De zegen en vloek van digitale politiesurveillance

Wouter Landman

Op de bovenste verdieping van het Amsterdamse hoofdbureau zitten zo'n dertig agenten achter aaneengeschakelde computerschermen. Op de schermen: kaarten van Amsterdam, openstaande databases en een gekleurde lijst met meldingen die zijn binnengekomen via 112. Op een gigantische zwarte wand komen live camerabeelden van de hele stad voorbij. Fietsers die zoeven over een kruispunt, jongeren die hangen op de Dam, het Leidseplein. De camera's zoomen voortdurend in op personen. Dit is het Real Time Intelligence Center (RTIC) van de eenheid Amsterdam. Zijn kerntaak: snel informatie verzamelen bij schietpartijen, overvallen, straatroven, huiselijk geweld en andere 112-meldingen waar iedere seconde telt. Terwijl politieagenten met loeiende sirenes op een melding afgaan, moeten de medewerkers van het RTIC binnen enkele minuten zo veel mogelijk informatie in kaart brengen. Ten behoeve hiervan raadplegen zij politiesystemen, sociale media en (andere) open bronnen. Het RTIC van Amsterdam speelde op 6 juli 2021 een cruciale rol in de aanhouding van de verdachten van de aanslag (later moord) op Peter R. de Vries. Op camerabeelden werd de grijze Renault van de vermeende schutter gesignaleerd, maar het kenteken was niet volledig leesbaar. Door het raadplegen van systemen werd het gehele kenteken gevonden. Dit kenteken werd ingevoerd in een referentielijst voor het netwerk met camera's met *Automatic Number Plate Recognition* (ANPR). Zo kon de vluchtauto worden gevolgd en op de A4 bij Leidschendam worden klemgereden door politieauto's. Naar aanleiding van de aanhouding van de verdachten vergeleek de chef van het RTIC de gang van zaken met voorheen. Hij zei:

> 'Tien tot vijftien jaar geleden werden verdachten in soortgelijke situaties minder snel gepakt. Toen moesten de lokale eenheden op een viaduct boven de snelweg of op de vluchtstrook worden gepositioneerd om te zien of de verdachten voorbijkwamen.'[1]

1 Politiesurveillance: activiteiten van burgers zichtbaar maken

In *Windows into the soul* laat Gary Marx (2016) zien dat het begrip 'surveillance' in ons taalgebruik vaak op vage en ongedefinieerde wijze wordt gebruikt. De term is gerelateerd aan het Latijnse begrip 'vigilare': het in de gaten houden van hen beneden. In dit essay staat het in de gaten houden van burgers door de politie centraal: politiesurveillance. Surveillance is een belangrijk onderdeel van politiewerk. In de

1 Deze beschrijving is gebaseerd op www.nrc.nl/nieuws/2021/07/16/hoe-verdachten-aanslag-peter-r-de-vries-zo-snel-konden-worden-gearresteerd.

doi: 10.5553/TCC/221195072023013002005

samenleving speelt zich een voortdurende stroom van activiteiten en gebeurtenissen af: burgers zijn met iets bezig (Landman, 2015). Burgers kunnen met hun activiteiten inbreuk maken op de openbare orde of strafrechtelijke orde in de samenleving. Het is dan aan de politie om op te treden. Om dit te kunnen doen, moet zij activiteiten van burgers zichtbaar maken (Stol, 1996).
Er vindt bij voortduring ontwikkeling plaats in de wijze waarop de politie activiteiten van burgers zichtbaar maakt. Dit wordt veroorzaakt door het type activiteiten dat burgers uitvoeren én door de mogelijkheden die de politie heeft om activiteiten van burgers zichtbaar te maken. Technologische ontwikkelingen in de samenleving beïnvloeden beide. Digitale technologie heeft er bijvoorbeeld toe geleid dat burgers steeds meer activiteiten online uitvoeren, én heeft de politie allerlei nieuwe mogelijkheden geboden om offline en online activiteiten van burgers zichtbaar te maken. Dit essay gaat over deze nieuwe mogelijkheden. Mijn stelling is dat digitale politiesurveillance fundamenteel verschilt van traditionele politiesurveillance en dat dit zowel een zegen als een vloek is.

