Waarom we in gesprek moeten over big data en algoritmes als het over veiligheid gaat

Making Surveillance Public

Digitale surveillancetechnieken kunnen een prima hulpmiddel zijn bij bestrijding van de criminaliteit. Maar alleen als de ervaring van praktijkprofessionals meer wordt betrokken bij ontwikkeling ervan, vindt de Rotterdamse hoogleraar Digitale Surveillance Marc Schuilenburg.

Wat hebben de Amazon videodeurbel Ring en de elektrische auto's van Tesla met elkaar gemeen? Op het eerste gezicht niet zoveel, behalve dat het hierbij gaat om consumentengoederen waaraan een flinke prijskaart hangt. Enkele jaren geleden bracht Amazon de slimme deurbel Ring op de markt. De deurbel werkt via Wifi en wanneer iemand op de bel drukt, komt deze persoon in beeld op de smartphone waarna de bewoner kan besluiten om iemand wel of niet binnen te laten.
In de elektrische auto's van Tesla is een vergelijkbaar bewakingssysteem geïnstalleerd, de zogeheten Sentry Mode-functie. Met deze functie maken de ingebouwde camera's van de Tesla niet alleen opnamen van het rijgedrag van de bestuurder, maar wordt ook alles buiten de auto in de gaten gehouden – van personen die de Tesla willen beschadigen of die een inbraakpoging doen.
Hoe verschillend de Ring deurbel en de Sentry-bewakingsmodus in de Tesla ook lijken, ze komen overeen in dat het manieren zijn van digitale surveillance, waarbij grote hoeveelheden data met algoritmes worden ontsloten met als doel de samenleving veiliger te maken.

Surveillance

Surveillance komt uit het Latijn en het Frans. Het Latijnse woord *vigilāre* betekent waken of bewaken. Het Franse woord *surveiller* duidt op bovenaf (*sur*), waken over en toezicht houden (*veiller*). Dit toezicht houden op gebeurde aanvankelijk met het blote oog. Daarbij was een duidelijk onderscheid tussen degene die keek en het individu dat werd bekeken.

Het idee erachter is dat er een disciplinerend effect van spiedende camera's van uitgaat

Deze fysieke vorm van kijken wordt aan het begin van de jaren 1990 aangevuld met een groeiend aantal surveillancecamera's – op straat en in winkelcentra. Het idee hierachter is dat er een disciplinerend effect van spiedende camera's van uitgaat en dat hierdoor criminaliteit beter kan worden aangepakt.

Aan het begin van de jaren 2000 worden deze camera's met elkaar verbonden waardoor er een vernetwerking van vormen van herkenning en toezicht ontstaat, met als meest bekende voorbeeld hiervan CCTV in het Verenigd Koninkrijk waarbij de verplaatsing van personen over een lange afstand en tijd kan worden gevolgd via een netwerk van duizenden camera's.

Sinds een klein decennium is onze samenleving het tijdperk van big data en algoritmes binnengetreden en dit vormt óók de aanleiding tot de derde – en meest recente – periode van surveillance. Om bij het voorbeeld van de camera te blijven: door digitalisering en algoritmisering is de bewakingscamera nu uitgerust met automatische gezichtsherkenningstechnologie, waarbij de beelden van de camera worden vergeleken met afbeeldingen in enorme databases, van veroordeelden tot foto's van voetbalhooligans.

Zes ontwikkelingen

Minstens zes ontwikkelingen dragen eraan bij dat veel van de kenmerken van de klassieke surveillance hun vanzelfsprekendheid hebben verloren.

Digitalisering is zo belangrijk geworden dat ze alle kenmerken heeft van een nieuwe infrastructuur.

- *Digitalisering*

Digitalisering is – net als onze watervoorziening, maar ook als het wegen- en elektriciteitsnet – zo belangrijk geworden dat ze alle kenmerken heeft van een nieuwe infrastructuur. Als gevolg van digitalisering komen er zowel meer dingen in onze omgeving die data produceren als data beschikbaar die iets over ons leven vertellen. De WRR spreekt van een 'systeemtechnologie', een uitvinding met een systematisch effect door heel de samenleving heen, zoals elektriciteit dat was in de 19e eeuw en de verbrandingsmotor in de vorige eeuw.

- *Dataficering*

Met de vele apparaten die met het internet zijn verbonden wordt de berg digitale data steeds groter. En met nieuwe technische mogelijkheden om deze dataverzamelingen te analyseren, groeit ook het aantal surveillancetoepassingen in de verschillende domeinen. Dataverzameling vindt vaak buiten de controle en het zicht van personen of groepen plaats en zonder dat die personen of groepen het weten of hiervoor toestemming hebben gegeven. Daarbij wordt gebruik gemaakt van profielen die besluitvormingsprocessen kunnen ondersteunen en waarbij personen anders worden behandeld wanneer ze in een ander profiel zijn ingedeeld.

