ARTIKELEN

‘Garbage in, garbage out’

Over predictive policing en vuile data

Abhijit Das & Marc Schuilenburg[*]

Inleiding

Het gebruik van data-analyses via voorspellende algoritmen speelt een steeds grotere rol in het overheidsdomein. Landelijke organisaties als de politie en de Belastingdienst, maar ook zorginstellingen en gemeenten gebruiken deze systemen om criminaliteit en ander risicovol gedrag te voorspellen, van het Systeem Risico Indicatie (SyRI), waarmee uitkerings- en belastingfraude worden opgespoord, tot de Verwijsindex Risicojongeren, waarin risicosignalen van hulpverleners over jongvolwassenen worden verzameld (WRR, 2016). In dit verband wordt gesproken van de dreiging van een ‘algocratie’, waarmee wordt verwezen naar de toenemende invloed van algoritmen op de besluitvorming binnen de overheid en andere organisaties, zonder dat duidelijk is hoe dat precies gebeurt (Danaher, 2016). Het is daarom van belang om rekenschap af te leggen over de wijze waarop algoritmen werken en welke data worden gebruikt om voorspellingen te doen.

In dit artikel richten we ons op het gebruik van voorspellende data-analyses door de overheid in het kader van de voorkoming en opsporing van strafbare feiten. Het meest bekende voorbeeld hiervan is het Criminaliteits Anticipatie Systeem (CAS) van de Nationale Politie. Dit systeem is een vorm van predictive policing en toont op een rasterkaart van Nederland met vakjes van 125 bij 125 meter op welke plaatsen en op welk moment een vergrote kans bestaat dat bepaalde vormen van criminaliteit gaan plaatsvinden (Mali, Bronkhorst-Giesen & Den Hengst, 2017; Rienks & Schuilenburg, 2020). Dit wordt een ‘begeleide’ of ‘gestuurde analyse’ genoemd (Schermer, 2011). In het geval van CAS is hiervoor een algoritme opgesteld dat een verhoogde kans op criminaliteit voorspelt. Dit gebeurt door op verschillende peilmomenten het risico op criminaliteit vast te leggen door middel van een analyse van voorgaande incidenten in combinatie met de nabijheid van verschillende risicofactoren, waardoor een buurt in een stad kan worden aangewezen waar de kans groot is dat er in de komende weken bijvoorbeeld veel zal worden ingebroken (Willems & Doeleman, 2014).

Het voorkomen en opsporen van criminaliteit via CAS heeft een grote invloed op zowel het optreden van de overheid als de maatschappij en is een belangrijk

* Mr. Abhijit Das is docent/onderzoeker straf(proces)recht aan de afdeling Strafrecht en Criminologie van de Vrije Universiteit Amsterdam. Mr. dr. Marc Schuilenburg is universitair docent criminologie aan de afdeling Strafrecht en Criminologie van de Vrije Universiteit Amsterdam.