2 Digitale politiesurveillance: een fundamentele verandering

Politiesurveillance wordt van oudsher uitgevoerd door politiemensen – onder wie 'surveillanten' – die via uiteenlopende methoden waarnemen waarmee burgers bezig zijn. Met de opkomst van informatie- en communicatietechnologie werden deze waarnemingen niet meer vastgelegd op schrift, maar in informatiesystemen. De essentie was echter nog steeds dat politiemensen de activiteiten van burgers waarnamen en deze vastlegden. De opkomst van digitale technologie heeft deze praktijk fundamenteel veranderd. Het voorbeeld waarmee dit essay is geopend, maakt dit duidelijk. Voorheen stonden er politiemensen op een viaduct of andere positie te kijken of zij de auto zagen die voldeed aan de kenmerken van de vluchtauto. Nu stond er een ANPR-camera die het kenteken van de vluchtauto registreerde, dit kenteken vergeleek met kentekens in een database en op basis hiervan signaleerde dat de vluchtauto voorbijreed. Dit signaal was direct bekend in het RTIC van de politie en werd doorgegeven aan de politie-eenheden die bezig waren met de klopjacht op de verdachten.
Digitale politiesurveillance is een ander soort activiteit dan traditionele politiesurveillance (zie ook Ferguson, 2022). De actor verandert: het waarnemen door politiemensen wordt in toenemende mate aangevuld dan wel vervangen door het waarnemen door technologie. De ANPR-camera is bijvoorbeeld onderdeel van een groeiend aantal sensoren dat activiteiten van burgers zichtbaar maakt. Het zichtbaar maken van activiteiten gebeurt niet alleen in de fysieke wereld, maar ook online. De politie beschikt over steeds meer (geavanceerde) softwareprogramma's waarmee online activiteiten van burgers worden gemonitord, geselecteerd en nader bestudeerd (zie Landman & Groothuis, 2022). Kortom: door digitale technologie raakt het vermogen tot het zichtbaar maken van activiteiten van burgers in toenemende mate 'ontkoppeld' van het waarnemend vermogen van politiemensen. Digitale politiesurveillance heeft daardoor een grootschaliger bereik én een meer continu – en tot op zekere hoogte ook onzichtbaarder – karakter dan traditi-

doi: 10.5553/TCC/221195072023013002005

onele politiesurveillance. De ogen van de politie zien meer, staan langer open en zijn door burgers tegelijkertijd moeilijker te zien.

Er is echter meer aan de hand. Het gaat namelijk niet alleen om de losse datapunten: de registratie van een camera op een bepaalde plek of de tweet die door het algoritme wordt uitgelicht. De politie zet digitale technologie ook in voor het combineren van data en het analyseren van deze gecombineerde data. Voorheen werden data verwerkt door politiemensen. Digitale technologie is ook op deze praktijk gaan ingrijpen. In metaforische zin gaat het dan om het brein van de politie: het vermogen tot dataverwerking. Het verwerken van data vindt in toenemende mate plaats door algoritmen die worden gebruikt voor het reconstrueren van wat er is gebeurd, het waarnemen van wat er gaande is en het voorspellen van wat er zou kunnen gaan gebeuren (Schuilenburg & Soudijn, 2021; Terpstra & Salet, 2020). Door gebruik van een groeiend aantal algoritmen wordt het vermogen van de politie tot dataverwerking substantieel uitgebreid. Het cognitieve vermogen van de politie wordt niet meer beperkt tot de cognitieve vermogens van politiemensen (Ariel, 2019). Hierdoor worden (grootschalige) vormen van gegevensverwerking mogelijk die voorheen onmogelijk waren (Joh, 2018).

Het gebruik van digitale technologie voor het combineren en analyseren van data heeft als voornaamste gevolg dat er meer inzicht kan worden verkregen in activiteiten van burgers. Ieder gegeven op zichzelf geeft wellicht nog niet zoveel inzicht, maar het resultaat van het combineren en analyseren doet dit wel. Een voorbeeld kan dit verduidelijken. Door de politie is geëxperimenteerd met een 'interactieve criminele kaart'. Dit is een digitale beeldtafel waarop allerlei plaatsen – waaronder woonadressen en bedrijven – worden weergegeven. Plaatsen worden geclassificeerd: is er iets verdachts aan de hand? Deze classificatie vindt plaats op basis van uiteenlopende data die door een algoritme worden verwerkt: politiedata en data van andere organisaties, zoals de Kamer van Koophandel. De gebruiker kan op adressen inzoomen om zodoende inzicht te krijgen in onderliggende data. De criminele kaart wordt door de politie beschouwd als een aanvulling voor de politieagenten op straat. 'Wanneer hij rondrijdt ziet een agent natuurlijk niet wat er achter de deuren afspeelt, deze kaart biedt hem de mogelijkheid om eigen kennis, ervaring en inzicht te koppelen aan andere gegevens', zo valt op de website van de politie te lezen.[2] Dit citaat van de politie laat zien wat het effect is van digitale technologie op politiesurveillance: door het combineren en verwerken van data kan een vollediger inzicht worden verkregen in het leven van burgers.

