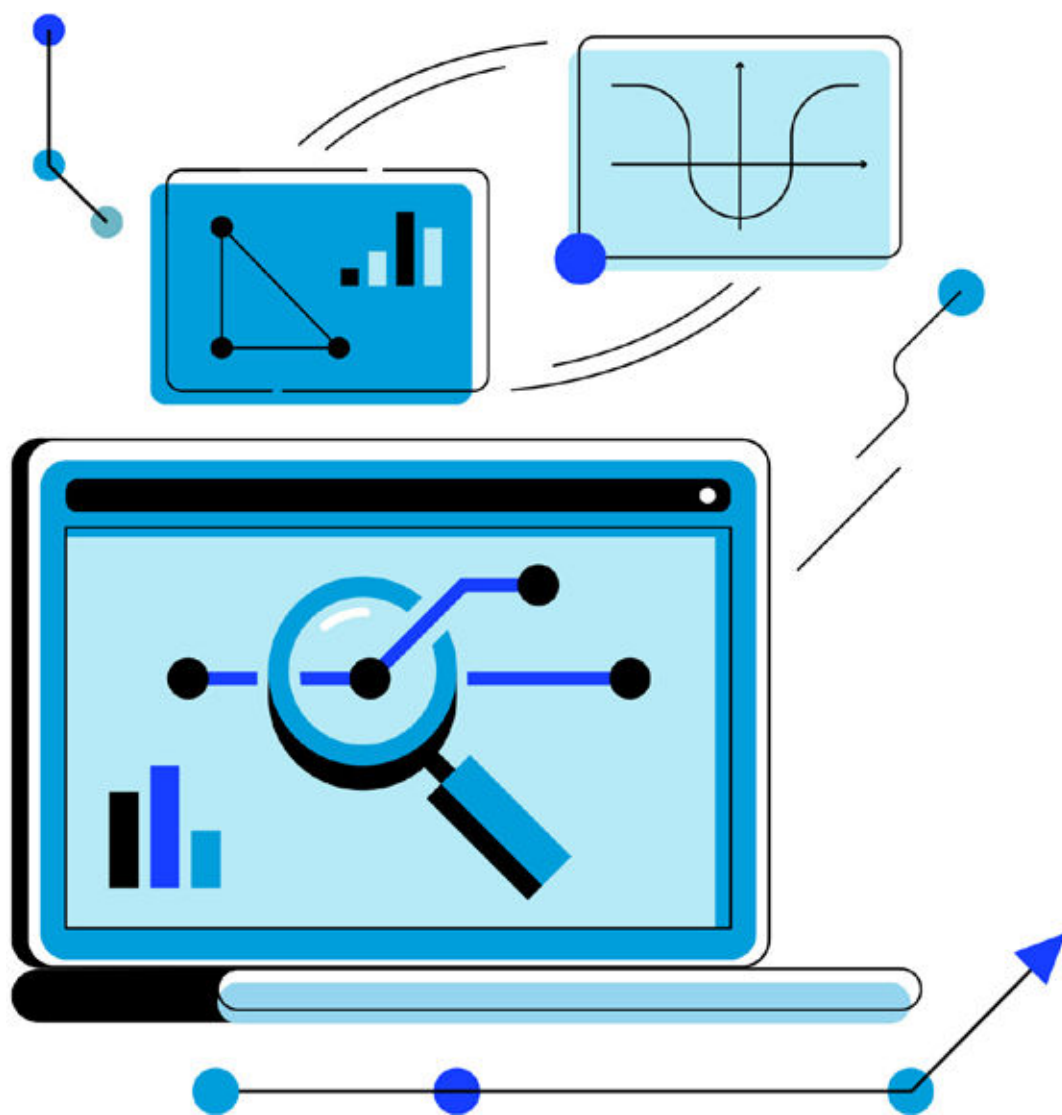
een klein aantal landen waar de meerderheid van de technologiebedrijven hun hoofdzetel hebben, een grote impact op de rest van de wereld. Dat onevenwicht beperkt vaak het onderzoek naar het algemeen belang en kan de inzet op gelijkheid belemmeren, wat net een oplossing kan zijn voor de noden binnen de context van onderbestudeerde en gemarginaliseerde gemeenschappen. Het gebruik van AI-technologie, waarvan de totale impact nog onbekend is, leidt tot extra uitdagingen in onderzoek naar en de kennis van het informatie-ecosysteem.

De beschikbaarheid, de kwaliteit en de toegankelijkheid van data- en informatiegebruik moeten worden opgedreven om een meer genuanceerde globale

kennis van informatiemilieus te kunnen verkrijgen en doelgerichte acties op basis van duidelijk bewijs te kunnen versterken met oog op het bevorderen van de informatie-integriteit.

Toegang verlenen tot de tot gegevens met privacy-behoud aan een breed scala aan onderzoekers zal de algemene inzet versterken om de lacunes en oneffen-

heden van onderzoekweg te werken. Academici, journalisten en het maatschappelijk middenveld moeten beschermd en gesteund worden tijdens de uitvoering van hun essentiële werk, zonder daarvoor ook maar ergens voor te vrezen, noch zich geïntimideerd te voelen.



# Oproep tot actie

Het doel van de volgende aanbevelingen is om de vijf principes te vertalen naar concrete maatregelen voor de betrokken partijen in het informatie-ecosysteem. De aanbevelingen zijn bedoeld als een algemeen plan en gaan van juridische verplichtingen van de staten tot de verantwoordelijkheden van de technologische sector, en ook de beste praktijken voor de media en het maatschappelijk middenveld.



## AANBEVELINGEN VOOR DE BETROKKEN PARTIJEN

---

- → TECHNOLOGISCHE BEDRIJVEN
- → ACTOREN ACTIEF IN ARTIFICIËLE INTELLIGENTIE (AI)
- → ADVERTEERDERS EN ANDERE ACTOREN VAN DE PRIVÉSECTOR
- → NIEUWSMEDIA
- → ONDERZOEKERS EN ORGANISATIES VAN HET MAATSCHAPPELIJK MIDDENVELD
- → STATEN EN POLITIEKE ACTOREN

# Technologische bedrijven

Grote technologische bedrijven, die vaak hun hoofdzetel hebben op plaatsen waar de reglementering op het vlak van technologie beperkt is, hebben enorm veel macht. Zij maken gebruik van grote hoeveelheden verzamelde data over het gedrag van gebruikers, waardoor zij de transnationale informatiestromen kunnen vormgeven en de digitale ervaring op wereldschaal kunnen besturen.

Om dat machtsonevenwicht te bestrijden, is er een kader nodig dat zowel transparantie als onafhankelijke controle vooropstelt. Gebruikers hebben het recht om zelf hun gegevens en hun online-ervaringen in de hand te hebben en te beschikken over duidelijke klachtmogelijkheden en rechtsmiddelen. Er zijn regelingen nodig rond verantwoordingsplicht, zodat technologische bedrijven de verantwoordelijkheid opnemen voor de gevolgen van hun producten op de mensenrechten en de sociale

cohesie, ook in crisis- en conflictsituaties. Daarvoor is een kritische en transparante evaluatie nodig van de architectuur van de platformen, die kenmerken kan identificeren die haaks staan op de informatie-integriteit en de mensenrechten. Er moeten strategieën opgezet worden met als doel die erosie te voorkomen en tegen te gaan, en ondertussen moeten de vrijheid van meningsuiting en de toegang tot informatie gevrijwaard blijven. Desinformatie en haat zouden geen maximale zichtbaarheid en enorme winsten mogen opleveren. Nieuwe, duurzame commerciële modellen die niet gebaseerd zijn op programmatische, doelgerichte reclame zouden innovatie kunnen bevorderen, de autonomie van gebruikers verhogen en het algemeen belang dienen. Die veelzijdige aanpak kan een evenwichtiger informatie-ecosysteem creëren dat de rechten van haar gebruikers respecteert en bijdraagt aan een betrouwbare online omgeving.

## Aanbevelingen



### **a. Veiligheid en respect voor het privéleven integreren van ontwerp tot oplevering.**

Integreren van sterke beleidsmaatregelen op het vlak van veiligheid en bescherming van het privéleven in de hele levenscyclus van alle producten en diensten, van het ontwerp tot ontwikkeling, tot de aflevering en het buiten gebruik stellen, en die maatregelen consequent toepassen op media gemaakt door zowel mensen als AI. Samenwerken met onafhankelijke organisaties en derden om doorlopende evaluaties op te zetten en te publiceren over de risico's voor de mensenrechten van alle producten en diensten, om zo die risico's proactief te verkleinen en mogelijke schade te beperken. Maatregelen nemen voor de bescherming en emancipatie van kwetsbare en gemarginaliseerde groepen, leden van het maatschappelijk middenveld en anderen die vaak een doelwit zijn online, en voor de strijd tegen geweld op basis van geslacht en andere vormen van geweld die plaatsvinden of versterkt worden door middel van technologie. Innoveren om nieuwe uitdagingen aan te pakken, waaronder de mogelijke risico's die AI-technologieën vormen voor de integriteit van het informatie-ecosysteem. Zorgen voor diversiteit en inclusie in elk stadium van productontwikkeling en in teams die instaan voor betrouwbaarheid en veiligheid. Procedures opzetten voor het intern delen van informatie, om te garanderen dat risico-evaluaties en beleidsmaatregelen collectief worden gedeeld en ingebed in alle niveaus en functies van bedrijven, ook in het bestuur. Er op toezien dat alle maatregelen op het vlak van betrouwbaarheid en veiligheid consequent worden toegepast.



