Big data policing

Schets van de belangrijkste vraagstukken, partijen en nieuwste trends in de praktijk

Cahiers Politiestudies
Jaargang 2023-1, nr. 66
p. 53-70

ISBN 978-94-6371-424-2

Marc Schuilenburg[1]

Dit artikel trekt het fenomeen van big data policing breder dan tot nu toe is gedaan in de literatuur hierover. Verschillende elementen van big data policing zijn uitgediept, waaronder de partijen ('door', 'boven', 'naast' en 'onder' de politie) die actief zijn op dit gebied. Bijzondere aandacht is besteed aan het fenomeen 'luxe surveillance', waarbij commerciële bedrijven zoals Amazon en Tesla surveillanceproducten op de markt brengen waarmee consumenten zowel toezicht op anderen als op zichzelf houden. Tot slot zijn vier vraagstukken benoemd waarover nog onvoldoende wetenschappelijke duidelijkheid bestaat, waaronder de verschillende type datasets en algoritmes die worden gebruikt voor verschillende bigdatatoepassingen en de noodzaak tot zowel breder als meer empirisch onderzoek naar big data policing.

1. Inleiding

Enkele jaren geleden bracht het Amerikaanse techbedrijf Amazon de slimme videodeurbel Ring op de markt. Met deze deurbel kun je zien wie er voor de deur staat. De deurbel werkt via wifi en wanneer er op de bel wordt gedrukt is deze persoon in beeld op je smartphone of tablet. De deurbel is meer dan alleen een deurbel. Ze functioneert ook als een beveiligingscamera die via een ingebouwde sensor alle bewegingen registreert en ze geeft hiervan een notificatie in de app, bijvoorbeeld als er een ongewenste persoon rondloopt voor het huis.[2] In de meest luxe versie van deze digitale surveillance worden ook de paar seconden gefilmd voordat er verdachte bewegingen worden geregistreerd, zodat er te zien is wat er vooraf heeft plaatsgevonden.

De deurbel Ring is een voorbeeld van, wat Gilliard en Golombia (2021) noemen, 'luxury surveillance'. Andere voorbeelden van luxe surveillance zijn de Apple Watch en de Fitbit waarmee je je gezondheid en sportprestaties kunt monitoren. Maar denk ook aan de slimme, zelfrijdende rolkoffer Ovis, met een prijskaartje van bijna achthonderd euro, die voorzien is van een 170-graden-camera waarmee hij zijn omgeving kan zien, en van een gewichtssensor en locatietracking, zodat de koffer makkelijk kan

[1] Als bijzonder hoogleraar Digital Surveillance verbonden aan de Erasmus Universiteit Rotterdam en de Vrije Universiteit Amsterdam.
[2] https://nl-nl.ring.com Geraadpleegd 19 juni 2022.

worden teruggevonden wanneer hij is kwijtgeraakt. Bijzonder aan deze voorbeelden van luxe surveillance is dat personen bereid zijn er veel geld voor te betalen en dat de mogelijkheden die deze producten bieden, van tracking tot monitoring van jezelf en van andere personen, worden gezien als positieve eigenschappen ervan.

De opkomst van luxe surveillance zoals de Amazon deurbel Ring heeft de afgelopen jaren relatief weinig stof doen opwaaien. Maar ze roept wel tal van vragen op over het bredere fenomeen waaronder ze kan worden geschaard: big data policing. Big data policing is het gebruik van grote hoeveelheden data die via algoritmes worden ontsloten met als doel de samenleving veiliger te maken. De opkomst en snelle groei van big data policing heeft verschillende oorzaken (e.g. Brayne, 2017; Ferguson, 2017; Schuilenburg & Soudijn, 2021). Een reden is dat de berg beschikbare digitale data met het dagelijks gebruik van internet, sociale media, mobiele telefoons en allerlei productinnovaties zoals grootschalige klantenbestanden steeds groter is geworden (Smith & O'Malley, 2017). Verder wordt big data policing geholpen door de toegenomen technische mogelijkheden om dergelijke grote hoeveelheden data te verzamelen, te bewerken en te analyseren via algoritmes, evenals de mogelijkheden om de uitkomsten ervan te gebruiken in het kader van politieachtige taken (e.g. Ferguson, 2017; Smith, Moses & Chan, 2018; Brayne, 2021). Minstens zo belangrijk is de politieke en maatschappelijke context. De wijze waarop en door wie big data policing wordt gebruikt, wordt ook bepaald door de politieke en culturele krachten in een samenleving. Die variëren van de wens om criminaliteit in een steeds 'vroegtijdiger stadium' aan te pakken (Zedner, 2007; Van Brakel, 2016), financiële argumenten ('budget issues') en claims dat bigdatatoepassingen leiden tot 'snellere' werkprocessen en 'efficiëntere' vormen van opsporing van criminaliteit en overlast (e.g. Brayne, 2017; Ferguson, 2017), tot een sterk geloof in techniek als 'de' oplossing voor maatschappelijke problemen als onveiligheid (Morozov, 2013).

Ondanks de populariteit van en groeiende wetenschappelijke aandacht voor big data en algoritmes om de samenleving veiliger te maken is er veel onduidelijkheid over de toepassing en de effecten ervan in de praktijk. Wetenschappelijke aandacht beperkt zich vooral tot predictive policing door politieorganisaties en de collectieve schade hiervan voor de samenleving, zoals etnisch profileren en de discriminatie (en oneerlijke behandeling) van kwetsbare groepen. De vraag is of dit niet een te eenzijdig en onvolledig beeld is van het fenomeen 'big data policing' (Schuilenburg & Soudijn, 2021). Het voorbeeld van de Amazon deurbel Ring laat zien dat meer partijen als alleen de politie zich bezighouden met het veilig maken van de samenleving via het verzamelen van data en dat bovendien doen met uiteenlopende digitale surveillancetools. Dit artikel heeft daarom als doel het fenomeen van big data policing breder te trekken dan tot nu toe is gedaan in de literatuur hierover. De vraag die hierbij centraal staat is: hoe beïnvloeden big data en algoritmes de politiefunctie?

In de volgende paragraaf worden eerst vier vraagstukken onderscheiden die relevant zijn voor een beter begrip van big data policing en waarover nog onvoldoende rekenschap wordt afgelegd in de wetenschappelijke literatuur. Een van die vraagstukken is het speelveld van big data policing: welke partijen zijn hierop actief? In antwoord hierop wordt een overzicht gegeven van partijen die zich bezighouden met big data policing. Daarna wordt dieper ingegaan op het fenomeen 'luxe surveillance' en deze

bijdrage wordt afgesloten met een reflectie over de implicaties van dit alles voor verder onderzoek naar big data policing.

2. Big data policing: vier vraagstukken

Policing is de activiteit om de samenleving veilig te maken, ook wel de politiefunctie genoemd (Bayley & Shearing, 2001; Schuilenburg, 2015). Een belangrijke socio-technische ontwikkeling binnen de politiefunctie is de opkomst van big data en algoritmes. Door verschillende wetenschappers is erop gewezen dat de politiefunctie "*cannot be understood without a sense of how the quest for 'big data' approaches are becoming increasingly central*" (Lyon, 2015: 68-69; Van Brakel, 2016). Voor een beter begrip van deze ontwikkeling onderscheid ik vier vraagstukken waarover nog onvoldoende duidelijkheid bestaat of rekenschap van wordt afgelegd in de literatuur.

