WYNIA'S WEEK

Risico: de digitale overheid kan uitsluiting, discriminatie en verlies van privacy veroorzaken

Door Gastauteur - 9 november 2022
Geplaatst in Digitalisering - Dwingeland

Digitalisering heeft de samenleving in korte tijd ingrijpend veranderd. De overheid is meegegaan met de digitalisering en dat had ingrijpende gevolgen voor de relatie tussen overheid en burger.

Er zijn verschillende positieve gevolgen. Door digitalisering kan de overheid snel en gemakkelijk de burger bereiken en vice versa. Ook wordt aan beide kanten veel onnodig papierwerk voorkomen. Zo kan de belastingaangifte tegenwoordig online worden gedaan, waarbij burgers de vooraf ingevulde gegevens alleen maar hoeven te controleren, in plaats van alles zelf op te zoeken en in te vullen.

Bovendien kan de burger via een DigiD-account gemakkelijk zijn identiteit bij allerlei overheidsinstanties verifiëren en zaken digitaal afhandelen, in plaats van bij een loket langs te moeten gaan.

Tegelijkertijd kan digitalisering een aantal nadelige effecten hebben op de relatie tussen burger en overheid, zoals *uitsluiting, discriminatie en een gebrek aan transparantie en verantwoording*.

Uitsluiting

Allereerst kan niet iedereen meekomen in de digitaliseringsdrang van de overheid. Digitale geletterdheid is nog altijd niet vanzelfsprekend. Denk aan ouderen, maar ook aan immigranten en laaggeletterden.

Risico: de digitale overheid kan uitsluiting, discriminatie en verlies van privacy veroorzaken

Deze burgers komen in de knel wanneer ze geconfronteerd worden met een digitaliserende overheid. Ze kunnen zelfs afhankelijk worden van anderen om privacygevoelige overheidszaken af te handelen. Daarnaast heeft niet iedereen dezelfde materiële toegang tot de digitale wereld.

Niet elke burger is in het bezit van een smartphone, laptop of tablet. Bovendien is er ook een groep burgers die niet mee wíl komen in de digitale plannen van de overheid. Zij willen niet dat de overheid op die manier allerlei gegevens over hen kan verzamelen. Bovendien maken ze zich zorgen over de veiligheid van al die data. Niet geheel onterecht, zo blijkt. In 2020 kwam zo'n 20 procent van de gemelde datalekken van de overheid.

De vraag is dan ook in hoeverre de overheid rekening dient te houden met digibeten en sceptici. Anders dan op de markt, hebben burgers niet de mogelijkheid over te stappen naar een andere partij.

De overheid mag zich dan ook niet dezelfde vrijheid permitteren als een private partij op dit gebied. Zij is er voor ons allemaal, dus ook voor burgers die niet mee kunnen of willen gaan in haar digitale ambities. Iedere burger heeft immers recht op een gelijkwaardige behandeling.

Dat betekent dat de overheid altijd ook non-digitale communicatiemogelijkheden moet blijven aanbieden. Hoewel dat wellicht als een onnodige kostenpost wordt gezien, moet de overheid beseffen dat zij niet haar eigen wensen, maar de wensen en behoeften van de burger als uitgangspunt voor het beleid moet nemen.

Tegelijkertijd valt niet te ontkennen dat digitale vaardigheden onmisbaar zijn geworden in de huidige samenleving. Van het vinden van werk, tot het onderhouden van sociale contacten; het leven speelt zich nu voor een belangrijk deel online af.

De overheid kan hier een ondersteunende rol spelen, zodat burgers zelfredzaam kunnen blijven. Denk aan het aanbieden van cursussen voor digibeten. Door een faciliterende, richtinggevende, maar niet-dwingende houding aan te nemen, kan de overheid zo zorgen voor meer digitale inclusie in de samenleving.

Discriminatie

De overheid is tevens gebruik gaan maken van algoritmen. Daarmee kan er meer inzicht worden verschaft in bepaalde situaties in de maatschappij. Denk aan het berekenen van welke straten in een stad een verhoogde kans op eenzaamheid kennen.

Met name worden algoritmen ingezet voor risicosignalering. Op die manier kan de overheid gerichter te werk gaan. Er zijn echter verschillende risico's te noemen bij het gebruik van algoritmen door de overheid.

Zo kan er sprake zijn van een onbedoeld terugkoppelingseffect. De politie doet nu bijvoorbeeld aan '*predictive policing*', waarbij algoritmen op basis van allerlei data berekenen welke wijken een

Risico: de digitale overheid kan uitsluiting, discriminatie en verlies van privacy veroorzaken

verhoogde kans op criminaliteit kennen. De politie zet vervolgens extra eenheden in deze wijken in, waardoor hier ook meer incidenten zullen worden waargenomen. Die data worden teruggekoppeld naar het algoritme, dat daarop nog meer zal benadrukken dat die wijken een verhoogd risico kennen en meer politie-inzet vereisen. Andere wijken krijgen juist minder aandacht, waardoor incidenten hier buiten het zicht blijven.

Verder kunnen de data waarop een algoritme zich baseert gebrekkig zijn. Ze kunnen verouderd, gebaseerd op gekleurde beslissingen uit het verleden of op een verkeerde manier ingevoerd zijn. Bovendien wordt vaak ten onrechte gedacht dat data inherent objectief zijn. Hier liggen echter altijd bepaalde keuzes achter voor welke data je wel en niet selecteert en op welke manier die worden gecategoriseerd. Dat is een subjectieve afweging, die een vertekend beeld kan geven van de werkelijkheid.