**b. Bedrijfsmodellen opnieuw evalueren.** Nagaan of en hoe de architectuur van platformen bijdraagt aan de erosie van de integriteit van het informatie-ecosysteem of de mensenrechten aantast, en proportionele maatregelen nemen om dat te beperken en tegen te gaan zonder de vrijheid van meningsuiting te schaden. Uitbreiden van innovatieve en duurzame commerciële modellen die niet gebaseerd zijn op programmatisch doelgerichte reclame en die het algemeen belang dienen.



**c. Kinderen beschermen.** Invoeren en toepassen van maatregelen die de kinderrechten beschermen en respecteren, zoals leeftijdsverificatie en ouderlijk toezicht. Maatregelen en praktijken invoeren voor het voorkomen en bestrijden van uitbuiting en seksueel misbruik van kinderen die plaatsvinden of versterkt wordt door technologie. Invoeren en bekendmaken van speciale mechanismen voor aangiften en klachten van kinderen.



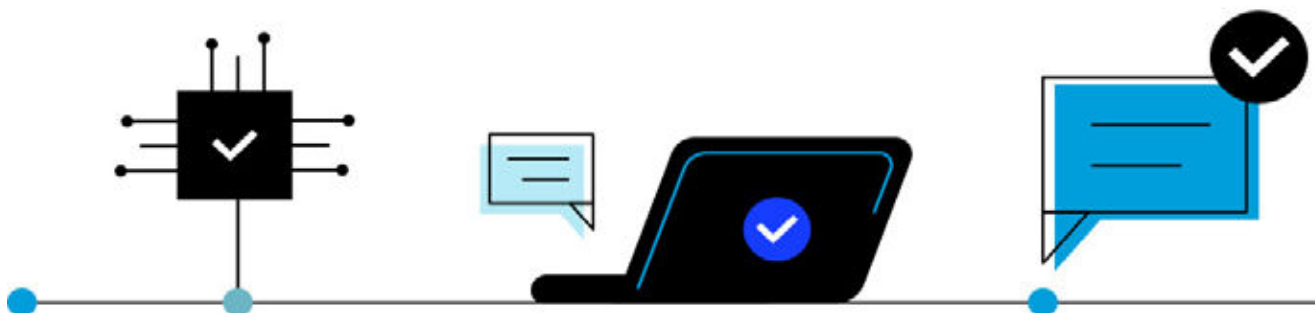
**d. Middelen toewijzen.** Toewijzen van middelen en interne competenties die voldoen en duurzaam zijn op het vlak van betrouwbaarheid en veiligheid, in verhouding met het risiconiveau. Genoeg middelen voorzien om rekening te houden met socioculturele en linguïstische contexten, werktalen en de verschillende noden van kwetsbare en gemarginaliseerde groepen, en dan vooral in contexten van conflict en instabiliteit.



**e. Consequente inhoudsmoderatie verzekeren.** Samenwerken met onafhankelijke organisaties om inhoudsmoderatieprocessen te ontwikkelen die in overeenstemming zijn met internationale normen inzake mensenrechten en erop toezien dat dat beleid consequent en niet willekeurig wordt toegepast in alle sectoren. Voldoende middelen toewijzen aan zowel menselijke als automatische inhoudsmoderatie en het beheer ervan, en die consequent inzetten in alle talen en in alle mogelijke contexten. Maatregelen nemen om inhoud te bestrijden die ingaat tegen de communityrichtlijnen van platformen of tegen de mensenrechten. Voorbeelden daarvan zijn het inperken van algoritmische versterking, labeling en demonetisatie. Openbaar toegankelijk maken van uitgesplitste gegevens over de invoering van maatregelen over inhoudsmoderatie en over de middelen die aan inhoudsmoderatie worden toegewezen, naargelang de taal en de context.



**f. De arbeidsnormen respecteren.** Arbeidsomstandigheden bieden die in overeenstemming zijn met het internationale arbeidsrecht en de mensenrechten, en prioriteit geven aan initiatieven



die het welzijn, de veiligheid en de kwaliteit van de opleiding van alle werknemers garanderen, inclusief inhoudsmoderators, die betrokken zijn bij inspanningen op het gebied van vertrouwen en veiligheid.



**g. Een onafhankelijk controlesysteem opzetten.** Regelmatig onafhankelijke externe audits van de mensenrechten laten uitvoeren met betrekking tot de bedrijfstoestand en de communautaire normen, het vertrouwen, het veiligheids- en reclamebeleid, het risicobeheer, de impact van reclame- en verwijzingssystemen in verschillende talen en operationele contexten, inhoudsmoderatie, de klachten- en beroepsprocedures, de transparantiemechanismen en de toegang tot gegevens voor onderzoekers.

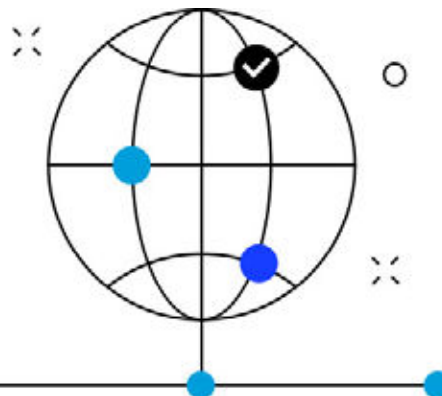
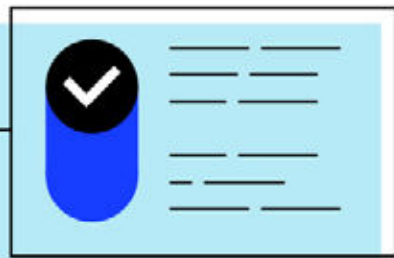
Het effect van producten en diensten op kwetsbare en gemarginaliseerde groepen, op gendergelijkheid en op kinderrechten beoordelen. De resultaten van deze audits openbaar, toegankelijk en begrijpelijk voor alle gebruikers maken.



**h. Standaarden voor de industrie ontwikkelen.** Partnerschappen opzetten met het maatschappelijk middenveld en andere belanghebbenden om samen kaders te ontwikkelen voor de verantwoordingsplicht van de sector, met duidelijk gedefinieerde rollen en verantwoordelijkheden, om zo te streven naar geverifieerde openbare rapporten en onafhankelijk toezicht, alsook de strenge normen te respecteren op het gebied van privacy, transparantie, risicobeheer, vertrouwen en beveiliging. Specifieke voorzieningen treffen om tegemoet te komen aan de behoeften van groepen in kwetsbare en gemarginaliseerde situaties en in fragiele contexten, door effectieve middelen in te voeren om risico's voor de mensenrechten te meten en aan te pakken. Zorgen voor samenwerking tussen platforms en diensten, met het besef dat risico's zich kunnen verspreiden over verschillende informatieruimten, elk met unieke ontwerpfouten en politieke lacunes die kunnen worden uitgebuit.



**i. De crisisrespons verbeteren.** Samenwerken met belanghebbenden die actief zijn in gebieden met een hoog risico, processen instellen voor vroegtijdige waarschuwing en escalatie met een versnelde en tijdige respons in crisis- en conflictcontexten. Mechanismen opzetten om omvangrijke en snelle toegang te bieden tot betrouwbare en accurate informatie die het algemeen belang dient.





**j. Politieke processen ondersteunen.** Risicobeoordeling van mensenrechten uitvoeren voor alle producten en diensten voor en tijdens verkiezingen en andere politieke processen en ze beschikbaar maken voor het publiek. Alle samenhangende beleidsmaatregelen toepassen om de integriteit van informatie te behouden, door stappen te nemen in de strijd tegen desinformatie, intimidatie en geweld tegen vrouwen en andere groepen die over het algemeen het doelwit zijn in het openbare leven, met inbegrip van politieke kandidaten.



**k. Samenwerken met belanghebbenden.** Zich proactief inzetten met een breed scala aan belanghebbenden, waaronder de lidstaten, de universiteiten, het maatschappelijk middenveld, kinderen, jongerenorganisaties en de technische gemeenschap om de risico's te begrijpen die van belang zijn voor de integriteit van het informatie-ecosysteem en om de mechanismen voor vertrouwen en beveiliging in lijn hiermee te versterken en te kalibreren.