 doi: 10.5553/BenM/138900692020047003002 - Beleid en Maatschappij 2020 (47) 3

onderwerp om vanuit het perspectief van regulering te bestuderen. Zo kan een doelgericht gebruik van dit systeem een belangrijke bijdrage leveren aan de criminaliteitsbestrijding. Een voorwaarde hiervoor is wel dat de gebruikte datasets geen onjuiste of onrechtmatige gegevens bevatten. Dergelijke gegevens kunnen immers leiden tot onbetrouwbare of niet-integere uitkomsten (onder andere Mayer-Schönberger & Cukier, 2013; Ferguson, 2017; Richardson, Schultz & Crawdford, 2019). Dit tast zowel de integriteit van de strafvordering als de legitimiteit van de eventuele latere strafrechtelijke vervolging aan.
In het geval van CAS is de voorspelling waar en wanneer criminaliteit gaat plaatsvinden gebaseerd op speciale datasets die door de Nationale Politie zijn geselecteerd en die geprepareerd zijn voor data-analyse door middel van algoritmen. De vraag is in hoeverre toezicht bestaat op de kwaliteit van de gegevens in deze datasets. Met betrekking tot het toezicht op het gebruik van gegevens in voorspellende systemen als zodanig spreekt de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) van 'een hiaat in de regelgeving voor gegevensverwerking' (WRR, 2016, 105). Dit leidt tot de volgende vraag: hoe kunnen onjuiste of onrechtmatige gegevens uit voorspellende data-analyses als CAS worden geweerd?
In antwoord op deze vraag gaan we eerst in op wat predictive policing inhoudt en waarom deze voorspellende methode goed past in de huidige maatschappelijke context van criminaliteitsbestrijding. We besteden hierbij aandacht aan drie factoren die aanleiding hebben gegeven tot de landelijke invoering van CAS: technologische, politieke en culturele factoren. Vervolgens richten we ons op het fenomeen van onjuiste en onrechtmatige gegevens. Dit is het probleem van 'vuile data'. Hierna laten we zien welke mogelijkheden er bestaan om vuile data te weren uit de datasets die worden gebruikt bij CAS. Tot slot betogen wij dat een discussie over de mogelijkheden om vuile data uit voorspellende analyses te houden cruciaal is voor de integriteit van het overheidsoptreden, in het bijzonder wanneer het gaat om het voorkomen en opsporen van criminaliteit en ander risicovol gedrag.

Maatschappelijke context

Predictive policing is het berekenen van risico's in relatie tot criminaliteit, op basis waarvan de politie actie kan ondernemen om deze risico's te verkleinen (onder andere Perry e.a., 2013; Schuilenburg, 2016; Bennett Moses & Chan, 2018; Rienks & Schuilenburg, 2020). In het geval van CAS worden hiervoor datasets gebruikt die komen uit de bestanden van de Nationale Politie – aangiftes van burgers en criminaliteitscijfers – en het Centraal Bureau voor de Statistiek (CBS), waaronder het aantal uitkeringen per wijk, leeftijden, geslacht en gezinssamenstellingen. Daarnaast worden in CAS gegevens geanalyseerd zoals de aanwezigheid van cafés, winkels en uitvalswegen in bepaalde gebieden (Mali e.a., 2017). Op basis hiervan worden voorspellingen gedaan over de locaties en periodes met een verhoogde kans op criminaliteit, zoals woninginbraken en straatroof. Dit wordt gevisualiseerd met *heat maps* en lijndiagrammen.

De landelijke inzet van predictive policing door de Nationale Politie is geen opzichzelfstaande ontwikkeling. De implementatie van voorspellende data-analyses vindt niet in een maatschappelijk vacuüm plaats. Zo maakt de inzet van CAS onderdeel uit van een serie mondiale ontwikkelingen die door technologische, politieke en culturele factoren in gang zijn gezet. Predictive policing werd voor het eerst in gebruik genomen in de Verenigde Staten. Sinds 2008 werkt de Los Angeles Police Department (LAPD) met het systeem PredPol, waarmee de LAPD voorspelt waar en wanneer criminaliteit gaat plaatsvinden. Naar aanleiding van de positieve resultaten van PredPol besloten ook andere politiekorpsen PredPol of vergelijkbare systemen in te zetten (Schuilenburg, 2019, hoofdstuk 5). Naast PredPol zijn er inmiddels voorspellende systemen met namen als HunchLab (Philadelphia), Palantir (New Orleans), Precobs (Duitsland), ProMap (Verenigd Koninkrijk), KeyCrime (Italië), Maprevelation (Frankrijk) en CAS (Nederland).

Een belangrijke technologische factor voor het gebruik van predictive policing is dat er steeds meer data beschikbaar zijn die de overheid iets over menselijk gedrag vertellen, en er ook steeds meer dingen in onze omgeving zijn die data produceren. Dit is het gevolg van de digitalisering, die zich voltrekt in alle aspecten van ons leven. Met het dagelijks gebruik van internet, sociale media en mobiele telefoons wordt de berg digitale data steeds groter. Deze zal alleen maar groter en beter toegankelijk worden door ontwikkelingen als big data, *cloud robotics* en het internet der dingen (WRR, 2016). De verwachting hierbij is dat door het gebruik van ICT-applicaties als CAS en technologische hulpmiddelen als *smart objects* (bodycams, geluidssensoren, peilbakens, verlichting) het gemakkelijker wordt om criminaliteit of ongewenst gedrag te voorspellen en om gerichter capaciteit in te zetten op basis van de uitkomsten van de analyses (Ferguson, 2017; Smith, Bennett Moses & Chan, 2017). In de literatuur wordt in dit verband gesproken van 'paradigm shift' (Willis & Mastrofski, 2014), 'future of law enforcement' (Pearsall, 2010) en 'a new era' (Christin, Rosenblat & Boyd, 2015).

