HET 'PUBLIEK MAKEN' VAN AI en algoritmes

ESSAY

AI-TOEPASSINGEN DRINGEN IN EEN STEEDS SNELLER TEMPO DOOR IN DE SAMENLEVING. HET IS GEMAKKELIJK OM JE TE VERLIEZEN IN DE BELOFTEN VAN AI EN ALGORITMES, VOOR HET VERBETEREN VAN DE VEILIGHEID, BIJVOORBEELD. MAAR ZIJN ALLE TECHNOLOGISCHE INNOVATIES WEL WENSELIJK?

tekst MARC SCHUILENBURG
beeld ADOBE STOCK

OF HET NU GAAT OM DE CAmera's van de Amazon Ring Bel of Tesla's Sentry Mode die alles opnemen en hun omgeving scannen op 'verdachte' personen; algoritmes die rechters adviseren over het recidiverisico van gedetineerden; slimme lantaarnpalen die geluiden als brekend glas, knallen en geschreeuw herkennen en horen of er wordt ingebroken in een woning; camera's boven snelwegen die kentekens, merken en modellen van 'risicovolle' auto's registreren om mobiel banditisme te bestrijden; afvalcontainers die worden gebruikt om inzamelingsroutes van vuilnisauto's te verbeteren en het dumpen van afval sneller op te sporen; of gemeenten en politie die zich bezighouden met het voorspellen van woninginbraken, geweld en fraude rondom uitkeringen – surveillance door AI en algoritmes bepaalt steeds meer hoe de veiligheidspraktijk functioneert.

De term 'surveillance' komt uit het Latijn en het Frans. Het Latijnse woord *vigilare* betekent 'waken' of 'bewaken'. Het Franse woord *surveiller* duidt op 'bovenaf' (*sur*), 'waken over' en 'toezicht houden' (*veiller*). De klassieke betekenis van surveillance betekent 'het oog houden op' en dit gebeurde aanvankelijk door menselijke activiteiten. Deze fysieke manier van bewaking was zeer arbeidsintensief en daarbij werden relatief weinig data bijgehouden. De moderne staat is het meest bekende voorbeeld van een instituut dat steunt op verschillende methoden van surveillance.

De Britse socioloog Anthony Giddens noemt surveillance een van de vier institutionele ontwikkelingen – naast industrialisatie, kapitalistische economie en militaire macht – die is verbonden met de moderniteit. Giddens waarschuwt niet alleen voor de steeds langer wordende informatietentakels van de staat die zich uitstrekken tot alle uithoeken van de samenleving, maar ook voor de dreiging van een totalitair regime dat alles wil weten van zijn burgers en daarom surveillance gebruikt voor toezicht en bewaking. Discussies in de media over dat we slaapwandelen richting een surveillance-samenleving sluiten aan bij dit dystopische beeld.

BIG DATA POLICING

In de afgelopen eeuw is de betekenis van 'surveillance' langzaam maar zeker veranderd in 'zichtbaar en voorspelbaar maken'. Dit gebeurt door het verzamelen van grote hoeveelheden data, om die data vervolgens te analyseren en te interpreteren via algoritmes waarna er besluitvorming plaatsvindt en concrete acties kunnen worden ondernomen, bijvoorbeeld door op de juiste plek te surveilleren bij de dreiging van woninginbraken. Een ander verschil met klassieke surveillance is dat dit alles niet meer hoeft te gebeuren door menselijke activiteiten, maar zich volledig geautomatiseerd – en dus niet zichtbaar voor het grote publiek – kan voltrekken. Data maken daarbij steeds meer deel uit van 'vernetwerkte' datastromen en de inzet ervan verandert van betekenis, afhankelijk waarvoor en door wie de data worden gebruikt. Je zou ook kunnen zeggen dat surveillance vloeibaar en continu is geworden, en daar komt de digitalisering via AI en algoritmes nu overheen.

