ARTIKELEN

Digitale surveillance

Achtergrond, opkomst en onderzoek

Marc Schuilenburg & Melvin Soudijn

1 De surveillancesamenleving

Tijdens een congres over digitale surveillance op de Erasmus Universiteit Rotterdam gingen veel lezingen en gesprekken over nieuwe manieren van herkenning en toezicht. Een van de buitenlandse sprekers vroeg zich af in welke mate hij nu in beeld was gekomen. De docent was vanuit Italië met het vliegtuig op Schiphol geland, had vandaar de trein naar Rotterdam genomen, en verbleef hier twee dagen in een hotel alvorens weer terug te vliegen naar Palermo.
Dit lijkt een simpele vraag, maar het is lastig er een goed en volledig antwoord op te geven. Een reden hiervoor is dat surveillance vaak onzichtbaar blijft voor het grote publiek of door burgers niet meer als surveillance wordt gezien of herkend. De Italiaanse docent reisde binnen de Europese Unie en had daardoor geen visumplicht. Wel werd zijn paspoort fysiek gecontroleerd door de Koninklijke Marechaussee (KMar). Ook op andere manieren weet de KMar dat hij Nederland binnenkomt doordat de luchtvaartmaatschappij de nodige gegevens vastlegt, het zogeheten *Passenger Name Record* (PNR), dat centraal wordt verwerkt en opgeslagen. Na aankomst op Schiphol had de man bij een ING-automaat bankbiljetten gepind om de taxi naar Rotterdam te kunnen nemen. Onderweg was het hem opgevallen dat er overal camera's hingen – op het vliegveld, bij de pinautomaat, boven de snelweg. Eenmaal aangekomen in Rotterdam was hij naar het hotel gelopen om hier zijn reservering te claimen. Daarvoor moest hij zich met zijn paspoort identificeren.
Het lijkt tot nu toe vooral te gaan om klassieke manieren van surveillance, van menselijk toezicht in het hotel en door het douanepersoneel tot de bewakingscamera's op het vliegveld en op straat. Toch betekent dit niet dat de Italiaanse gast verder onbespied in Nederland verblijft. De Nederlandse overheid heeft wellicht weinig redenen om iets met zijn persoonsgegevens te doen, maar dit geldt niet voor private bedrijven. Dat begint al bij het boeken van zijn hotel via Booking.com. Dit platformbedrijf biedt niet alleen diensten aan om een overnachting te zoeken, het hotel is ook een manier geworden om je persoonlijke gegevens te verzamelen, personen te scoren op basis van hun gedrag en om te experimenteren met geautomatiseerde besluitvorming (inclusief profilering gebaseerd op bijzondere categorieën van persoonsgegevens). Zo worden tijdens de onlineboeking niet alleen zijn persoons- en creditcardgegevens vastgelegd, maar weet Booking.com ook welk IP-

doi: 10.5553/TCC/221195072023013002001

adres wordt gebruikt, het merk van zijn computer, het tijdstip en dankzij *cookies* ook een groot deel van zijn browsergeschiedenis.
Zijn bank en creditcardmaatschappij op hun beurt checken iedere transactie met behulp van algoritmes, onder andere om te kijken of deze binnen zijn normale uitgavenpatroon valt. Afwijkend gedrag kan op controle van de bank stuiten. Aangezien hij bereikbaar wil zijn, heeft de Italiaanse gast ook de hele dag zijn telefoon aanstaan. De mobiele telefoon zendt continu signalen uit, zodat zijn geografische positie kan worden bepaald. Omdat de koffie op de campus van de Erasmus Universiteit alleen digitaal kan worden afgerekend, registreert zowel de *vendor* als de bank het gebruik van de aankoop in combinatie met zijn betaalpas.
Daarnaast draagt de Italiaan om zijn rechterpols een Fitbit, een geavanceerde activiteitstracker die niet alleen zijn bewegingspatroon bijhoudt, maar ook zijn hartslag, zuurstofverzadiging en slaap monitort. Deze informatie wordt opgeslagen in de Fitbit-app en zijn data hebben een grote economische waarde voor het bedrijfsleven. Data zijn koopwaar geworden en bedrijven gebruiken zijn gegevens om hun eigen producten en diensten te verbeteren of om advertenties en aanbod af te stemmen op de persoonlijke voorkeuren van de Italiaanse gast (Gandy, 1993; Zuboff, 2019).

