De prijs van een surveillancesamenleving

Een overzichtsessay over betekenis, werking en risico's van surveillerende computers

Introductie

Het debat over surveillancetechnologie dat de afgelopen jaren op stoom is gekomen, laat zien dat er zeer verschillend over deze technologie wordt gedacht.

Zo worden we bestookt met dringende waarschuwingen. Amnesty International concludeert dat Google en Facebook met hun slimme algoritmes en grootschalige dataverzameling mensenrechten schenden.[1] Wetenschapper Shoshana Zuboff legde de werkwijze van deze 'surveillancekapitalisten' bloot, en analyseerde nauwgezet hoe ze handelen in digitale profielen en zelfs onze keuzes beïnvloeden.[2] Denktanks publiceren alarmerende rapporten over de mondiale opkomst van surveillancedictaturen, die met behulp van drones, biometrische technologie en hacksoftware burgers op de voet volgen, dissidenten en etnische minderheden onderdrukken en het publieke debat smoren.[3] En politici waarschuwen dat ook de Nederlandse opsporingsdiensten zich steeds meer gaan gedragen als 'een soort van surveillancestaat'.[4]

In Brussel klinkt ondertussen een gemengder geluid. Aan de ene kant worden de risico's van surveillancetechnologie volmondig erkend. Zo wil de Europese Commissie in een nieuwe conceptverordening over artificiële intelligentie (AI) bijvoorbeeld systemen verbieden die met behulp van biometrie in de openbare ruimte mensen realtime identificeren, evenals systemen die burgers subliminaal, zonder dat ze het bewust doorhebben, beïnvloeden.[5] Ook kwalificeert de conceptverordening een aantal AI-toepassingen als *high risk* – deze toepassingen moeten voldoen aan strenge voorwaarden. Aan de andere kant ziet de Europese Commissie ook het nut van surveillancetoepassingen voor opsporings- en immigratiediensten, en beschouwt ze veel AI-systemen die data van burgers verzamelen als *low risk*. De Commissie pleit er dus voor om onderscheid te maken tussen verschillende soorten systemen.

En dan zijn er ook nog sceptische wetenschappers en journalisten die zowel de belofte als het gevaar van surveillancetechnologie met een korreltje zout nemen. Zij zetten bijvoorbeeld kanttekeningen bij de effectiviteit van algoritmes die via slimme advertenties de voorkeur van burgers kunnen beïnvloeden, en bij digitale systemen die crimineel gedrag voorspellen.[6]

---

[1] Amnesty International (2019). Surveillance giants: How the business model of Google and Facebook threatens human rights. 21 november 2019.

[2] Zuboff, S. (2019). The Age of Surveillance Capitalism. Profile Books. Zuboff, S. (2020). 'You are now remotely controlled'. In *The New York Times*, 24 januari 2020.

[3] Zie bijvoorbeeld Polyakova, A. & Meserole, C. (2019). Exporting digital authoritarianism. Brookings Institute. Augustus 2019.

[4] Zie de uitspraken van toenmalig Tweede Kamerlid Kees Verhoeven, zie Bak, L. (2019). 'Kees Verhoeven (D66) wil burger beschermen tegen oprukkende algoritmen'. Innovation origins. November 2019.

[5] European Commission (2021). Artificial Intelligence Act. 2021/0106 (COD).

[6] Gordon, B., F. Zetelmeyer, N. Bhargava en D. Chapsky (2018). A Comparison of Approaches to Advertising Measurement: Evidence from Big Field Experiments at Facebook. Marketing Science Vol. 38, Nr. 2, 193-225. Zie ook Frederik, J. & M. Martijn (2019). "The new dot com bubble is here: it's called online advertising". In The

Surveillancetechnologie hangt nauw samen met artificiële intelligentie en volgens de sceptici is de werking van allerlei AI-systemen niet bewezen. Ze roepen op om kritischer naar surveillancesystemen te kijken en onze verwachtingen te temperen.

Het moge duidelijk zijn: de opkomst van surveillancetechnologie heeft geleid tot een complex debat. Is surveillancetechnologie nu een groot gevaar, een maatschappelijke kans of een hype? Welke technologieën moet je eigenlijk beschouwen als surveillancetechnologie – en hoe hangen die technologieën precies samen met AI?

In dit essay maken we de balans op, en gidsen we de lezer door de even bruisende als beruchte wereld van surveillancetechnologie. Ons doel is erachter komen welke prijs de samenleving betaalt voor surveillancetechnologie – en wat we daarvoor terugkrijgen. Dat doen we door drie cruciale vragen te beantwoorden.

I. Wat is surveillancetechnologie?
II. Werkt surveillancetechnologie wel?
III. Welke prijs betaalt de samenleving voor surveillancetechnologie?

Gaandeweg zullen we ontdekken dat we niet alle surveillancetechnologie over één kam kunnen scheren – maar ook dat surveillancetechnologie nooit onschuldig is. Want het toepassen van surveillance brengt altijd maatschappelijke kosten met zich mee, en het is lang niet altijd duidelijk dat daar voldoende opbrengst voor de samenleving tegenover staat.
Dit essay is het eerste deel in een reeks over surveillancetechnologie. In de volgende delen gaan we nader in op het gebruik van surveillancetechnologie door migratiediensten, en op de geopolitieke rol van surveillancetechnologie.