- *Algoritmisering*

Algoritmes zorgen ervoor dat de verzameling van data (*input*) via verwerking (*throughput*) tot een conclusie (*output*) leidt. Een algoritme is geen objectieve rekenhulp zonder karakter of richting. Het is opgesteld door ICT-experts, en dit betekent dat het politiek en cultureel gevoelig is.

Een algoritme is opgesteld door ICT-experts en dit betekent dat het politiek en cultureel gevoelig is.

Zo kunnen tal van onvoorziene effecten optreden waarbij de impact, afhankelijk van de context en de aard van de toepassing, potentieel groot is, met als recente voorbeelden hiervan het Systeem Risico Indicatie (SyRI) om fraude met sociale voorzieningen op te sporen en het gebruik van algoritmes door de Belastingdienst bij de Toeslagenaffaire.

- *Multi-sensorisch*

Surveillance draait niet langer om het blote oog. Technologische ontwikkelingen maken het mogelijk dat ook horen, ruiken en proeven bronnen van informatie zijn geworden. Zo zijn er lantaarnpalen in gebieden met een verhoogd inbraakrisico die met behulp van complexe algoritmes verdachte geluiden, zoals brekend glas, knallen en geschreeuw, herkennen om te horen of er wordt ingebroken in een woning. Ook kunnen deze lantaarnpalen de looppatronen van voorbijgangers analyseren op de kans dat een inbreker de wijk verkent of dat er zakkenrollers actief zijn.

- *Softening*

Nieuwe vormen van surveillance zijn minder zichtbaar en opdringerig. Dit is de *softening* van surveillance, van urine- en DNA-testen tot scanapparatuur op luchthavens waarmee mensen worden gefouilleerd zonder dat hiervoor fysiek contact nodig is. Deze zachte

vormen van informatie verzamelen staan in contrast met harde en de meer klassieke methoden van surveillance, waaronder een huiszoeking.
Surveillance wordt hierdoor grotendeels onzichtbaar en ontastbaar – en in veel gevallen zelfs intiem. Inmiddels is er een toilet op de markt die de gebruiker herkent aan zijn achterwerk en de ontlasting meet op waarden zoals te veel eiwitten, ongezonde stoffen of andere eigenaardigheden. Bij deze vorm van 'gezichtsherkenning' is de anus een soort van vingerafdruk en worden je gezondheidsgegevens direct opgenomen in het elektronische patiëntendossier.

- *Normalisering*

Ten slotte is er sprake van normalisering oftewel: surveillance is volledig geïntegreerd in onze routineactiviteiten en levensstijlen.

We merken niet op dat we worden gesurveilleerd omdat het dagelijkse praktijk is.

Van luxe surveillanceproducten zoals de Fitbit en de Apple Watch, die boordevol sensoren zitten zoals een elektrische hartslagsensor en temperatuursensor waarmee je je gezondheid kunt monitoren, tot techproducten op de werkvloer, in de klas, de auto en in de woning. We merken niet op dat we worden gesurveilleerd omdat het dagelijkse praktijk is en surveillance onderdeel is geworden van routinehandelingen – net zoals we ons aankleden voordat we naar het werk gaan of een dag 24 uur telt.
In dat opzicht doet surveillance denken aan de parabel van de Amerikaanse schrijver David Foster Wallace. Het verhaal gaat over twee jonge vissen die aan het zwemmen zijn en een oudere vis tegenkomen die de andere kant opzwemt. '*Morning, boys. How's the water?'*, vraagt de oude vis. De twee jonge vissen zwemmen verder en als de oude vis uit zicht is, zeggen ze tegen elkaar: '*What the hell is water?*'

Big data policing

De aandacht voor AI en algoritmes in de opsporing blijft tot nu toe vooral beperkt tot manieren van predictive policing, waarbij de politie probeert te voorspellen of er een verhoogde kans is op criminaliteit. Maar wie alleen denkt aan een klassieke overheidsmacht en het voorspellen van criminaliteit, loopt het risico veel aspecten van digitale surveillance over het hoofd te zien. De Amazon deurbel Ring en de Sentry Mode-bewakingsmodus in de auto's van Tesla bewijzen dat er partijen boven, onder en naast de politie zich bezighouden met het veilig maken van de samenleving en dat doen met hun eigen big data-tools.