2 De betekenis van surveillance

Regelmatig lees en hoor je dat we zijn beland in een 'surveillancesamenleving', een samenleving waarin je voortdurend door alles en iedereen in de gaten wordt gehouden. Maar wat betekent de term 'surveillance'? Surveillance is een leenwoord met wortels in 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*). In de Engelse taal wordt de term vanaf de negentiende eeuw gebruikt in de betekenis van 'een oog houden op', wat verschillende activiteiten oproept die dikwijls door elkaar worden gebruikt en als synoniem van elkaar worden gezien, van inspecteren en bekijken tot observeren van personen en objecten. David Lyon heeft deze verschillende betekenissen als volgt samengevat: 'Surveillance both enables and constrains, involves care and control' (2001: 3). Vanuit deze optiek kan aan surveillance ook een positieve betekenis worden toegekend. Zo gebruikt Gary Marx in zijn boek *Windows into the soul* de term 'positieve surveillance' (2016: 231) en wijst hierbij op de zorg van ouders voor de ontwikkeling van hun kinderen en die van dokters, via diagnostiek, behandeling en monitoring, voor hun patiënten.
Maar surveillance kent ook een donkere kant. Althans, als er heimelijk (of soms zelfs openlijk), al dan niet op grootschalige wijze, gegevens worden verzameld en daarbij een schending van publieke waarden plaatsvindt, waaronder het recht op gelijke behandeling en de privacy van burgers. Al snel rijst dan het dystopische beeld op van een totalitair regime dat alles wil weten van zijn bevolking middels manieren van toezicht en bewaking. Als schrikbeeld wordt hierbij vaak China genoemd, een land dat toezicht koppelt aan het op repressieve wijze besturen van wat wel en wat niet mag. Zo kan in het geval van het zogeheten 'landelijk sociaal-

doi: 10.5553/TCC/221195072023013002001

kredietsysteem' verkeerd oversteken of het kopen van 'subversieve' literatuur (in de praktijk voldoet een gamemagazine al aan de omschrijving) reden zijn voor puntenaftrek op iemands maatschappelijke kredietscore. Een te lage score resulteert dan in uitsluiting van bepaalde faciliteiten of de toekenning van bijvoorbeeld een hypotheek (Schuilenburg, 2021).
De angst voor dergelijke ontwikkelingen is begrijpelijk, maar wie bij grootschalige en ingrijpende vormen van digitale surveillance alleen aan China denkt, komt bedrogen uit. Ook in Nederland wordt op grote schaal digitale surveillance ingezet om maatschappelijke problemen zoals onveiligheid en leefbaarheid aan te pakken, van onzichtbare algoritmes in politie- en gemeentelijke systemen om criminaliteit te voorkomen en fraude rondom uitkeringen te bestrijden (SyRI) tot het ophangen van slimme camera's met gezichtsherkenning op universiteiten om te registreren hoeveel studenten er in de collegezalen en bibliotheken zitten.