De meest recente ontwikkelingen met betrekking tot AI en algoritmes in het veiligheidsvraagstuk vinden plaats onder de noemer *big data policing*. *Policing* betekent het 'veilig maken van de samenleving', en hierbij heeft de inzet van AI en algoritmes geleid tot een intensivering van zowel de omvang als de diepgang van surveillance. Door AI en algoritmes wordt surveillance breder ingezet en graaft deze dieper in het privéleven omdat burgers van alle kanten en door iedereen worden bekeken. Dit gebeurt niet alleen door de politie en gemeenten; *big data policing* vindt ook 'naast' (private techbedrijven), 'boven'

(EuroJust, Europol) en 'onder' de politie plaats, namelijk door burgers zélf. Denk hierbij aan *do-it-yourself-surveillance* met luxe gadgets zoals de Apple Watch en Fitbit, die beide boordevol sensoren zitten waarmee je zelf je hartritme, reactievermogen, slaap en activiteiten kunt monitoren.

VEILIGHEIDSPROBLEMEN

Binnen alle goede redenen om AI en algoritmes in het veiligheidsvraagstuk toe te passen, is een hoofdrol weggelegd voor economische argumenten als effectiviteit en efficiëntie. Gedreven door al dan niet gefundeerde angst voor criminaliteit en overlast heeft zich een ongebreidelde behoefte van de samenleving en politiek meester gemaakt om risico's te voorkomen en te beperken, om zo de veiligheid adequater te waarborgen. Tel hierbij het geloof op dat alles is te vatten in data en dat veiligheidsproblemen sneller en beter met de nieuwste AI-tools kunnen worden aangepakt, en dit resulteert, om de Britse schrijver Mark Fisher te parafraseren, in 'innovatie-realisme' – ideologisch geladen politieke keuzes, vermomd als onontkoombare technologische processen.

Neem de Amazon Ring Bel. Private partijen als Amazon (van oorsprong een boekwinkel) faciliteren steeds vaker en indringender de Nederlandse veiligheidszorg. Ze voeren politieachtige taken uit en werken daarbij met grote datasets en algoritmes, waarbij ze aan veel minder regels zijn gebonden dan de nationale staat en publieke partijen. Inmiddels hebben ruim 1,2 miljoen Nederlandse huishoudens een digitale deurbel met een camera erin, waarbij je met de smartphone of tablet kunt zien wie er voor de deur staat. Honderd jaar na het beroemde sociaal-ruimtelijke model van de stadsgeografen van de Chicago School – de zones rond de binnenstad volgens een patroon van concentrische cirkels – ontstaat nu een volledig nieuwe surveillance-ring om buurten veiliger te maken, wat de verhoudingen en grenzen tussen privé en publieke belangen op scherp zet.

***Het gebruik van de digitale deurbel is* allesbehalve een onschuldige exercitie.**

GEVAARLIJKE COCKTAIL

Het gebruik van de digitale deurbel is allesbehalve een onschuldige exercitie. De handleidingen van de deurbellen staan vol met termen als *security* en *protect*. Het Amerikaanse bedrijf spreekt zelfs van 'een moderne buurtwacht', maar wat zijn de consequenties hiervan voor het veiligheidsvraagstuk? Marktmacht en datamacht kunnen een gevaarlijke cocktail zijn, vooral als er veel vragen zijn over onderwerpen als het eigenaarschap van data en er sprake is van stigmatisering en discriminatie. Zo werkt het bedrijf →

MARC SCHUILENBURG IS HOOGLERAAR DIGITAL SURVEILLANCE AAN DE ERASMUS UNIVERSITEIT ROTTERDAM. BEGIN DIT JAAR VERSCHEEN ZIJN NIEUWE BOEK *MAKING SURVEILLANCE PUBLIC: WHY YOU SHOULD BE MORE WOKE ABOUT AI AND ALGORITHMS.*

Ring aan een gezichtsherkenningssysteem waarbij een signaal komt via de functie *watch list* wanneer een 'verdacht' persoon wordt herkend op de camerabeelden van de deurbel. Daarmee dreigt het gevaar van geautomatiseerd etnisch profileren wanneer personen enkel op uiterlijke kenmerken als 'verdacht' worden bestempeld, van hangjongeren met zwarte capuchons tot donkergekleurde mannen met een baard.

