AUTORITEIT
PERSOONSGEGEVENS

Bouwen aan de waardengedreven inzet van AI-systemen: uitdagingen voor beleid, toezicht en regelgeving

Artificiële intelligentie (AI) dringt in rap tempo de samenleving binnen. De economische en maatschappelijke belofte is groot. Recente oproepen vanuit het Europese bedrijfsleven en discussies over het Europese concurrentievermogen benadrukken het belang van AI-innovaties. Tegelijkertijd is Nederland al meerdere keren geconfronteerd met de risico's van AI en algoritmes voor de grondrechten van mensen. En veel AI en algoritmes die onderzocht worden vertonen tekortkomingen. Denk aan de beheersing van discriminatierisico's. Kortom, AI biedt grote kansen maar het kan ook goed misgaan. De Autoriteit Persoonsgegevens (AP) maakt zich daarom sterk voor een samenleving waarin we profiteren van AI-innovaties en tegelijkertijd grondrechten gewaarborgd zijn.

In dit position paper zetten we tien acties uiteen om de waardengedreven inzet van AI in Nederland mogelijk te maken. Volksvertegenwoordigers, de overheid en toezichthouders hebben een belangrijke rol om deze te realiseren. Het toezicht op AI en algoritmes is daarbij nog volop in ontwikkeling. De AP neemt het voortouw als coördinerend toezichthouder op algoritmes en AI, in nauwe samenwerking met andere digitale toezichthouders. De bijlage van dit position paper geeft een overzicht van ontwikkelingen op het gebied van AI- en algoritmetoezicht.

AI brengt grote maatschappelijke veranderingen, daarop moeten we ons voorbereiden, juist ook om grondrechten en fundamentele waarden te beschermen

Beleid

1 Stel een Nationaal Deltaplan voor algoritmes en AI op.

Hiertoe heeft de AP eerder al een oproep gedaan, inclusief aanzet voor vijf pijlers die het fundament kunnen vormen (menselijke regie, veilige applicaties en systemen, organisaties in control, sterk nationaal ecosysteem en infrastructuur, internationale standaarden en samenwerking). Een langetermijnvisie is nodig om economische kansen te verzilveren en tegelijkertijd grondrechten en fundamentele waarden te beschermen. Dat gaat verder dan alleen toezicht. Overheid, bedrijven en burgers hebben allemaal een rol.

OKTOBER 2024

2 Breng de kennis van AI in de Nederlandse samenleving op peil.

De verantwoorde inzet van AI lukt alleen als iedereen in Nederland – van jong tot oud – basiskennis heeft van de werking (en beperkingen) van AI-systemen.

3 Maak als organisatie op een gepaste wijze gebruik van AI en hou rekening met algoritmevervorming.

AI is geen wondermiddel; bedenk dus van tevoren goed waarom AI voor een probleem de gepaste oplossing is. Pas ook op voor algoritmevervorming: de onvoorziene gevolgen van de interactie tussen systeem en omgeving. Zo hebben mensen in onze digitale wereld een grote verantwoordelijkheid gekregen om zelf gegevens correct aan te leveren, maar hierin is niet iedereen even bekwaam. De keuze voor een algoritme is nooit neutraal.

AI is een systeemtechnologie en brengt veel innovaties mee, een goede aansluiting op het toezicht kan dit in goede banen leiden

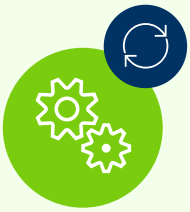
Toezicht en innovatie

4 Investeer in het ecosysteem voor duurzame AI-innovaties en het opzetten van effectieve testomgevingen.

De AI-verordening voorziet in het opzetten van testomgevingen om nieuwe AI-systemen te ontwikkelen, bijvoorbeeld voor start-ups of het mkb. De AP werkt samen met andere toezichthouders aan een pilot voor een regulatory sandbox waarin AI-ontwikkelaars geholpen worden met compliance vraagstukken rondom innovatieve AI-toepassingen. Om bedrijven én toezichthouders daadwerkelijk te helpen met een dergelijke sandbox moet geïnvesteerd worden in de opvolging van de pilotfase met een volwaardige testomgeving.