2.1 Welke datasets en welke algoritmes?

Allereerst is het gebied van big data policing omgeven met verzameltermen waarover weinig tot geen duidelijkheid bestaat over de precieze betekenis en rol bij de uitvoering ervan in de praktijk. Big data wordt doorgaans uitgelegd aan de hand van 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' (*volume*, *velocity*, *variety* en *digital*) (Ridgeway, 2018). Verschillende wetenschappers wijzen erop dat meer duidelijkheid nodig is over het palet van databronnen en de integratie hiervan in uiteenlopende datasets om uitspraken te kunnen doen over de uitkomsten van de analyses van deze gegevens in het kader van de politiefunctie (Ferguson, 2017; Kirkpatrick, 2017). In het geval van criminologisch relevante databronnen kunnen verschillende datasets en subtypen worden onderscheiden, van *found data* (data die verzameld zijn door een passief, niet-observationeel dataverzamelingsproces) tot *automated data* (data die automatisch en inherent worden gegenereerd door apparaten en systemen). Snaphaan en Hardyns (2021) hebben in dit verband laten zien dat bij ieder van deze datasets op het vlak van de meetprocessen een aantal fouten kunnen optreden: specificatiefouten, meetfouten en verwerkingsfouten.

Ook kunnen algoritmes in verschillende typen worden onderverdeeld en bovendien voor verschillende rollen worden gebruikt in het kader van big data policing. Algoritmes lopen uiteen van eenvoudige – op regels gebaseerde – toepassingen, waaronder beslisbomen en data-uitwisselingssystemen, tot technisch zeer complexe toepassingen. In het laatste geval kan worden gedacht aan geluids- en beeldherkenningssystemen en zelflerende algoritmes, zoals machine learning en varianten hierop als deep learning (of een combinatie hiervan) die patronen voorspellen en nieuwe vormen van kennis destilleren uit gegevensbronnen. Met betrekking tot de rollen die ze vervullen kunnen algoritmes zowel voorspellend als realtime worden ingezet, maar ook worden gebruikt om terug te kijken in het verleden. In de politiepraktijk bijvoorbeeld kan een algoritme worden gebruikt om criminaliteitsvoorspellingen te doen of om informatie te verzamelen in het kader van actuele criminele fenomenen, bijvoorbeeld de drugshandel op het darkweb (Algemene Rekenkamer, 2022; Schuilenburg & Wessels, 2022).

Op basis van haar onderzoek naar big data policing door de politie van Los Angeles (LAPD) concludeert Brayne dat "*data are used for predictive, rather than reactive or explanatory, purposes*" (2017). Uit onderzoek naar de Nederlandse politiepraktijk blijkt echter dat de toepassing van algoritmes voor vormen van voorspellen nog het *minst* gebruikelijk is (Schuilenburg & Soudijn, 2021). De Nederlandse politie gebruikt vooral toepassingen die retrospectief en in het hier-en-nu en worden ingezet, variërend van automatische kentekenplaatherkenning (ANPR), drones, bewakingscamera's en gezichtsherkenningstechnologie, en waarmee grote databestanden gekoppeld worden, waardoor sneller informatie kan worden gevonden. Ondanks de populariteit van deze surveillancetools is de effectiviteit ervan nog grotendeels onbekend (*vraagstuk 3*). Ook hier geldt dat een beter zicht op het type algoritme dat wordt gebruikt bij een concrete toepassing noodzakelijk is om zowel de rol van het algoritme bij de uitvoering van de politiefunctie te kunnen duiden als de negatieve en positieve effecten ervan beter te kunnen identificeren (*vraagstuk 2*).

2.2 Welke ethische risico's en juridische vraagstukken?

Het tweede vraagstuk zijn de ethische risico's van en de juridische regelgeving omtrent bigdatatoepassingen op het gebied van policing. Dit komt in de kern neer op vragen of we bigdatatoepassingen *willen* gebruiken en, zo ja, hoe de data gebruikt *mogen* worden. In de literatuur over de risico's van big data policing keren aandachtspunten terug als digitale bureaucratisering (Peeters & Schuilenburg, 2018), *selffulfilling prophecies* en discriminatie van minderheden (e.g. Ferguson, 2017; O'Neil, 2016; Benjamin, 2019), vuile data (Richardson, Schultz & Crawford, 2019; Das & Schuilenburg, 2020) en het risico van controleverlies wanneer datasets, expertise en eigendomsrechten door publieke partijen uit handen worden gegeven aan commerciële bedrijven (Pasquale, 2015; Zuboff, 2019; Schuilenburg & Soudijn, 2021). Vanuit nationale wetgeving en de Europese Commissie worden daarom steeds meer eisen gesteld aan het ontwerp en gebruik van bigdatatoepassingen. Ook nieuwe technologieën zullen zich immers moeten verhouden tot grondwettelijke vereisten. De Europese Commissie heeft in de *Regulation on a European Approach for Artificial Intelligence* vier AI-systemen onderscheiden waarbij geldt dat er striktere regels gelden naarmate het risico dat de technologische toepassing met zich meebrengt, groter is. Ook heeft de Europese Unie een overzicht gemaakt van technologische eisen en ethische beginselen waaraan bigdatatoepassingen moeten voldoen, waaronder (a) respect voor menselijke autonomie, (b) preventie van schade, (c) rechtvaardigheid en (d) verantwoording.[3] Op die manier wil de Europese Unie burgers beter beschermen tegen de nadelige gevolgen van AI.

Een van de achterliggende ideeën hierbij is dat voor elk algoritme en elke dataset je kunt controleren hoe groot de ethische en juridische risico's hiervan zijn. Hiervoor is het wel noodzakelijk zicht te hebben op het type algoritme en de datasets die worden gebruikt bij een bigdatatoepassing (*vraagstuk 1*). Dat is nu nog onvoldoende het geval. Zo zullen de risico's voor burgers, denk aan zaken als etnisch profileren en discriminatie van minderheden, groter worden wanneer een algoritme volledig de vrije hand wordt gegeven. Bovendien, en nauw verbonden met de vorige lacune in de literatuur over big data policing, zal meer kennis nodig zijn welke bigdatatoepassingen daadwerkelijk worden gebruikt door partijen in het veilig maken van de samenleving. Zo zullen de

[3] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai Geraadpleegd 7 juni 2022.

ethische risico's van een concrete bigdatatoepassing anders zijn wanneer het gaat om een digitale tool om sociale netwerkanalyses te maken van berichten op in beslag genomen telefoons van criminelen ('terugkijken') als wanneer het gaat om het voorspellen van criminaliteit op basis van gegevens uit politiesystemen, aangevuld met informatie uit verschillende publieke datasets, in het geval van predictive policing bijvoorbeeld.