Maar ook op andere gebieden ontstaan hierdoor tal van ingewikkelde kwesties. Van wie zijn de data bijvoorbeeld die personen achterlaten op het Ringplatform? Waar eindigt de private ruimte en begint de publieke ruimte? Is het wenselijk dat zowel Amazon als de politie kunnen meekijken wat er gebeurt rond een woning?

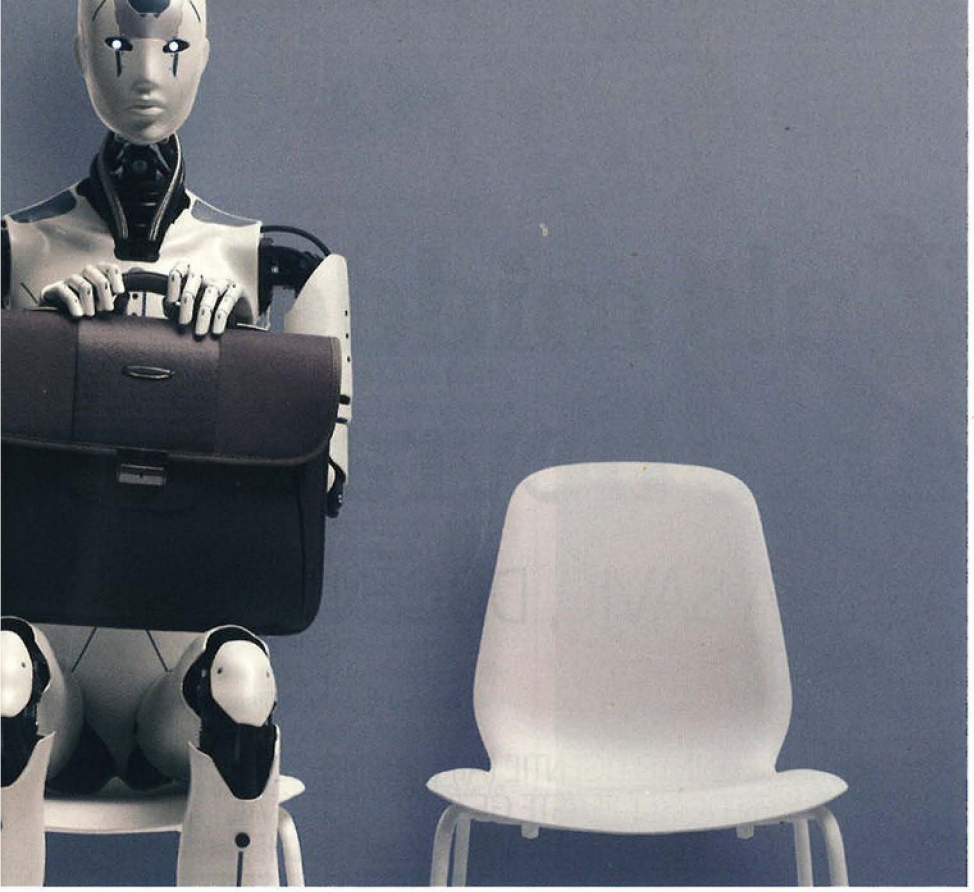
'Publiek maken' is voor mij een kernbegrip om op deze vragen een antwoord te geven en sociologische abstracties als de 'surveillance-samenleving' reduceerbaar en ervaarbaar te maken. De kwestie van het 'publiek maken' van AI en algoritmes vertrekt vanuit het idee dat met nieuwe technieken de activiteiten van burgers zichtbaar en voorspelbaar worden gemaakt, maar dat de middelen die hiervoor worden gebruikt vaak onzichtbaar blijven voor het grote publiek. 'Publiek maken' staat zo voor het zichtbaar maken van wat verborgen is of wat wij niet meer als surveillance zien of ervaren. Denk opnieuw aan de zelfsurveillance van burgers met luxeproducten als de Apple Watch en Fitbit, waarbij de dataverzameling en de analyse ervan automatisch plaatsvindt. En denk ook aan algoritmes die werken op basis van *machine learning* en zelf een weg zoeken door de datastromen heen waarbij zij niet alleen zich onttrekken aan het zicht van buitenstaanders, maar ook door de gebruikers zelf niet meer worden begrepen of kunnen worden uitgelegd.