I. Wat is surveillancetechnologie?

Iedereen observeert alles
Hoewel het woord steeds meer wordt gebruikt, is het niet gelijk duidelijk wat we precies onder surveillancetechnologie moeten verstaan. Is alle digitale technologie ook gelijk surveillancetechnologie? Of alleen de digitale technologie die opsporings- en inlichtingendiensten inzetten om mensen te volgen?

Wij begrijpen in dit essay de term als volgt. Een surveillant is iemand die doorgaans twee dingen probeert te doen: hij wil anderen observeren, en als dat nodig is gedrag sturen. Daarom is het woord in de context van politieagenten, leraren en dokters ook op zijn plek. Zij moeten ons in de gaten houden, en hebben de bevoegdheid om waar nodig in te grijpen. Bijvoorbeeld als een automobilist te hard over de weg scheurt, een leerling zit te spieken of een patiënt dreigt te overlijden.

Maar past de term ook bij het inzetten van computers? Worden we door middel van computers geobserveerd en gestuurd?

Correspondent, 6 november 2019. En Meijer, A. & M. Wessels (2019). Predictive Policing: Review of Benefits and Drawbacks. International Journal of Public Administration, Vol. 42, Nr. 12, 1031-1039.

Jazeker. Laten we beginnen bij de digitale observatie. Met behulp van digitale technologie wordt er in de huidige samenleving een gigantische hoeveelheid data verzameld. Dertig jaar geleden hadden onze telefoons nog geen camera's, laat staan uitstekende camera's. Vandaag heeft vrijwel iedereen de technologie op zak om anderen in beeld te brengen en worden er miljoenen foto's en filmpjes online gezet. Daarnaast zijn er de afgelopen jaren miljoenen beveiligingscamera's bij gekomen. Een studie van IHS Markit voorspelde twee jaar geleden dat er in 2021 wereldwijd 1 miljard beveiligingscamera's zouden zijn om burgers in de gaten houden.[7] Waar aan het begin van de jaren negentig een bescheiden aantal camerabeelden bij de politie binnenstroomde, heeft de politie vandaag te maken met een oceaan van beelden.

En wat dacht je van onze online kliks? Vele miljoenen mensen werken op computers, bestellen digitaal boodschappen of boeken online een reis, en klikken daarbij voortdurend dingen aan op een scherm. Al die kliks zijn data, gegevens die je kan analyseren, en worden op grote schaal verzameld door de sites en toepassingen van bedrijven als Amazon, Facebook en Google.

Camerabeelden en kliks leveren een enorme hoeveelheid gegevens op, maar zijn slechts twee databronnen. Dataverzameling vindt overal plaats. Zo scant en bewaart de overheid het DNA van verdachten, vermisten en veroordeelden.[8] Spraakassistenten luisteren in steeds meer huiskamers en slaapkamers naar onze instructies, en sturen een verslag van die gesprekken naar hun ontwikkelaar.[9] En binnen de Europese Unie moeten autobedrijven verplicht het eCall-systeem installeren, dat bij een ernstig ongeval de GPS-locatie doorgeeft aan hulpdiensten.[10]

Beeld, zoekgeschiedenis, DNA, locatie, gesprekken – de hoeveelheid data die vandaag verzameld wordt, is onbevattelijk groot. Iedereen doet eraan mee. Bedrijven monitoren het gebruik van hun miljoenen apps en slimme apparaten. Overheden registreren de gegevens van talloze mensen en proberen in het huidige coronatijdperk goed zicht te krijgen op grote samenscholingen, reisbewegingen en zelfs de virusdeeltjes die we afscheiden en die in het riool belanden. Consumenten installeren camera's op hun voordeur en sturen drones de lucht in.

Iedereen draagt bij aan de data-explosie.
En dat is slechts de eerste stap. Computers kunnen op basis van alle verzamelde data de werkelijkheid namelijk steeds nauwkeuriger observeren. Denk weer aan de oceaan gevuld met beelden. Computers kunnen die beelden analyseren en de patronen van gezichten herkennen – waardevolle informatie voor bijvoorbeeld de politie. En computers kunnen ook veel beter menselijke spraak herkennen en begrijpen.[11] Dus waar computers eerst slechts pixels zagen en

[7]Lin, L. & N. Purnell (2019). "A World With a Billion Cameras Watching You Is Just Around the Corner". In *The Wall Street Journal*, 6 december 2019.
[8]Zie bijvoorbeeld de Nederlandse politiedatabase HAVANK, of de Nederlandse DNA-databank van het Nederlands Forensisch Instituut.
[9]Soms gaat de dataverzameling verder dan dat, en worden ook andere gesprekken beluisterd. Zie Vincent, J. (2019). "Yep, human workers are listening to recordings from Google Assistant, too". *The Verge* 11 juli 2019.
[10]De Europese Unie. eCall: automatische noodhulpoproep door uw voertuig. Zie https://europa.eu/youreurope/citizens/travel/security-and-emergencies/emergency-assistance-vehicles-ecall/index_nl.htm.
[11]Zie Hamer, J., S. Doesborgh en L. Kool (2020). Hoor wie het zegt – Handvatten voor het verantwoorde gebruik van spraaktechnologie. Den Haag, Rathenau Instituut.

geluid hoorden, kunnen ze nu zien wie er spreekt, en horen wat er gezegd wordt.[12] Niet alleen het aantal databronnen groeit, maar ook het vermogen om aan de hand van die data rijkere waarnemingen te doen.