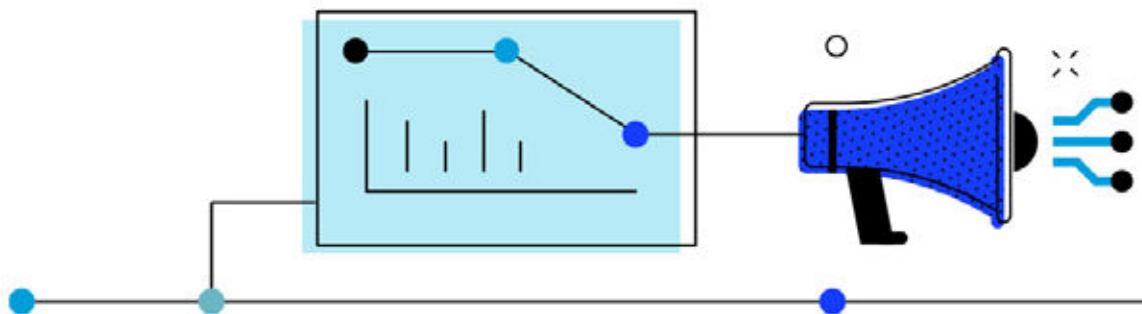
**l. Degelijke klachtenmechanismen opzetten.** Transparante, veilige, beveiligde en toegankelijke mechanismen wanneer nodig garanderen voor klachten, rapporten, oproepen en bezwaren door gebruikers en niet-gebruikers, inclusief speciale processen voor mensen in kwetsbare en gemarginaliseerde situaties. Procedures vaststellen en implementeren om misbruik van meldings- en klachtenmechanismen te voorkomen, bijvoorbeeld door gecoördineerd inauthentiek gedrag.



**m. Duidelijke beleidsregels communiceren.** Algemene voorwaarden, beleid, communautaire normen en aanvraagprocedures gemakkelijk toegankelijk, samenhangend en begrijpelijk maken, ook voor kinderen. Alle beleidsregels, richtlijnen en regels met betrekking tot actualiteit en politieke inhoud duidelijk uitleggen.



**n. Het reclamebeleid handhaven.** Duidelijke en strenge beleidsregels opstellen, bekendmaken en handhaven voor reclame en de monetisatie van inhoud. Bestaande partnerschappen met uitgevers en adverteerders van reclametechnologie regelmatig evalueren om te bepalen of dit beleid wordt nageleefd door partners in de toeleveringsketen van reclametechnologie. Elk jaar publiekelijk verslag uitbrengen over de effectiviteit van de toepassing van het beleid en eventuele andere maatregelen.





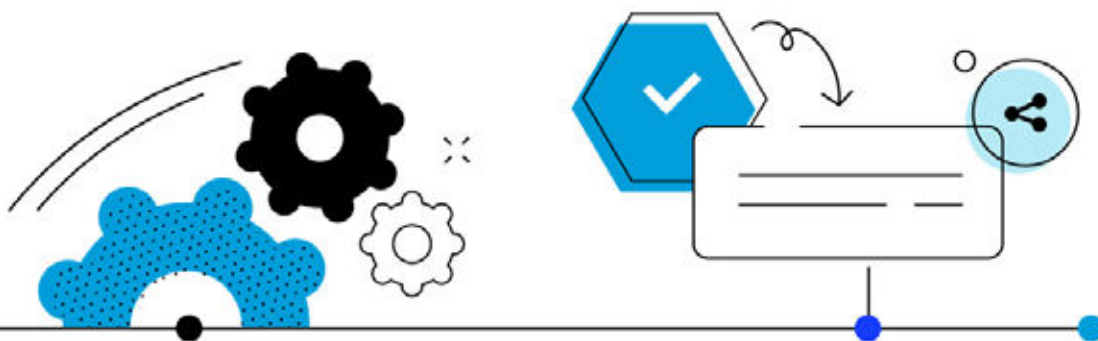
**O. Transparantie in reclame aantonen.** Alle advertenties duidelijk markeren, zodat informatie over de adverteerder, de gebruikte parameters voor het doelpubliek en elk gebruik van AI-gegenereerde of AI-gemedieerde inhoud transparant is voor gebruikers. Volledige, toegankelijke, actuele en doorzoekbare advertentiebibliotheken bijhouden, met informatie over de bron of koper, het bestede bedrag en de doelgroep. Adverteerders en onderzoekers voorzien van gedetailleerde gegevens over waar advertenties precies zijn verschenen in een bepaalde periode en de nauwkeurigheid en effectiviteit van controles en diensten met betrekking tot advertentieplaatsingen en merkadvertenties. Transparant zijn over inkomstenbronnen en overeenkomsten voor het delen van inkomsten met adverteerders en contentmakers. Alle politieke reclame duidelijk labelen, vooral om aan te geven welke inhoud is gegenereerd of verspreid door AI, en gemakkelijk toegankelijke informatie verstrekken over waarom ontvangers worden benaderd, wie voor de reclame heeft betaald en hoeveel.



**P. Veiligheid en diversiteit in de media ondersteunen.** Een omgeving creëren die bevorderlijk is voor de verspreiding van informatie vanuit diverse perspectieven, zodat consumenten toegang hebben tot een scala aan mediabronnen. Onafhankelijke, vrije en pluralistische media ondersteunen, meer bepaald lokale en burgerjournalistiek in verschillende talen en contexten, met respect voor de redactionele onafhankelijkheid. Alle nodige maatregelen nemen om te waarborgen dat de rechten van journalisten en mensen die met online media werken worden gerespecteerd. Expliciete en transparante bepalingen maken om journalisten en mediawerkers te helpen beschermen tegen intimidatie, misbruik en bedreigingen met geweld, rekening houdend met de risico's die journalisten lopen, vooral op cruciale momenten voor de samenleving zoals verkiezingen, natuurrampen en door de mens veroorzaakte crisissen. Beleid en praktijken op het gebied van vertrouwen en veiligheid bijwerken om het systematisch benadelen en aanvallen van vrouwelijke journalisten te verminderen en tegen te gaan.



**Q. Toegang tot gegevens verlenen.** Onderzoekers, universiteiten en academici uit alle onderzoeksdomeinen, journalisten, het maatschappelijk middenveld en internationale organisaties toegang verlenen tot gegevens die zij nodig hebben zodat ze de betrouwbaarheid van informatie makkelijker kunnen beoordelen, beleid en best practices verduidelijken en het verantwoordelijkheidsgevoel stimuleren met respect voor de privacy en het intellectuele eigendom van de gebruikers. Die gegevens moeten verfijnd worden om een grondige studie uit te kunnen



voeren over de betrouwbaarheid van het informatielandschap, de maatschappelijke risico's, de gevolgen voor gemeenschappen en verschillende bevolkingsgroepen, de moeilijkheden met het gebruik van AI-technologie, de potentiële impact op de uitvoering van de Duurzame Ontwikkelingsdoelstellingen en de doeltreffendheid van risicobeperkende maatregelen. Die gegevens zouden informatie moeten verstrekken over algoritmegestuurde aanbevelingssystemen, inclusief informatie over hoe algoritmes getraind worden om inhoud te rangschikken, aan te bevelen, te verspreiden en weer te geven. Daarnaast moeten de gegevens informatie bieden over opgeschorte, verboden of tijdelijk geblokkeerde accounts. Ook moet het de gebruikte bronnen in beeld brengen in alle talen en voor alle contexten voor het vertrouwen en veiligheid. Het moet makkelijker worden om gegevens tegen een minimale kost aan onderzoekers te verstrekken voor systemen die toegankelijk en leesbaar zijn door machines.

**f. Openbaarmaking verzekeren.** Overheidsverzoeken indienen voor het verwijderen of plaatsen van inhoud. Alle samenwerkingen met bedrijven die factchecken openbaar maken, inclusief de betaling, andere steun en de betaling aan politieke organen en kandidaten.

**s. Controle en keuze bieden.** Middelen, functies en sociale media aanbieden die een geïnformeerde toestemming garanderen en ervoor zorgen dat mensen de touwtjes online in eigen handen hebben dankzij de samenwerking met andere media. Tegelijkertijd wordt het aanbod uitgebreid door de consument een geïnformeerde toestemming te geven over wat die te zien krijgt en hoe de gegevens worden gebruikt.

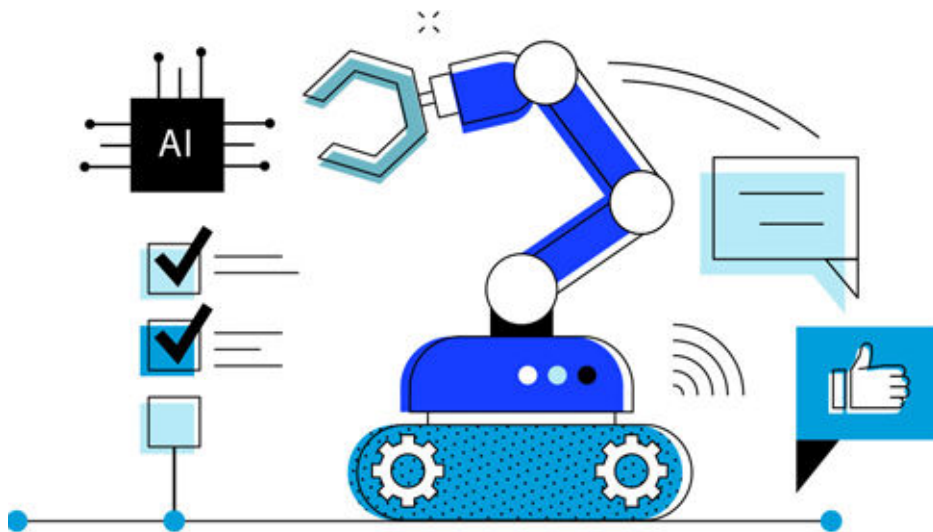
**t. AI-inhoud uitlichten.** Het moet duidelijk worden aangegeven wanneer inhoud door AI wordt gegenereerd of gebruikt door investeringen in de ontwikkeling van oplossingen op bedrijfsniveau. Op die manier kunnen de gebruikers de inhoud makkelijk herkennen in plaats van die zomaar in zich op te nemen, waardoor het vertrouwen van de gebruikers in het informatielandschap over het algemeen versterkt wordt. Het gaat daarbij vooral over informatie van metagegevens die aanduiden dat een inhoud gecreëerd of gebruikt werd door AI.