2.3 Welke bigdatatoepassingen werken?

Het derde vraagstuk is dat van *evidence-based policing*. Bigdatatoepassingen moeten bij voorkeur 'bewezen werkzaam' zijn en 'nut' hebben in de praktijk (De Wree, Devroe, Broer & Van der Laan, 2010). Dit is belangrijk voor zowel de acceptatie in de organisatie als de daadwerkelijke resultaten die worden bereikt met het gebruik ervan. Lastig is dat het empirische onderzoek naar de werkzaamheid van bigdatatoepassingen, variërend van cameragebruik (CCTV) tot gezichtsherkenningstechnologie, van beperkte omvang en vooral anekdotisch van aard is (Slobogin & Brayne, 2022). Een stevige empirische evaluatie van de effecten van bigdatatoepassingen ontbreekt en de schaarse evaluaties die er wel zijn laten tegenstrijdige resultaten zien. Zo is met betrekking tot predictive policing in een aantal Amerikaanse steden een positief effect vastgesteld, terwijl in Europese landen het toepassen van predictive policing geen aantoonbaar effect heeft gehad op het verminderen van vormen van criminaliteit, waaronder het aantal woninginbraken (e.g. Mohler et al., 2015; Mali et al., 2016; Meijer & Wessels, 2019; Ratcliffe et al., 2021).

Tegelijk prevaleert in de discussies over bigdatatoepassingen de technische kant ervan. Maar data en algoritmes moeten worden begrepen als "*being contingent, ontogenetic and performative in nature*" (Kitchin, 2017). Dit betekent dat ze voortdurend doorwerken in de dagelijkse praktijk en daarbij allerlei emoties en gevoelens oproepen bij zowel gebruikers als burgers. Het sociale aspect van big data policing gaat daarmee zowel over de inbedding ervan binnen organisaties die zich hiermee bezighouden, waarbij zaken als 'cultuur', 'discretionaire ruimte' en 'werkstijlen' een belangrijke rol spelen (e.g. Smircich, 1983; Reiner, 1985; Terpstra & Salet, 2020), als de impact ervan voor bepaalde groepen of gemeenschappen. Ook hier valt op dat stevige empirische studies naar, wat ik noem, de 'surveillance-ervaringen' van gebruikers en burgers met betrekking tot bigdatatoepassingen ontbreken, terwijl die ervaringen wel van invloed kunnen zijn op de resultaten van big data policing.

2.4 Welke veiligheidspartijen?

Het vierde vraagstuk is het speelveld van big data policing. Het gaat hierbij om de partijen die op dit gebied actief zijn. Sinds het einde van de twintigste eeuw is er sprake van een toenemende versplintering en privatisering van de politiefunctie, waarbij commerciële partijen een steeds belangrijke rol spelen in het veiligheidsvraagstuk (Schuilenburg, 2015). Kijken we naar de literatuur over big data policing, dan gaat de aandacht vooral uit naar de politieorganisatie en de toepassing van predictive policing, waarbij wordt geprobeerd te voorspellen wat de kans is op criminaliteit in een specifiek gebied en een bepaalde periode om daar vervolgens de inzet van de politie op af te stemmen (Perry e.a., 2013; Ratcliffe, 2014; Hardyns & Rummens, 2017). Hierbij wordt met name gelet op de Amerikaanse en Britse context. De risico's hiervan zijn dat er zowel te veel nadruk wordt gelegd op Angelsaksische bevindingen als dat wordt verondersteld dat de uitkomsten van deze onderzoeken ook voor andere landen opgaan,

waaronder Nederland en België (Neiva, Rafaela & Machado, 2022). Tegelijk worden bigdatatoepassingen op het gebied van veiligheid ook ingezet door andere partijen als de politie. De brede toepassing van big data op het gebied van de politiefunctie is vooral zichtbaar in *smart cities* waar private partijen zoals IBM, Cisco en Siemens met slimme technieken grootstedelijke problemen willen oplossen op tal van gebieden, waaronder criminaliteit en overlast (Kitchin 2014; Schuilenburg & Peeters, 2018; Schuilenburg & Pali, 2020). Data uit de stad en online apparaten waaronder sensoren en camera's worden hiervoor met elkaar gecombineerd om de stad meer leefbaar en veilig te maken. Een goed voorbeeld hiervan is crowdmanagementtechnologie, dataverzameling via sensoren en ontsloten door algoritmes om de veiligheid in de openbare ruimte te verbeteren.

Kijken we bij dit vraagstuk naar de partijen die actief zijn op het gebied van big data policing, dan kan een onderscheid worden gemaakt tussen partijen 'boven' (bv. Europese Unie), 'naast' (bv. private bedrijven en gemeenten) en 'onder' (burgers) de politie (cf. Loader, 2000). In de praktijk zal het onderscheid tussen deze categorieën in elkaar overlopen. Niet alleen zal het in veel gevallen gaan om een gezamenlijke inspanning om urgente veiligheidsproblemen aan te pakken. Ook kunnen private bedrijven bigdatatoepassingen ontwikkelen voor publieke partijen zoals de gemeente en de politie of zelf de gegevens verwerken en analyseren, wat weer tot risico's kan leiden zoals vendor lock-in (Zuboff, 2019). Om meer zicht te krijgen op de vraag welke partijen zijn actief zijn op het gebied van big data policing, ga ik in de volgende paragraaf dieper in op het hiervoor gemaakte onderscheid: door, boven, naast en onder de politie.

3. Big data policing: door, boven, naast en onder de politie

Hiervoor is gesteld dat het gebruik van bigdatatoepassingen om de samenleving veilig te maken niet exclusief is voorbehouden aan de politie (*vraagstuk 4*). Big data policing vindt ook plaats door partijen 'boven', 'naast' en 'onder' de politie die veiligheidstaken van de politie hebben overgenomen of in samenspraak met de politie uitoefenen. Om beter zicht te krijgen door 'wie' big data policing wordt uitgeoefend, worden deze vier categorieën hieronder verder besproken.

3.1 Big data policing 'door' de politie

De opkomst van big data policing binnen de politieorganisatie past in een historisch perspectief om de politieprestaties te verbeteren via het gebruik van data en statistische methoden. Dit begint in de negentiende eeuw wanneer gegevens worden bewerkt met statistische technieken om achterliggende patronen en verschillen in tijd en in plaats te ontdekken. Tot de grondleggers hiervan behoren wetenschappers als Adolphe Quetelet en André Michel Guerry (Morrisson, 1897; Beirne, 1987; Rienks & Schuilenburg, 2020). In de laatste twee decennia van de twintigste eeuw komt het fenomeen 'actuarial justice' op waarbij op basis van technieken uit de verzekeringswereld wordt geprobeerd het risico te voorspellen op crimineel gedrag (Simon, 1987; 1988; Feeley & Simon, 1994; Ericson & Haggerty, 1997). Ericson en Haggerty omschrijven in *Policing the risk society* politiemedewerkers als 'information managers' en laten zien hoe "*policing is subject to intensive 'informating' (translating events and objectives into visible information via formats) and 'automating' or 'fordization' (machine appropriation of human skills and labour*" (1997: 36).