3 Onderzoek naar surveillance

Het beeld van diepgaand en alom aanwezig toezicht en bewaking vormt sinds het begin van de jaren 1990 een belangrijke stimulans voor wetenschappelijk onderzoek naar surveillance. Welke manieren van surveillance worden er gebruikt? Wat weten we over de effecten en neveneffecten ervan? Dit gebeurt vooral in Angelsaksische landen en in het onderzoek hiernaar kunnen drie fases worden onderscheiden.
De eerste fase vangt aan in het begin van de jaren 1990. Dan wordt vooral gekeken naar manieren waarop de rol van fysieke vormen van toezicht en bewaking wordt overgenomen door een groeiende verzameling surveillancecamera's op straat, in winkelcentra, op vliegvelden en in het openbaar vervoer (Galič, Timan & Koops, 2017). Een belangrijke veronderstelling hierbij is dat de spiedende bewakingscamera's een disciplinerend effect hebben. Hierdoor kunnen maatschappelijke problemen, zoals de toenmalige stijging van criminaliteit en overlast, beter worden aangepakt. Het denken over dergelijke gedragsaanpassingen is schatplichtig aan het boek *Surveiller et punir* (1975) van Michel Foucault en het beeld dat hij hierin schetst van het Panopticon, een cirkelvormig gevangenismodel met in het midden een wachttoren die met geblindeerde ramen uitzicht biedt op alle cellen. Ook wanneer er geen bewaker aanwezig is in de toren, blijven de gevangenen zich bespied voelen en gaan over tot een vorm van zelfsurveillance, waarbij het toezicht als het ware wordt geïnternaliseerd en het gedrag wordt aangepast aan wat wordt gedacht dat van hen wordt verwacht. Al snel wordt in dit verband ook gewezen op de negatieve effecten van cameratoezicht, waaronder het zogeheten 'chilling effect'. Dit houdt in dat personen zich bespied wanen, ongeacht of dit ook daadwerkelijk het geval is. Daardoor voelen zij zich niet meer volledig vrij en zullen zij zich anders gaan gedragen (Fussey & Murray, 2019).
Aan het eind van de jaren 1990 vindt de tweede fase van wetenschappelijk onderzoek naar surveillance plaats. De Franse filosoof Gilles Deleuze (1990) beargumenteert dat de door Foucault beschreven disciplinaire samenleving langzaam is veranderd in een controlesamenleving. Controle heeft zich hierin losgemaakt van de

beslotenheid van de functiegebonden instellingen van weleer, waaronder gevangenissen en fabrieken. Controle wordt een permanent proces en opereert via steeds veranderende netwerken die voortdurend in elkaar doorwerken. In de surveillanceliteratuur wordt dit gethematiseerd met concepten zoals 'surveillance web' (McCahill, 2002) en 'surveillant assemblage' (Haggerty & Ericson, 2000; 2006; Ericson 2007). Het meest bekende voorbeeld hiervan is CCTV (*closed-circuit television*) in het Verenigd Koninkrijk. Bij CCTV kan de verplaatsing van personen over een lange afstand en tijd *live* worden gevolgd via een netwerk van duizenden camera's. Hierbij is het bovendien mogelijk dat publieke en private partijen samenwerken, waarbij de operationele regie wordt gevoerd door de politie, gemeente of een particulier beveiligingsbedrijf – of een samenspel tussen deze drie partijen.
De derde – en meest recente – fase in het wetenschappelijk onderzoek naar surveillance valt samen met de opkomst van big data en algoritmes. David Lyon stelt dat 'surveillance today cannot be understood without a sense of how the quest for "big data" approaches are becoming increasingly central' (2015: 68-69). Big data worden gekenmerkt door vier technische eigenschappen: het gaat om zeer grote 'volumes' van data, er is sprake van een zeer grote 'snelheid' waarin deze data worden verzameld, de data zijn ongestructureerd en 'gevarieerd', en de data zijn 'digitaal' (Laney, 2001; Gartner, 2011). Big data worden via algoritmes ontsloten en deze algoritmes bestaan in verschillende typen, van eenvoudige toepassingen, waaronder beslisbomen en data-uitwisselingssystemen, tot technisch zeer complexe toepassingen, zoals *machine learning*, *machine teaching* en varianten hierop als *deep learning* (of een combinatie hiervan). Om terug te keren naar het voorbeeld van de camera uit de eerste en tweede fase van onderzoek: door de digitalisering kan de camera nu worden uitgerust met geluidsanalyse en automatische gezichtsherkenningstechnologie, een vorm van biometrie waarbij de beelden van de camera worden vergeleken met afbeeldingen in enorme databases van opgeslagen personen, foto's van arrestanten en veroordeelden tot foto's van asielzoekers en voetbalhooligans. Dergelijk cameratoezicht staat nog in de kinderschoenen, toch wordt nu al gesproken van 'algoritmische surveillance' (Norris, Moran & Armstrong, 1998; Murphy, 2017; Kosta, 2022).