Boven en onder politie

In het geval van boven de politie moet worden gedacht aan big data-achtige toepassingen door organisaties die opereren boven de nationale staat, van EuroJust tot Europol. Een actueel voorbeeld hiervan zijn de databanken voor het grensbeheer in de Europese Unie, waaronder het Schengeninformatiesysteem – het meest gebruikte en grootste informatie-uitwisselingssysteem voor veiligheid en grensbeheer in Europa.

Ook burgers gebruiken big data-achtige toepassingen – om de veiligheid in de buurt te verbeteren bijvoorbeeld. In ons land patrouilleren steeds meer burgers in buurtpreventieteams en maken daarbij gebruik van speciaal hiervoor ontworpen apps, zoals in het geval van de app *Veiligebuurt*. Dergelijke *non-police databases* bevatten vaak gegevens die weer door de politie kunnen worden gebruikt.

Naast politie

Techpartijen zoals Amazon en Google faciliteren steeds vaker en indringender de 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. Zo worden in Nederland volledig slimme steden opgetuigd door techbedrijven om criminaliteit te bestrijden.

Tegelijk nemen steeds meer slimme apparaten – met ingebouwde camera's, richtmicrofoons en trackingsapparatuur – in woningen de hele dag beelden en geluiden op om je huis beter te beschermen tegen personen waarvan je niet weet wat je van hen kunt verwachten. In het geval van de Ring deurbel werkt Amazon aan gezichts-herkenning waarbij een signaal komt via de functie *watch list* wanneer een verdacht persoon wordt herkend op de camerabeelden van de deurbel. Hiermee ontstaat een volledig nieuwe surveillance-ring om buurten veiliger te maken.

Het gevaar hiervan is dat wijkbewoners minder op elkaar gaan letten

Het gevaar hiervan is dat wijkbewoners minder op elkaar gaan letten, met het gevolg dat de sociale cohesie in de wijk verdampt en daarmee de onderlinge controle. Terwijl juist sociale controlemechanismen belangrijk zijn in de strijd tegen criminaliteit en overlast – de menselijke factor met andere woorden.

Door politie zelf

De opkomst van datagedreven policing door de politie past in een historisch perspectief om politieprestaties te verbeteren met behulp van data en statistische methoden. Dat

neemt een aanvang in de negentiende eeuw wanneer politiekorpsen zich intensiever gaan bezighouden met het aanleggen van grote archieven van foto's van gezichten en vingerafdrukken van personen om bij te houden wie eerder in aanraking was gekomen met de politie. Datagedreven politiewerk krijgt een verdere impuls met instrumenten zoals *crime mapping, Intelligence Led Policing* en *predictive policing.*

Op basis van ons onderzoek naar de manieren van big data policing door de Nederlandse politie blijkt dat het voorspellen van criminaliteit steeds minder centraal staat. Big data-achtige toepassingen hebben vooral betrekking op interne en administratieve processen en wanneer het gaat om de opsporing van criminaliteit dan worden deze niet voorspellend, maar vooral in *real time* en retrospectief ingezet.

In het eerste geval worden toepassingen gebruikt om politiecapaciteit te verlichten en het politiewerk te versnellen, en om informatie te verwerken die met enkel menselijke inzet niet meer valt te verwerken. Zo beschikken politiesurveillanten op straat over een smartphone waarmee zij via een dashboard direct toegang hebben tot verschillende politie-apps die vertellen waar een verdachte zich bevindt, of iemand vuurwapengevaarlijk is, hoe groepen relschoppers zich begeven door de stad en wat er op sociaal media gebeurt.

Bij retrospectieve toepassingen kan worden gedacht aan toepassingen in rechercheonderzoek, vooral als er grote hoeveelheden data moeten worden verwerkt, zoals bij het lezen van de miljoenen onderschepte data van de door criminele organisaties gebruikte chatdienst *EncroChat*.

Algoritmes die zijn getraind met verschillende taalmodellen en gelabelde indicatoren kunnen de data filteren op prioriteit en heel snel verbanden vinden die relevant zijn voor een opsporingsthema zoals witwassen of mensenhandel. Op deze manier worden de in beslag genomen gegevensdragers als het ware teruggespoeld en functioneren big data-achtige toepassingen als een tijdmachine die de politie in plaats van de toekomst naar het verleden leidt.

In weerwil van alle mediaverhalen over AI die te slim wordt en de mens volledig overbodig maakt, gaat het hierbij vooralsnog om vormen van zeer zwakke kunstmatige intelligentie waarbij algoritmes niet volledig de vrije hand worden gegeven, maar door middel van bepaalde hypothesen worden benaderd.