De digitale kaart van de wereld wordt iedere dag complexer en informatiever. En het wordt steeds moeilijker om je aan het zicht van de digitale kaartenmakers te onttrekken.

De slag om ons gedrag

Digitale technologie wordt massaal ingezet om ons in de gaten te houden. Maar worden deze observaties ook gebruikt om ons gedrag te sturen – het tweede element van surveillance?

Ook hier moet het antwoord veelal bevestigend zijn – en ook hier doet vrijwel iedere denkbare actor mee. In alle domeinen van de samenleving wordt digitale observatie ingezet om het gedrag van mensen te sturen, te beginnen bij de overheid. Van oudsher vindt overheidssurveillance vooral plaats in het veiligheidsdomein. De politie gebruikt cameratoezicht om wetsovertredingen op te sporen, de marechaussee om op vliegvelden en in havens de grenzen te bewaken. Inlichtingendiensten infiltreren in computersystemen om spionnen te dwarsbomen.[13] Maar ook uitvoeringsorganisaties in andere domeinen, zoals de Belastingdienst en de Sociale Verzekeringsbank monitoren burgers met digitale ogen zodat ze snel kunnen optreden als iemand een stap verkeerd zet.[14] Dat draait overigens niet altijd om het corrigeren en eventueel straffen van burgers die de wet overtreden. Soms is het juist de bedoeling om burgers op te sporen die geholpen moeten worden – bijvoorbeeld omdat ze een gevaarlijke schuldenlast opbouwen.

Al met al zet de overheid surveillancetechnologie in steeds meer domeinen en op steeds meer bestuurlijke niveaus in – van de rijksoverheid tot de uitvoeringsdienst en van het politiebureau tot de gemeente. En terwijl vrijwel iedereen in Nederland stelt dat de overheid weg moet blijven van ‘Chinese toestanden’, is er te weinig maatschappelijk debat over wat de huidige inzet van technologie nu al betekent. In China kunnen over een paar jaar vrijwel alle publieke ruimtes met beveiligingscamera’s bekeken worden.[15] Waaruit blijkt dat Nederland niet ook die kant op gaat? Ook hier breidt het cameratoezicht, mede doordat burgers hun camera’s bij de politie kunnen aanmelden, verder uit.[16] In China eist de overheid dat ze met encryptiesleutels toegang krijgt tot versleutelde bestanden van burgers en bedrijven.[17] Zou Nederland dat ook moeten doen? De demissionaire minister van Justitie en Veiligheid stelt momenteel voor om de encryptie af te zwakken voor opsporingsdoeleinden.[18] In China wordt het gedrag van burgers nauw gevolgd

[12]Zie ten aanzien van gezichtsherkenning Sample, I. (2019). “What is facial recognition - and how sinister is it?”. In the Guardian, 29 juli 2019. En ten aanzien van spraakherkenning Protalinski, E. (2017). “Google’s speech recognition technology now has a 4.9% word error rate”. *Venture beat* 17 mei 2017.

[13]Zie bijvoorbeeld Algemene Rekenkamer (2020). Digitalisering aan de grens. Rapport 20 april 2020. 19.

[14]Zie Algemene Rekenkamer (2021). Aandacht voor Algoritmes. 26 januari 2021. Zie ook de Algemene IV-strategie SVB, 2021-2025.

[15]Polyakova et al. 2019.

[16]Dit gaat via de databank ‘Camera in Beeld’. De politie kijkt niet live mee, maar kan om de beelden vragen als daar aanleiding voor is.

[17]Blanchard, B. (2015). China passes controversial counter-terrorism law. Reuters, 28 december 2015.

[18]Modderkolk, H. (2020). Plan Grapperhaus voor aftappen van Facebook en WhatsApp sneuvelt voortijdig. In: *De Volkskrant* 7 december 2020.

om ze een sociale score te geven, en waar nodig sancties uit te delen.[19] Dat gebeurt in Nederland gelukkig niet, maar onlangs bleek wel dat gemeentes met nepaccounts het gedrag van burgers op sociale platformen surveilleren – terwijl dat volgens de wet helemaal niet mag.[20] Nederland is in surveillanceopzicht nog lang geen China – maar er zijn genoeg zorgelijke overeenkomsten op te noemen.

Daar komt bij dat de coronacrisis de overheidssurveillance verder heeft aangewakkerd. Dat is goed te begrijpen: het is tijdens een epidemie van groot belang om te weten wie ziek is en in quarantaine moet gaan. Om die reden is geïnvesteerd in verschillende surveillancemiddelen, waaronder corona-apps en nauw gemonitorde testevenementen. Hoewel bij al deze initiatieven expliciet wordt stilgestaan bij de privacy van burgers, wordt ook deze Coronasurveillance bekritiseerd.[21] Over de effectiviteit van de corona-apps bestaat discussie, en critici werpen de vraag op of alle surveillance niet een te hoge prijs heeft – en in vergelijking met langetermijninvesteringen in het voorkomen van pandemieën niet te weinig oplevert. Ook is onduidelijk wat de verantwoordelijkheden zijn van de private ontwikkelaars waarmee de overheid samenwerkt, en waarvan ze zich afhankelijk heeft gemaakt.