**u. Respect voor het privéleven garanderen.** Er moet gegarandeerd worden dat de verzameling, het gebruik, de verspreiding, de verkoop en de opslag van gegevens het privéleven van de gebruikers respecteren. Bovendien moeten zij makkelijk toegang hebben tot de manier waarop hun gegevens geëxtraheerd worden, inclusief de algoritmische keuzes en de manier waarop hun persoonlijke gegevens worden gedeeld met andere instellingen en hoe ze door die instellingen verkregen worden.

**v. Een digitale cultuur verkiezen.** Opleidingscampagnes en informatie om digitale competenties te stimuleren, onder andere over het algemene begrip van de digitale werking, de effecten ervan en de nadelen van algoritmes. Middelen aan alfabetisering en vaardigheidstoename in alle talen en vakgebieden besteden, vooral voor mensen in kwetsbare contexten. Zorgen voor trainingsmateriaal over veiligheid voor kinderen en jongeren. Onafhankelijke externe evaluaties van de effectiviteit van alfabetiseringsinitiatieven mogelijk maken en die openbaar maken.

# Actoren actief in artificiële intelligentie (AI)

Overheidsinstellingen, particulieren en openbare spelers die betrokken zijn bij ten minste één fase van de levenscyclus van artificiële intelligentie.



Technologieën op het vlak van artificiële intelligentie (AI) ontwikkelen zich snel en staan op het punt om onze wereld te veranderen. Van de automatisering van alledaagse taken tot bijstand voor wetenschappelijke ontdekkingen, de potentiële voordelen zijn enorm. Met die vooruitgang wordt het echter noodzakelijk om ervoor te zorgen dat AI veilig, beveiligd en betrouwbaar wordt ontworpen, ontwikkeld, ingezet en buiten gebruik wordt gesteld. Vooroordelen en een gebrek aan diversiteit in leergegevens kunnen ertoe leiden dat AI-systemen misleidende informatie genereren en onrecht verspreiden.

Dat vermogen om realistische inhoud te genereren kan op grote schaal de betrouwbaarheid van het informatielandschap in gedrang brengen. Opkomende risico's kunnen worden beperkt door voorrang te geven aan transparantie en eerlijkheid in de levenscyclus van AI-technologieën. Overheden, technologiebedrijven en academische instellingen en onderzoeksinstituten moeten samenwerken zodat AI gedurende de hele levenscyclus veilig en verantwoord wordt ontworpen, ontwikkeld, ingezet en buiten gebruik wordt gesteld. Door samen te werken kunnen deze belanghebbenden verzekeren dat AI-technologieën voordelig zijn voor de samenleving en het menselijke welzijn.

# Aanbevelingen



**a. Veilige, beveiligde en betrouwbare AI waarborgen.** Maatregelen nemen om de veiligheid, beveiliging en betrouwbaarheid te waarborgen bij het ontwerp, de ontwikkeling, de implementatie, het gebruik en de buitengebruikstelling van AI-technologieën. De gevolgen van alle innovaties of ontwikkelingen op dit gebied die risico's kunnen vormen voor de integriteit van het informatie-ecosysteem aankaarten en openbaar maken, waaronder misbruik van AI-technologieën, afhankelijkheid van AI-technologie zonder menselijke controle en het mogelijke verdere verlies van vertrouwen in verschillende geografische en maatschappelijke contexten. AI trainen met betrouwbare en inclusieve informatiebronnen over kwesties die cruciaal zijn voor het publieke welzijn en maatregelen nemen om vooroordelen in trainingsgegevens te verminderen, met name op het gebied van gender en etnische afkomst. Samenwerken met een reeks belanghebbenden om risicobeoordelingen op vlak van mensenrechten te verwezenlijken, om proactief maatschappelijke risico's te minimaliseren en potentiële vooroordelen te beperken, onder meer voor vrouwen, kinderen, jongeren en andere kwetsbare en gemarginaliseerde groepen.



**b. Onafhankelijke audits laten uitvoeren.** Zich ertoe verbinden om toegang en een juridische en technische veilige omgeving te bieden aan institutionele en individuele onderzoekers om onafhankelijke audits van AI-modellen uit te voeren, met passende garanties, zoals conformiteit met het beleid van het bedrijf inzake de openbaarmaking van kwetsbaarheden. De toegang van het publiek tot de resultaten van onafhankelijke audits waarborgen, tot gegevens over risico's van AI-systemen, zoals de mogelijkheid van negatieve discriminatie en "hallucinaties", ofwel inhoud die feitelijk lijkt maar die volledig verzonnen is, en tot de getroffen maatregelen om mogelijke vooroordelen te voorkomen, te beperken en aan te pakken.



**c. Intellectueel eigendom respecteren.** Intellectuele eigendomsrechten respecteren en een billijke compensatie garanderen voor het gebruik van intellectueel eigendom, waaronder originele journalistiek die gebruikt werd bij de training van AI-tools.



**d. De oorsprong van de informatie weergeven.** Oplossingen en beleidslijnen uitwerken en implementeren over de herkomst van informatie, zowel in zichtbare als in onzichtbare vormen, zoals certificering van authenticiteit, watermerken en labels. Met meerdere belanghebbenden samenwerken om gebruiksvriendelijke labeling te standaardiseren.



**e. Geletterdheid bevorderen.** Op organisatieniveau investeren in de ontwikkeling en uitrol van geletterdheidsinitiatieven om het publiek te helpen de werking van AI-modellen en gevolgen voor informatieconsumenten wereldwijd beter te begrijpen, waarbij nadruk wordt gelegd op de risico's voor de informatie-integriteit..



**f. Feedback van gebruikers mogelijk maken.** Gebruikers de mogelijkheid geven om onnauwkeurige of misleidende informatie van bronnen aan te wijzen of te rapporteren, terwijl de privacy van gebruikers wordt beschermd.



# Adverteerders

Adverteerders kunnen een unieke invloed uitoefenen op de integriteit van het informatie-ecosysteem. Zo kunnen ze financiële stimuli wegnemen van partijen die profijt willen halen uit desinformatie en haat. Op die manier

kunnen adverteerders hun merken beter beschermen en materiële risico's aanpakken, waardoor hun resultaten verbeteren terwijl ze hun activiteiten uitvoeren in overeenstemming met de waarden van hun bedrijf.

## Aanbevelingen



**a. Reclame die mensenrechten respecteert implementeren.** Voorzorgsmaatregelen nemen om ervoor te zorgen dat reclame geen risico's vormt voor de informatiesectoren en de mensenrechten respecteert, waaronder kinderrechten. Discriminerende targetingpraktijken vermijden die gebaseerd zijn op gevoelige data en waargenomen gebruikerskenmerken. Adverteren bij media en platforms die de informatie-integriteit versterken, waaronder journalistiek van openbaar nut, via methoden als opt-in/opt-out-lijsten, advertentieverificatietools en handmatige controle. Advertentietechnologiebedrijven verplichten om criteria te publiceren waaraan een website of kanaal moet voldoen alvorens inkomsten te kunnen genereren.



**b. De industriestandaarden beheersen.** De industriestandaarden gebruiken om duidelijke beleidslijnen uit te werken die risico's voor de informatie-integriteit minimaliseren en de veiligheid van het merk waarborgen.



**C. Coalities vormen.** Samenwerken met de hele sector en maatschappelijke organisaties om tijdig best practices en ervaringen te delen over informatie-integriteit. Hieronder vallen de beoordeling van de invloed van reclame en de systematische beperking van potentiële risico's en schade die voortvloeien uit reclame en het genereren van inkomsten uit inhoud.



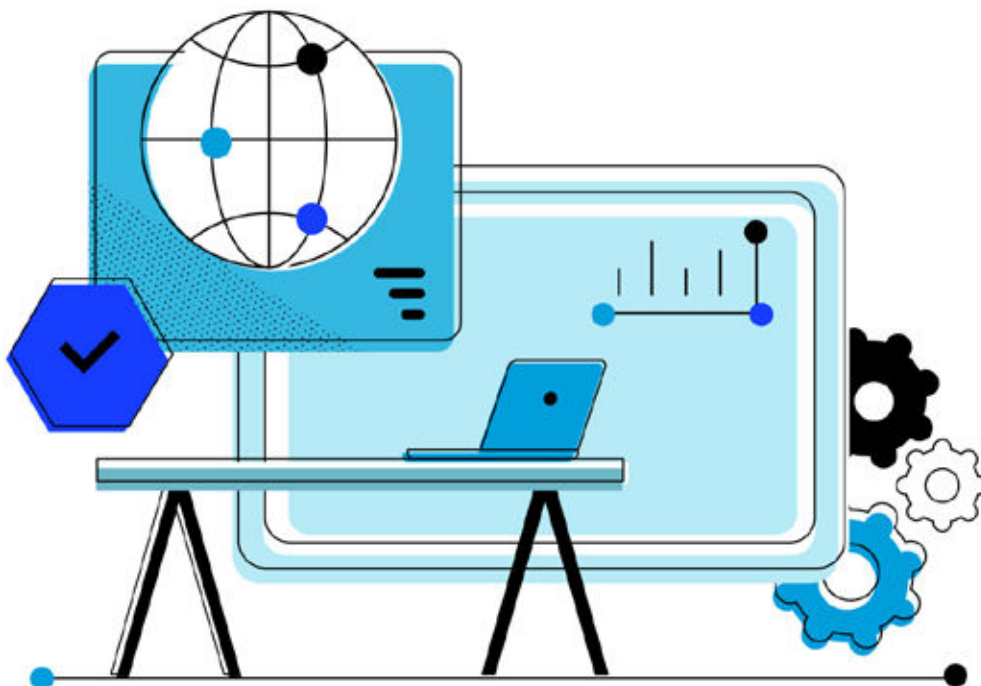
**d. Vereiste gegevens.** Op regelmatige basis een volledig en gedetailleerd overzicht opstellen van de reclameadvertenties, waarbij gedetailleerde gegevens worden vereist die aantonen waar de advertenties verschenen zijn en waarbij geschiktheidscontroles uitgevoerd worden voor de plaatsing van advertenties. Grondige audits uitvoeren van advertentiecampaagnes.