MAATSCHAPPELIJKE ROL

Daarnaast heeft 'publiek maken' betrekking op de maatschappelijke rol van surveillance door AI en algoritmes. Die dient mede bij te dragen aan de veiligheid, waarbij veiligheid kan worden beschouwd als het publieke goed *par excellence*. Zo kan met AI een belangrijke efficiëntieslag worden gemaakt in de preventie en opsporing van criminaliteit en het maken van veiligheidsbeleid door gemeenten en de landelijke overheid. Een actueel voorbeeld op het gebied van de opsporing is het lezen en analyseren van de miljoenen onderschepte crypto-communicatiedata van de door criminele organisaties gebruikte chatdienst EncroChat. Algoritmes die zijn getraind met verschillende taalmodellen en gelabelde indicatoren filteren de data op prioriteit (welke berichten moeten als eerste worden gelezen) en vinden heel snel verbanden die relevant zijn voor een opsporingsthema als drugshandel.

Maar niet moet worden vergeten dat AI-toepassingen ook tal van risico's voor grond- en mensenrechten en de integriteit van de opsporing met zich meebrengen. Hoe baanbrekend de nieuwste technologie ook is, deze kan zeer vervelende gevolgen hebben voor de personen tegen wie zij wordt gebruikt. Tal van onvoorziene effecten kunnen optreden waarbij de impact, afhankelijk van de context en de aard van de AI-toepassing, potentieel groot is, van discriminatie van minderheden tot *overpolicing* als gevolg van *bias* en zelfversterkende effecten, waardoor bepaalde personen of gebieden met verscherpt politietoezicht te maken krijgen. Publieke waarden gaan dan enerzijds over juridische beginselen die betrekking hebben op onze collectieve en individuele vrijheid, zoals het recht op gelijke behandeling en de privacy van burgers. Anderzijds staan publieke waarden voor een goede invulling van procesmatige beginselen van AI-toepassingen, waaronder transparantie en een juiste verantwoording over de gebruikte algoritmes, oftewel *accountability*.

Tot slot staat 'publiek maken' voor het verzamelen van meer stemmen rond een AI-kwestie die hen aangaat. Dit is het derde aspect van de publieke kant van AI en algoritmes. Zo dient naar mijn mening meer aandacht te komen voor de wijze waarop iedere techniek als een mal werkt waarbinnen de kennis van bepaalde personen, de *coding elite* in het bijzonder, de overhand krijgt en die van andere personen wordt vergeten of als niet waardevol wordt gezien. Onder *coding elite* versta ik een overwegend witte, mannelijke en heteroseksuele groep van data-professionals die in het ontwerp- en ontwikkelproces van AI en algoritmes al belangrijke keuzes maakt. De zeer techni-



sche expertise van deze personen bemoeilijkt een al te strikte interne controle. Ook bestaat het risico dat deze groep handelt zonder oog voor hun eigen geprivilegieerde positie en onvoldoende rekening houdt met de risico's van ongewenste neveneffecten, waaronder potentiële discriminatie, privacy-schending of andere risico's die samenhangen met AI en algoritmes.