Ook bij bedrijven zien we veel variatie in de technologie die zij inzetten om het gedrag van consumenten in kaart te brengen en te beïnvloeden. Zo zijn tal van toepassingen ontwikkeld op het gebied van productoptimalisatie, advertenties en het sturen van werknemers. Bij productoptimalisatie surveilleren bedrijven het gedrag van consumenten, zodat ze producten kunnen verbeteren en consumenten overhalen ze nog meer of nog gemakkelijker te gebruiken. Zo worden de data van slimme spraakassistenten nauwgezet opgeslagen en geanalyseerd.[22] Daarnaast wordt met name op sociale media en bij zoekmachines surveillance ingezet om mensen over te halen om op advertenties en links te klikken.[23] Het aantal partijen dat hiervan gebruikmaakt, is immens: van democratische politieke partijen tot autocratische regimes, en van winkelketens tot advocatenkantoren.

Ten slotte wordt surveillance ook gebruikt om werknemers te sturen. Zo kunnen werkgevers veel data over hen verzamelen, bijvoorbeeld over de sites die ze bezoeken, de uren die ze werken en de routes die magazijnwerkers lopen.[24] Werkgevers kunnen die data laten analyseren, en vervolgens werknemers adviseren en natuurlijk ook controleren. Zo zijn de berekeningen van Uber-algoritmes zo belangrijk dat de baanzekerheid van chauffeurs ervan afhangt.[25] En verschillende grote bedrijven zetten bij de werving van nieuwe mensen surveillancetechnologie in die analyseert wie geschikt is, en wie niet.[26]

[19]Polyakova et a. 2019.
[20]NOS (2021). ‘Gemeenten speuren anoniem op sociale media’. 18 mei 2021.
[21]Mulder, F. (2021). “We moeten de afgrond in de ogen durven zien”. De Groene Amsterdammer, 21 april 2021.
[22]Hamer 2020.
[23]Amnesty International (2019). Surveillance Giants: how the business model of Google and Facebook threatens human rights. 21 november 2019.
[24]Das, D., R. de Jong en L. Kool, m.m.v. J. Gerritsen (2020). Werken op waarde geschat - Grenzen aan digitale monitoring op de werkvloer door middel van data, algoritmen en AI. Den Haag: Rathenau Instituut. 40-45.
[25]Rosenblat, A. (2018). When your boss is an algorithm. In: *The New York Times* 12 oktober 2018.
[26]Das 2020, 33.

De impact van dit soort surveillance is moeilijk te overschatten. Als het bedrijven *lukt* om te sturen hoe we digitale technologie gebruiken, welke online informatie we tot ons nemen, welke producten we kopen en op welke politieke partijen we stemmen, oefenen ze een bijna onvoorstelbare invloed uit op onze levens. Maar het is de vraag of deze gedragssturing ook echt slaagt. Op dit punt komen we hieronder terug.

Naast overheden en bedrijven voeren ook burgers zelf gedragsinterventies uit op basis van digitale observatie. Zo is de beslissing om iemand binnen te laten vaak gekoppeld aan informatie van de slimme deurbel. De gegevensverzameling van de stappenteller moet ertoe leiden dat we gezonder gaan leven. De gedeelde agenda van je partner voorkomt dat je onhandige afspraken maakt.

De slag om ons gedrag wordt dus niet alleen geleverd door grote staten en bedrijven, maar ook door veel burgers – vrijwel iedereen surveilleert mee. Dus: leven we in een surveillancesamenleving? Jazeker.

Dat betekent niet meteen dat we in een Orwelliaanse dystopie leven. Surveillance *kan* verstrekkende gevolgen hebben voor onze vrijheid, maar daarvoor kunnen redenen zijn – bijvoorbeeld als de politie de technologie inzet om misdaad te bestrijden. Bovendien lijkt sommige surveillance relatief onschuldig, zoals een *fitbit* of een gedeelde agenda. Een genuanceerde ethische analyse is nodig om het kaf van het koren te scheiden, en te bepalen welke technologie te ver gaat, te veel risico met zich meebrengt of zijn doel voorbij schiet.

Bovendien is het niet afdoende om vast te stellen dat vrijwel iedereen het gedrag van zichzelf en anderen *probeert* te beïnvloeden. We moeten ook weten of dat lukt. Kunnen we met surveillancetechnologie het gedrag van anderen effectief sturen? Voordat we de maatschappelijke prijs van digitale surveillance bespreken, moeten we deze vraag eerst beantwoorden.

II Werkt surveillancetechnologie wel?

De belofte van artificiële intelligentie

Om de werking van surveillancetechnologie in te schatten, moeten we het eerst hebben over artificiële intelligentie (AI). De sceptici die twijfelen aan de vermogens van surveillancetechnologie zetten namelijk vooral vraagtekens bij de vermogens van AI.
AI draait om computers die een vorm van intelligent gedrag vertonen, en wordt opgedeeld in systemen die *wel* en *niet* in staat zijn om zichzelf instructies – algoritmes – te geven. AI-systemen die algoritmes kunnen schrijven, noem je *lerende* AI. Die worden doorgaans weer opgedeeld in wel en niet *zelflerende* AI. Met name deze laatste soort systemen wordt omschreven als zeer complex en geavanceerd omdat ze zo snel rekent en uit zichzelf zo veel variabelen uitprobeert, dat zelfs programmeurs niet altijd begrijpen hoe een systeem tot bepaalde uitkomsten komt.[27]

[27]Rudin, C. en J. Radin (2019). Why Are We Using Black Box Models in AI When We Don't Need To? A Lesson From An Explainable AI Competition. *Harvard Data Science Review* 1.2, herfst 2019.