De eerste conclusie op basis van het voorgaande is dat digitale politiesurveillance als praktijk een ander karakter heeft dan traditionele politiesurveillance, omdat menselijke vermogens worden uitgebreid en overgenomen door technologie. De tweede, en meest belangrijke, conclusie is dat de veranderende aard van politiesurveillance ook leidt tot andere opbrengsten. De omvang en diepgang van politiesurveillance nemen substantieel toe (zie ook Brayne, 2021). Er worden over meer burgers data verzameld (omvang) én in het leven van sommige burgers wordt meer inzicht verkregen (diepgang).

2 Zie www.politie.nl/nieuws/2019/augustus/28/08-opening-criminele-kaart-op-team-weerijs.html.

De toevoeging 'sommige' in bovenstaande conclusie is van belang: de diepgang van politiesurveillance richt zich niet op alle burgers, maar op bepaalde groepen burgers. Een onderscheid in doelgroepen is van belang. In een artikel over *digital policing* stelt Andrew Ferguson (2022) dat politiële surveillancetechnologieën kunnen worden beschouwd als concentrische cirkels. Dit is een bruikbaar beeld om de oriëntatie van digitale politiesurveillance te duiden. In de buitenste (grootste) cirkel bevinden zich vrijwel alle burgers die op de een of andere manier onderdeel zijn van monitoring, bijvoorbeeld omdat ze een ANPR-camera passeren en hun kenteken enkele weken wordt opgeslagen. In de binnenste cirkel – de *bull's eye* – bevinden zich de verdachten van strafbare feiten. In de cirkel daartussen bevinden zich burgers die weliswaar (nog) niet worden verdacht van een strafbaar feit, maar over wie wel meer data worden verzameld en/of worden verwerkt. Dit zijn burgers die vanuit een veiligheidsperspectief als een hoog risico worden getaxeerd: risicoburgers. Het onderscheid tussen verdachte en onverdachte (risico)burgers is van belang voor het vervolg.

3 De zegen van digitale politiesurveillance: de potentie tot effectiviteit

Ik veronderstel dat de toenemende omvang en diepgang van politiesurveillance kan bijdragen aan de effectiviteit van de taakuitvoering door de politie. Zeker weten doe ik dit niet: er kunnen vooralsnog geen onderbouwde uitspraken worden gedaan over de invloed van digitale politiesurveillance op de effectiviteit van de taakuitvoering door de politie. Dit komt niet alleen doordat het doen van dit type uitspraken sowieso lastig is, maar ook doordat er vooralsnog in zowel binnen- als buitenland weinig onderzoek is verricht naar de effecten van digitale politiesurveillance (zie ook Landman, 2023). Ik beperk me daarom tot een aanname, die ik hieronder specificeer in de verschillende effectiviteitsbijdragen die digitale politiesurveillance kan leveren.

Digitale politiesurveillance kan in de eerste plaats bijdragen aan het voorkomen van criminaliteit en onveiligheid. Dit vindt plaats door proactief op te treden op basis van het algoritmisch taxeren van risicovolle personen, situaties en plaatsen. Er zijn voorbeelden van risicotaxatiepraktijken die vermoedelijk hebben geleid tot het voorkomen van openbareordeverstoringen en criminaliteit, al weet je dit nooit zeker. Hierbij kan worden gedacht aan het voeren van stopgesprekken met personen die – op basis van geïdentificeerde socialemediaberichten – van plan waren om te gaan rellen en het waarschuwen van personen die mogelijk slachtoffer zouden worden van excessief geweld in de onderwereld op basis van het *threat to life*-algoritme.[3]