Een andere stap naar big data policing binnen de politie zijn ontwikkelingen als *Intelligence Led Policing*, waarbij criminaliteitstrends in gebieden worden gevisualiseerd zodat de politie beter kan anticiperen op criminaliteit en overlast (Ratcliffe, 2016). Manning wijst in *The technology of policing* (2008) op de lange geschiedenis van 'crime mapping' en 'crime analysis', via de stadsdiagrammen van de Chicago School aan het begin van de twintigste eeuw tot de invoering van nieuwe instrumenten zoals Compstat ('Computer Stats') om sneller en nauwkeuriger informatie te krijgen over de ontwikkeling van criminaliteit in wijken van grote steden. Het bekendste voorbeeld van big data policing door de politie is het hiervoor genoemde predictive policing. Naast Amerikaanse systemen als PredPol en HunchLab worden in andere landen vergelijkbare applicaties toegepast met namen als Precobs (Duitsland), KeyCrime (Italië), Maprevelation (Frankrijk) en CAS (Nederland). Hoewel de werking van deze systemen onderling verschilt, delen ze de volgende kenmerken: het gebruik van algoritmes en big datasets met als doel te voorspelen of er een verhoogde kans is op criminaliteit binnen een bepaalde tijd en plaats.

3.2 Big data policing 'boven' de politie

Big data policing vindt niet alleen plaats door de politie, in de afgelopen decennia zijn toepassingen op dit gebied ook ontplooid door uiteenlopende initiatieven die opereren boven de nationale staat. Transnationaal big data policing (Sheptycki, 2000) gebeurt door samenwerking tussen nationale staten op internationaal niveau. Een actueel voorbeeld hiervan is het Prüm systeem, een Europees netwerk dat is opgericht voor de geautomatiseerde uitwisseling van vingerafdrukken, DNA-profielen en informatie over motorvoertuigen (Neiva, Rafaela & Machado, 2022). Joh (2014) noemt DNA-databanken één van de drie meest gebruikte toepassingen op het gebied van big data policing, naast het voorspellen van criminaliteit en massasurveillance. De Egmont Group of Financial Intelligence Units, een internationaal samenwerkingsverband die zich richt op het verbeteren van de internationale gegevensuitwisseling tussen landelijke financiële intelligence-eenheden, is een ander actueel voorbeeld. In een briefing geeft de Egmont Group aan dat zij betrokken is bij "*incorporating different digital tools to assist their operational efforts. These tools range from automation to the use of large datasets, big data and advanced analytics such as artificial intelligence (AI) and machine learning.*"[4] Big data en algoritmes vormen ook belangrijke speerpunten in de *Security Strategy* (2020-2025) van de Europese Unie. Zo stelt de Europese Unie dat "*artificial intelligence, space capabilities, Big Data and High Performance Computing are integrated into security policy in a way which is effective both in fighting crimes and in ensuring fundamental rights*".[5] Hierbij wordt onder meer verwezen naar de risico's van terrorisme, georganiseerde criminaliteit, drugshandel, mensensmokkel en cybercriminaliteit.

Transnationaal big data policing gebeurt ook door supranationale organisaties, waaronder Europol en EuroJust. Zo heeft Europol het Europol Informatie Systeem (EIS) opgezet, dat wordt gevuld door gegevens van politieorganisaties uit de Europese Unie.[6]

4 https://egmontgroup.org/wp-content/uploads/2022/01/Digital-Transformation-executive-summary.pdf Geraadpleegd 9 juni 2022.

5 https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605 Geraadpleegd 9 juni 2022.

6 https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-information-system. Geraadpleegd 31 mei 2022.

Tegelijk wil de Europese Unie het gebruik van bigdatatoepassingen op het gebied van de politiefunctie die aan een individueel belang raken beter reguleren. Dat blijkt uit de in de vorige paragraaf genoemde *Regulation on a European Approach for Artificial Intelligence* waarin een classificatie is gemaakt van 'hoog risico'-AI-systemen (Annex II), die onder meer worden gebruikt door de politie ('systems for predicting the occurrence of crimes') en de rechterlijke macht ('systems to assist judges at court'). In de AI Act zijn bovendien strikte eisen gesteld aan bigdatatoepassingen in de rechtshandhaving die onder meer worden gebruikt voor (i) het voorspellen van een daadwerkelijk of potentieel strafbaar feit, (ii) de profilering van personen tijdens de opsporing van strafbare feiten en (iii) misdaadanalyses waarmee grote hoeveelheden data worden doorzocht om onbekende patronen op te sporen of verborgen relaties te ontdekken in de gegevens.[7]

3.3 Big data policing 'naast' de politie

De snelle groei en populariteit van big data policing komt mede doordat andere overheidspartijen (denk hierbij aan gemeenten en bijzondere opsporingsdiensten) en private bedrijven steeds meer digitale activiteiten ontplooien om zelf de samenleving veilig te maken. Zo gebruiken verschillende Nederlandse gemeenten digitale opsporingstools om criminaliteit en ander risicovol gedrag te voorspellen, zoals het Systeem Risico Indicatie (SyRI) om fraude met sociale voorzieningen op te sporen in achterstandswijken van grote steden. Tegelijk werken tal van private partijen, van Apple tot Tesla, met grote datasets en algoritmes en zijn daarbij aan minder regels gebonden dan de nationale staat en publieke partijen. Hierbij zal het vaak gaan om klassieke surveillancedoelen als het naleven van regels ('compliance') en het voorkomen van criminaliteit ('preventie'). Maar big data policing door private partijen kan ook andere doelen hebben, van verificatie van een persoon tot het maken van winst en het verkrijgen van strategisch voordeel (Marx, 2016: 65). Zo verwerken technologiebedrijven bigdatatoepassingen in 'smart homes' (Sadowski, Strengers & Kennedy, 2021) en in voertuigen (Feldstein, 2019; Cooke, 2021) om verdachte gebeurtenissen in en rondom die objecten te signaleren. In dit verband wordt onder meer gesproken van luxe surveillance waarvoor "*[p]eople pay for and whose tracking, monitoring, and quantification features are understood by the user as benefits they are likely to celebrate*" (Gilliard & Golombia, 2021). Een goed voorbeeld van luxe surveillance is de Sentry-bewakingsmodus in de elektrische auto's van Tesla waarmee zowel het rijgedrag van de bestuurder als de omgeving buiten de auto wordt gemonitord en geregistreerd op verdachte bewegingen, om bijvoorbeeld onvoorzichtige fietsers of potentiële autodieven vast te leggen (Eski & Schuilenburg, 2022). Een andere belangrijke ontwikkeling op het gebied van big data policing 'naast' de politie is dat techbedrijven via digitale platforms hun slimme surveillance (en de updates) verkopen en daarbij hun klanten monitoren op hun gedrag. Politiewerk wordt zo steeds meer platform policing. 'Cloud' of 'platform policing' is aantrekkelijk voor commerciële partijen "*as they can potentially access a wide suite of new software applications and technologies through rental contracts and can additionally tailor these to the specific needs of their agency*" (Wilson, 2021: 51).

7 https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206. Geraadpleegd 31 mei 2022.