**e. Transparantie opleggen.** Reclametechnologiebedrijven verplichten om enerzijds transparantienormen vast te leggen die end-to-end-verificatie van de toeleveringsketen van reclametechnologie mogelijk maken, en om anderzijds alle gegevens met betrekking tot reclamecampagnes te delen met klanten en onderzoekers, met inbegrip van beleggings- en blokkeringsinformatie achter een betaalmuur.



**f. Audits uitvoeren.** Reclametechnologiebedrijven ertoe verplichten dat ze onafhankelijke audits door derden laten uitvoeren en dat ze toeleveranciers van reclamemarkten controleren.



# Andere actoren in de privésector

De acties van een breder scala aan entiteiten binnen de privésector, die niet rechtstreeks betrokken zijn bij de technologiesector, kunnen invloed hebben op de informatieruimte. Ze kunnen zowel de informatie-integriteit verzwakken als ondersteunen. Bedrijven hebben de verantwoordelijkheid om de mensenrechten

te respecteren, waaronder het recht op vrijheid van meningsuiting en toegang tot informatie. Daarnaast kunnen ze samenwerkingsverbanden aangaan met andere belanghebbenden om bij te dragen aan een gezonder informatie-ecosysteem.

## Aanbevelingen



**a. De integriteit beschermen.** Verdedig de mensenrechten, waaronder het recht op vrijheid van mening en meningsuiting, en vermijd het opzettelijk verspreiden of financieren van risico's die de integriteit van het informatie-ecosysteem schaden, zij het om financiële redenen of wegens andere strategische doelstellingen.



**b. Investeren in geletterdheid.** Investeer in media- en informatiegeletterdheid op organisatieniveau door samen te werken met relevante maatschappelijke actoren en gebruik te maken van hun expertise.

# Nieuwsmedia

Onafhankelijke, vrije en diverse media zijn cruciaal om het publiek te informeren over maatschappelijke kwesties, burgerbetrokkenheid te stimuleren en machthebbers verantwoordelijk te houden.

De onafhankelijkheid, vrijheid en diversiteit van de media staan onder druk door directe en indirecte bedreigingen. Ook de achteruitgang van lokale en publieke journalistiek kan die essentiële functies in gevaar

brengen. Wanneer professionele normen niet strikt worden nageleefd, kunnen nieuwsmedia de betrouwbaarheid van informatie schaden. Journalisten leveren een onmisbare dienst aan de samenleving en helpen het evenwicht te herstellen in een informatie-ecosysteem dat onder druk staat. Dat kunnen ze doen dankzij ethische verslaggeving, transparantie, kwaliteitsvolle opleidingen en degelijke arbeidsomstandigheden.

## Aanbevelingen



**a. De betrouwbaarheid van informatie belichten.** Investeer in capaciteitsversterking voor datagestuurde onderzoeksjournalistiek, zodat de media proactief verslag kunnen uitbrengen over risico's voor de integriteit van het informatie-ecosysteem. Hanteer sterke redactionele processen en normen, vooral bij informatieverzameling, om het vertrouwen van mediagebruikers te behouden en te versterken. Zorg voor betrouwbare factchecking die het publiek houvast biedt.



**b. In actie komen tijdens crisissen.** Waak erover dat het doelpubliek gratis en tijdig toegang heeft tot betrouwbare informatie in noodsituaties en crisissituaties, waarin de risico's voor de integriteit van het informatie-ecosysteem vaak groter zijn.



**c. Professionele en ethische normen handhaven.** Zet je in voor en houd je aan internationaal erkende normen en praktijken voor professionele en ethische journalistiek, ten dienste van het publiek, met nadruk op onpartijdigheid en redactionele onafhankelijkheid. Stimuleer zelfregulering en verantwoordingsmechanismen. Bied regelmatig hoogwaardige training om ethische, nauwkeurige en onpartijdige journalistiek te bevorderen en vaardigheden up-to-date te houden. Moedig innovatie en aanpassingsvermogen aan binnen het steeds veranderende medialandschap, bijvoorbeeld via een oplossingsgerichte of constructieve benadering van journalistiek. Maak transparant waar de financiering vandaan komt, hoe de eigendomsstructuur eruit ziet en welke financiële belangen er spelen, zodat mensen beter geïnformeerd keuzes kunnen maken over de informatie die zij consumeren.



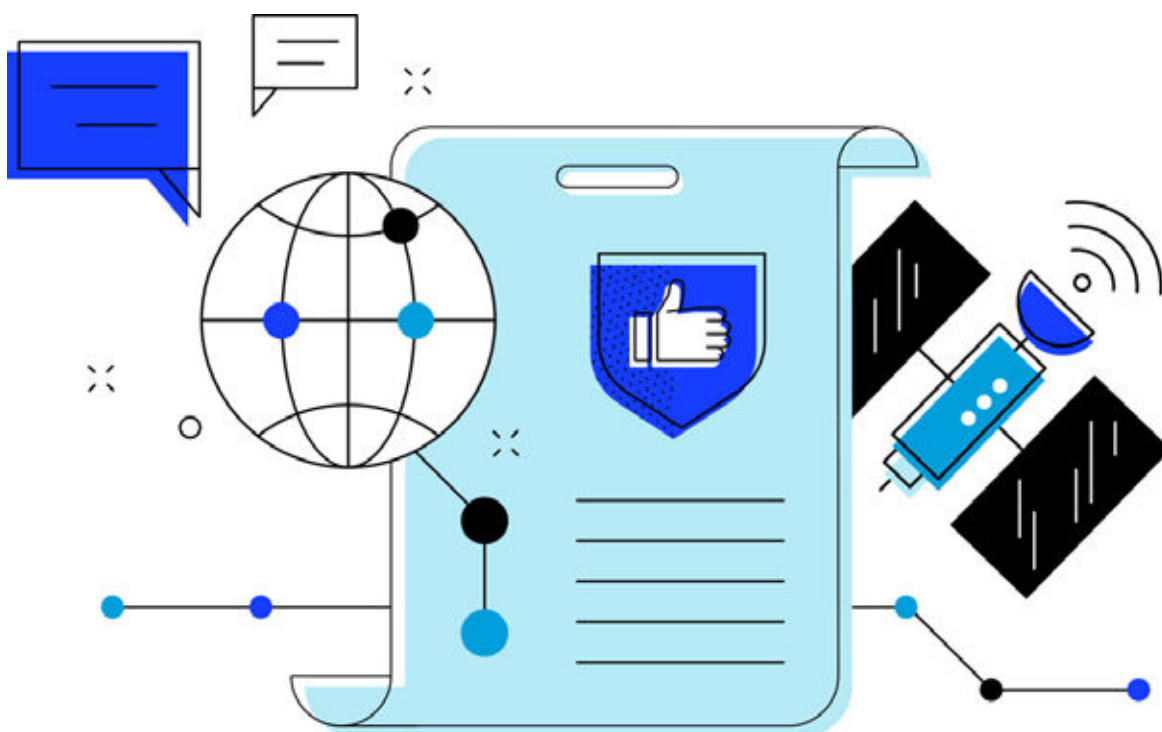
**d. AI op een ethische manier gebruiken.** Stel duidelijke richtlijnen op voor het ethische gebruik van AI-technologieën, waaronder expliciet gelabelde AI-gegenereerde of AI-gemodereerde content bij publicatie of verspreiding. Zorg ervoor dat metadata informatie bevatten die AI-gegenereerde inhoud identificeert.



**e. Transparante reclame waarborgen die de mensenrechten respecteert.** Neem maatregelen om te voorkomen dat advertenties de informatieruimte ondermijnen. Maak een duidelijk onderscheid tussen nieuws, opinies en gesponsorde inhoud. Wees transparant over de financiering van opiniestukken en mogelijke belangenconflicten. Label alle advertenties en gesponsorde content, inclusief AI-gegenereerde reclame, op een duidelijke manier. Publiceer transparante rapporten over bronnen van advertentie-inkomsten en hanteer toegankelijke en duidelijke reclamebeleid en -praktijken.