DEMOCRATISCHE OEFENINGEN

Een scherpe blik op deze publieke kant van AI en algoritmes betekent dat de ontwerpfase van AI en algoritmes geïnformeerd moet worden door een grotere diversiteit aan stemmen. Je zou ook kunnen stellen dat er nood is aan een 'goede democratische oefening' bij de ontwikkeling van AI. Hierbij kan worden gedacht aan het betrekken van verschillende lagen van de bevolking bij het ontwerp en de implementatie van nieuwe technologie. Vanuit het oogpunt van transparantie en *accountability* is het denkbaar om een zo divers en inclusief mogelijk team in termen van gender, leeftijd en achtergrond mee te nemen bij het ontwerp van AI-toepassingen. Op die manier kan niet alleen een stem worden gegeven aan wie deze stem op dit gebied nog niet of onvoldoende heeft, waaronder de *silenced voices* van zwakke, kwetsbare of gemarginaliseerde groepen als jongeren en minderheden. Ook kan hiervan worden geleerd om je beter te verplaatsen in de manier hoe dergelijke groepen denken over nieuwe technologie, bijvoorbeeld over de inzet van slimme sensoren in hun buurt om de veiligheid en leefbaarheid te verbeteren.

Dit derde aspect van 'publiek maken' kan zover gaan dat ook de natuur een plek aan de ontwerptafel krijgt. Er is geen samenleving zonder technologie en er is geen technologie zonder samenleving. Dat maakt alles socio-technologisch en daarmee alle klassieke opposities tussen het sociale en het technische ongegrond. Dit simpele argument wordt nog steeds niet goed begrepen. Het betekent dat – in navolging van de ideeën van de Franse socioloog Bruno Latour – ook het actorschap van niet-menselijke entiteiten – de natuur in dit geval – moet worden meegenomen bij de belangenafweging die wordt gemaakt in het ontwerp en toepassing van AI-tools. De infrastructuur van AI, van het trainen van algoritmes tot de apps op een Iphone, kan namelijk niet functioneren zonder energieslurpende servers in datacenters, waarop computerprogramma's draaien en gegevens worden bewaard van sociale media als X en Instagram en de software van Microsoft Windows. Kijken we naar de ecologische voetafdruk van AI, dan zijn datacenters verantwoordelijk voor een kleine vier procent van de wereldwijde CO_2-uitstoot – en daarmee vormen zij een grote bedreiging voor het klimaat.

AFSTAND NEMEN

Kortom, het wordt hoog tijd om afstand te nemen van een denken over AI en algoritmes, waarbij de veronderstelde technisch-economische voordelen ervan prevaleren en sociologische aspecten als 'macht,' 'kennis' en 'ervaringen' onderbelicht blijven. In zo'n technisch-economische benadering gaat het om zaken zoals de snelheid waarmee zeer grote hoeveelheden data kunnen worden verzameld, of om efficiencyargumenten dat door het gebruik van AI-toepassingen werkprocessen grondig zouden verbeteren. Dit zijn belangrijke publieke waarden en het is begrijpelijk dat efficiëntie en effectiviteit beoordelingsmaatstaven zijn. Maar de praktijk van AI en algoritmes, zo heb ik laten zien, behelst veel meer dan de enorme technische en economische mogelijkheden ervan. Het simpele feit dat iets mogelijk is, maakt het immers niet meteen wenselijk. Weegt het oogmerk van een AI-toepassing bijvoorbeeld op tegen de risico's ervan? Wat als er veel eenvoudigere en menselijkere oplossingen gewoon onder onze neus liggen?

Je kunt ook zeggen dat er nood is aan een publieke sociologie die zich mengt in het debat over AI en algoritmes, vooral als haar inzichten pijn doen en niet in de smaak vallen van de politiek en het grootkapitaal van techbedrijven. ✗

Wat als er veel eenvoudigere en *menselijkere oplossingen gewoon onder onze neus liggen?*