3.4 Big data policing 'onder' de politie

In de praktijk kunnen ook burgers beschikken over bigdatatoepassingen om de veiligheid te verbeteren. Hierbij kan onder meer worden gedacht aan apps op smartphones die in combinatie met sensordata, waaronder intelligente camera's en geluidssensoren, verdachte bewegingen in de wijk melden. Wereldwijd patrouilleren steeds meer burgers in buurtpreventieteams en maken daarbij gebruik van speciaal hiervoor ontworpen apps. Deze digitale 'do-it-yourself surveillance' groepen (Jacobs, 1961) delen daarbij informatie op Facebookpagina's met hun volgers (Westall, 2019; Van Steden & Mehlbaum, 2021). Een ander voorbeeld van big data policing 'onder' de politie is de hiervoor genoemde slimme deurbel van Amazon-dochterbedrijf Ring, waarmee bewoners kunnen zien wie aanbelt bij hun woning of door de straat loopt (West, 2019). Dergelijke systemen nemen de hele dag beelden op en de gebruikers ervan kunnen deze beelden later terugkijken en delen met andere personen. Morris schrijft dat bewoners zich hierdoor veiliger voelen en meer controle menen te hebben over hun leefomgeving: "*People like them because they think that crime is rising and they say it helps them feel safer in their homes and in their neighborhood*" (2021: 241). In de Verenigde Staten werkt Ring inmiddels samen met ruim vierduizend politiekorpsen, waardoor de beelden die de slimme deurbel maakt door burgers kunnen worden gedeeld met de politie via de 'neighbours-app'.[8] Hierdoor ontstaat er letterlijk een volledig nieuwe surveillance-ring in stedelijke gebieden om buurten veiliger te maken, wat juridische problemen oproept als waar de private ruimte eindigt en de publieke ruimte begint (*vraagstuk 2*). Dit alles leidt – tot slot – tot de vraag wat luxe surveillance is en hoe ze doorwerkt in de praktijk van big data policing.

4. Luxe surveillance: vier kenmerken

De Ring deurbel wordt op de website van Amazon als volgt gepromoot: 'Houd alles in de gaten. Zowel binnen als buiten.' Het verzamelen, opslaan en analyseren van gegevens en het bijbehorende gedrag van de kijkers en bekeken personen is een vorm van 'consumer surveillance' (Pridmore, 2012). Commerciële bedrijven kunnen hierbij met behulp van big data en algoritmes het gedrag van consumenten monitoren en de producten die ze aanbieden, kunnen worden aangepast op basis van de uitkomsten van de analyses. Naast de deurbel van Amazon zijn er talloze andere voorbeelden van luxe surveillance op de markt. Een bekend voorbeeld hiervan is de iRobot vacuümstofzuiger waarin smart mapping-technologie is verwerkt. Deze technologie zorgt ervoor dat het huis van de gebruiker in kaart wordt gebracht zodat de stofzuiger hierdoor slimmer kan navigeren door de kamers van je woning. Een ander voorbeeld van luxe surveillance is de Ray-Ban Stories bril, een slimme bril die is ontwikkeld door Facebook en Ray-Ban. In de bril zijn camera's verwerkt voor het maken en opnemen van video's en foto's. Ook zijn microfoons ingebouwd voor telefoongesprekken en het geven van spraakcommando's. Maar denk bij luxe surveillance ook aan de elektrische auto's van Tesla met de ingebouwde Sentry-bewakingsmodus waarbij de scheiding tussen kijker en geobserveerde steeds ondoorzichtiger wordt (Marx, 2016; Eski & Schuilenburg, 2022).

[8] https://www.theverge.com/2021/1/31/22258856/amazon-ring-partners-police-fire-security-privacy-cameras. Geraadpleegd 29 oktober 2022.

Luxe surveillance is onderdeel van socio-technische ontwikkelingen als de versplintering van de politiefunctie en de democratisering van surveillance. Om een beter begrip van de impact hiervan te krijgen op het gebied van big data policing, onderscheid ik vier kenmerken van luxe surveillance. Aan de hand hiervan wordt de complexiteit van de politiefunctie duidelijk in tijden van big data en algoritmes.

4.1 Vrijwillige basis

Gilliard en Golombia stellen in het artikel 'Luxury surveillance' (2021) dat personen luxe surveillanceproducten vrijwillig aanschaffen met als doel zowel toezicht op anderen als op zichzelf te houden: *zelf-surveillance*. Gegevens waar deze personen eerder geen kennis van hadden – bijvoorbeeld je remgedrag (Tesla) of je hartslag en het aantal uren dat je slaapt gedurende de nacht (Fitbit) – worden zo toegankelijk en inzichtelijk gemaakt. Stark en Levy (2018) spreken in dit verband van de opkomst van de *surveillant consumer,* een ontwikkeling waarbij surveillance plaatsvindt van consumenten en waarbij die consumenten ook zelf surveillance-activiteiten uitvoeren. Opvallend is dat dit op vrijwillige basis gebeurt en dat personen bereid zijn hiervoor veel geld te betalen. Luxe surveillance verschilt daarmee, zo schrijven Gilliard en Golombia, van *imposed surveillance*: "*surveillance the subject would prefer not to have but is required to for one reason or another*" (2021). Denk in het laatste geval aan de elektronische enkelband, een soort van Apple Watch voor gestraften, waarmee gedetineerden hun straf buiten de muren van de cel ondergaan omdat via een zendertje in de enkelband kan worden gecontroleerd waar zij zich bevinden.

4.2 Exclusiviteit (levensstijl)

Er hangt een flinke prijskaart aan luxe surveillance, wat maakt dat ze voor bepaalde personen een uithangbord zijn om hun identiteit en status mee uit te drukken. Zo betaal je voor de duurste versie van de Ray-Ban Stories-bril 409 euro en van de robotstofzuiger is een versie op de markt die 2198 euro kost. De doelgroep van deze producten zijn vaak jonge mensen met een hoog opleidingsniveau en inkomen die het bezit ervan, van een Tesla-auto bijvoorbeeld, zien als 'statussymbool' (Li et al., 2021). Luxe surveillance is daarmee nauw verbonden met een exclusieve levensstijl waarmee personen zich kunnen onderscheiden van andere consumenten. Fabrikanten van deze producten spelen hierop in door deze surveillance aan te prijzen via verschillende vormen van 'storytelling' met als doel "*securing and strengthening their market position*" (Söderström, Paasche & Klauser, 2014: 309). Zo kreeg Tesla in 2020 een prijs van de lezers van PC Magazine voor de beste auto met connectiviteitsfuncties waarmee Tesla haar belofte zou waarmaken dat "de auto van de toekomst autonoom, verbonden, elektrisch en gedeeld zal zijn".[9] 'Storytelling' is zo een strategisch middel om luxe surveillance te verkopen door een alternatieve versie van de werkelijkheid te laten zien waarmee kapitaalkrachtige personen zich kunnen identificeren. De slogan 'Tech for good' is hiervan een actueel voorbeeld. Zo worden de duurzame e-bikes en bijbehorende app van het futuristische Nederlandse fietsenmerk VanMoof aangeprezen als: "VanMoof S3 & X3 transformeren steden over de hele wereld. Ervaar de toekomst zelf."[10]

9 https://insideevs.com/news/432348/tesla-connected-car-award-pc-magazine-readers Geraadpleegd 15 juni 2022.