De landelijke uitrol van predictive policing hangt ook samen met de politieke keuze om (bepaalde vormen van) criminaliteit in een vroegtijdig stadium aan te pakken. Relevant hierbij is dat het politieke vertoog over criminaliteit in de laatste decennia steeds meer in het teken is komen te staan van risicobeheersing en een daaruit voortvloeiend voorzorgsdenken (onder andere Ewald, 2002; Ericson, 2007; Simon, 2007; Pieterman, 2008). Een van de gevolgen hiervan is het zo vroeg mogelijk willen inzetten van het strafrecht, wat door Borgers (2007) als 'de vlucht naar voren' is getypeerd. Zedner (2007) spreekt in dit verband van een '*pre-crime*-denken', waarin het niet langer gaat om het bestraffen van een inbreuk op de (straf)wet, maar om het voorkomen van potentieel risicovol gedrag. Deze politieke doelstelling gaat gepaard met een groot geloof in technieken die menselijk gedrag voorspellen en tijdig kunnen bijsturen (*nudging*). Technologische toepassingen die aangeven waar en wanneer *high impact crimes* als woninginbraken en straatroven gaan plaatsvinden, maar ook wie 'kleinere' criminaliteit als uitkerings- en belastingfraude gaat plegen, worden daarom steeds populairder.

Veiligheid als technologisch en politiek vraagstuk kan niet los worden gezien van haar culturele kant, met opvattingen over hoe veilig en onveilig burgers zich voe-

len en waarin steun van burgers bepalend is voor de aanpak van bepaalde criminaliteitsproblemen (Garland, 1990; Schuilenburg, 2015). Zo wordt formele besluitvorming om voorspellende data-analyses in te zetten mede ingegeven door de gevoelens en emoties van burgers over hoe veilig zij zich voelen en de beelden die zij hebben van wat zij van de overheid kunnen verwachten. Kenmerkend voor de tijdsgeest is dat burgers bezorgd blijven over de wijze waarop de huidige samenleving zich ontwikkelt en zich bang voelen in een uiteindelijk heel veilige samenleving (Schuilenburg & Van Swaaningen, 2013). Wanneer media deze angsten of zorgen van burgers uitvergroten, kan dit leiden tot overtrokken, negatieve reacties op bepaalde gebeurtenissen, personen of groepen (vergelijk Cohen, 1972; Goode & Ben-Yehuda, 2009; Schuilenburg, 2019). Het verlangen naar meer veiligheid onder burgers vertaalt zich dan in een reeks van instrumenten die worden ingezet om te voorkomen dat criminaliteit of ander ongewenst gedrag plaatsvindt. Naast de inzet van predictive policing kan hierbij worden gedacht aan de installatie van bewakingscamera's, poortjessystemen en andere controle- en detectieapparatuur in de openbare ruimte die de kans op criminaliteit moet verkleinen (Graham, 2010). Tegelijk is een steeds groter aantal 'lichtblauwe' handhavers actief, die burgers moeten beschermen tegen criminaliteit, van private beveiligers tot WhatsApp-buurtpreventie (onder andere Lub, 2013; Schuilenburg, 2018).