Een tweede bijdrage heeft betrekking op het detecteren van criminaliteit: het vaststellen van (de uitvoering van) een strafbaar feit op het moment dat het plaatsvindt, zodat de verdachten vrijwel direct kunnen worden aangehouden. Door digitale politiesurveillance kan er op meer plekken en voortdurend worden

3 Dit algoritme is onder andere gebruikt tijdens het live meelezen van de berichten tijdens de EncroChat-operatie (zie verder Landman, 2023).

doi: 10.5553/TCC/221195072023013002005

waargenomen. Dit maakt dat er in potentie meer criminaliteit kan worden gedetecteerd en de heterdaadkracht kan worden versterkt (zie ook Simmons, 2019). De aanhouding van de verdachten van de moord op Peter R. de Vries is een voorbeeld van hoe dit werkt.

Digitale politiesurveillance kan tevens bijdragen aan het tegenhouden van criminaliteit: het dusdanig verstoren van de uitvoering van criminele processen dat het moeilijker wordt om bepaalde delicten te plegen. Door digitale politiesurveillance (dataverzameling en -verwerking) is er meer inzicht gekomen in criminele processen in het kader van onder andere drugscriminaliteit en cybercriminaliteit. Dit inzicht wordt – zeker in het domein van cybercriminaliteit – veelvuldig gebruikt om criminele processen te verstoren (zie bijvoorbeeld Van den Eeden, Van Berkel, Lankhaar & De Poot, 2021). Hierdoor wordt het (tijdelijk) moeilijker gemaakt om bijvoorbeeld ransomware- of ddos-aanvallen uit te voeren. Of dit ook leidt tot een enigszins duurzame reducering of beheersing van het probleem is onbekend.

Tot slot: digitale politiesurveillance kan bijdragen aan het ophelderen van criminaliteit. Dit betreft het reconstrueren van gepleegde strafbare feiten, zodat verdachten kunnen worden geïdentificeerd, aangehouden en vervolgd. Digitale politiesurveillance maakt dat de politie in potentie over veel gegevens kan beschikken waarmee gepleegde strafbare feiten kunnen worden gereconstrueerd: data van camera's en andere sensoren, metadata van allerlei door burgers gebruikte apparaten, data die door burgers zijn geproduceerd (teksten, afbeeldingen, video's) en zijn opgeslagen op apparaten en servers, online gegevens en ga zo maar door (zie ook Henseler & De Poot, 2020). De datapunten functioneren bij elkaar opgeteld in toenemende mate als een 'tijdmachine' (Ferguson, 2020). Op het moment dat er ergens criminaliteit is gepleegd, kan er – in ieder geval op onderdelen – worden 'teruggespoeld'. Slimme algoritmen helpen de politie bij het verwerken van de steeds grotere hoeveelheden data waarover zij beschikt. Het gebruik van de onderschepte cryptocommunicatiedata illustreert de potentie van digitale politiesurveillance voor het ophelderen van criminaliteit. Op basis van de berichten, locatiedata en afbeeldingen zijn in strafdossiers onder andere tijdlijnen gemaakt waarop de activiteiten van de verdachten zijn weergegeven. Er zijn inmiddels vele kopstukken uit de onderwereld opgespoord, vervolgd en veroordeeld, en er volgt vermoedelijk nog meer.

Kortom: digitale politiesurveillance heeft zeker de potentie om bij te dragen aan de effectiviteit van de taakuitvoering door de politie. Deze potentie heeft echter ook schaduwzijden.

4 De vloek van digitale politiesurveillance: mensenrechten onder druk

De datahonger van de politie vloeit naar mijn indruk voort uit goede bedoelingen, maar *the road to hell is paved with good intentions*. De voortschrijdende digitale politiesurveillance gaat gepaard met maatschappelijke risico's. Hierbij moeten we vooral oog hebben voor de onverdachte burger in het algemeen en de veronderstelde risicoburger in het bijzonder.