10 https://www.vanmoof.com/blog/nl/building-the-future-de-ontwikkeling-van-onze-app Geraadpleegd 15 juni 2022.

4.3 Coolness (esthetiek)

Luxe surveillanceproducten zijn bedoeld om in positieve zin visueel op te vallen en hebben een bepaalde *coolness* voor de gebruikers ervan (Gilliard & Golumbia, 2021). Zo streeft Tesla naar een futuristisch en 'cool' ontwerp voor hun elektrische auto's. Veel van deze luxeproducten hebben dan ook een *sleek* en compact uiterlijk, denk aan de Apple Watch of Fitbit die boordevol sensoren zitten zoals een omgevingslicht, elektrische hartslagsensor en temperatuursensor. Fergusson (2011) omschrijft cool "*as being in opposition to mainstream culture; whatever holds with the norms and values of mainstream culture inherently cannot be cool*". Relevant is dat dergelijke producten vaak onderdeel zijn van een 'brandscape' (Wood & Ball, 2013), plekken waar consumenten aan een merk wordt gebonden en waar ze voortdurend worden verleid om ernaar terug te keren. Een goed voorbeeld van zo'n plaats voor luxeproducten is een digitaal platform waar personen lid van kunnen worden om hier gebruik te kunnen maken van de digitale surveillancetechnologieën van techbedrijven zoals Amazon, van de Amazon Halo (fitnessarmband met gezondheidsmetingen), Amazon Echo Dot (luidspreker die verbinding maakt met Amazon Alexa, een in de cloud gebaseerde spraakdienst, om muziek af te spelen, timers en alarmen in te stellen en compatibele smart home-apparaten te bedienen) en de Amazon Astro Robot (robot op wielen om taken in huis uit te voeren) – producten die allemaal met elkaar kunnen worden verbonden.

4.4 Platform surveillance (abonnement)

Luxe surveillance wordt vaak aangeboden met een maandelijks abonnement, met als doel op die manier de kwaliteit en effectiviteit van deze producten – en daarmee de surveillance – te optimaliseren. Het gaat hierbij dus om digitale platforms en digitale surveillancetechnologie waarbij de content alleen kan worden bekeken wanneer je lid hiervan bent. In het geval van de meest luxe versie van de Amazon Ring deurbel kun je lid worden van een webplatform waarop anoniem videobeelden worden gedeeld die met de Ring Bel zijn opgenomen. Ook ontvangen de gebruikers van dit platform meldingen over 'verdachte' activiteiten in hun wijk. Op vergelijkbare wijze werkt de Fitbit. Hiervoor is een Premium-abonnement nodig om toegang te krijgen tot de meetwaarden ervan. Met de Tesla-app, een ander voorbeeld van luxe surveillance, kunnen de bezitters van Tesla-auto's de nieuwste functionaliteiten in hun voertuig installeren via een draadloze verbinding tussen de app en hun auto. Hierdoor kunnen personen niet alleen zichzelf monitoren (*zelf-surveillance*), maar worden ze zelf ook weer bekeken door het bedrijf dat alle gegevens op het betreffende platform verzamelt (*co-surveillance*). Zo kan onder meer worden gemonitord wat de persoonlijke voorkeuren van de gebruikers zijn op basis waarvan de bedrijven nieuwe diensten en producten ontwikkelen en specifieke marketing inzetten. Zuboff (2019) noemt de informatie die op deze platforms wordt achtergelaten door alle activiteiten en gedragingen *behavioral surplus*. In haar boek *The age of surveillance capitalism* haalt Zuboff Eric Schmidt aan, voormalig CEO bij Google, die stelt dat "*almost nothing, short of a biological virus, can scale as quickly, efficiently, or aggressively as these technology platforms, and this makes the people who build, control, and use them powerful too*" (2019: 180).

5. Conclusie en discussie

Dit hoofdstuk heeft als doel het fenomeen van big data policing breder te trekken dan tot nu toe wordt gedaan in de literatuur hierover. Verschillende elementen van big data policing zijn hiervoor uitgediept, waaronder de uiteenlopende partijen die actief zijn op dit gebied en het fenomeen van luxe surveillance. Om de implicaties van de geschetste ontwikkelingen beter te kunnen onderkennen, zijn in dit hoofdstuk vier vraagstukken benoemd waarover nog onvoldoende wetenschappelijk duidelijkheid bestaat, waaronder de verschillende type datasets en algoritmes die worden gebruikt voor verschillende bigdatatoepassingen. Een beter zicht op deze datasets en algoritmes is noodzakelijk omdat op basis hiervan ook de ethische risico's en juridische vraagstukken omtrent een concrete bigdatatoepassing beter kunnen worden geduid. Dit alles leidt tot de volgende vier bevindingen.

Ten eerste is geconstateerd dat het gebruik van bigdatatoepassingen op het gebied van veiligheid mede wordt ingezet door andere partijen als de politie. Dit is de socio-technische trend van versplintering van de politiefunctie genoemd en in dit verband is een onderscheid gemaakt tussen partijen 'boven', 'naast' en 'onder' de politie. In de praktijk zal dit onderscheid in elkaar overlopen, zoals in het geval van de voorbeelden van luxe surveillance ('naast' en 'onder' de politie). Zo worden in de Verenigde Staten de beelden van de Ring videodeurbellen – van het moederbedrijf Amazon – gedeeld met meer dan vierduizend politiekorpsen. Het bedrijf spreekt in dit verband van 'een moderne buurtwacht'.[11]

Ten tweede valt op basis van dit hoofdstuk te constateren dat big data policing, van smartphone-applicaties tot surveillanceproducten zoals de Ring Bel, Fitbit, Apple Watch en de elektrische auto's van Tesla – als het ware is gedemocratiseerd of genormaliseerd (Stark & Levy, 2018). Andrejevic (2012) spreekt in dit verband van 'ubiquitous surveillance' en verwijst hiermee naar een samenleving waarin het steeds moeilijker is te ontsnappen aan digitale surveillance.[12] Zo zijn veel van de genoemde voorbeelden van luxe surveillance, die aanvankelijk alleen waren weggelegd voor een kleine groep van welvarende personen, in de loop van de tijd steeds meer betaalbaar geworden voor een groter publiek.

Ethische risico's als geautomatiseerd etnisch profileren worden nu in een adem genoemd met instrumenten als predictive policing waarmee politieorganisaties criminaliteit proberen te voorkomen. Maar dergelijke ongewenste effecten spelen ook een rol bij andere vormen van big data policing, zoals Dixon (2017) heeft aangetoond bij buurt-whatsapp-groepen in Zuid-Afrika. Dit is de derde bevinding. Dit betekent dat het debat over ethische risico's en juridische vraagstukken omtrent big data en algoritmes op het gebied van de politiefunctie breder moet worden gevoerd. In dat licht is het interessant

[11] https://www.rtlnieuws.nl/tech/artikel/4829646/amazon-dochterbedrijf-ring-slimme-cameras-deurbellen-beelden-delen-polite Geraadpleegd 18 juni 2022.

