

De opmars van manipulatie en hyperpersonalisatie

Maak digitale grondrechtenbescherming toekomstbestendig



Bericht aan het parlement

Op 18 maart 2025 spreekt de commissie Digitale Zaken over de bescherming van persoonsgegevens en andere digitale grondrechten. Opkomende technologieën zoals generatieve AI, immersieve technologie en neurotechnologie, zetten grondrechten onder druk. Hyperpersonalisatie en manipulatie zijn twee belangrijke trends rondom deze opkomende technologieën. Er zal meer nodig zijn dan het huidige – voorgenomen – beleid om de bescherming van grondrechten toekomstbestendig te maken. Uw Kamer kan dit helpen vormgeven. Het Rathenau Instituut geeft hiervoor zes handelingsopties.

1. **Versterk de kennispositie van bestuur en parlement**
2. **Versterk de informatiepositie van gebruikers van opkomende technologieën**
3. **Versterk de AVG om intieme gegevens beter te beschermen**
4. **Creëer de mogelijkheid om XR in de publieke ruimte te reguleren**
5. **Garandeer dat schadelijke GAI- en XR-toepassingen van de markt kunnen worden gehaald in de AI-verordening**
6. **Waarborg sterk toezicht**

Hieronder vindt u een nadere toelichting op bovengenoemde trends en handelingsopties.

Inleiding: trends in opkomende technologieën - hyperpersonalisatie en manipulatie

Generatieve AI (GAI) en immersieve technologieën (ofwel *extended reality* (XR) waaronder *virtual reality* (VR) en *augmented reality* (AR) ontwikkelen zich razendsnel. De technologieën worden steeds vaker gecombineerd. Met elkaar, en met andere technologieën zoals *brain computer interfaces* (BCI). Daarmee ontstaan omgevingen – online en offline – die steeds verder te personaliseren en te manipuleren zijn.

- **Hyperpersonalisatie**

Bij XR worden data uit handbewegingen, pupilreflexen en in de toekomst mogelijk ook breinactiviteit gebruikt om de VR- of AR-ervaring af te stemmen op de gebruiker en de fysieke omgeving. De gegevens kunnen ook gebruikt worden om persoonlijke gevoelens, kenmerken en voorkeuren af te leiden. Deze gegevens vallen niet automatisch onder de categorieën bijzondere persoonsgegevens van de Algemene Verordening Gegevensbescherming. Verder is de verwachting dat GAI steeds meer verschillende typen databronnen zal combineren. Daarmee is intieme informatie te achterhalen over individuen (zoals dit model dat 'door muren heen kon kijken'). Zo maken GAI en XR *online tracking* van individuen makkelijker, invasiever en intiemer. Dit brengt zorgen mee over privacyschending, massasurveillance en discriminatie, zoals benadrukt wordt in de petitie die de Privacy Collective begin 2024 aanbood aan de Kamer. Dit komt omdat online tracking kan leiden tot *hyperpersonalisatie*, waarbij zowel de fysieke als virtuele omgeving, als de informatie die we tot ons krijgen, vergaand op de gebruiker wordt afgestemd. Momenteel doet het Rathenau Instituut op verzoek van de commissie Digitale Zaken nader onderzoek naar online tracking.

- **Manipulatie**

Online tracking en hyperpersonalisatie kunnen bijvoorbeeld ingezet worden om consumenten of kiezers te verleiden tot bepaald koop- of stemgedrag, via gerichte (politieke) advertenties op basis van gebruikersprofielen. XR kan het gedrag en de emoties van gebruikers onbewust beïnvloeden omdat het kan zorgen voor sterke sensorische illusies. GAI kan eenvoudig iemands stem, beeltenis of werkstijl nabootsen, tot een niet-onderscheidbare imitatie. Hierdoor

verschijnen meer *deep fakes*, van *deep nudes* en 'wraakporno', tot aan gemanipuleerde politieke filmpjes. Nep en echt zijn zo steeds lastiger te onderscheiden. Daarmee kan onze gedeelde werkelijkheid in gevaar komen. En dat kan op zijn beurt de democratie onder druk zetten.

Digitale manipulaties worden ook gebruikt om overleden personen te imiteren. Het doel is betere rouwverwerking, maar wetenschappers voorspellen het ontstaan van '*death capitalism*', waarin de dood een digitaal product gaat worden en controle over je virtuele identiteit steeds lastiger te behouden is.

