Digitale uitdagingen vragen politieke aandacht & voldoende tegenmacht

Als een van de meest gedigitaliseerde landen van Europa biedt digitale technologie iedere Nederlandse burger de mogelijkheid om online bankzaken te doen en zonder problemen thuis te werken. Deze diensten zijn erg handig, maar om onze samenleving veilig te houden en iedere burger vrij en autonoom te laten leven is de bescherming van onze gegevens essentieel.

Als onafhankelijk toezichthouder op het grondrecht van de bescherming van persoonsgegevens maakt de Autoriteit Persoonsgegevens (AP) zich dagelijks sterk voor verantwoorde digitalisering. Met als doel: de optimale bescherming van de persoonsgegevens en digitale grondrechten van alle burgers.

Digitalisering in verkiezingsprogramma's

Nederland staat voor een aantal grote uitdagingen, denk alleen al aan onderwerpen als stikstof, migratie of de woningnood. Maar ook de steeds verdergaande digitalisering vraagt om stevige politieke aandacht en actie. Juist omdat digitalisering alle onderwerpen raakt. De AP roept daarom op om digitalisering de plaats te geven die het verdient in het politieke debat en de verkiezingsprogramma's. Hiervoor doet de AP een aantal concrete voorstellen.

AP vraagt aandacht voor drie digitaliseringskwesties:

1. **Democratische rechtsstaat onder druk door Big Tech**
   Big Tech neemt steeds meer publieke diensten over en er is onvoldoende besef over de impact van deze 'gratis' diensten.

2. **Datahonger van de overheid**
   Overheden verzamelen vaak voor legitieme doelen veel gegevens. Af en toe gaat het echter stevig mis en ontstaan door deze verzamelwoede crises.

3. **Digitale veiligheid niet op orde**
   Door cyberincidenten belanden vaak gevoelige persoonsgegevens op straat. Goede bescherming van persoonsgegevens staat aan de basis van de digitale veiligheid van Nederland.

1. Democratische rechtsstaat onder druk door Big Tech

Mensen laten online steeds meer sporen, persoonlijke informatie over hun leven, achter. Deze persoonsgegevens zijn geld waard. Voor veel 'gratis' diensten en producten betaal je eigenlijk met je persoonlijke data.

Grote techbedrijven worden door het verzamelen van enorme hoeveelheden data van burgers steeds invloedrijker. Met behulp van algoritmes kunnen deze bedrijven burgers beïnvloeden en manipuleren. Dit heeft verstrekkende gevolgen voor de veiligheid, vrijheid en autonomie van burgers. Ook heeft het gevolgen voor kinderen die online zijn; denk alleen al aan online pesten, chantage en het beïnvloeden van het gedrag van kinderen.

Risico's van het gebruik van deze enorme hoeveelheden data zijn bijvoorbeeld de snelle verspreiding van desinformatie rond verkiezingen, de mogelijkheid om deepfakes te maken van bekende personen en politici en doxing. De gevolgen hiervan zetten de democratische rechtsstaat onder druk. De opkomst van kunstmatige intelligentie (AI) versnelt dit proces.

Burgers en overheden zijn bovendien steeds vaker aan Big Tech overgeleverd, omdat er geen alternatief is voor wat deze bedrijven bieden. Er is voldoende tegenmacht vanuit de politiek en de (Europese) digitale toezichthouders nodig om ervoor te zorgen dat Big Tech bedrijven zich aan de wet houden.

AUTORITEIT PERSOONSGEGEVENS

AUGUSTUS 2023

2. Datahonger van de overheid

Overheidsinstanties willen steeds meer – vaak gevoelige en bijzondere – persoonsgegevens verzamelen en bestanden combineren. Vaak worden de gegevens ingezet om maatschappelijke problemen aan te pakken en dient dit dus een goed doel, zoals het tegengaan van fraude en armoede- en ziektepreventie. Maar af en toe gaat het ook stevig mis en wordt bijvoorbeeld onnodig, onrechtmatig én op discriminatoire wijze een dubbele nationaliteit vastgelegd. Of openen wetsvoorstellen de deur voor ongekende massasurveillance, bijvoorbeeld door het willen monitoren van alle banktransacties van burgers.

Dit creëert langdurig soms 'onzichtbare' en lastig te controleren problemen voor de meest kwetsbare burgers. De impact van deze geautomatiseerde processen op individuele burgers is enorm en schaadt hun vertrouwen in de overheid. Iedereen moet er in een vrije en democratische samenleving op kunnen vertrouwen dat de overheid zorgvuldig met hun (gevoelige) gegevens omgaat. Ook juist omdat een burger geen keuze heeft – je ben afhankelijk van de overheid. Zoals ook de Raad voor het Openbaar Bestuur aangeeft, is het waarborgen van publieke verantwoording over het sturen met data van groot belang. Daarom moet juist de overheid zich houden aan de beginselen van privacy-by-design, dataminimalisatie en transparantie. Ook bij de inzet van algoritmes & AI. Want een open overheid is ook transparant bij het gebruik van AI, zo stelt de Open State Foundation.