**f. Arbeidsnormen respecteren.** Garandeer werkomstandigheden die in lijn zijn met internationale arbeidsnormen en mensenrechten. Geef voorrang aan initiatieven die het welzijn en de veiligheid van journalisten bevorderen, ook in digitale omgevingen. Besteed bijzondere aandacht aan discriminatie, misbruik, intimidatie en dreiging met geweld tegen vrouwelijke journalisten en mediapersoneel.



# Onderzoekers en het maatschappelijk middenveld

Onderzoekers en maatschappelijke organisaties spelen een belangrijke rol in de inspanningen om de veelzijdige impact van risico's op de integriteit van het informatiesysteem te begrijpen en aan te pakken. Hun werk helpt risico's binnen informatieruimten bloot te leggen, versterkt de databasis voor belangenbehartiging en

bevordert veerkracht, vooral voor kwetsbare en gemarginaliseerde groepen. Samenwerkingsverbanden en kennisuitwisseling zijn essentieel om de kloof tussen onderzoeksresultaten en doeltreffende oplossingen te overbruggen.

## Aanbevelingen



**a. Werk samen.** Bouw partnerschappen op met belanghebbenden uit diverse regio's en contexten om effectieve en ethische benaderingen te delen die de integriteit van informatie-ecosysteem versterken.



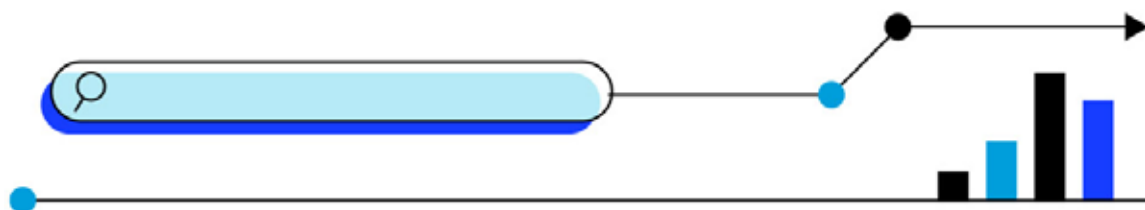
**b. Respecteer integriteit en ethische normen.** Respecteer de mensenrechten en vermijd het opzettelijk verspreiden of ondersteunen van risico's die de informatie-integriteit schaden. Voer onderzoek uit met respect voor ethiek, transparantie en privacy.



**c. Bevorder open access.** Onderneem initiatieven voor open toegang, maak onderzoeksresultaten vrij toegankelijk en stimuleer de interdisciplinaire samenwerking.



**d. Versterk inclusief onderzoek.** Verken multidisciplinair onderzoek naar het informatie-ecosysteem over geografische gebieden, talen en thematische domeinen heen, met aandacht voor de potentiële impact van risico's voor de informatie-integriteit op de Duurzame Ontwikkelingsdoelstellingen. Focus op onderbestudeerde, kwetsbare en gemarginaliseerde contexten en gemeenschappen. Ontwikkel nauwkeurige methodologieën om die risico's en de bijbehorende schade te meten.

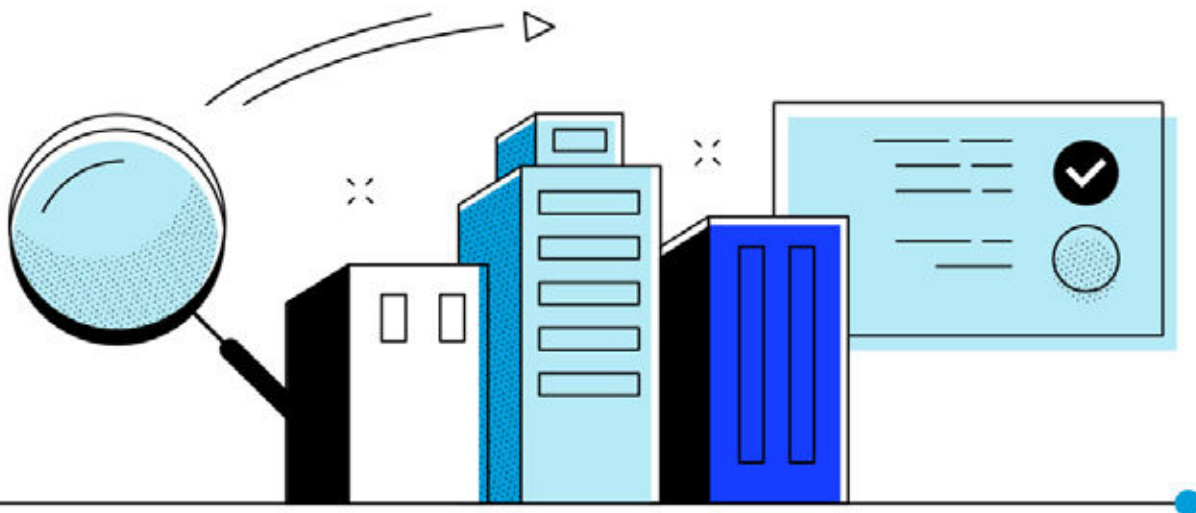




## AANBEVELINGEN VOOR NETWERKEN EN ORGANISATIES DIE FACTCHECKEN

**a. Behoud professionele normen.** Streef naar professionaliteit en ethiek door onafhankelijkheid, onpartijdigheid en transparantie in acht te nemen. Dat moet zichtbaar zijn in de samenstelling en bestuur, financieringsbronnen, eigendom en werkwijze van de organisatie.

**b. Maak financiering transparant.** Neem maatregelen om de financieringsbronnen en eventuele samenwerkingen met belanghebbenden, zoals technologiebedrijven, de media en maatschappelijke organisaties, openbaar te maken.



# Staten

Staten nemen de verantwoordelijkheid op zich om de internationale principes voor informatie-integriteit te consolideren. Dat houdt in dat de staten zich inzetten om de mensenrechten te respecteren, te beschermen en te bevorderen, in het bijzonder het recht op de vrijheid van meningsuiting, met inbegrip van het recht om informatie op te zoeken, te ontvangen en te verspreiden.

Staten spelen een centrale rol bij de vormgeving van informatieruimtes, onder andere vanwege hun juridische en regelgevende autoriteit, hun controle van de publieke middelen en hun vermogen om nationale en internationale coalities te vormen. In het kader van hun verplichtingen op het gebied van mensenrechten moeten de staten bescherming bieden tegen schendingen van die rechten op hun grondgebied of onder hun jurisdictie door ondernemingen. Dat doen ze door geschikte maatregelen te nemen om dergelijke schendingen te voorkomen, te onderzoeken, te bestraffen en te herstellen door middel van doeltreffende beleidsstukken, wetgevingen, reglementeringen en rechterlijke beslissingen.

Staten die zich inzetten voor het informatie-ecosysteem hebben immers allemaal verschillende technische en financiële mogelijkheden. Ongelijkheden in de infrastructuur en in de toegang tot technologie en financiële middelen hebben bijgedragen aan de digitale kloof. Tegelijkertijd zijn talrijke grote technologische ondernemingen gevestigd in een klein aantal landen in het Globale Noorden, maar slagen ze er toch in om de wereldmarkt te betreden en te domineren. Om te garanderen dat alle staten aan het informatie-ecosysteem kunnen bijdragen en er voordeel uit kunnen halen zijn er dringend duurzame initiatieven nodig om de staten beter in staat te stellen hun digitale connectiviteit uit te breiden, het ontstaan van een "AI-kloof" proactief te voorkomen en hun vermogen te versterken om risico's in informatieruimtes adequaat aan te pakken, met respect voor de mensenrechten. Die inspanningen zullen uiteindelijk de informatie-integriteit versterken, mensenrechten bevorderen en bijdragen aan de verwezenlijking van de Duurzame Ontwikkelingsdoelstellingen.

## Aanbevelingen



**a. Mensenrechten respecteren, beschermen en bevorderen.** Respecteer, bescherm en bevorder mensenrechten, in het bijzonder het recht op de vrijheid van meningsuiting, met inbegrip van het recht op informatie, op basis van internationale normen en standaarden op het vlak van mensenrechten. De staten zien er beter op toe dat de reglementering of andere maatregelen die van kracht zijn om de verschillende aspecten van informatie-integriteit te behandelen, in overeenstemming zijn met het internationaal recht dat van toepassing is, met inbegrip van de internationale mensenrechtenwetgeving, met volledige betrokkenheid van het maatschappelijk middenveld, in het kader van een grotere inspanning die als doel heeft om de mensenrechten te consolideren en vertrouwen op te bouwen. Erop toezien dat beperkingen op het recht op de vrijheid van meningsuiting uitzonderlijk zijn en dat, op het moment dat er beperkingen opgelegd worden, ze in overeenstemming zijn met de wetten van het internationaal recht, dat wil zeggen dat ze voorzien zijn door de wet evenals nodig zijn voor de bescherming van de rechten of reputatie

van anderen, of van de nationale veiligheid, de openbare orde, de volksgezondheid of de publieke moraliteit, en het proportionaliteitsprincipe respecteren. De staten verbinden zich om erover te waken dat de beperkingen er in de praktijk niet toe dienen om de vrijheid van meningsuiting te onderdrukken. Doeltreffend beschermingsmaatregelen voor de vertrouwelijkheid van persoonlijke gegevens aannemen en toepassen die in overeenstemming zijn met het internationale recht, met inbegrip van de internationale mensenrechten.