5 Zorg dat AI-toezichthouders op nationaal niveau goed kunnen samenwerken en op Europees niveau goed kunnen meepraten over AI-regulering en AI-toezicht.

De AI-verordening raakt vele sectoren en aandachtsgebieden. Op AI-terrein is de samenwerking en wisselwerking tussen toezichthouders met sectorspecifieke- en horizontale toezichtsdomeinen cruciaal. De adviezen van de AP en de RDI over inrichting van het AI-toezicht geven hiertoe richting. Op Europees gebied komt de coördinatie van toezicht en uitleg van de regelgeving samen in de AI Board. Zodra nationale AI-toezichthouders zijn aangewezen, is het belangrijk dat zij op Europees niveau in gezamenlijkheid hun rol pakken om ten behoeve van toezicht te werken aan uniforme uitleg en uitvoering. Daarmee ontstaat zekerheid, zowel voor mensen als voor organisaties.



Transparantie-eisen en heldere normen zijn de basis voor risicobeheersing en vertrouwen in AI

Regelgeving en normering

6 Maak de registratie van impactvolle algoritmes en AI-systemen verplicht, ook voor semi-publieke organisaties.

Verplichte registratie in het algoritmeregister vergroot het zicht op de inzet van (hoog-risico) algoritmes en AI in de publieke dienstverlening en draagt bij aan bewustwording en transparantie binnen de eigen organisatie en richting mensen. Het voorstel in het regeerprogramma voor een wet voor transparante algoritmes is een mogelijk middel om deze verplichting te realiseren. Ook semi-publieke organisaties zouden bij deze registratieplicht meegenomen moeten worden, denk aan woningcoöperaties die AI gebruiken om woonfraude op te sporen. Ook bij andere organisaties kan algoritmeregistratie gestimuleerd worden.

7 Streef naar duidelijkheid in de normering van AI-systemen.

De AP signaleert het risico op een wildgroei van kaders en normen voor algoritmes en AI. Hierdoor kunnen ontwikkelaars door de bomen het bos niet meer zien en kan er selectief gebruik worden gemaakt van kaders. De AP spant zich vanuit haar coördinerende rol in voor duidelijke standaarden die zorgen voor een hoog beschermingsniveau van grondrechten, maar die ook proportioneel en werkbaar zijn voor organisaties.

Sterke governance en periodieke audits zorgen niet alleen dat AI op een veilige en beheerste manier ingezet kan worden, maar ook dat grondrechtenschendingen zoals discriminatie of willekeur sneller gesignaleerd en aangepakt kunnen worden

Governance en risicobeheersing

8 Stimuleer (overheids)organisaties om voldoende financiële en personele capaciteit te reserveren voor de beheersing van AI-systemen.

Verantwoorde inzet van AI vereist eerst flinke investeringen in de beheersinfrastructuur en voldoende goed opgeleid personeel. AI-geletterdheid is ook een vereiste in de AI-verordening. Wees hierbij bewust van de AI-paradox: de veelal beoogde efficiëntieslagen en kostenbesparingen vragen gelijktijdig om forse investeringen vooraf om risico's te beheersen.

9 Voer periodieke audits van AI-systemen uit en hanteer hierbij stevige en concrete standaarden.

Met periodieke audits kunnen risico's (zoals discriminatie) tijdig worden opgespoord. Standaarden zijn een belangrijk hulpmiddel voor organisaties als het gaat om risicobeheersing.

10 Stel duidelijke eisen aan de governance van AI-systemen binnen organisaties.

Het is van groot belang dat binnen organisaties duidelijk is wie verantwoordelijk is voor de inzet van AI-systemen. Het opstellen van een AI-strategie of het aanstellen van een AI-officer kan hierbij helpen. Hiertoe kan bijvoorbeeld binnen de overheid gedacht worden aan stelselafspraken.

Bijlage: stand van zaken in het toezicht op AI

Wat doet de AP als coördinerend toezichthouder op algoritmes en AI?