Maar ook niet-zelflerende AI, en AI die slechts gebaseerd is op vooraf opgestelde regels kan zeer complex zijn. Denk bijvoorbeeld aan een AI-systeem van de Belastingdienst dat verschillende omvangrijke datasets aan elkaar koppelt. Zo'n systeem kan ook moeilijk te doorgronden zijn en, als er fouten gemaakt worden, moeilijk te repareren.[28]

Welke soort AI het ook betreft, de verwachtingen van ontwikkelaars en gebruikers zijn hooggespannen. AI-systemen zouden nu zo goed kunnen rekenen dat ze een cruciale bijdrage kunnen leveren aan de economie van morgen, en aan het oplossen van complexe maatschappelijke problemen – van criminaliteitsbestrijding tot het klimaat, en van de arbeidsmarkt tot de zorg.[29] Maar het is de vraag of dit zo is. Volgens de sceptici maakt AI lang niet alle hooggespannen verwachtingen waar – en ze hebben een punt.

Grofweg kan je stellen dat met behulp van AI de wereld al heel goed *waargenomen* kan worden, maar dat AI de wereld lang niet altijd goed kan *voorspellen*.

Eerst de waarneming. We schreven hierboven dat met surveillancetechnologie de wereld meer dan ooit in de gaten wordt gehouden. Het zijn doorgaans AI-systemen die de grenzen van wat computers kunnen observeren nog verder verleggen. Zo zijn doorbraken in gezichtsherkenning en spraakherkenning met name te danken aan AI, net als het verbeterde vermogen van computers om huidkanker te herkennen of spammail te identificeren.[30]

Natuurlijk zien AI-systemen het soms verkeerd, bijvoorbeeld omdat de onderliggende dataset niet gebalanceerd is. Zo blijven computers worstelen met het correct waarnemen van huidskleur.[31] Dit is inmiddels een praktisch probleem, bij goede training en zorgvuldig ontwerp kan mogelijke bias ondervangen worden. Maar er zijn ook fundamentelere uitdagingen. Zo is het maar de vraag of de huidige AI-systemen bepaalde complexe menselijke eigenschappen, zoals gevoelens, kunnen detecteren. Uit wetenschappelijk onderzoek blijkt dat ze mensen nog vaak de verkeerde emotie toeschrijven, omdat onze emoties niet altijd samenvallen met onze gezichtsuitdrukkingen – iemand die glimlacht, kan eigenlijk verdrietig zijn.[32] Maar de ontwikkelingen gaan hard. Zoveel partijen investeren inmiddels in emotieherkenning dat het niet verbazingwekkend zou zijn als binnen een paar jaar ons gemoed redelijk betrouwbaar met een computer kan worden waargenomen.[33] Een slim AI-systeem zou data over je spraak, je gezicht en je gedrag met elkaar kunnen combineren.

---

[28]Widlak, A. & R. Peeters (2018). De digitale kooi. Over (on)behoorlijk bestuur door informatiearchitectuur. Of: hoe we de burger weer centraal zetten in een digitaliserende overheid. Den Haag: Boom Bestuurskunde 2018. 109.
[29]Zie bijvoorbeeld de kamerbrief 'Industriebeleid' van Staatssecretaris van Economische Zaken en Klimaat Mona Keijzer, Kamerstuk 29826-124.
[30]Marcus, G. (2018). Deep Learning: A Critical Appraisal. Working paper, arXiv. 2 januari 2018. Simonite, T. (2020). This Algorithm Doesn't Replace Doctors—It Makes Them Better. In: *Wired* 17 juli 2020. Dada, E. en J. Bassi, H. Chiroma, S. Abdulhamid, A. Adetunmbi en O. Ajibuwa (2019). Machine learning for email spamfiltering: review, approaches and open research problems. *Heliyon* 5 2019.
[31]Simonite, T. (2019). The Best Algorithms Struggle to Recognize Black Faces Equally. In: *Wired* 22 juli 2019.
[32]Zie Sample 2019. Vincent, J. (2019). "AI 'emotion recognition' can't be trusted". The Verge 25 juli 2019. Zie ook Barrett, L., R. Adolphs, S. Marsella, A. Martinez, S. Pollak (2019). Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements. *Psychological Science in the Public Interest* 2019, Vol. 20, Nr. 1, 1-68. 1-6.
[33]Zie voor een bespreking van investeringen in emotieherkenning in spraakassistenten Hamer 2020.

We kunnen dus de conclusie trekken dat AI-systemen met grote snelheid de grenzen van digitale observatie verleggen.