4 Surveillance in de criminologie

In tegenstelling tot de Angelsaksische wereld heeft in de Nederlandstalige criminologie het thema 'surveillance' nooit een grote plaats ingenomen. Dat is opvallend omdat ontwikkelingen op dit gebied nauw verbonden zijn met de aanpak van criminaliteit en overlast door publieke partijen, in het bijzonder de politie. Zonder de herkenning en registratie van personen die als risicovol worden beschouwd (of die moeten worden beschermd), kan de politie immers niet veel beginnen (De Graaf, 2013). Wanneer het gaat over de onderliggende trend van digitalisering, dan richt de criminologie zich vooral op de toename van cybercriminaliteit via internet, e-mail of app (Oerlemans & Van der Wagen, 2021). Het slachtofferschap ervan neemt flink toe en de impact op de samenleving is groot. Maar digitalisering heeft ook gevolgen voor de opsporing en handhaving van criminaliteit en overlast. In de

aanpak hiervan worden door de politie steeds meer digitale surveillancetechnieken ingezet, met als doel om het politiewerk beter en sneller uit te voeren.
Digitale toepassingen op dit gebied lopen sterk uiteen en kunnen variëren in complexiteit, functies en toepassingen (Schuilenburg & Soudijn, 2021). Er zijn applicaties die worden gebruikt om nieuwe vormen van criminaliteit te voorspellen. Andere toepassingen hebben als doel meer zicht te krijgen op criminele gebeurtenissen in het verleden, bijvoorbeeld wapen- en drugshandel op het darkweb, of op patronen die gerelateerd kunnen worden aan actuele criminele fenomenen. Denk in het laatste geval aan instrumenten als autonoom opererende webcrawlers die op een methodische en geautomatiseerde manier seksadvertenties scannen in de strijd tegen mensenhandel. Andere bekende toepassingen die momenteel worden gebruikt, zijn het gezichtsherkenningssysteem CATCH en de *Automatic Number Plate Recognition*-camera's (ANPR) langs provinciale wegen en boven snelwegen in Nederland.
Tegelijk faciliteren techpartijen 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. Koop een elektrische auto van Tesla bijvoorbeeld en je krijgt camerasurveillance er gratis bij. Staat de Sentry Mode-bewakingsfunctie in de Tesla aan, dan maken de vier camera's aan de buitenkant van de auto standaard beeldopnames indien de auto 'merkt' dat er gevaar is, in dit geval van personen die de Tesla beschadigen of die een inbraakpoging willen doen (Eski & Schuilenburg, 2022). Techbedrijven kijken ook naar de stad vanuit het idee dat de veiligheid in wijken kan worden verbeterd dankzij data en surveillancesensoren. In zogeheten *smart cities* werken bedrijven als KPN en IBM samen met gemeenten in 'pilots' en 'living labs' om steden veiliger te maken en overlast te bestrijden. Daarbij worden onder andere wifitrackers, parkeersensoren en slimme beveiligingscamera's ingezet (Sadowsky, 2019; Pali & Schuilenburg, 2020; Hayward, 2021).
Bij dit alles is er veel onduidelijkheid over de effecten ervan in de praktijk. Weegt het oogmerk van een digitale surveillancetool bijvoorbeeld op tegen de meerwaarde van andere oplossingen? Hoe veranderen dergelijke technieken de politiefunctie? Hoe kunnen publieke waarden als recht op privacy en algoritmische verantwoording hierbij worden geborgd? Maar ook: wat zijn de ervaringen van de personen die kijken en die worden bekeken?