De opkomst van de risicoburger moet worden begrepen tegen de achtergrond van het risicobeheersingsparadigma dat in de afgelopen veertig jaar in politiek en samenleving dominant is geworden (zie onder andere Garland, 2001; Schuilenburg, 2017). Maatschappelijke ontwikkelingen worden bij voortduring in termen van onveiligheid gedefinieerd en op bedreigingen op het gebied van veiligheid wordt bij voorkeur vroegtijdig geanticipeerd. In deze voorzorg- of anticipatielogica speelt de politie een belangrijke rol: zij moet ingrijpen voordat het kwaad is geschied en niet (te ver) 'achter de feiten aan lopen'. Dit is een fundamentele ontwikkeling, aangezien het politiewerk van oorsprong juist bestaat uit achter de feiten aan lopen. Bijvoorbeeld: waar de politie vroeger alleen gegevens vastlegde over personen die (vermoedelijk) iets hadden gedaan of met wie anderszins bemoeienis gerechtvaardigd was, worden er al geruime tijd ook gegevens vastgelegd over onverdachte personen (Tazelaar, 2017).

Digitale politiesurveillance is vanuit een risicobeheersingsparadigma buitengewoon aantrekkelijk, omdat zij bijdraagt aan een omvangrijker en diepgaander inzicht in risico's in het algemeen en risicovolle personen in het bijzonder. De keerzijde hiervan is dat politiesurveillance in toenemende mate het karakter krijgt van een sleepnet waarbij grote groepen onverdachte burgers in beeld worden gebracht, om vervolgens te beoordelen welke burgers een risico vormen voor de samenleving (Brayne, 2021; WRR, 2016). Vooral bij de risicoburger neemt de diepgang van surveillance toe: de risicoburger wordt nader bestudeerd en geanalyseerd en met mogelijk politieoptreden geconfronteerd. Zo publiceerde de onderzoeksjournalisten van Investico begin maart 2023 een artikel waaruit blijkt dat de politie op grote schaal persoonsgegevens van demonstranten vergaart.[4] Zelfs de gegevens van familieleden van nooit veroordeelde demonstranten worden – via de uitwisseling tussen de politiesystemen en de basisregistratie personen – verzameld.[5] Het is aannemelijk dat de politie bij dergelijke praktijken een meer dan geringe inbreuk op de persoonlijke levenssfeer (privacy) van burgers maakt, terwijl het hier veelal gaat om burgers die niet worden verdacht van een strafbaar feit.[6] Dit is een onwenselijke ontwikkeling, die ook in termen van rechtmatigheid ter discussie staat.

Ik heb de risicoburger vooralsnog behandeld als een ongedifferentieerde categorie, maar dat is die niet. Het is – om verschillende redenen – zeer aannemelijk dat bepaalde groepen burgers eerder als een hoog risico worden aangemerkt dan andere groepen burgers. Daar kunnen goede redenen voor zijn, maar we moeten beseffen dat de algoritmen die risico taxeren niet perfect zijn. Er doen zich valspositieven en valsnegatieven voor. De verdeling van valspositieven en valsnegatieven onder de bevolking is om verschillende redenen niet evenredig. Kathalijne Buitenweg (2021: 220) vat het treffend samen: 'Voorspellende algoritmen blijken in de praktijk vooral gunstig uit te pakken voor mensen die het toch al getroffen hebben in het leven.'

4 Zie www.platform-investico.nl/artikel/politie-verzamelt-op-grote-schaal-persoonsgegevens-demonstranten.

5 Deze uitwisseling verloopt via de 'personenserver' van de politie. Zie de 0-meting Privacy & Security by Design van deze personenserver uit 2019: www.politie.nl/binaries/content/assets/politie/wet-open-overheid/00-landelijk/nulmetingen-2019/24.-rapport-0-meting-psbd-personenserver-20190425-v2.0_geredigeerd.pdf.

6 Zie in dit verband ook het rapport van Amnesty International (2023).

doi: 10.5553/TCC/221195072023013002005

Kortom: de valspositieven hebben vooral betrekking op burgers in kwetsbare omstandigheden. Zij worden vaker aangemerkt als hoog risico, terwijl hier geen aanleiding voor is. Zo kwam Khalid uit de Amsterdamse Diamantbuurt zonder antecedenten in de Top600 terecht, wat onder andere leidde tot veelvuldige politiecontroles (zie Peeters & Van Dongen, 2022). Digitale politiesurveillance is dus niet alleen een risico voor het recht op privacy, maar ook voor het recht op gelijke behandeling. Het kostte Khalid nogal wat moeite om van de lijst af te komen, wat een aanvullend probleem illustreert: de risicoburger geniet weinig rechtsbescherming. Een verdachte heeft in zeker opzicht meer rechten.