Het AI-orakel

Die conclusie valt moeilijker te trekken op het gebied van digitale voorspelling. Ook hier vinden enorme investeringen plaats, en ook hier liegen de ambities er niet om. Zo wordt er veel verwacht van AI-systemen die kunnen voorspellen wanneer industriële machines en bouwwerken zoals windmolens een onderhoudsbeurt nodig hebben – *predictive maintenance*.[34] Maar vooral als het gaat om voorspellingen in complexe sociale domeinen zoals veiligheid, commerciële advertenties en de arbeidsmarkt verschijnen er met regelmaat wetenschappelijke studies en journalistieke analyses die vraagtekens zetten bij de vermogens van AI.[35] Precies die domeinen dus, waar machtige partijen zoals staten en bedrijven menselijk gedrag graag zouden willen sturen.

Neem bijvoorbeeld de surveillance van Facebook. Facebook probeert zijn gebruikers zo goed te analyseren, dat het kan voorspellen welke advertenties goed aanslaan bij wie. Maar wat blijkt? Die persoonlijke advertenties blijken helemaal niet zo effectief.[36] Het is zelfs moeilijk om aan te tonen dat het advertentiebeleid van Facebook mensen beter overtuigt dan traditionele methodes om producten en diensten te verkopen. Vaak blijken mensen die op advertenties klikken en producten kopen dat eerder al van plan te zijn geweest.

Dit onderzoeksresultaat is niet verrassend. Menselijke keuzes zijn complex en worden door veel variabelen beïnvloed. Om het technisch te formuleren: de probleemruimte is enorm groot.[37] Duizenden kleine en grote oorzaken sturen de keuzes die we maken en het gedrag dat we vertonen, van onze genetische opmaak tot ons maandagochtendhumeur. Wat onze keuzes precies bepaalt, is moeilijk te voorspellen. En dat geldt niet alleen voor onze commerciële keuzes, maar bijvoorbeeld ook voor de beslissingen die we jarenlang tijdens een dienstverband nemen, en die een goede of een slechte medewerker van ons maken. Voorspellen of een sollicitant succesvol gaat zijn, is vooralsnog dus niet mogelijk.[38]

Tegelijkertijd rekenen de computers dag en nacht door, en experimenteren datalabs voortdurend met de variabelen van menselijk gedrag. En soms zal er raak geschoten worden. Zo bleek uit een recente studie van onderzoekers van de Universiteit van Amsterdam dat politieke micro-targeting, een van de meest controversiële toepassingen van AI-voorspellingen, wel degelijk effect kan sorteren.[39] Hun experimenten lieten zien dat een AI-systeem kan beoordelen of iemand meer introvert of meer extrovert is, en hier bij het sturen van politieke advertenties gebruik van kan maken. Introverte mensen blijken namelijk gevoeliger te zijn voor

[34]Zo ziet TNO *predictive maintenance* als één van de belangrijkste toepassingsgebieden van AI, zie TNO.nl.
[35]Meijer 2019, Gordon 2018, Frederik 2019 en Das 2020.
[36]Gordon 2018.
[37]B. Schermer, J. Van Ham en K. Falkena (2020). Onvoorziene effecten van zelflerende algoritmen. Considerati 14 september 2020.
[38]Das 2020.
[39]Zarouali, B. en T. Dobber, G. De Pauw, C. De Vreese (2020). Using a Personality-Profiling Algorithm to Investigate Political Microtargeting: Assessing the Persuasion Effects of Personality-Tailored Ads on Social Media. *Communication Research* 0(00), 1-26.

angstige berichten, terwijl extroverte mensen sneller overtuigd zijn van een enthousiasmerende boodschap. Let wel: dit betekent nog niet dat een linkse introverte stemmer zomaar overtuigd kan worden om rechts te stemmen. Maar de stemmer kan misschien wel beïnvloed worden om een extremere linkse boodschap aan te hangen.

Laten we de balans opmaken. Werkt surveillancetechnologie? Deels wel en deels niet. Surveillancetechnologie is volop in ontwikkeling. De grens van wat computers kunnen zien en begrijpen, verschuift iedere dag een beetje. De surveillancesamenleving is voor een deel al realiteit geworden, omdat computers de wereld ongelofelijk goed in kaart kunnen brengen en een aantal soorten voorspellingen mogelijk zijn. Maar voor een deel is de surveillancesamenleving nog sciencefiction, en kunnen de ontwikkelaars hun grote claims niet bewijzen. Maar wat niet is, kan wellicht nog komen. Misschien zien computers een mislukte carrière of een politieke omwenteling straks van tevoren aankomen.

Het werk van wetenschappers zoals Shoshana Zuboff laat goed zien hoe vastberaden softwareontwikkelaars zijn om hun torenhoge ambities waar te maken – en wat voor enorme datavergaring, data-analyse en datahandel is opgetuigd om grip te krijgen op menselijke keuzes.[40] Hierdoor vormt surveillance de kern van het huidige platformeconomie, waarin dataprofielen als product worden verhandeld. Daarmee wordt onze eigen wil misschien nog niet gecontroleerd vanachter het bureau van Mark Zuckerberg – maar de vermogens van bedrijven als Facebook moeten nooit worden onderschat. Ze hebben een grote impact op onze levens en kunnen zonder twijfel onze vrijheid schaden. We betalen een prijs voor surveillancetechnologie. De vraag is alleen: hoe hoog is die prijs precies?