5 Digitale onderzoeksagenda

Technologische innovaties op digitaal vlak, ontwikkelingen met betrekking tot big data en algoritmes, en maatschappelijke en culturele veranderingen op het gebied van veiligheid zijn voortdurend met elkaar in wisselwerking. Vooralsnog ontbreekt het echter in de criminologie aan theoretische kaders hoe digitale surveillance in relatie tot de veiligheidspraktijk zich verhoudt. Ook zijn er tot nu toe nauwelijks stevig empirische onderzoeken naar de effecten van digitale manieren van surveillance op zowel het gebied van de opsporing van criminaliteit als breder binnen de

forensische zorg en het gevangeniswezen. Om hierin verandering te brengen kan aan de volgende drie onderzoeksthema's worden gedacht.

(a) Partijen en digitale surveillancetools
Wetenschappelijk onderzoek naar de digitalisering van surveillance beperkt zich vooralsnog tot het fenomeen van *predictive policing* en de manieren van surveillance die de politie hiervoor gebruikt, waarbij de kans op criminaliteit in een specifiek gebied gedurende een bepaalde periode wordt voorspeld om daar vervolgens de surveillance-inzet van de politie op af te stemmen (Perry, McInnis, Price, Smith & Hollywood, 2013; Ratcliffe, 2014; Hardyns & Rummens, 2017). De vraag is of dit niet een te eenzijdig en onvolledig beeld is van de diversiteit aan digitale tools en partijen in de veiligheidspraktijk. Digitale surveillance vindt niet alleen plaats 'door' de politie, maar ook 'boven' (Europol en Eurojust bijvoorbeeld), 'naast' (gemeenten en techbedrijven) en 'onder' de politie, waarbij in het laatste geval kan worden gedacht aan burgers die met speciaal ontworpen apps hiervoor patrouilleren in de buurt (Schuilenburg, 2023). In de meest geavanceerde apps worden op basis van sensordata – van intelligente camera's en geluidssensoren in de wijk – zelfs 'verdachte' bewegingen via de app gemeld. Dit alles roept vragen op als welke digitale tools door wie worden gebruikt, tot welke resultaten ze leiden, maar ook: tegen wie ze worden gebruikt.

(b) Ethische risico's en andere algoritmische vraagstukken
Ondanks de groeiende inzet van digitale manieren van surveillance in de veiligheidspraktijk is er veel onduidelijkheid over de neveneffecten ervan. In de literatuur wordt onder andere gewezen op risico's zoals het verlies van privacy, discriminatie van minderheden en het identificeren van risicogroepen op basis van bepaalde kenmerken en categorieën (onder andere Ferguson, 2017; Peeters & Schuilenburg, 2018).[1] Ook rechtsstatelijke zorgen worden in dit verband regelmatig geuit, variërend van het probleem van vuile data tot de schending van het onschuldbeginsel bij het online vergaren van gegevens (OSINT) (bijvoorbeeld Das & Schuilenburg, 2020; Landman, 2023). Het gebruik van zelflerende algoritmes in digitale tools kan zelfs leiden tot controleverlies, variërend van het 'black box'-probleem van AI tot het uit handen geven van data, expertise en *intellectual property rights* aan techbedrijven (Pasquale, 2015; Zuboff, 2019). Het is daarom van belang dat er meer onderzoek komt naar de risico's van digitale surveillance en hoe deze risico's kunnen worden voorkomen of beter worden begrensd.

1 Neem bijvoorbeeld de discussies die nu spelen over de mogelijke invoering van *central bank digital currencies* (CBDC's) in westerse landen. Centrale bankvaluta zijn digitale munten die direct door een centrale bank worden uitgegeven zonder tussenkomst van commerciële banken. Een heet hangijzer vanuit surveillanceoogpunt is hoe het hierbij met de privacy van burgers zit. Omdat de digitale munt aan persoonsgegevens gekoppeld zal zijn, betekent dit in theorie dat de overheid precies zou kunnen nagaan waar het geld aan wordt uitgegeven. Ook is de digitale munt programmeerbaar, waardoor bepaalde soort uitgaves geblokkeerd kunnen worden. In dit kader kan ook worden gewezen op een recent voorstel in de Tweede Kamer om te komen tot een transactiemonitoring van het betaalverkeer boven de 100 euro ('finanveiller').