[12] In de bestuurskunde wordt gesproken van de bredere trend naar een 'algocratie' (Aneesh, 2009) waarbij steeds meer aspecten van het leven beheerd en bestuurd worden door algoritmes die op basis van grote hoeveelheden datasets besluiten voor ons nemen. Andere termen die in dit verband worden gebruikt, zijn 'algorithmic regulation' (O'Reilly 2013; Yeung 2017; 2018) en 'algorithmic governmentality' (Rouvroy & Berns, 2013; Rouvroy & Stiegler, 2016; Hannah-Moffat, 2019) (zie voor de verschillen tussen deze termen: Peeters & Schuilenburg, 2023).

dat het bedrijf Ring op dit moment werkt aan een gezichtsherkenningssysteem waarbij er een signaal komt via de functie 'watch list' wanneer een 'verdachte persoon' wordt herkend op de camerabeelden van de deurbel.

De vierde en laatste bevinding sluit nauw aan bij de voorgaande bevindingen. Wanneer het gemaakte onderscheid tussen partijen 'boven', 'naast' en 'onder' de politie in de praktijk door elkaar loopt, zoals bij de Amazon Ring Bel, zal ook meer zicht moeten worden verkregen op de algoritmes die worden gebruikt om datasets te kunnen delen tussen partijen. Denk hierbij niet alleen aan het delen van informatie tussen private partijen, maar ook aan ketenpartners als gemeenten en de politie op het gebied van veiligheid. Ook vragen rond de borging en beheer van deze gedeelde datasets worden dan belangrijk.

Kortom, veel onderzoek naar big data policing heeft een beperkte focus. Er wordt vaak ingezoomd op een specifiek aspect, van een ethisch risico zoals etnisch profileren tot een concrete toepassing door de politieorganisatie, waardoor de samenhang en het overzicht verloren gaan van de verschillende vraagstukken rondom big data policing en de publieke en private partijen die op dit gebied actief zijn. Toekomstig onderzoek naar big data policing zal daarom zowel breder als empirischer moeten plaatsvinden – en de manier waarop dat gebeurt, begint bij een betere conceptualisering van dit onderwerp dat in de komende jaren steeds belangrijker gaat worden.

Bibliografie

Algemene Rekenkamer (2022), *Algoritmes getoetst. De inzet van 9 algoritmes bij de overheid*. Den Haag.

Andrejevic, M. (2012), Ubiquitous surveillance. In: K. Ball, K. Haggerty & D. Lyon (eds.), *Routledge Handbook of Surveillance Studies* (pp. 91-98). New York: Routledge.

Aneesh, A. (2009), Global Labor: Algocratic Modes of Organization. *Sociological Theory,* 27 (4): 347-370.

Bayley, D.H. & C. Shearing (2001), *The New Structure of Policing: Description, Conceptualization, and Research Agenda*. Washington, DC: National Institute of Justice.

Beirne, P. (1987), Adolphe Quetelet and the Origins of Positivist Criminology, *American Journal of Sociology,* 92(5), 1140-1169.

Benjamin, R. (2019), *Race After Technology: Abolitionist Tools for the New Jim Code*. Cambridge: Polity Press.

Brayne, S. (2017), Big Data Surveillance: 'The Case of Policing', *American Sociological Review, 82*(5), 977-1008.

Brayne, S. (2021), *Predict and Surveil. Data, Discretion, and the Future of Policing*. Oxford: Oxford University Press.

Cooke, P. (2021), Three Disruptive Models of New Spatial Planning: "Attention", "Surveillance" or "Sustainable" Capitalisms? *Journal of Open Innovation: Technology, Market, and Complexity,* 7(46), 1-20.

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

De Wree, E., Devroe, E., Broer, W. & Van der Laan, P. (red.) (2010), Evidence-based policing, *Cahier Politiestudies*, 17. Antwerpen/Apeldoorn: Maklu.

Dixon, N. (2017), Stranger-ness and Belonging in a Neighbourhood WhatsApp Group, *Open Cultural Studies*, 1, 493-503.

Ericson, R.V. & K. Haggerty (1997), *Policing the risk society*. Toronto: University of Toronto Press.

Eski, Y. & M. Schuilenburg (2022), On Tesla: Balancing sustainable car connectivity, silent lethality and luxury surveillance (with Y. Eski), *Criminological Encounters*, 5(1), 234-251.

Feeley, M. & J. Simon (1994), 'Actuarial justice. The emerging new criminal law'. In: D. Nelken (ed.), The futures of criminology (pp. 173-201). London: Sage.

Feldstein, S. (2019), *The global expansion of AI surveillance* (Vol. 17). Washington, DC: Carnegie Endowment for International Peace.

Ferguson, S. (2011) A global culture of cool? Generation Y and their perception of coolness. *Young Consumers*, 12 (3): 265-275.

Ferguson, A.G. (2017), *The rise of big data policing. Surveillance, race, and the future of law enforcement*. New York University Press.

Gilliard, C. & D. Golombia (2021), Luxury Surveillance: People pay a premium for tracking technologies that get imposed unwillingly on others, *Real Life Magazine*, July 6.

Hannah-Moffat, K. (2019), Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates. *Theoretical Criminology*, 23(4), 453-470.

Hardyns, W. & A. Rummens (2017), Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges. *European Journal on Criminal Policy and Research, 24*, 201-218.

Jacobs, J. (1961), *The Death and Life of Great American Cities*. New York, NY: Vintage Books.

Joh, E. (2014), Policing by numbers: Big Data and the fourth amendment. *Washington law review*, 89(1), 35-68.

Kirkpatrick, K. (2017), It's not the algorithm, it's the data. *Communications of the ACM*, *60*(2), 21-23.

Kitchin, R. (2014), The real-time city? Big data and smart urbanism. *GeoJournal*, 79 (1): 1-14.

Kitchin, R. (2017), Thinking Critically about and Researching Algorithms. *Information Communication & Society*, 20, 14-29.

Li, Y., Lin, J. & Xu, S. (2021). *Analysis of Tesla's Business Model: A Comparison with Toyota*. 2021 International Conference on Financial Management and Economic Transition (FMET 2021), Guangzhou, China. doi.org/10.2991/aebmr.k.210917.006

Loader, I. (2000), Plural policing and democratic governance, *Social and Legal Studies*, 9(3), 323-345.

Lyon, D. (2015), *Surveillance after Snowden*. New York: Polity.

Mali, B., C. Bronkhorst-Giesen, & M. den Hengst (2017), *Predictive policing: lessen voor de toekomst. Een evaluatie van de landelijke pilot*. Apeldoorn: Politieacademie.

Manning, P. (2008), *The technology of policing: Crime mapping, information technology, and the rationality of crime control*. New York & London: NYU-Press.

Marx, G. (2016), *Windows into the Soul, Surveillance and society in an age of high technology*. Chicago: University of Chicago Press.

Meijer, A. & M. Wessels (2019), Predictive Policing; Review of Benefits and Drawbacks. *International Journal of Public Administration*, *42*, 1031-1039.

Mohler, G.O., M.B. Short, S. Malinowski, & M. Johnson (2015) Randomized Controlled Field Trials of Predictive Policing. *Journal of the American Statistical Association*, *110*(512), 399-1411.