3. Digitale veiligheid niet op orde

De online beveiliging van grote en kleine databestanden is vaak niet op orde. Dit heeft grote gevolgen: voor onze digitale veiligheid, voor overheden en organisaties, maar ook voor burgers van wie de persoonsgegevens onderdeel worden van een datalek. De schaal waarop persoonsgegevens door cyberincidenten op straat belanden is immens. Bij de drie grootste gemelde cyberaanvallen van 2022 gaat het om de gegevens van naar schatting 900.000 burgers.

Het gaat bij datalekken regelmatig om uiterst gevoelige gegevens, waarmee de slachtoffers veel schade kan worden berokkend. Denk aan chantage met gevoelige medische informatie. Goede bescherming van persoonsgegevens staat aan de basis van de digitale veiligheid van Nederland. Als het gaat over cybersecurity en informatiebeveiliging, moet het dus ook expliciet gaan over persoonsgegevens. En wanneer er wordt geïnvesteerd in digitale veiligheid moet dus ook worden gekeken naar de rol en het budget van de AP.

Algoritmes & AI

In juli 2023 publiceerde de AP haar eerste halfjaarlijkse Rapportage Algoritmerisico's Nederland. Hierin stelt de AP dat het werken aan een beheersbare en gereguleerde inzet van algoritmes om politiek draagvlak vraagt, omdat algoritmische systemen en toepassingen zich snel blijven ontwikkelen en steeds breder worden toegepast. Als coördinerende autoriteit voor risicosignalering, advisering en samenwerking in het toezicht op algoritmes, zal de AP blijven bijdragen aan de verantwoorde inzet van algoritmes.

Concrete voorstellen verkiezingsprogramma's

1 **Zorg voor voldoende financiering van tegenmacht, dus voldoende budget voor de Nederlandse digitale toezichthouders**

Zo stelt ook NLdigital in haar Verkiezingsmanifest 2023. Een onderdeel hiervan is het versterken van de AP door toekenning van een structurele financiering van € 100 mln per jaar, vergelijkbaar met het budget van andere toezichthouders. De versterking van de AP draagt ook bij aan de versterking van het Europese privacytoezicht, onder andere op Big Tech.

2 **Stel een Minister van Digitale Zaken aan**

Deze bewindspersoon zorgt voor tegenmacht binnen het kabinet, bijvoorbeeld rond de toetsing van wetgeving aan digitale grondrechten. Bovendien speelt deze minister een belangrijke rol in het op verantwoorde wijze vormgeven van (overheidsinvesteringen in) digitalisering in Nederland.

3 **Versnel de inspanningen rond algoritmes & AI**

Algoritmische systemen en toepassingen ontwikkelen zich in razend tempo en we dreigen achter de feiten aan te lopen. Dit vraagt dus om versnelde inspanning rond het opstellen van beleid, het implementeren van de AI-verordening en het vesterken van het interne én externe toezicht dat ziet op algoritmes en AI.

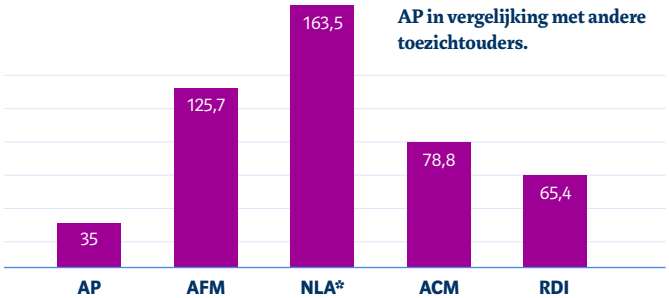
4 **Zorg voor stevig intern privacytoezicht**

Een overheid die zicht houdt aan privacyregels is een overheid waarin de burger kan vertrouwen. Een belangrijk onderdeel van het interne én externe toezicht is het op orde krijgen en houden van algoritme- en verwerkingenregisters.

5 **Maak digitale grondrechten randvoorwaarden van innovatie**

De inzet van nieuwe digitale technologieën vraagt om publieke regie en sterk toezicht om te zorgen dat digitale grondrechten worden gewaarborgd. Daarmee worden deze beginselen randvoorwaarden en unique selling points van (Nederlandse) digitale innovatie. Voorbeelden hiervan zijn de datakluis om de regie op gegevens van burgers te herwinnen en de Europese cloud om data veilig in Europa op te slaan.

AP in vergelijking met andere toezichtouders.



CIJFERS UIT 2023. BEDRAGEN IN MILJOENEN EURO.

*NLA = NEDERLANDSE ARBEIDSINSPECTIE