GAI en XR kunnen individuele grondrechten als zelfbeschikking, (mentale) privacy en non-discriminatie onder druk zetten. Evenals collectieve waarden en rechten verbonden aan duurzaamheid en democratie. Zie de Rathenau Scans Immersieve technologie en Generatieve AI voor een overzicht.

Het is daarom zaak dat het parlement bespreekt hoe deze grondrechten en publieke waarden ook richting de toekomst voldoende beschermd kunnen worden. We geven daarvoor zes suggesties.

Handelingsopties

1. Versterk de kennispositie van bestuur en parlement

Nieuwe technologische toepassingen kunnen diep ingrijpen in onze economie, democratie en maatschappij. Zowel bij bestuur als parlement is er daarom behoefte aan kennis over opkomende technologieën en hoe deze onze samenleving kunnen raken. Het Rathenau Instituut heeft de wettelijke taak het parlement van informatie en duiding te voorzien over (opkomende) technologieën en heeft hier ook jarenlange ervaring mee¹. **Het Rathenau Instituut denkt graag met u mee over hoe wij, ook op nieuwe manieren, uw Kamer kunnen informeren en kennis kunnen ontsluiten.**

2. Versterk de informatiepositie van gebruikers

Het is voor gebruikers van GAI en XR haast onmogelijk om bewust, specifiek en geïnformeerd toestemming te geven. Enerzijds omdat het lastig is te weten welke gevoelige informatie af te leiden is uit onbewust gedrag zoals pupilreflexen, bijvoorbeeld over fysieke aandoeningen of seksuele voorkeuren. Anderzijds omdat gebruikers weinig tot geen controle hebben over de te verwerken gegevens, zoals hun hartslag of pupilreflex. Bij GAI geven gebruikers via prompts veel verschillende soorten informatie mee aan het systeem, vaak zonder zich daar bewust van te zijn. Bescherming van privacy en autonomie begint daarom bij voorlichting aan consumenten over de informatie die zij 'weggeven':

- Licht consumenten voor over de informatie die XR en GAI verzamelen, wat daaruit af te leiden is, en hoe dit kan worden gebruikt om hen te beïnvloeden.

¹ Naast onze concrete aanbevelingen in de Berichten aan het parlement, nemen wij deel aan rondetafelgesprekken, geven we technische briefings, verstrekken we onafhankelijke informatie aan kennispartners en fractieondersteuning binnen het parlement, en voeren we zowel korte- als meer langdurige onderzoekstrajecten uit. Zie bijvoorbeeld ook ons AI- traject voor de Eerste Kamer.

Dit kan door het dataverkeer tussen VR-brillen en afgeleide gegevens door GAI-systemen onafhankelijk te (laten) onderzoeken, en consumenten over de uitkomsten in te lichten. **Kamerleden kunnen het ministerie van Binnenlandse Zaken en Koninkrijksrelaties hiernaar vragen.**

- Daarnaast is het zaak aanbieders aan hun verplichtingen te houden als het gaat om de informatievoorziening aan en toestemmingsverlening door consumenten. **Kamerleden kunnen de Autoriteit Persoonsgegevens hierop wijzen.**

3. Versterk de AVG om intieme gegevens beter te beschermen

Maar betere informatievoorziening alleen is niet voldoende. Een sterk wettelijk kader is nodig om privacy en autonomie van gebruikers te beschermen. De AVG, AI-verordening, en Digitaledienstenverordening (DDV) reguleren gegevensverwerking. Maar de risico's voor beïnvloeding en misleiding zijn dusdanig dat het Rathenau Instituut de noodzaak ziet om de AVG meer aan te scherpen dan nu gebeurt.

Overweeg:

- Een verruiming van het begrip '**biometrische gegevens**' in de AVG, door de verwerking van fysieke, fysiologische of gedragsgegevens niet afhankelijk te maken van het verwerkingsdoel identificatie of verificatie (zoals andere categorieën bijzondere persoonsgegevens ook niet aan een specifiek verwerkingsdoel gekoppeld zijn). De Europese wetgever lijkt in de AI-verordening de nauwe definitie in de AVG te erkennen, en biedt aanvullende bescherming voor slechts enkele specifieke biometrische toepassingen, zoals emotieherkenning in de klas of op de werkvloer. Maar daarmee zijn niet alle risicovolle verwerkingen van fysieke, fysiologische en gedragsgegevens gedekt. Een verruiming op dit punt past bij strategie 2 die wordt geschetst in het WODC-onderzoek om het wettelijk kader beter te laten aansluiten op technologische veranderingen. **Kamerleden kunnen bewindspersonen vragen deze verruiming van de AVG op de Europese agenda te zetten.**
- Aanvullende verboden in de AVG op de verwerking van bepaalde type data (zoals pupilreflexen en neurodata - ook dit punt past binnen strategie 2 in het WODC-onderzoek). **Kamerleden kunnen er bij bewindspersonen op aandringen dit op de Europese agenda te zetten.**
- Een actieve handhaving van de verplichte 'voorafgaande raadpleging' in de AVG voor risicovolle verwerkingen. **Kamerleden kunnen de Autoriteit Persoonsgegevens hiernaar vragen.**
- De invoering van een **datacodicil** om de persoonsgegevens van overleden personen beter te beschermen. In een datacodicil geven individuen aan hoe zij willen dat hun data na hun dood mogen worden gebruikt. De AVG beschermt doorgaans niet de persoonsgegevens van overleden personen. **De Kamer kan de minister vragen om dit op de Europese agenda te zetten.**