Risico's van predictive policing

De Nationale Politie meent dat met predictive policing criminaliteit beter kan worden bestreden en dat beschikbare middelen hierdoor ook adequater kunnen worden ingezet (Willems & Doeleman, 2014). Zo kan op basis van de uitkomsten van CAS worden bepaald welke opsporingsmethode door politieagenten dient te worden gebruikt op de plek waar de kans het grootst is dat binnenkort iets dreigt te gebeuren (Rienks & Schuilenburg, 2020). Opvallend is dat wetenschappelijk onderzoek hoe voorspellende systemen werken en welk effect deze hebben op de opsporing van criminaliteit en ander risicovol gedrag schaars is en de evaluaties naar de resultaten van predictive policing wisselende resultaten laten zien (Hunt, Saunders & Hollywood, 2014; Mohler e.a., 2015; Mali e.a., 2017). Zo blijkt dat het gebruik van CAS nog geen aantoonbaar positief effect heeft op het aantal woninginbraken in het bijzonder en de landelijke ontwikkeling van de totale criminaliteit in Nederland in het algemeen (Mali e.a., 2017).

Naast het probleem van de (vermeende) effectiviteit van predictive policing wordt in de literatuur gewezen op andere keerzijden van het gebruik van predictive policing. Zo bestaat het risico dat de opsporingsautoriteiten zich blijven richten op dezelfde buurten en typen criminaliteit, het zogeheten risico van de *self-fulfilling prophecy* (Custers, 2016; Schuilenburg, 2016). Het gebruik van data en algoritmen om criminaliteit te voorspellen kan ook leiden tot bureaucratisering (Peeters & Schuilenburg, 2018), discriminatie van minderheden (Smith e.a., 2017) en het identificeren van risicogroepen op basis van bepaalde kenmerken en catego-

rieën, het zogenoemde *social sorting* (Lyon, 2003; Andrejevic, 2017; Das & Schuilenburg, 2018; Završnik, 2019).
Dat de uitkomsten van voorspellende data-analyses in de praktijk kunnen leiden tot een *self-fulfilling prophecy* en *social sorting* hoeft niet intentioneel te zijn, maar kan verscholen liggen in de datasets die worden gebruikt om voorspellingen over criminaliteit te doen. Doordat de input het fundament vormt waar de voorspelling op wordt gebouwd, kunnen data die zelf bijvoorbeeld onjuist zijn, leiden tot een output in de vorm van voorspellingen die ook problematisch zijn. Een goed voorbeeld hiervan zijn verouderde data. Stel dat de politie verouderde data meeneemt in haar data-analyses over het aantal uitkeringen en de gezinssamenstellingen van een wijk, dan bestaat de kans dat de resultaten iets zeggen over het verleden – en niet over het heden. Dit is het probleem van 'vuile data'. In de literatuur wordt ook gesproken van *dirty data* (Marx, 1984) of van *black data* (Ferguson, 2017).
Om verschillende redenen kunnen data als 'vuil' – en dus als problematisch als grondslag voor later overheidsoptreden – worden aangemerkt. Om reden van beperking richten wij ons in dit artikel op data afkomstig van politieoptreden die óf onrechtmatig zijn verkregen óf onjuist zijn. Met onrechtmatig doelen we op de schending van regels bij de vergaring van de betreffende data. Het kan hierbij gaan om de schending van wettelijke normen, van verdragsbepalingen van bijvoorbeeld het Europees Verdrag voor de Rechten van de Mens of van ongeschreven normen, waaronder de beginselen van een behoorlijke procesorde (het strafrechtelijke equivalent van de beginselen van behoorlijk bestuur). Een voorbeeld hiervan zijn data die komen uit of zijn afgeleid van bevooroordeelde of strafbare praktijken, zoals discriminatie (waaronder etnisch profileren) en andere vormen van onrechtmatig handelen door opsporingsautoriteiten (Richardson e.a., 2019). Zo blijkt uit onderzoek dat etnisch profileren, een vorm van discriminatie die juridisch onrechtmatig is omdat hierbij op basis van uiterlijke kenmerken wordt gecontroleerd door de politie, ook als hiervoor geen objectieve en redelijke rechtvaardiging bestaat, ook in Nederland voorkomt (Çankaya, 2012; Amnesty International, 2013; Mutsaers, 2013). Met betrekking tot onjuiste data gaat het om zaken als de manipulatie van criminaliteitscijfers, het bewust buiten de boeken houden van strafbare feiten door de politie. Een voorbeeld hiervan is de opdracht van de leiding van het New York City Police Department aan politieagenten om bepaalde klachten van burgers niet te rapporteren, met als doel de officiële criminaliteitsstatistieken er beter uit te laten zien (Eterno & Silverman, 2012). De vraag is dan hoe in de praktijk vuile data uit voorspellende data-analyses als CAS kunnen worden geweerd.