**b. Integriteit waarborgen.** De staten onthouden zich om informatieoperaties uit te voeren en te ondersteunen, op het nationale of transnationale niveau, die opzettelijk desinformatie of haatspraak verspreiden. Internettoegang niet afsluiten of beperken. De relevante besluiten van de Veiligheidsraad van de Verenigde Naties respecteren en implementeren, met inbegrip van de besluiten die betrekking hebben tot de bescherming van de vredesoperaties van de Verenigde Naties tegen de risico's op inbreuk van de integriteit van het informatie-ecosysteem, wat een weerslag heeft op de toepassing van het mandaat.



**c. De bevolking beschermen.** De inspanningen herbevestigen en versterken om in het recht en in de praktijk de emancipatie van kwetsbare en gemarginaliseerde groepen die vaak het doelwit worden in informatieruimtes online en offline, zoals vrouwen, personen uit de LGBTQI+-gemeenschap of etnische of religieuze minderheidsgroepen, te garanderen, waarbij rekening wordt gehouden met de specifieke behoeften en rechten van kinderen. De plicht respecteren, op grond van het internationale mensenrecht, om bepaald bij wet propaganda ten gunste van oorlog of haatspraak op nationaal, raciaal of religieus vlak die een aansporing tot discriminatie, vijandigheid of geweld vormt te verbieden.



**d. Toegang tot informatie voorzien.** Een snelle toegang tot openbare informatie, zonder discriminatie – met inbegrip van informatiemedia – in alle talen en onder alle vormen die begrijpelijk en bruikbaar zijn voor iedereen, waarbij de toegang van benadeelde gemeenschappen vooropgesteld wordt. Toegang waarborgen tot betrouwbare en precieze informatie in crisissituaties. Ethische en betrouwbare communicatiepraktijken aannemen om op een proactieve manier de gemeenschappen te betrekken en het vertrouwen in het openbaar bestuur te versterken.



**e. Mediavrijheid verzekeren.** Een vrije, levensvatbare, onafhankelijke en pluralistische mediaomgeving verzekeren, beschermen en ontwikkelen door doeltreffende maatregelen te nemen om journalisten, mediaprofessionals en factcheckers, waarbij een specifieke aandacht besteed wordt aan vrouwen en aan leden van kwetsbare en gemarginaliseerde groepen, te beschermen tegen alle vormen van discriminatie, misbruik, intimidatie en geweldsbedreigingen. In het recht en in de politiek de rechten van de makers van digitale content en van burgerjournalisten respecteren en beschermen.



**f. Onderzoekers en maatschappelijke organisaties beschermen.** Bescherm academici en de burgermaatschappij tegen intimidatie, pesterijen of vergelding, met inachtneming van de academische vrijheid.



**g. Transparantie verzekeren.** Verzeker een volledige transparantie wat betreft de gegevensvereisten – en verzoeken die worden opgelegd aan technologiebedrijven en mediaorganisaties. Neem maatregelen ter bestrijding van niet-transparante en misleidende lobbytactieken en belangenconflicten tussen technologiebedrijven en beleidsmakers die de integriteit van informatie ondermijnen, zoals onethische wervingspraktijken en financiële prikkels.



**h. Wereldwijde solidariteit, opleiding en ontwikkelingshulp versterken.** Zich vooral in ontwikkelingslanden inzetten voor grensoverschrijdende samenwerkingsverbanden en partnerschappen ter ondersteuning van opleiding om de informatie-integriteit te versterken en de weerbaarheid tegen risico's voor informatieruimten te vergroten. Wijs op transparante wijze financiële middelen toe voor opleiding en opleiding voor digitale, informatie – en mediageletterdheid. Bied bewustmakingsprogramma's aan met inbegrip van AI-technologieën in alle talen. Steun ontwikkelingslanden via nationale inspanningen om maatschappelijke veerkracht op te bouwen tegen de risico's voor de integriteit van het informatie-ecosysteem door het verstrekken van degelijke opleidingen in media – en informatievaardigheden en ondersteunen van media van openbaar belang, onder meer door gerichte en passende ontwikkelingshulp. Bied steun aan het werk van openbare instellingen, waaronder bibliotheken, om zo toegang tot alfabetiseringstraining-en middelen te verbeteren.



**i. Politieke deelname promoten.** Bescherm de toegang van alle belanghebbenden bij de verkiezingen tot nauwkeurige en tijdige informatie gedurende het verkiezingsproces. Neem maatregelen om inclusieve en politieke participatie en leiderschap te bevorderen. Bescherm de vrouwenrechten in het openbare leven tegen alle vormen van discriminatie, misbruik, intimidatie en bedreiging met geweld.



**j. Prioriteit verlenen aan inclusief en maatschappelijk relevant onderzoek.** Geef in het licht van de opkomende en nog onbekende mogelijkheden en gevolgen van AI-technologieën prioriteit aan, investeer in en ondersteun onafhankelijk onderzoek. Bij dergelijk onderzoek worden de ethische normen en het onderzoek in alle disciplines met informatie-integriteit in acht genomen. Ondersteun onderzoek op verschillende geografische, taal- en themagebieden, inclusief de potentiële impact van risico's voor de integriteit van het informatie-ecosysteem op Duurzame Ontwikkelingsdoelstellingen. Focus hierbij in het bijzonder op onvoldoende bestudeerde en risicovolle contexten en gemeenschappen. Bevorder en publiceer open toegang tot onderzoeksresultaten om een eerlijke uitwisseling van informatie binnen en tussen landen mogelijk te maken.



**k. Alfabetisering bevorderen.** Door digitale vaardigheden van jongs af aan naadloos te integreren in formele en informele onderwijsprogramma's, worden kritische en geïnformeerde discussies door gerichte acties op vlak van media- en informatievaardigheden aangemoedigd. Bevorder actief het begrip en de bewustmaking van het publiek rond onlinerechten, de werking

van digitale informatieomgevingen en het gebruik van persoonsgegevens, waarbij er rekening gehouden wordt met de specifieke sociale, culturele en taalkundige behoeften van mensen van alle leeftijden en achtergronden. Prioriteer de alfabetiseringsbehoeften van individuen en groepen in kwetsbare en gemarginaliseerde situaties, waaronder vrouwen, kinderen, jongeren, ouderen, mindervalide mensen en miljarden mensen die binnenkort toegang zullen krijgen tot digitale verbindingen. Lever alfabetiseringsinspanningen rond specifieke kwesties die in verband staan met AI-technologieën en die voortdurend worden aangepast aan nieuwe en opkomende technologieën en uitdagingen.



**I. Kinderen, ouders, voogden en opvoeders een verantwoordelijkheidsgevoel geven.**

Verstrek duurzame hulpmiddelen aan kinderen, ouders, voogden en opvoeders over veilig en verantwoordelijk digitaal gedrag, navigeren in online media en kennis van de rechten van kinderen op vrijheid van meningsuiting en informatie. Betrek alle partijen bij de ontwikkeling van richtlijnen en initiatieven op het gebied van media en digitale geletterdheid voor een veiligere online-ervaring en maak tegelijkertijd gebruik van de digitale kennis van jongeren.



## AANBEVELINGEN VOOR ALLE POLITIEKE ACTOREN

Personen, groepen en entiteiten die betrokken zijn bij en invloed uitoefenen op politieke processen.

**a. Integriteit van de verkiezingen behouden** Blijf weg van informatie-aantasting en maak publiekelijk melding van pogingen om de informatie-integriteit aan te tasten, met name met betrekking tot de kiesgerechtigheid, de stemming, de stemmentelling en de resultaten.

**b. Inclusie beschermen.** Publicly dMaak publiekelijk melding van misbruik en intimidatie van kandidaten en functionarissen, vooral vrouwen en leden van kwetsbare en gemarginaliseerde groepen, en neem maatregelen om dergelijk misbruik te verhelpen.

**C. Transparantie aanbieden.** Wees transparant tijdens de communicatie, inclusief over de financieringsbronnen van advertenties en het gebruik van datagestuurde doelgerichtheidstechnieken.

# De Verenigde Naties

De wereldwijde principes voor de informatie-integriteit zijn van toepassing op de Verenigde Naties en hun internationale ambtenaren. Door die internationale principes na te leven, geven de VN een krachtig voorbeeld van verantwoord beheer van informatie-integriteit binnen de wereldbevolking. Door hun inspanningen te

intensiveren om de integriteit van het informatiesysteem te versterken, dragen ze bij aan de missie van de VN: vrede waarborgen, duurzame ontwikkeling bevorderen en mensenrechten voor iedereen beschermen en bevorderen.

## De Verenigde Naties zullen



**a. Meer inspanningen leveren.** Inspanningen opvoeren om de informatie-integriteit te versterken, onder meer door specifiek contextonderzoek, opvolging, risicobeoordeling, gemeenschapsbetrokkenheid en samenwerkingsverbanden opzetten in verschillende contexten en talen. Daarnaast zal informatie-integriteit worden geïntegreerd in programma's en transacties, zodat preventie, beperking en respons verbeteren en nieuwe kansen en uitdagingen sneller worden geïdentificeerd.



**b. Opleidingsinitiatieven ondersteunen.** Staten helpen om hun opleidingen te versterken door initiatieven voor vaardigheidsontwikkeling te stimuleren, waaronder opleidingen voor jongeren. Daarbij wordt speciale aandacht besteed aan de behoeften van ontwikkelingslanden, met als doel de informatie-integriteit te versterken.