We moeten dus alert zijn op de negatieve effecten van digitale politiesurveillance op de mensenrechten.[7] De vraag is echter wie 'we' is. Het gebruik van digitale surveillancetechnologie door de politie vindt grotendeels buiten het gezichtsveld van politiek en samenleving plaats. Marc Schuilenburg noemde het jaren geleden een 'stille revolutie'.[8] Naar de Tweede Kamer worden algemene brieven gestuurd over artificiële intelligentie en *sensing* bij de politie, maar wie weet eigenlijk (goed) wat de politie doet en wie zorgt voor (democratische) controle? De stilte wordt doorbroken als er bijvoorbeeld een rapport van Amnesty International (2020) verschijnt over de *sensing*-proeftuin in Roermond en keert vervolgens weer snel terug. Dit is een algemeen probleem met het gebruik van digitale technologie door uitvoeringsorganisaties: het evenwicht der machten komt onder druk te staan doordat politici en magistraten weinig grip hebben op de min of meer autonome digitalisering van de uitvoerende macht (zie ook Passchier, 2021). We kunnen er niet van uitgaan dat het zonder dit evenwicht wel goed komt. Daarvoor zijn er inmiddels te veel voorbeelden waaruit het tegendeel blijkt. Er is dus werk aan de winkel, ook met betrekking tot digitale politiesurveillance. Andrew Ferguson (2017: 166) formuleert het mooi: 'Police departments cannot live in the dark.' De politie in Nederland neemt weliswaar ook zelf maatregelen die ervoor moeten zorgen dat digitale surveillance op verantwoorde wijze plaatsvindt, maar deze maatregelen zijn geregeld te vrijblijvend.[9] Het Kwaliteitskader Big Data kan als voorbeeld dienen. De term 'kader' geeft de indruk dat het aangeeft waar het gebruik van big data aan moet voldoen, maar het blijkt vooral een hulpmiddel te zijn met vragen waarop 'geen goede of foute antwoorden zijn' (zie OM & Politie, 2020).

5 Oproep: burgers bekijken, maar hen ook blijven zien

Digitale politiesurveillance is zowel een zegen als een vloek. De balans tussen zegen en vloek kan per toepassing verschillen. Met cryptocommunicatiedata en analysetechnologieën de gewelddadige onderwereld aanpakken is toch iets anders dan jongeren zonder antecedenten algoritmisch in een hoge risicocategorie plaatsen en

7 Zie ook de beschouwingen over het recht op een eerlijk proces in verband met het gebruik van de cryptocommunicatiedata door de politie (o.a. Te Molder, 2022; Schermer & Oerlemans, 2022).

8 Zie www.nrc.nl/nieuws/2018/01/11/de-besliscomputer-disciplineert-iedereen-ook-de-rechter.

9 Hierbij doen zich verschillen voor tussen toepassingen. Een voorbeeld van een stevig, verplichtend kader is het Inzetkader Gezichtsherkenningstechnologie Politie, dat begin 2023 is gepubliceerd (Politie, 2023).

op basis daarvan intensiever (proactief) controleren. Het is daarom van belang dat het evenwicht der machten rondom digitale politiesurveillance wordt hersteld en er tijdig over de wenselijkheid van specifieke digitale surveillancepraktijken wordt geoordeeld. Dit laat onverlet dat de politie als uitvoerende macht een stevige eigen verantwoordelijkheid heeft. We weten inmiddels wat er gebeurt als een uitvoeringsorganisatie burgers alleen nog maar bekijkt als object en niet meer ziet als mens (zie voor dit onderscheid Nap, 2014). De politie moet daarom steviger gaan staan voor de waarden van de democratische rechtsstaat om ook met digitale surveillance een macht ten goede te zijn.

Literatuur

Amnesty International. (2020). *We sense trouble. Automated discrimination and mass surveillance in predictive policing in the Netherlands*. London: Amnesty International.

Amnesty International (2023). *Ongecontroleerde macht. ID-controles en gegevensverzameling van vreedzame demonstranten in Nederland*. London: Amnesty International.

Ariel, B. (2019). Technology in policing: Advocate. In D. Weisburd & A.A. Braga (Eds.), *Police innovation. Contrasting perspectives* (pp. 485-515). Cambridge: Cambridge University Press.

Brayne, S. (2021). *Predict and surveil. Data, discretion, and the future of policing*. New York: Oxford University Press.