De juridische regels omtrent vuile data

Bij de verwerking van data om te voorspellen waar en wanneer criminaliteit gaat plaatsvinden door middel van voorspellende systemen is het relevant dat de data die hierbij worden gebruikt niet vuil – dus onrechtmatig verkregen of onjuist – zijn. Het gebruik van vuile data om criminaliteit te voorspellen kan er namelijk

toe leiden dat de uitkomsten ook vervuild zijn. Dit volgt uit de doelstellingen van het strafproces in algemene zin. In het strafproces draait het in de eerste plaats om de vraag of de rechter (of de officier van justitie wanneer de zaak door middel van een strafbeschikking wordt afgedaan) het materiaal dat is verzameld tijdens het opsporingsonderzoek betrouwbaar genoeg vindt om voor het bewijs te gebruiken (Corstens, 2018, 8 e.v.).

Maar het strafproces draait niet alleen om de bewijsvraag. Ook tijdens het opsporingsonderzoek moet op basis van betrouwbare informatie worden gehandeld. Naast de betrouwbaarheid is ook de rechtmatigheid van het overheidsoptreden van belang (Keulen & Knigge, 2016, 8-9). Ook hier geldt dat het overheidsoptreden vanaf de eerste handelingen van de politie in het opsporingsonderzoek tot en met de eindbeslissing van de rechter rechtmatig moet zijn (Kuiper, 2014, 199 e.v.). Het onderscheid tussen juistheid en rechtmatigheid is hierbij van belang, omdat het een niet met het ander hoeft samen te vallen (Dubbelaar, 2009). De waarneming dat er een vuurwapen ligt op de bijrijdersstoel van de burger die op discriminatoire gronden aan een verkeerscontrole is onderworpen, kan betrouwbaar zijn, maar dit neemt niet weg dat deze waarneming onrechtmatig is gedaan omdat ze het directe resultaat is van een onrechtmatige controle (Corstens, 2018, 879). Hetzelfde geldt wanneer er drugs worden aangetroffen in een woning bij een doorzoeking die niet volgens de wettelijke regels verloopt: dat er drugs zijn aangetroffen staat vast, maar dit bewijsmateriaal is onrechtmatig verkregen en daarmee 'vuil'.

Het algemene standpunt met betrekking tot het weren van onjuiste en onrechtmatige data uit het strafproces wordt met betrekking tot de verwerking van de gegevens in de datasets van CAS geconcretiseerd in de Wet politiegegevens (Wpg). Deze wet bevat verschillende voorschriften (artikel 3 lid 2 en artikel 4) die bepalen dat gegevens slechts (verder) mogen worden verwerkt wanneer het gaat om juiste, nauwkeurige en rechtmatig verkregen gegevens (Groenhart, 2019). Anders gezegd: gegevens die niet aan deze maatstaf voldoen, kunnen niet worden verwerkt door de politie en mogen ook niet worden gebruikt als inputdata bij predictive policing.

Met betrekking tot onrechtmatig verkregen data lijkt in deze bepalingen een heldere regel besloten te liggen: wanneer in strijd is gehandeld met het geldend recht, moeten data als onrechtmatig verkregen worden aangemerkt en worden geweerd uit voorspellende analyses (Groenhart, 2019). Een kanttekening hierbij is dat er een discrepantie kan bestaan tussen wat in juridische zin als onrechtmatige data worden aangemerkt en wat in de bredere discussie als zodanig worden gezien. De maatstaf van strafrechtelijke onrechtmatigheid wil niet zeggen dat alle gegevens die in maatschappelijk opzicht als problematisch worden ervaren, uit datasets worden gehouden. Zo wordt in het strafrecht een beperkte opvatting gehanteerd van wat discriminatoir overheidsoptreden inhoudt. Een verkeerscontrole door de politie, bijvoorbeeld, moet uitsluitend of in overwegende mate op basis van de etniciteit van de gecontroleerde worden verricht om als discriminatoir te worden aangemerkt. Dergelijke stringente criteria bergen het risico in zich van schijnconstructies of verhullend gedrag (Rodrigues & Van der Woude, 2016).