De AP heeft sinds januari 2023 de taak om overkoepelend toezicht te houden op de inzet van algoritmes en AI. Hiervoor is binnen de AP de Directie Coördinatie Algoritmes (DCA) opgericht. Deze directie van de AP brengt overkoepelende risico's en effecten van algoritmes en AI-systemen in kaart en levert hiermee een bijdrage aan de bescherming van grondrechten en fundamentele waarden. Hiervoor wordt naar meer gekeken dan alleen de bescherming van persoonsgegevens. Bijzondere aandacht is er voor non-discriminatie, het tegengaan van willekeur, het bevorderen van transparantie en het voorkomen van manipulatie en misleiding.

Als nieuwe (sectoroverstijgende) systeemtechnologie vraagt het toezicht op AI om een overkoepelende blik en nauwe samenwerking met andere toezichthouders. Het bestaande toezicht richt zich in de meeste gevallen op sectoren, toepassingen of specifieke rechtsgebieden. Samenwerking en het signaleren van overkoepelende risico's zijn daarom essentieel. Zo kunnen grondrechten optimaal beschermd worden en kan verantwoorde innovatie worden gestimuleerd.

De sectoroverstijgende impact van AI vraagt daarnaast om een overkoepelende beleidsreactie. Mede hierom pleit de AP voor het opstellen van een Nationaal Deltaplan AI.

Om zicht te krijgen op de overkoepelende risico's signaleert en agendeert de AP de incidenten en risico's van AI en algoritmes. De AP werkt intensief samen met andere toezichthouders rondom o.a. standaarden, verboden AI, AI-geletterdheid en organiseert consultaties om de maatschappij te betrekken bij het toezicht op AI-systemen. Daarnaast heeft de AP een coördinerende rol in het opbouwen en inrichten van AI-regelgeving en AI-toezicht. Om risico's van AI en algoritmes in beeld te brengen, publiceert de AP twee keer per jaar de Rapportage AI en Algoritmerisico's Nederland (RAN).

Over inhoudelijke- en samenwerkingsvraagstukken vindt structureel overleg plaats in de Algoritme & AI-Kamer (AAK) van het Samenwerkingsplatform Digitale Toezichthouders (SDT). In de SDT-AAK zijn de toezichthouders op het gebied van algoritmes en AI samengebracht. Sinds de start in mei 2023 is de SDT-AAK tien keer bij elkaar gekomen.

Welke huidige risico's ziet de AP bij de inzet van AI in Nederland?