**c. Bewustwordingsactiviteiten uitvoeren.** Zowel wereldwijd als op lokaal niveau de internationale principes actief ondersteunen en verdedigen. Daarbij wordt bijzondere aandacht besteed aan kwetsbare en gemarginaliseerde groepen. De VN dragen bij aan sociale cohesie en versterken de veerkracht van gemeenschappen tegen bedreigingen voor informatie-integriteit, door inspanningen te ondersteunen om de Duurzame Ontwikkelingsdoelstellingen te bereiken.



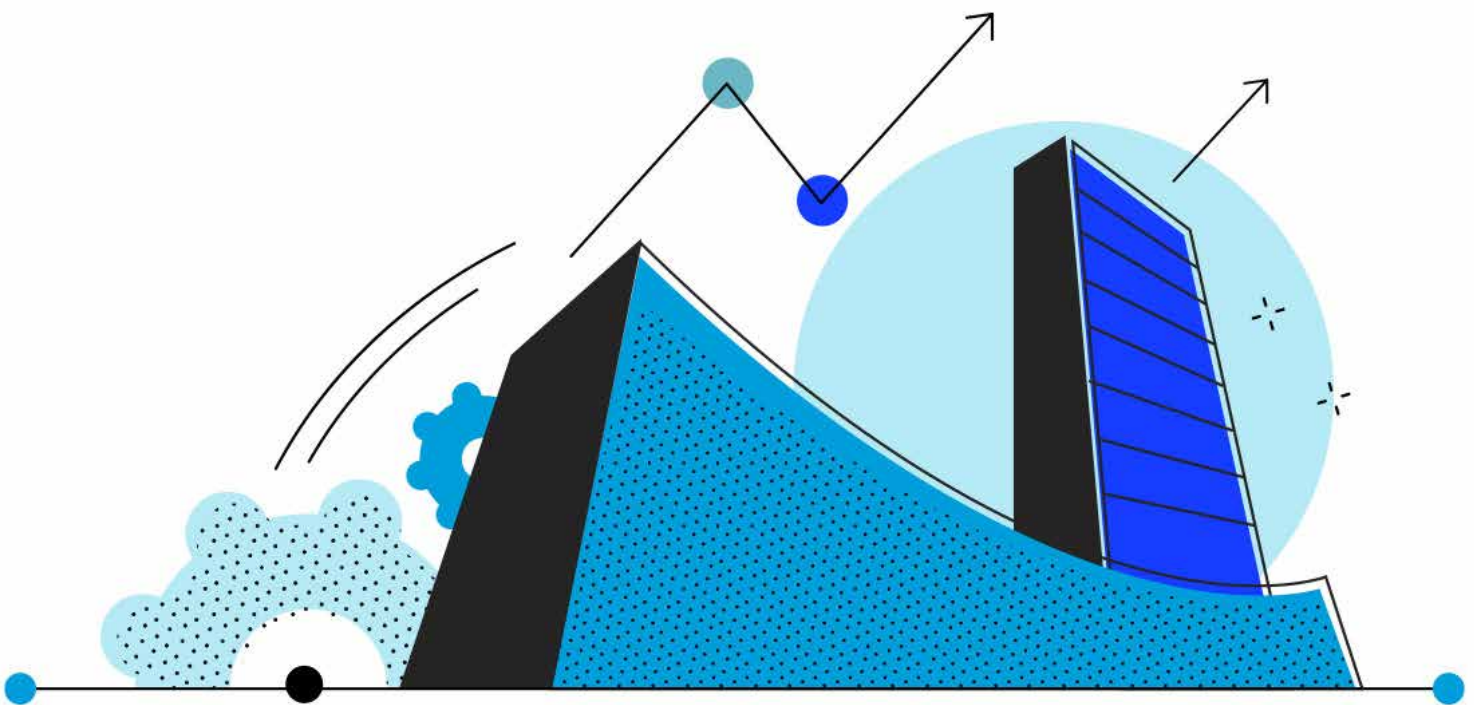
**d. Toegewijde expertise vergroten.** Er zal binnen het VN-Secretariaat een centrale eenheid worden opgericht om innovatieve en genuanceerde strategieën te ontwikkelen tegen bedreigingen voor de informatie-integriteit, zodat de uitvoering van het VN-mandaat en kernprioriteiten gewaarborgd blijft. Dat gebeurt in nauwe samenwerking met bestaande structuren en ten dienste van het gehele VN-systeem.



**e. Flexibele communicatiestrategieën ontwikkelen.** Innovatieve, op feiten gebaseerde en wendbare communicatiestrategieën benutten, zowel online als offline, om het algemeen belang te ondersteunen en beter in te spelen op de behoeften van alle mensen die de Verenigde Naties dienen.

**f. Meertalige hulpmiddelen beschikbaar stellen.** Een online meertalig kenniscentrum opzetten over informatiebetrouwbaarheid. Dat platform zal onderzoek, richtlijnen en best practices bevatten die toepasbaar zijn in verschillende contexten, ter ondersteuning van initiatieven op internationaal, regionaal en nationaal niveau.

**g. Multi-stakeholderactieplannen ondersteunen.** Regionale en nationale plannen voor actie door meerdere belanghebbenden en samenwerkingsverbanden ondersteunen, waarbij gebruik wordt gemaakt van bestaande mechanismen en de eigen expertise in opleiding en internationale coördinatie.



# Volgende stappen

Het kan niet genoeg worden benadrukt hoe dringend de versterking van de informatie-integriteit is, gezien de toenemende risico's voor de integriteit van het informatie-ecosysteem en de snelle opkomst van toegankelijke ontwikkelingen in AI-technologieën. De internationale principes bieden een holistisch en verenigd actieplan

om de informatie-integriteit te beschermen en te bevorderen, terwijl de wereld zich door de complexiteit van het digitale tijdperk navigeert en op zoek is naar multilaterale oplossingen tijdens de Top van de Toekomst.

## Om dat te bereiken, worden belanghebbenden verzocht om:

- ✓ Zich **publiekelijk** in te zetten, de internationale principes van de Verenigde Naties voor informatie-integriteit **goed te keuren en actief te bevorderen** als een plan voor onmiddellijke actie.
- ✓ De internationale principes te gebruiken om deel te nemen en bij te dragen aan **brede intersectorale coalities over informatie-integriteit**, waarbij verschillende vaardigheden en benaderingen worden samengebracht, inclusief opleiding, betrokkenheid van de samenleving, universiteiten, media, overheden en de internationale privésector, en ervoor te zorgen dat jongeren volledig en betekenisvol betrokken worden, bijvoorbeeld via jeugdadviesgroepen.
- ✓ Samen te werken aan de ontwikkeling van **plannen** op regionaal, nationaal en lokaal niveau, door gemeenschappen te betrekken bij de ondersteuning van lokale initiatieven en daaruit te leren, en ervoor te zorgen dat jongeren zich volledig en betekenisvol inzetten.

Door de Internationale principes van de Verenigde Naties voor informatie-integriteit toe te passen, kunnen belanghebbenden uit alle sectoren solidariteit tonen en gezamenlijk een pad creëren naar een vernieuwd informatie-ecosysteem dat vertrouwen, kennis en individuele keuzevrijheid voor iedereen bevordert.

# Bijlage

## BRONNEN

1. United Nations Secretary-General's "Our Common Agenda policy brief 8: information integrity on digital platforms" (2023)

<https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-information-integrity-en.pdf>

2. UNESCO Guidelines for the Governance of Digital Platforms (2023)

<https://www.unesco.org/en/internet-trust/guidelines>

3. Report of the Secretary-General, "Countering disinformation for the promotion and protection of human rights and fundamental freedoms", 2022 (A/77/287)

[https://digitallibrary.un.org/record/3987886?ln=en&v=pdf&\\_gl=1\\*15snwt9\\*\\_ga\\*MTk3NzE0MjlyOC4xNzlwNjYzNzg1\\*\\_ga\\_TK9BQL5X7Z\\*MTcyMDcxMzU1Ny4yLjEuMTcyMDcxMzc3OC4wLjAuMA..](https://digitallibrary.un.org/record/3987886?ln=en&v=pdf&_gl=1*15snwt9*_ga*MTk3NzE0MjlyOC4xNzlwNjYzNzg1*_ga_TK9BQL5X7Z*MTcyMDcxMzU1Ny4yLjEuMTcyMDcxMzc3OC4wLjAuMA..)

4. UNESCO Recommendation on the Ethics of Artificial Intelligence (2021)

<https://unesdoc.unesco.org/ark:/48223/pf0000381137>

5. United Nations Strategy and Plan of Action on Hate Speech (2019)

[https://www.un.org/en/genocideprevention/documents/advising-and-mobilizing/Action\\_plan\\_on\\_hate\\_speech\\_EN.pdf](https://www.un.org/en/genocideprevention/documents/advising-and-mobilizing/Action_plan_on_hate_speech_EN.pdf)

6. Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (2012)

<https://www.ohchr.org/en/documents/outcome-documents/rabat-plan-action>

7. Guiding Principles on Business and Human Rights (2011)

[https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinessshr\\_en.pdf](https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinessshr_en.pdf)