Ook met betrekking tot het gebruik van onjuiste data bevat de Wet politiegegevens een ogenschijnlijk heldere regel. Er wordt niet verwacht dat de betrouwbaarheid van de gegevens die worden verwerkt, als zodanig wordt beoordeeld. Het gaat er vooral om dat als het evident is dat bepaalde gegevens onjuist of onnauwkeurig zijn, deze moeten worden geweerd uit CAS (Groenhart, 2019). Een goed voorbeeld hiervan is het verwijderen van informatie uit politiesystemen over een verdachte die is vrijgesproken van een bepaald feit. Deze marginale toetsing is begrijpelijk, omdat bij de verwerking van data men zich helemaal aan het begin van het strafproces bevindt, waar de eisen die worden gesteld aan wat juiste informatie is veel lager liggen dan wanneer de rechter de vraag moet beantwoorden of hij tot een vrijspraak of veroordeling komt. Dit neemt niet weg dat er kritiek is op deze marginale toetsing, omdat het risico groot blijft dat onjuiste gegevens terechtkomen in de politiesystemen (Buruma, 2010).
Kortom, de ratio van de omgang met zowel onrechtmatig verkregen als onjuiste data is dat men zich bewust moet zijn van de waarde die aan bepaalde data kan worden toegekend. Wanneer deze waardering zodanig problematisch is dat de data onjuist of onrechtmatig zijn, moeten deze uit de politiesystemen worden geweerd of gefilterd. Dit roept de vraag op welk mechanisme er wordt gehanteerd om vuile data te weren uit datasets van de politie en hoe effectief dit mechanisme is. In antwoord hierop onderscheiden we twee filters om vuile data te weren uit voorspellende analyses: aan de voorkant en aan de achterkant.

De filter aan de voorkant

Het is één ding om te weten welke data verwijderd moeten worden uit de datasets die worden gebruikt bij voorspellende analyses als CAS, een tweede vraag is door wie dit moet gebeuren. De verantwoordelijkheid voor deze regulering ligt allereerst bij de Nationale Politie zelf. Door vuile data uit datasets te weren wordt reeds aan de voorkant van het proces van predictive policing voorkomen dat vuile data in de voorspellende analyses worden betrokken. In dit geval kan bijvoorbeeld worden gedacht aan de taak van privacyfunctionarissen of beleidsmedewerkers van de Nationale Politie om vuile data te identificeren en te verwijderen uit de datasets van CAS (artikel 4 jo. artikel 1 onder f Wpg). Opmerkelijk is dat het regime van de Wet politiegegevens niet voorziet in serieuze betrokkenheid van de officier van justitie, de autoriteit die verantwoordelijk is voor de opsporing van strafbare feiten en die, wanneer rechten en vrijheden van burgers in het geding zijn, algauw ook betrokken wordt bij de inzet van concrete opsporingsmethoden.
Vuile data kunnen aan de voorkant op verschillende manieren aan het licht komen. Zo kan in een eerder strafproces zijn vastgesteld dat de betreffende data onrechtmatig zijn verkregen, bijvoorbeeld in het geval de rechter heeft geoordeeld dat er sprake was van discriminatoir overheidsoptreden. Dan bestaat de verplichting tot terugkoppeling daarvan aan de verwerkingsverantwoordelijke binnen de Nationale Politie (artikel 7 lid 1 onder g en j onderdeel 3 jo. artikel 11b Besluit justitiële en strafvorderlijke gegevens).[1] Hiermee wordt – in theorie – ervoor gezorgd dat vuile data geen tweede leven krijgen in de datasets die worden