Buitenweg, K. (2021). *Datamacht en tegenkracht. Hoe we de macht over onze gegevens kunnen terugkrijgen*. Amsterdam: De Bezige Bij.

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

Ferguson, A.G. (2020). Structural sensor surveillance. *Iowa Law Review*, 47-112.

Ferguson, A.G. (2022). Why digital policing is different. *Ohio State Law Journal*, 1-32.

Garland, D. (2001). *The culture of control. Crime and social disorder in contemporary society*. Oxford/New York: Oxford University Press.

Henseler, H. & Poot, C.J. de (2020). De betekenis van digitale sporen voor bewijs op activiteitniveau. *Expertise en Recht*, *2*, 50-59.

Joh, E.E. (2018). Artificial intelligence and policing: Hints in the Carpenter decision. *Ohio State Journal of Criminal Law*, *16*, 281-290.

Landman, W. (2015). *Blauwe patronen. Betekenisgeving in politiewerk*. Den Haag: Boom Lemma.

Landman, W. (2023). *Politiewerk aan de horizon. Technologie, criminaliteit en de toekomst van politiewerk* [manuscript accepted for publication].

Landman, W. & Groothuis, S. (2022). *Politiewerk op het web. Een verkennend onderzoek naar online gegevensvergaring door de politie*. Den Haag: Sdu.

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

Nap, J.A. (2014). *Macht ten goede?! Sterke arm in een complexe samenleving*. Apeldoorn: Politieacademie.

OM & Politie (2020). *Kwaliteitskader Big Data*. Programma Toekomstbestendig Opsporen en Vervolgen.

Passchier, R. (2021). *Artificiële intelligentie en de rechtsstaat. Over verschuivende overheidsmacht, Big Tech en de noodzaak van constitutioneel onderhoud*. Den Haag: Boom juridisch.

Peeters, T. & Dongen, T. van (2022). *Schijnwerpers op de straat. Over de lessen van de aanpak van de Van Wougroep en andere criminele jeugdgroepen*. Utrecht: Verwey-Jonker Instituut.

Politie. (2023). *Inzetkader Gezichtsherkenningstechnologie Politie. Een eerste kader ter toetsing van operationele inzetten*. Politie Nederland.

Schermer, B.W. & Oerlemans, J.J. (2022). De EncroChat-jurisprudentie: teleurstelling voor advocaten, overwinning voor justitie? *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, *2*, 82-89.

Schuilenburg, M. (2017). *The securitization of society. Crime, risk, and social order*. New York: New York University Press.

Schuilenburg, M. & Soudijn, M. (2021). Big data in het veiligheidsdomein. Onderzoek naar big data-toepassingen bij de politie en de positieve effecten hiervan voor de politieorganisatie. *Tijdschrift voor Veiligheid*, *4*, 1-19.

Simmons, R. (2019). *Smart surveillance. How to interpret the Fourth Amendment in the twenty-first century*. Cambridge: Cambridge University Press.

Stol, W.P. (1996). *Politie-optreden en informatietechnologie. Over sociale controle van politiemensen*. Lelystad: Koninklijke Vermande.

Tazelaar, P. (2017). IGP en ethiek, oftewel: wat mag wel en wat mag niet. In M. den Hengst, T. ten Brink & J. ter Mors (Eds.), *Informatiegestuurd politiewerk in de praktijk* (pp. 93-101). Deventer: Vakmedianet.

Te Molder, R.M. (2022). Digitaal forensische zoekmachines, effectieve verdedigingsrechten en de modernisering van het Wetboek van Strafvordering: is aanpassing van het conceptwetsvoorstel gewenst? *Boom Strafblad*, *5*, 178-186.

Terpstra, J. & Salet, R. (2020). Big data policing als sociale praktijk. In J. Janssens, W. Broer, M. Crispel & R. Salet (Eds.), *Informatiegestuurde politie* (pp. 25-38). Turnhout/'s-Hertogenbosch: Gompel & Svacina.

Van den Eeden, C.A.J., Berkel, J.J. van, Lankhaar, C.C. & Poot, C.J. de (2021). *Opsporen, vervolgen en tegenhouden van cybercriminaliteit*. Den Haag: WODC.

WRR (Wetenschappelijke Raad voor het Regeringsbeleid). (2016). *Big data in een vrije en veilige samenleving*. Amsterdam: Amsterdam University Press.