III. Wat is de prijs van surveillancetechnologie?

Laten we de zaken op een rij zetten.
Dit essay laat zien dat surveillancetechnologie inmiddels alomtegenwoordig is en dat allerlei actoren proberen om er menselijk gedrag mee in kaart te brengen en te sturen. Hierover is enorme ophef ontstaan: er wordt gewaarschuwd voor surveillancedictaturen en surveillancekapitalisten die onze autonomie en vrijheid willen beknotten. Tegelijkertijd blijkt dat niet alle surveillancetechnologie even goed werkt. Met name AI-voorspellingen van sociale uitkomsten – van complex menselijke gedrag – blijken de hooggespannen ambities nog niet waar te maken.

Wat betekent dat voor de dreiging die uitgaat van surveillancetechnologie? Welke prijs betalen we precies voor het ontwikkelen en inzetten ervan? Door het wijdverspreide en gevarieerde gebruik van surveillancetechnologie, en de verschillende technologieën die meespelen, kent deze vraag niet een eenduidig, universeel antwoord. Surveillancetechnologie is te complex om over een kam te scheren. Je moet telkens weer onderzoeken welke technologie precies gebruikt wordt, en wat de impact ervan is op ons gedrag. Het helpt dus niet om alle surveillancetechnologie in een alomvattend angstbeeld te plaatsen. Je kunt beter accepteren dat de surveillancesamenleving divers en ingewikkeld is.

[40] Zuboff 2020.

Toch kunnen we wel een aantal grote lijnen trekken. We stellen vier vuistregels voor die de politiek, het bedrijfsleven en ons allemaal helpen om van geval tot geval de prijs van surveillancetechnologie in te schatten.

1. Surveillance heeft altijd een prijs.
2. Soms is de prijs van surveillance zo hoog dat je een verbod moet overwegen.
3. Onderschat de prijs van overheidsobservatie en -dwang niet.
4. Voorkom dat de samenleving een prijs betaalt en er een ongeluk voor terugkrijgt.

1. Surveillancetechnologie heeft altijd een prijs

Het enkele feit dat mensen geobserveerd worden, kan al genoeg zijn om hun vrijheid te schaden. Als je je bekeken voelt, ga je vaak anders gedragen – dit noemt men een *chilling effect*. En misschien ga je anders nadenken over degene die je bekijkt. Zo kan de staatsobservatie van burgers hun vertrouwen in de overheid ondermijnen, en bij hen paranoïde gevoelens aanwakkeren. Denk aan de berichtgeving over de pogingen van het Nederlandse leger om de leden van de actiegroep Viruswaarheid digitaal te volgen en hun gedrag te voorspellen.[41] Ook als het leger verder geen actie zou ondernemen tegen de actiegroep, kunnen de observatie en analyse impact hebben. Bijvoorbeeld omdat de leden van Viruswaarheid het idee krijgen dat ze tegenstanders van de staat zijn.

Daarnaast kunnen observaties misbruikt worden. Als je eenmaal je privéleven surveilleert, of laat surveilleren, kan het digitale systeem gehackt worden en tegen je worden gebruikt. Denk maar aan alle gevoelige informatie die je bespreekt op je werk, in je huiskamer of in je auto. Wat als iemand privéfoto's steelt en vergrendelt om je af te persen? De digitale wereld is al decennia oud maar wordt helaas almaar onveiliger.[42] Surveillancetechnologie creëert vrijwel altijd een nieuw veiligheidsrisico.

Het is goed om dit te laten inzinken. Want als surveillancetechnologie altijd een prijs heeft, moet het ook altijd de moeite waard zijn om deze prijs te betalen. Dan heeft surveillancetechnologie de samenleving iets te bewijzen, en is een zorgvuldige ethische analyse vrijwel altijd wenselijk en nodig. Wat dat betreft roept de strategie van de Europese Commissie een risico in het leven, aangezien ze voorstelt allerlei surveillancetechnologie als *low risk* te bestempelen. Want ook die technologie zal zich aan wettelijke plichten moeten houden en de moeite waard moeten zijn. Het onderscheid van de Commissie moet dus niet als gevolg hebben dat de overheid het toezicht op *low risk*-toepassingen laat versloffen, of dat het maatschappelijk debat over de wenselijkheid ervan verstomt.

[41]Berkhout, K. (2020). 'Militairen zouden dit zelf heel netjes moeten willen regelen'. In: NRC 16 november 2020.
[42]Hamer, J., R. van Est, L. Royakkers, met medewerking van N. Alberts (2019). Cyberspace zonder conflict – Op zoek naar de-escalatie van het internationale informatieconflict. Den Haag: Rathenau Instituut.

2. Soms is de prijs van surveillance zo hoog dat je een verbod moet overwegen
Surveillancetechnologie zal niet altijd de prijs waard zijn, zeker als de risico's voor de rechten van burgers ernstig zijn. De samenleving en de politiek zullen dus bereid moeten zijn om waar nodig tot een verbod over te gaan. Dit is zeker het geval bij het ontwikkelen en inzetten van biometrische surveillance, waarmee mensen op afstand geïdentificeerd kunnen worden, en waarmee verregaande gezondheids- en zelfs gemoedsanalyses uitgevoerd worden.

Het Rathenau Instituut heeft op basis van onderzoek laten zien dat biometrische identificatie op afstand in de publieke ruimte niet verantwoord kan worden toegepast.[43] We stellen daarom dat deze toepassing voor iedereen verboden moet zijn, en dat voor biometrische analyses in andere omgevingen een vergunning moet worden aangevraagd.