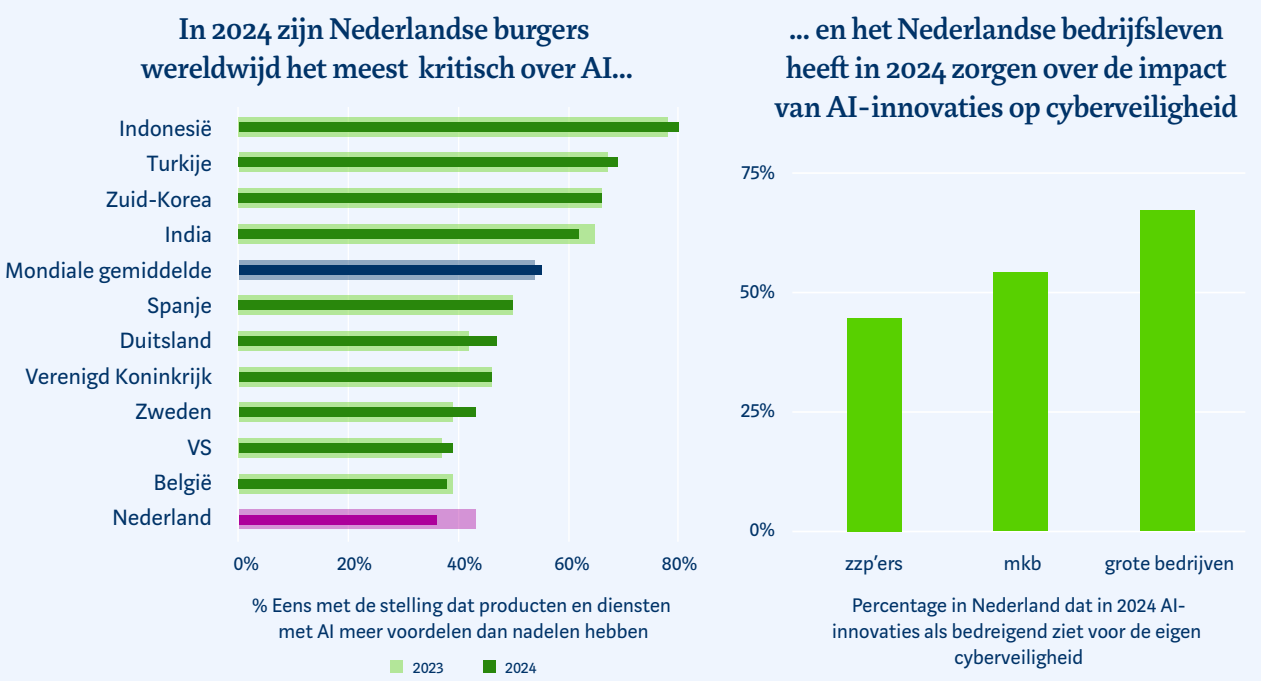
Het opzetten van AI-regulering en het beheersen van risico's gaat niet in hetzelfde tempo als de stormachtige ontwikkeling van AI. Hierover rapporteerde de AP afgelopen zomer in haar derde RAN. De concurrentiestrijd om nieuwe AI-technologie te ontwikkelen, aangewakkerd door de komst van generatieve AI, geeft een prikkel om op grote schaal te experimenteren met nieuwe AI-toepassingen. Zowel qua omvang als qua aard, worden er meer en nieuwe risico's voorzien waarvan de gevolgen nu nog moeilijk in te schatten zijn. Met de komst van de AI-verordening worden daadkrachtige stappen gezet om risico's te beheersen, maar dit is een proces van de lange adem.

Daarbij valt op dat het vertrouwen in AI onder Nederlandse burgers verhoudingsgewijs laag is – het bedrijfsleven maakt zich in toenemende mate zorgen over de impact van AI op cyberveiligheid. Waardengedreven toezicht en het beheersen van risico's kan bijdragen aan het maatschappelijk draagvlak voor de inzet van AI. Op dit moment is slechts 36 procent van de Nederlanders van mening dat producten en diensten met AI meer voordelen dan nadelen hebben.

Daarnaast hebben veel bedrijven (groot en klein) zorgen over de impact van AI-innovaties op de cyberveiligheid (zie figuur 1).

Met oog voor de risico's kunnen de kansen van AI het beste benut worden. De AP ziet dat AI veel kansen met zich meebrengt. Zo is de potentie van AI-innovaties zichtbaar voor het ondersteunen van mensen met een (functie)beperking, zoals automatische spraakherkenning voor doven en slechthorenden. In veel domeinen wordt dan ook geëxperimenteerd met AI om oplossingen te vinden voor (maatschappelijke) problemen. Maar niet allemaal zijn ze zonder risico. Zo zijn sommige adaptieve doorstroomtoetsen voor leerlingen uit groep 8 feitelijk AI-systemen, gebruiken Nederlandse bedrijven beeldherkenningscamera's om gedrag te monitoren en worden AI en scraping gebruikt door woningcorporaties voor de detectie van woonfraude. Het is onduidelijk of er bij deze toepassingen voldoende rekening wordt gehouden met de risico's, terwijl de gevolgen - en hersteloperaties - voor burgers groot kunnen zijn.

FIGUUR 1: PERCEPTIE VAN AI-RISICO'S ONDER NEDERLANDSE BURGERS EN BEDRIJVEN



BRON (LINKS): IPSOS AI MONITOR (N = 23.685, 32 LANDEN)
BRON (RECHTS): ABN AMRO (2024) IN SAMENWERKING MET ONDERZOEKSBUREAU MWM2

Een specifiek aandachtspunt is de democratische controle op de inzet van AI-systemen binnen de overheid. Uit onderzoek van de AP (zie hoofdstuk 3, RAN3) blijkt dat men zich op lokaal niveau vaak onvoldoende bewust is van de risico's van de inzet van AI-systemen voor grondrechten en fundamentele waarden. Daarom is democratische controle op de ontwikkeling en inzet van AI-systemen van groot belang. De AP pleit voor een democratische cyclus van sturing en verantwoording bij het gebruik van AI-systemen in de publieke sector.