(c) Surveillance-ervaringen
Digitale surveillance is naast een technisch vraagstuk óók altijd een sociale praktijk. Dat betekent dat de ervaringen van de personen die met surveillance in aanraking komen, van praktijkprofessionals tot burgers, moeten worden betrokken in het onderzoek hiernaar. Hierbij kan worden gedacht aan negatieve ervaringen zoals dwang en controle, maar ook aan manieren van verzet tegen indringende vormen van surveillance. Maar het criminologische onderzoek hiernaar hoeft zich hiertoe niet te beperken. Voor veel personen heeft surveillance ook een positieve kant, van plezier en spel tot ontspanning (onder andere Albrechtslund, 2008; Ball, 2009; Bell, 2009). Denk in dit geval aan vormen van luxe surveillance, van de Fitbit om de pols van de Italiaanse gast tot de e-bikes van het merk VanMoof, waarbij motorsensoren je gegevens via de app op je telefoon doorsturen naar de servers van het Nederlandse bedrijf om onder andere je rijtijd en afstand te berekenen. Dergelijke producten worden vrijwillig aangeschaft omdat het inzicht dat ze bieden in je persoonlijke leven als een positief aspect ervan wordt ervaren (Gilliard & Golombia, 2021; Schuilenburg, 2023). Kortom, welke surveillance-ervaringen kunnen er worden onderscheiden en op welke manier werken deze ervaringen door in de praktijken van digitale surveillance?

6 Dit themanummer

Om een aanzet te geven tot meer aandacht voor surveillance als een criminologisch relevant thema, worden in dit themanummer over digitale surveillance de volgende invalshoeken gepresenteerd.
Het eerste artikel van **Jing Hiah** gaat over de digitale platformeconomie, zoals apps die vraag en aanbod van allerlei diensten samenbrengen. Het blijkt dat zulke platformen vaak verregaande vormen van controle en surveillance uitoefenen op de werkers die aan deze platformen zijn verbonden. Zo wordt controle uitgeoefend door middel van algoritmische prijsstelling en het beheer van gebruikersgegevens. De werkers die aan dergelijke apps zijn verbonden, hebben daarbij weinig invloed op hun arbeidsomstandigheden, er is weinig keuzevrijheid, en hun privacy is een non-issue.
Pieter Leloup legt in het tweede artikel de nadruk op de historische continuïteit van surveillance. Er is in de samenleving een hang naar voortdurend nieuwe toepassingen, maar Leloup betoogt dat hedendaagse technologieën van surveillance vaak gebaseerd zijn op eerdere, historische ideeën omtrent het herkennen en registreren van personen. Het veronachtzamen van het verleden draagt het gevaar in zich om voorafgaande historische trends en gebeurtenissen te negeren en verkeerde conclusies te trekken over de impact en rol van hedendaagse fenomenen en gebeurtenissen. Als kapstok voor een reflectie hierover gaat Leloup in op fotografie als middel voor politionele en gerechtelijke surveillance gedurende de late negentiende en vroege twintigste eeuw in zowel de Belgische als de internationale context.
Ook **Miriam Rasch** introduceert in haar essay een soort van historisch perspectief. Het gaat haar om 'kolonialisme', maar dan in een moderne jas gestoken: datakolo-

nialisme. Ongebreidelde extractie van data en de uitbuiting van verregaande digitale surveillance die slechts voor de *happy few* winsten generen, vormen volgens Rasch een gevaar voor menselijke autonomie – een centrale waarde in een democratische maatschappij. In deze context klinken uitspraken van techgoeroes als 'we're moving to a new, uninhabited country and setting up a society' ineens heel anders in de oren.

Wouter Landman betoogt in zijn essay dat digitale politiesurveillance veel overeenkomsten met traditionele politiesurveillance heeft (zoals het vastleggen en registreren van personen, het proces waar Leloup ook op attendeert), maar dat er ook fundamentele verschillen zijn. De omvang van de controle, de manier van registreren, de snelheid waarmee een match kan worden gevonden, het acteren naar aanleiding van een hit – dit zijn allemaal aspecten die in een stroomversnelling zijn gekomen. De mens wordt daarbij steeds meer vervangen door technologie.