Het is bemoedigend dat de Europese Commissie in haar conceptverordening verschillende verboden voorstelt: vier categorieën maar liefst, waaronder een verbod op *real time* biometrische identificatie in de publieke ruimte en een verbod op bepaalde sturingssoftware. Tegelijkertijd is de tekst niet finaal en wordt biometrische identificatie in de publieke ruimte zeker niet in alle gevallen verboden. Het is maar de vraag welke verboden overeind blijven staan. Ook is het de vraag welke sturingssoftware nu precies onder het begrip subliminaal valt, en zou moeten vallen. De komende tijd is het maatschappelijk en politiek debat over deze verordening dus van groot belang. De samenleving zal moeten vaststellen hoe verschillende soorten surveillance gewogen moeten worden, gezien hun impact op het menselijk gedrag.

3. Onderschat de prijs van overheidsobservatie en -dwang niet
Je kan digitale observatie effectief combineren met fysieke dwang, en juist daarom brengt digitale observatie al risico's met zich mee. Veiligheidsdiensten kunnen op basis van camerabeelden, geluidsopnamen of online berichten iemand arresteren, of zijn stem smoren. En dat is precies wat er in surveillancedictaturen gebeurt. Met behulp van een uitvoerig observatienetwerk bespioneert de staat haar eigen burgers, en oefent keiharde dwang uit bij ongehoorzaamheid of verdacht gedrag, tot opsluiting in een strafkamp aan toe.[44] Daarbij spelen AI-voorspellingen lang niet altijd een rol. De surveillancedictatuur heeft vooral een geavanceerd systeem van digitale observatie nodig – en die technologie is voorhanden.

De discussie over surveillancestaten is wezenlijk anders dan de discussie over surveillancekapitalisten: aan de vermogens van surveillerende staten hoef je minder te twijfelen. En dus is het gevaar van deze vermogens ook reëler. Ook in Nederland kan uitvoerige digitale overheidsobservatie, als men niet uitkijkt, gepaard gaan met een onacceptabele en ondemocratische inperking van burgerrechten.

4. Voorkom dat de samenleving een prijs betaalt en er een ongeluk voor terugkrijgt
Het is niet alleen gevaarlijk als machtige actoren menselijk gedrag nauwgezet kunnen voorspellen. Het is ook gevaarlijk als machtige actoren dat niet kunnen, maar toch van de technologie gebruikmaken. Als leidinggevenden mensen aannemen op basis van AI-software

[43]Hamer 2020, Gerritsen, J., J. Hamer en L. Kool (2020). Beter beschermd tegen biometrie. In: *Beleid en Maatschappij*, aflevering 4, 2020. Zie ook de European Data Protection Supervisor (2021). 'Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary'. Website EDPS, 23 april 2021.
[44]Polyakova 2019.

die eigenlijk niet kan voorspellen of iemand zich zal ontpoppen tot een succesvolle medewerker. Als de fraudeopsporing op basis van AI-software achter onschuldige mensen aangaat. En als mensen op sociale media aangemoedigd worden om op extreme content te klikken, terwijl dit nooit de bedoeling van de algoritmeontwikkelaars is geweest.

Als surveillancetechnologie niet doet wat we willen, offeren we onze privacy, onze veiligheid en onze autonomie voor niets op. Om niet te spreken van de weggegooide financiële investeringen. Laten we daarom niet vergeten dat surveillancetechnologie niet de enige manier is om onze problemen op te lossen.

Dat klinkt misschien evident. Maar het is essentieel om voor ogen te houden dat geavanceerde surveillancetechnologie niet de enige manier is om onze straten veiliger te maken, om de juiste medewerker aan te nemen of om advertenties en boodschappen te verspreiden. Voor de komst van AI-systemen spoorden we al criminelen op, werd er aan sollicitatieprocedures gewerkt en bestond er een publieke ruimte waarin informatie rond ging. Dat werk werd doorgaans op een verantwoorde wijze gedaan, door professionals met oordeelsvermogen. Goede AI-systemen kunnen dit oordeelsvermogen aanscherpen – maar dat is lang niet altijd nodig.

De conclusie is helder: surveillancetechnologie is niet onschuldig maar riskant. Wie speelt met surveillancetechnologie speelt met vuur. En daarom is het zaak de technologie af te wegen tegen andere oplossingen, en pas dan een keuze te maken. Dat gebeurt nu te weinig. Dikwijls weegt de overheid de inzet van surveillancetechnologie niet zorgvuldig af, maar wordt er uit enthousiasme vrijblijvend mee geëxperimenteerd, en veranderen experimenten als *predictive policing* en het Systeem Risico Indicatie gaandeweg in nationaal beleid.

En zo geven we sluipenderwijs essentiële vrijheden en burgerrechten op, in ruil voor een ongewisse opbrengst. Dat is kwalijk. Want in een democratie die niet wil verworden tot een surveillancedictatuur, moet iedere inzet van surveillancetechnologie weloverwogen getoetst worden, en de prijs waard zijn.

Auteurs:
Jurriën Hamer en Linda Kool

Bij voorkeur citeren als:
Rathenau Instituut (2021). *De prijs van een surveillancesamenleving. Een overzichtsessay over betekenis, werking en risico's van surveillerende computers.* Den Haag (auteurs: Hamer, J. en L. Kool)