Volksvertegenwoordigers spelen hierin een cruciale rol: op lokaal, regionaal en nationaal niveau. Zij hoeven zich niet te laten afschrikken door de technische complexiteit van AI-systemen. De basis begint bij transparantie, objectieve toetsing van AI-systemen voorafgaand aan inzet en regelmatige auditering van AI-systemen en hun compliance met grondrechten en fundamentele waarden. Auditdiensten en rekenkamers spelen daarin een belangrijke rol.

Welke AI-systemen vallen binnen de reikwijdte van de AI-verordening?

De AI-verordening hanteert een brede definitie van een AI-systeem. Ook "simpele" algoritmes kunnen onderdeel zijn van een systeem dat binnen de definitie van de AI-verordening valt. Hierbij is aanpassingsvermogen geen noodzakelijke vereiste. Een doorslaggevend criterium is inferentie: het proces om van input of data output af te leiden, zoals een filmaanbeveling. Dit omvat ook AI-systemen waar het inferentieproces in de bouwfase heeft plaatsgevonden en waarbij het AI-systeem na ingebruikname een niet-adaptief karakter heeft.

Wel maakt de verordening duidelijk dat "eenvoudigere traditionele softwaresystemen of programmeringsbenaderingen [en] regels die uitsluitend door natuurlijke personen zijn vastgesteld om automatische handelingen uit te voeren" buiten de definitie van een AI-systeem vallen. Deze uitleg volgt mede uit de OESO-definitie, waarop de definitie van de AI-verordening is gebaseerd. De Europese Commissie zal met richtsnoeren komen om de praktische toepassing van de definitie verder te verduidelijken.

Wat staat er binnenkort te gebeuren voor de AI-verordening, het toezicht daarop en wat is daarvoor nodig?

FIGUUR 2: DE AI-VERORDENING TREEDT DE KOMENDE JAREN GETRAPT IN WERKING

De AI-verordening vormt een nieuwe basis voor het toezicht op AI en algoritmes, maar niet alle AI-systemen worden aan dezelfde eisen onderworpen. Dit is afhankelijk van de risicocategorie waarbinnen de toepassing valt. De vereisten voor de verschillende categorieën zullen gefaseerd in werking treden (zie figuur). Systemen met een onaanvaardbaar risico zijn verboden, bijvoorbeeld systemen die mensen (onbewust) uitbuiten of manipuleren. Systemen met een hoogrisicotoepassing, zoals die worden ingezet bij werving en selectie of in het onderwijs, moeten voldoen aan strenge eisen. Gedacht kan worden aan risicomanagement (waaronder non-discriminatie), menselijke controle en het bijhouden van documentatie. Systemen met een beperkt risico moeten voldoen aan verschillende transparantieregels; een systeem dat kunstmatig content genereert moet dit bijvoorbeeld duidelijk markeren.

De AP adviseert samen met de Rijksinspectie Digitale Infrastructuur (RDI) de ministeries van EZ en BZK over de inrichting van het toezicht op de AI-verordening in Nederland. Hierbij wordt samengewerkt met ruim tien verschillende toezichthouders, colleges en inspecties. In het tussenadvies van afgelopen mei wordt voorgesteld om de AP op een groot aantal domeinen als markttoezichthouder onder de AI-verordening aan te wijzen. Deze rol sluit aan bij de expertise en ervaring van de AP met toezicht op grondrechtenrisico's bij de inzet van AI en algoritmes. Zo wordt ook een goede aansluiting van toezichtdomeinen gewaarborgd en daarmee duidelijkheid voor organisaties die AI ontwikkelen of inzetten. Dit najaar zal er een eindadvies worden gepubliceerd waarin naar verwachting o.a. wordt ingegaan op het toezicht op General Purpose AI, transparantie-verplichtingen en nationale governance en samenwerking.