Bartek Chomanski en Lode Lauwaert gaan in hun essay 'Online consent en het recht op onwetendheid' in op de term 'het recht om niet te weten'. In een medische context staat dit recht voor de basisidee dat patiënten een bewuste keus kunnen maken om niet geïnformeerd te worden, bijvoorbeeld als zij een genetische aandoening hebben die op de lange termijn kan opspelen. Wanneer deze lijn van redeneren wordt doorgetrokken naar voorkeuren van internetgebruikers, zo betogen beide auteurs, dan is ongeïnformeerde toestemming voor online voorwaarden een stuk minder problematisch dan vaak wordt gedacht.

Het beeldessay is van **Gabry Vanderveen** en gaat over camerabewaking. Vanderveen laat hierin zien hoe in de voormalige DDR, in Erfurt, camera's worden ingezet op camperplaatsen. Vervolgens bespreekt **Martijn Wessels** in de rubriek 'Voorbij de horizon' de inzichten op het gebied van surveillance aan de hand van de meest recente boeken van Frank Pasquale, Sarah Brayne en Ben Shneiderman. Op basis hiervan formuleert Wessels verschillende beginselen voor een verantwoord gebruik van AI in het publiek domein.

In de rubriek 'Significant others' spreken **Marc Schuilenburg en Yarin Eski** met Chris Gilliard. Gilliard is een invloedrijke Amerikaanse denker die verschillende belangrijke concepten op het gebied van surveillance heeft gemunt. In het gesprek gaat Gilliard uitgebreid in op hoe historische vooroordelen altijd hun weg vinden naar digitale systemen en waarom deze systemen de meest kwetsbare en meest gemarginaliseerde groepen in de samenleving blijven schaden.

Tot slot wordt in de rubriek 'Doka' aandacht besteed aan het protest van studenten tegen het ophangen van surveillancecamera's op universiteiten.

Literatuur

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3), https://doi.org/10.5210/fm.v13i3.2142.

Ball, K. (2009). Exposure: Exploring the subject of surveillance. *Information, Communications and Society*, *12*(5), 630-657.

Bell, D. (2009). Surveillance is sexy. *Surveillance & Society*, *6*(3), 203-212.

Das, A. & Schuilenburg, M. (2020). Garbage in, garbage out: over predictive policing en vuile data. *Beleid en Maatschappij*, *47*(3), 254-268.