Verdacht door algoritme

Het belangrijkste bezwaar is dat dergelijke risicosignaleringssystemen kunnen resulteren in discriminatie en een ongelijke behandeling. In onze rechtsstaat wordt veel waarde gehecht aan de zogeheten onschuldpresumptie: een individu is onschuldig, totdat het tegendeel bewezen is.

Door dit soort algoritmen kunnen bepaalde burgers bij voorbaat al verdacht worden van illegale handelingen. Bovendien blijken geregeld discriminerende aspecten als etniciteit als risicofactor te worden meegewogen. Dit was ook het geval in de recente toeslagenaffaire. De overheid bleek daar gebruik te hebben gemaakt van een algoritme dat het hebben van een dubbele nationaliteit meewoog als risicofactor voor fraude. Onschuldige burgers werden daarbij aangewezen als fraudeur, met alle gevolgen van dien.

Het gebrek aan transparantie en verantwoording

Digitalisering heeft ervoor gezorgd dat allerlei overheidsprocessen geheel of gedeeltelijk zijn geautomatiseerd. Hierdoor zijn deze processen ook ondoorzichtiger geworden. Om ervoor te zorgen dat de burger niet buitenspel wordt gezet, is er behoefte aan meer transparantie en verantwoording. De overheid heeft bijvoorbeeld haar datahuishouding vaak niet op orde, waardoor burgers niet weten welke gegevens over hen bij die overheid bekend zijn, hoe zij hier precies mee omgaat en welke beslissingen op basis van die data worden gemaakt.

Onder de *Algemene verordening gegevensbescherming* (AVG) hebben burgers onder meer recht op inzage in, en rectificatie van hun persoonsgegevens. De overheid zou er daarom goed aan doen duidelijke verantwoordelijken voor het beheer van deze persoonsgegevens aan te wijzen en een systeem op te zetten waarbinnen burgers gemakkelijk hun eigen data in kunnen zien. Denk aan een 'digitale kluis' voor persoonsgegevens.

Risico: de digitale overheid kan uitsluiting, discriminatie en verlies van privacy veroorzaken

Onheldere deals met bedrijven

Ook ten aanzien van algoritmen is de overheid niet altijd transparant. Dit terwijl deze, zoals we gezien hebben in de toeslagenaffaire, een grote impact kunnen hebben op de levens van burgers.

De overheid geeft geregeld aan dat zij op het gebied van algoritmen samenwerkt met private partijen en dat die geen openheid kunnen geven in verband met hun bedrijfsgeheim. Dit is niet alleen geen geldig excuus voor haar transparantieplicht, maar het wijst ook op een onderliggend probleem dat de overheid transparantie en verantwoording pas als overwegingen achteraf ziet. De overheid zou al bij voorbaat dergelijke overeenkomsten niet aan moeten gaan. Zij moet zorgen voor duidelijke transparantiestandaarden en alleen gebruikmaken van technologieën die daarop aansluiten.

Het is wel belangrijk te duiden wat er dan precies wordt bedoeld met transparantie. Niet iedereen heeft namelijk dezelfde kennis over dergelijke technologieën.

Naar de burger toe moet de nadruk liggen op uitlegbaarheid. Denk aan het in duidelijke en begrijpbare taal uitleggen wat het doel is van een algoritme en welke (persoons)gegevens precies worden gebruikt. Anderzijds betekent transparantie dat er tevens inzicht wordt verschaft aan technische experts. Dit kan door ze bijvoorbeeld de gebruikte data en de broncode van een algoritme te laten doorlichten.

Ambtenaren geven daarnaast aan moeite te hebben op basis van hun eigen expertise af te wijken van het oordeel van een algoritme. Zij gaan er veelal van uit dat het algoritme het wel juist zal hebben, terwijl dat dus lang niet altijd het geval is. Er moeten dus handelingskaders worden opgesteld die ruimte bieden voor professionele autonomie.

Op die manier wordt er niet blind vertrouwd op het oordeel van een algoritme en wordt het gebruik van dit soort technologieën stilgelegd zodra er bijvoorbeeld een vermoeden van discriminatie bestaat. Het gaat uiteindelijk dus niet alleen om de techniek zelf, maar ook om de handelingskaders van degenen die er gebruik van maken.

Tot slot moet de overheid nagaan of het (gedeeltelijk) automatiseren van processen in bepaalde gevallen überhaupt verstandig is. Hoe complexer dergelijke processen in elkaar steken, hoe groter dan kans op fouten wanneer deze worden geautomatiseerd. Dat geldt al helemaal voor overheidsprocessen waarbij fouten tot grote schade kunnen leiden bij burgers. Bij de toeslagenaffaire had de complexiteit van het hele toeslagenstelsel een grote rol in de problemen die daarop volgden. Hier geldt dan ook 'eerst organiseren, dan pas automatiseren'.

drs. Wilbert Jan Derksen is wetenschappelijk medewerker bij de TeldersStichting. prof.dr.ir. Marijn Janssen is hoogleraar ICT & Governance aan de Technische Universiteit Delft.

Dit artikel is gebaseerd op een hoofdstuk uit het geschrift **Digitalisering en liberale kernwaarden.**

Risico: de digitale overheid kan uitsluiting, discriminatie en verlies van privacy veroorzaken

Vrijheid door grenzen te stellen in de digitale wereld *(2022). Deze publicatie is* ***HIER*** *te bestellen bij uitgeverij Gompel & Svacina.*