- Actieve deelname van Nederland aan het internationale debat over neurorechten om het recht op vrijheid van gedachte te borgen. **De Kamer kan hier bij de minister op aandringen.**

4. Creëer de mogelijkheid om XR in de publieke ruimte te reguleren

Hyperpersonalisatie kan ertoe leiden dat iedereen de fysieke en virtuele omgeving anders waarneemt en gebruikt, waardoor de gezamenlijke realiteitsbeleving onder druk komt te staan.

Overweeg:

- **Een verbod op het gebruik van XR in bepaalde publieke ruimtes**, zodat we publieke ruimtes op een gedeelde manier blijven waarnemen en gebruiken.
- **Het instellen van een AR-me-niet-register**, om de privacy, zelfbeschikking en veiligheid van niet-gebruikers te beschermen en overlast te voorkomen.

5. Garandeer dat schadelijke GAI- en XR-toepassingen van de markt kunnen worden gehaald in de AI-verordening

Hoewel de AI-verordening een belangrijk middel is om grond- en mensenrechten beter te beschermen, zullen niet alle risicovolle GAI- en XR-systemen gedekt worden. Bij sommige categorieën uit de wet is nog onduidelijk welke gevallen er precies wel en niet onder vallen. Ook leven er nog veel vragen over hoe de mensenrechtelijke normen via standaarden invulling zullen krijgen.

Daarom:

- **Blijf als parlement betrokken bij de concrete invulling van de mensenrechtelijke normen** van de AI-verordening, onder andere om bescherming van het non-discriminatiebeginsel te garanderen;
- **Monitor en evalueer als Kamer of aanscherpingen voor risicovolle toepassingen nodig zijn**, zoals een verplichte 'voorafgaande raadpleging' bij de toezichthouder (zoals in de AVG), jaarlijkse onafhankelijke beoordelingen en notice-and-action-mechanismes voor gebruikers, of een vergunningsstelsel.

6. Waarborg sterk toezicht

De AI-verordening, Digitaledienstenverordening en de Digitale Markten verordening betekenen nieuwe taken voor toezichthouders. De taak- en rolverdeling tussen de verschillende toezichthouders moet nog nader worden uitgewerkt. Zo is het niet altijd duidelijk onder welke toezichthouder een bepaalde XR-toepassing valt: dit is afhankelijk van het type dienst, de soort data, de opslaglocatie en de verwerkingswijze.

Toezichthouders zijn nog bezig expertise op te bouwen om deze elementen te beoordelen. Naar verwachting zullen het grote aantal AI-aanbieders op de markt, en de vereiste coördinatie tussen toezichtsvelden (gegevensbescherming, marktregulering, productregulering, etc.) leiden tot een aanzienlijke verzwaring van de handhavingslast.

- **Zorg voor voldoende expertise en middelen van toezichthouders**, en zie als parlement toe op hoe de samenwerking en coördinatie wordt ingevuld.

Gerelateerde publicaties

De onderstaande Rathenau-publicaties geven een uitgebreidere omschrijving van de werking, kansen en risico's van opkomende technologieën, en bieden aanvullende handelingsopties:

<u>Neurotechnologie</u>	Rathenau Scan	(2025)
<u>Generatieve AI</u>	Rathenau Scan	(2023)
<u>Immersieve Technologie</u>	Rathenau Scan	(2023)
<u>Tackling deep fakes in European policy</u>	Onderzoek STOA	(2021)
<u>Stel 10 ontwerpeisen voor de digitale samenleving van morgen</u>		
Rathenau Instituut, Manifest		(2020)

Verwacht

Online tracking	Rapport	maart 2025
-----------------	---------	------------