Deleuze, G. (1990). Post-scriptum sur les sociétés de contrôle. *L'Autre journal*, 3-7.
Ericson, R.V. (2007). *Crime in an insecure world*. Cambridge, UK: Polity Press.
Eski, Y. & Schuilenburg, M. (2022). On Tesla: Balancing sustainable car connectivity, silent lethality and luxury surveillance. *Criminological Encounters*, *5*(1), 234-251.
Ferguson, A.G. (2017). *The rise of big data policing. Surveillance, race, and the future of law enforcement*. New York: New York University Press.
Foucault, M. (1975). *Surveiller et punir: naissance de la prison*. Paris: Gallimard.
Fussey, P. & Murray, D. (2019). *Independent report on the London Metropolitan Police service's trial of live facial recognition technology*. Colchester: Human Rights Centre, University of Essex.
Galič, M., Timan, T. & Koops, B.J. (2017). Bentham, Deleuze and beyond: An overview of surveillance theories from the panopticon to participation. *Philosophy and Technology*, *30*, 9-27.
Gandy, O. (1993). *The panoptic sort: A political economy of personal information*. Boulder, CO: Westview.
Gartner (2011). *Gartner says solving 'big data' challenge involves more than just managing volumes of data*. Geraadpleegd op 7 juni 2023, van www.businesswire.com/news/home/20110627005655/en/Gartner-Says-Solving-Big-Data-Challenge-Involves-More-Than-Just-Managing-Volumes-of-Data.
Gilliard, C. & Golombia, D. (2021, 6 juli). Luxury surveillance. People pay a premium for tracking technologies that get imposed unwillingly on others. *Real Life Magazine*.
Graaf, B. de (2013). *Ecce homo: Herkenning en registratie in de geschiedenis en veiligheidsbeleid*. Universiteit Leiden.
Haggerty, K. & Ericson, R. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605-622.
Haggerty, K. & Ericson, R. (2006). The new politics of surveillance and visibility. In K. Haggerty & R. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 3-33). Toronto: University of Toronto Press.
Hardyns, W. & Rummens, A. (2017). Predictive policing as a new tool for law enforcement? Recent developments and challenges. *European Journal on Criminal Policy and Research*, *24*, 201-218.
Hayward, K. (2021). Five smart city futures: A criminological analysis. In M. Schuilenburg & R. Peeters (Eds.), *The algorithmic society: Technology, power, and knowledge* (pp. 172-192). London/New York: Routledge.
Kosta, E. (2022). Algorithmic state surveillance: Challenging the notion of agency in human rights. *Regulation & Governance*, *16*(1), 212-224.
Landman, W. (2023). Spanningen bij politiewerk op het web. *Het Tijdschrift voor de Politie*, *2*, 10-14.
Laney, D. (2001). *3D data management: Controlling data volume, velocity and variety*. META Group Research Note, 6.
Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Buckingham: Open University Press.
Lyon, D. (2015). *Surveillance after Snowden*. Cambridge, UK: Polity Press.
Marx, G. (2016). *Windows into the soul. Surveillance and society in an age of high technology*. Chicago: University of Chicago Press.
McCahill, M. (2002). *The surveillance web: The rise of visual surveillance in an English city*. Cullompton: Willan.
Murphy, H. (2017). Algorithmic surveillance: The collection conundrum. *International Review of Law, Computers & Technology*, *31*, 225-242.

Norris, C., Moran, J. & Armstrong, G. (1998). Algorithmic surveillance: The future of automatic visual surveillance. In C. Norris, J. Moran & G. Armstrong (Eds.), *Surveillance, closed circuit television and social control* (pp. 255-276). Aldershot: Ashgate.

Oerlemans, J-J. & W. van der Wagen (2021). Types of cybercrime and their criminalisation. In W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (Eds.), *Essentials in cybercrime. A criminological overview for education and practice* (pp. 53-97). The Hague: Eleven International Publishing.

Pali, B. & Schuilenburg, M. (2020). Fear and fantasy in the smart city. *Critical Criminology*, *28*(4), 775-788.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Boston: Harvard University Press.

Peeters, R. & Schuilenburg, M. (2018). Machine justice: Governing security through the bureaucracy of algorithms. *Information Polity*, *23*(3), 267-280.

Perry, W.L., McInnis, B., Price, C.C., Smith, S.C. & Hollywood, J.S. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*. Santa Monica: RAND Corporation.

Ratcliffe, J. (2014). What is the future of… predictive policing? *Translational Criminology, 6*, 4-5.

Sadowski, J. (2019). The captured city: The 'smart city' makes infrastructure and surveillance indistinguishable. *Realifemag.com*.

Schuilenburg, M. (2021). *Hysteria: Crime, media, and politics*. London/New York: Routledge.

Schuilenburg, M. (2023). Big data policing: schets van de belangrijkste vraagstukken, partijen en nieuwste trends in de praktijk. In T. Snaphaan et al. (Eds.), *Cahiers Politiestudies 66: Big data policing* (pp. 53-70). Oud-Turnhout: Gompel & Svacian.

Schuilenburg, M. & Soudijn, M. (2021). Big data in het veiligheidsdomein: onderzoek naar big data-toepassingen bij de Nederlandse politie en de positieve effecten hiervan voor de politieorganisatie. *Tijdschrift voor Veiligheid, 20*(4), 44-62.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York, NY: Public Affairs.