Het toezicht op de AI-verordening vereist voldoende capaciteit en de juiste randvoorwaarden. Er moet voldoende budget en personeel beschikbaar zijn bij alle betrokken toezichthouders zodat zij op tijd kunnen beginnen met hun taken. Daarnaast is AI een domeinoverstijgende systeemtechnologie waarop ook andere regelgevende kaders dan de AI-verordening van toepassing zijn. Toezicht op de AI-verordening en het bestaande toezicht moeten elkaar versterken en aanvullen. Samenwerking tussen toezichthouders, waarbij de AP als coördinerend algoritmetoezichthouder een voortrekkersrol heeft, is daarom essentieel.

Voor het toezicht op de AI-verordening geeft de AP dit najaar prioriteit aan de uitleg over verboden AI-systemen en AI-geletterdheid. De eisen die hieraan gesteld worden treden in februari al in werking. De AP heeft recentelijk een oproep tot input gepubliceerd zodat bedrijven, burgers, overheden en andere organisaties inbreng kunnen geven op de eerste twee verboden uit de verordening: manipulatieve AI-systemen en uitbuitende AI-systemen.

De AP is betrokken in het proces voor Europese productstandaarden voor AI, maar maakt zich zorgen over de snelheid waarmee deze moeten worden opgeleverd. Er is drie jaar de tijd gegeven voor de ontwikkeling, maar doorgaans neemt het opstellen van technische productstandaarden veel tijd in beslag. De standaarden bieden ontwikkelaars houvast om te kunnen voldoen aan de vereisten uit de AI-verordening. Een aandachtspunt is het belang deze standaarden publiek toegankelijk te maken.

Welke rol speelt de AVG bij het AI-toezicht?

De Algemene Verordening Gegevensbescherming (AVG) speelt een belangrijke rol bij het AI-toezicht. Veel AI-systemen werken met persoonsgegevens. Op de omgang met deze persoonsgegevens houdt de AP toezicht. Denk bijvoorbeeld aan de omgang met trainingsdata die persoonsgegevens bevatten. Belangrijke vereisten zijn het hebben van een grondslag voor het gebruik van de persoonsgegevens (rechtmatigheid), niet meer te gebruiken dan nodig (dataminimalisatie) en de juistheid van de gegevens. Als een AI-systeem wordt gebruikt om besluiten te nemen over betrokkenen moeten verwerkers informatie kunnen verstrekken over de onderliggende logica en de verwachte gevolgen hiervan. Een voorbeeld waarbij het recent misging is Clearview AI. Dit bedrijf kreeg een boete van de AP voor onder andere het verzamelen van biometrische gegevens zonder toestemming.

Zowel de AVG als de AI-verordening bieden belangrijke kaders voor het AI-toezicht en versterken elkaar. Zo biedt de verordening waarborgen voor de kwaliteit van AI-systemen (waaronder het beheersen van risico's voor fundamentele rechten) en de AVG biedt het kader voor de verwerking van persoonsgegevens. In de praktijk betekent dit bijvoorbeeld dat een Mensenrechten Impact Assessment (zoals voorgeschreven door de AI-verordening) tegelijkertijd kan worden uitgevoerd met een Data Protection Impact Assessment. De AI-verordening regelt de wijze waarop AI-toezicht kan samenwerken met ander toezicht dat gericht is op het beschermen van grondrechten.

De rol van algoritmes en AI in de steeds meer digitaliserende samenleving brengt toenemende uitdagingen voor de AVG-toezichthouder met zich mee. Bijna overal worden persoonsgegevens verwerkt. Met de opkomst van AI neemt de kans toe dat daarin fouten ontstaan of dat misbruik wordt gemaakt. Goede risicobeheersing en goed toezicht kan dit in goede banen leiden. De financiering van het toezicht van de AP blijft echter ver achter op de mate van digitalisering van Nederland. De opkomst van AI-systemen maakt de financieringsuitdaging in het toezicht alleen maar groter.