Van reactie naar regie

Vanuit een publiek perspectief is het belang dat de opsporing van criminaliteit zoveel mogelijk kan profiteren van de digitale tools. Maar dit betekent ook dat deze technieken beheersbaar en controleerbaar moeten worden gehouden binnen een kader van waarden waar onze democratische samenleving belang aan hecht. De ontwikkelingen op technologisch gebied gaan echter zo snel en worden door zo'n onstuimigheid gedreven, dat het zeer lastig is om met het huidige juridische instrumentarium er vat op te krijgen.

Bovendien heerst er op dit moment een zekere mate van mateloosheid als het gaat om de inzet van nieuwe digitale technieken. Deze mateloosheid wordt mede gevoed door de neiging om eerst technologie te ontwerpen, vervolgens de doeleinden ervan vast te stellen, en pas daarna een wettelijke grondslag hiervoor te zoeken.

Ik pleit ervoor om nieuwe technologie zo te ontwikkelen dat in de ontwerp- en ontwikkelfase al rekening wordt gehouden met datgene dat we als samenleving belangrijk vinden – waarbij ik denk aan zowel verankerende publieke waarden – privacy en non-discriminatie – als aan procesmatige waarden, transparantie en accountability bijvoorbeeld.

Bij de ontwikkeling van een technologie moet al worden gedacht over de in het spel zijnde publieke waarden.

Achterliggende idee hierbij is dat technologie geen neutraal hulpmiddel is en dat vanaf het begin, bij de eerste ontwikkeling van een technologie, moet worden gedacht over de in het spel zijnde publieke waarden en de wenselijke en onwenselijke effecten van technologie. Zo dient het bij de politie nooit alleen te gaan om maatstaven van efficiëntie en effectiviteit, ook rechtvaardigheid en een eerlijke behandeling van burgers zijn van belang.

Hiervoor is het noodzakelijk om andere vormen van kennis te betrekken bij het ontwerp van nieuwe technologie. Wanneer dit niet gebeurt, dan ontstaat de situatie dat ICT-experts in het ontwerp van technologie al belangrijke keuzes maakt, van de datasets die als input dienen tot de algoritmes voor de verwerking van de gegevens.

Niet alleen bestaat zo het risico dat de discretionaire ruimte van deze ICT-experts zich onttrekt aan controle en verantwoording, maar ook dat zij handelen zonder oog voor hun

eigen geprivilegieerde positie en de kans op discriminatoire praktijken bij het nemen van beslissingen op basis van algoritmische toepassingen.

Ik denk in dit verband niet alleen aan de kennis van ethici en juristen. Wanneer mens en techniek principieel met elkaar zijn verweven, dan moet ook worden gekeken naar de manier waarop praktijkprofessionals zich in de praktijk tot surveillance verhouden en naar de ervaringen op grond waarvan ze invulling geven aan hun relatie met surveillance.
Het gaat hierbij om het betrekken van wat de Amerikaanse socioloog James Scott in zijn boek *Seeing Like a State mētis* heeft genoemd – een oud-Grieks woord voor praktische ervaringen en vaardigheden van personen die niet volledig kunnen worden gestandaardiseerd. *Mētis* gaat om ervaringskennis – kennis die nog niet is gecodeerd in wetenschappelijke boeken, in procedures of in wiskundige formules. Deze kennis is lastig te digitaliseren – ze is niet te vangen in bits en bytes – omdat ze is verbonden met persoonlijke ervaringen en zeer context-specifiek is. Daarmee staat ze tegenover de technische kennis van ICT-experts.

Politieagenten en private beveiligers beschikken over ervaringskennis.

Voor veel praktische beroepen, denk aan politiewerk, is ervaringskennis (kennis die ontstaat door reflectie op eigen ervaringen) – van fundamenteel belang. Politieagenten en private beveiligers gebruiken deze kennis dagelijks, bij het bekijken van beelden van bewakingscamera's in de meldkamer of op straat in contact met wijkbewoners.

Het is daarom noodzakelijk om een zo divers en inclusief mogelijk team in termen van ervaring, gender, leeftijd en achtergrond mee te nemen bij het ontwerp van nieuwe technologie. Op die manier kan meer recht worden gedaan aan zowel de menselijke factor als aan de integratie van publieke waarden in het ontwerp- en ontwikkelproces van nieuwe technologie in de opsporing van criminaliteit.

Dit artikel is een korte weergave van de oratie die Marc Schuilenburg uitsprak bij de aanvaarding op vrijdag 23 juni van zijn leerstoel Digitale Surveillance aan de Erasmus Universiteit Rotterdam. De volledige tekst verschijnt eind dit jaar bij uitgever Eleven onder de titel: 'Making Surveillance Public: Why You Should Be More Woke About AI and Algorithms'.