Morozov, E. (2013), *To save everything, click Here*. New York: Public Affairs Books.

Morris, J. (2021), Surveillance by Amazon: The warrant requirement, tech exceptionalism, & Ring security, *Boston University Journal of Science & Technology Law, 27*, 237-269.

Morrison, W. (1897), The interpretation of criminal statistics, *Journal of the Royal Statistical Society*, 60, 1-24.

Neiva, L., G. Rafaela, & H. Machado (2022), Big Data applied to criminal investigations: expectations of professionals of police cooperation in the European Union, Policing and Society: 10.1080/10439463.2022.2029433.

O'Reilly, T. (2013), Open Data and Algorithmic Regulation. In: Goldstein, B., & Dyson, L. (eds.) *Beyond Transparency: Open Data and the Future of Civic Innovation*, pp. 289-300. Code for America Press, San Francisco.

Pali, B. & Schuilenburg, M. (2020), Fear and Fantasy in the Smart City, *Critical Criminology: An International Journal*, (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. & M. Schuilenburg (2018), Machine justice: Governing security through the bureaucracy of algorithms, *Information Polity*, *23*(3), 267-280.

Peeters, R. & M. Schuilenburg (2023), Algorithmic Governance: Technology, Power, and Knowledge. In: W. Housley, A. Edwards, R. Montagut & R. Fitzgerald (eds.), *The SAGE Handbook of Digital Society*, London: Sage, 439-457.

Perry, W.L. et al. (2013), *Predictive Policing, the Role of Crime Forecasting In Law Enforcement Operations*, Santa Monica: RAND Corporation.

Pridmore, J. (2012). Consumer surveillance: Context, perspectives and concerns in the personal information economy. In: *Routledge Handbook of Surveillance Studies*, K. Ball, K.D. Haggerty & D. Lyon (eds.), pp. 321-329. London and New York: Routledge.

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

Ratcliffe, J. (2016), *Intelligence Led Policing*, London: Routledge.

Ratcliffe, J.H., R.B. Taylor, A.P. Askey, K. Thomas, J. Grasso, K. Bethel, R. Fisher, & J. Koehnlein (2021), The Philadelphia predictive policing experiment. *Journal of Experimental Criminology, 17*(1): 15-41.

Richardson, R., J. Schultz & K. Crawford (2019), Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. *New York University Law Review Online, 94*(192): 192-233.

Ridgeway, G. (2018), Policing in the Era of Big Data, *Annual Review of Criminology,* 1, 401-419.

Rienks, R. & M. Schuilenburg (2020), Wat is er nieuw aan het voorspellen van criminaliteit? Over de ambities en knelpunten bij de implementatie van predictive policing. *Cahiers Politiestudies 54: Informatiegestuurde politie*, 39-54.

Rouvroy, A. & Berns, T. (2013), Algorithmic governmentality and prospects of emancipation. *Réseaux,* (1), 163-196.

Rouvroy, A. & Stiegler, B. (2016), The digital regime of truth: from the algorithmic governmentality to a new rule of law. *La Deleuziana: Online Journal of Philosophy, 3*, 6-29.

Sadowski, J., Strengers, Y., & Kennedy, J. (2021), More Work for Big Mother: Revaluing Care and Control in Smart Homes. *Economy and Space,* 1-16. doi: 10.1177/0308518X211022366.

Schuilenburg, M. (2015), *The securitization of society: Crime, risk, and social order.* New York: New York University Press.

Schuilenburg, M. & Peeters, R. (2018), Smart Cities and the Architecture of Security: Pastoral Power and the Scripted Design of Public Space. *City, Territory and Architecture,* 5(13), 1-9.

Schuilenburg, M. & M. Wessels (2022), Vier handvatten voor betrouwbare algoritmische toepassingen in het politiewerk, *Het tijdschrift voor de politie, 3, te verschijnen.*

Sheptycki, J.W.E. (ed.) (2000), *Issues in Transnational Policing*, London & New York: Routledge.

Simon, J. (1987), The emergence of a risk society. Insurance, law and the state, *Socialist Review*, 97, 61-89.

Simon, J. (1988), The ideological effects of actuarial practices, *Law and Society Review*, 22(4), 771-800.

Slobogin, C. & S. Brayne (2022), Surveillance Technologies and Constitutional Law, *Annual Review of Criminology,* vol. 6, pp. 1-22.

Smith, G.J.D., L.B. Moses, & J. Chan (2018), 'The Challenges of Doing Criminology in the Big Data Era: Towards a Digital and Data-driven Approach', *The British Journal of Criminology, 57*(2), 259-274.

Smith, G.J.D. & P. O'Malley (2017), 'Driving politics: Data-driven governance and resistance', *British Journal of Criminology*, 57(2), 275-298.

Snaphaan, T. & W. Hardyns (2021), Handvatten voor een kwaliteitsbeoordeling van big data: de introductie van het Total Error raamwerk. *Tijdschrift voor Veiligheid, (20)*4, 63-88.

Söderström, O., Paasche, T. & F. Klauser (2014). Smart cities as corporate storytelling. *City,* 18 (3): 307-320.

Stark, L. & K. Levy (2018), The surveillant consumer, *Media Culture & Society, 40*(8), 1202-1220.

Terpstra, J. & R. Salet (2020), Big Data Policing als sociale praktijk. Schets van een miskend, maar urgent onderzoeksterrein. *Cahiers Politiestudies 54: Informatiegestuurde politie,* 25-38.

Van Brakel, R. (2016), Pre-emptive big data surveillance and its (dis)empowering consequences: the case of predictive policing. In: B. van der Sloot, D. Broeders & E. Schrijvers (eds.), *Exploring the boundaries of big data*, Amsterdam: AUP, 117-141.

Van Steden, R. & S. Mehlbaum (2021), Do-it-yourself surveillance: The practices and effects of WhatsApp Neighbourhood Crime Prevention groups, *Crime, Media, Culture*, https://doi.org/10.1177/17416590211041017.

West, E. (2019), Amazon: Surveillance as a Service, *Surveillance & Society*, 17(1/2), 27-33.

Westall, J. (2019), Volunteer street patrols: An ethnographic study of three Manchester volunteer street patrols and their role in community safety and the policing family. PhD Thesis. Manchester Metropolitan University, Manchester.

Wilson, D. (2021), The New Platform Policing. In: A. Završnik & V. Badalic (eds.), Automating Crime Prevention, Surveillance, and Military Operations (pp. 47-68). Cham: Springer.

Wood, D.M. & Ball, K. (2013). Brandscapes of control? Surveillance, marketing and the co-construction of subjectivity and space in neo-liberal capitalism. *Marketing Theory, 13*(1), 47-67.

Yeung, K. (2017), '"Hypernudge": Big Data as a mode of regulation by design', *Information, Communication & Society,* (20) 1: 118-136.

Yeung, K. (2018), Algorithmic regulation: A critical interrogation. *Regulation & Governance,* 12 (4): 505-523.

Zedner, L. (2007), 'Pre-crime and post-criminology?', *Theoretical Criminology,* 11(2), 261-281.

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.