gebruikt voor CAS. In de praktijk blijkt dit niet altijd zo nauw te worden genomen en moet in rechte worden afgedwongen dat ontoelaatbare data ook daadwerkelijk worden verwijderd uit politiesystemen (Buruma, 2010). Een ander probleem is dat slechts in een fractie van de gevallen eerder zal zijn beoordeeld, bijvoorbeeld in een andere strafzaak, of er sprake is van onjuiste of onrechtmatig verkregen data (Oerlemans, 2018). Als hier geen sprake van is, zal in principe moeten worden vertrouwd op het vermogen van de Nationale Politie, althans de verwerkingsverantwoordelijke, om zelf het problematische karakter van de data te constateren. In de literatuur wordt betwijfeld of de politie inderdaad in staat is deze rol bij de gegevensverwerking te vervullen (Hildebrandt, 2016; Buruma, 2016; Schermer, 2017; Oerlemans, 2018).[2]

Vuile data kunnen ook aan de voorkant worden gefilterd wanneer de personen op wie bepaalde data betrekking hebben aan de bel trekken bij een privacyfunctionaris of beleidsmedewerker van de Nationale Politie. Zij hebben het recht om te verzoeken om verwijdering van bepaalde gegevens (artikelen 28 en 29 Wpg). Deze personen zouden zelf vuile data – wanneer zij deze identificeren – kunnen laten verwijderen, waardoor die data niet in datasets gebruikt kunnen worden. Ook hiervan kan in de praktijk weinig worden verwacht. Het gaat vooral om een papieren werkelijkheid. Zo blijkt uit onderzoek dat burgers niet weten wie hun gegevens verwerkt, dat zij rechten hebben en hoe zij deze kunnen uitoefenen (Custer & Lesier, 2019). Hoewel empirisch onderzoek nodig zal zijn om de kwaliteit van de filter aan de voorkant concreet te kunnen bepalen, kan vanuit een regulerend perspectief niet op voorhand van een transparante procedure worden gesproken die is gekoppeld aan sluitende inhoudelijke beoordelingsmaatstaven. Het risico dat vuile data doorsijpelen in voorspellende data-analyses als CAS is daarom op het eerste gezicht groot.

De filter aan de achterkant

Het filteren van vuile data uit voorspellende data-analyses kan ook aan de achterkant van het proces van predictive policing gebeuren, namelijk nadat de vuile data al zijn betrokken bij het genereren van een voorspelling. In het geval van CAS zijn er twee mogelijkheden om achteraf vuile data te identificeren en te verwijderen.

In de eerste plaats kan de strafrechter functioneren als het achteraf filtrerende mechanisme. Dit is het geval als de voorspelling van criminaliteit uiteindelijk tot een strafzaak leidt. In de praktijk is de betekenis van dit mechanisme echter zeer beperkt. Dit komt doordat slechts in een fractie van de zaken waarin op basis van een voorspelling wordt gehandeld door de overheid, het onderzoek aanleiding zal geven tot een strafvervolging. Van een sluitend filter is alleen al om deze reden geen sprake. Maar ook wanneer een zaak die begint met een voorspellende data-analyse wel tot een vervolging leidt, is het maar de vraag of de strafrechter zich zal buigen over de kwestie of de gebruikte datasets vuile data bevatten. Dat heeft te maken met de manier waarop voorspellende data-analyses als CAS worden gebruikt in strafzaken.

Voorspellingen zullen meestal worden gebruikt als instrument om te bepalen op welke gebieden de opsporingsaandacht wordt gericht, op basis waarvan vervolgens methoden gerichter kunnen worden ingezet die min of meer vrij ter beschikking staan van de autoriteiten, zoals het verrichten van verkeerscontroles of het kortstondig observeren van burgers (Das & Schuilenburg, 2018). In zeldzamere gevallen kan een voorspelling in samenhang met concrete observaties (ook) worden gebruikt om de verdenking te construeren die bijvoorbeeld de aanhouding van de verdachte legitimeert (Hoving, 2019). Zelfs dan is het goed denkbaar dat de bijkomende observaties van een zodanig gewicht zijn dat de voorspelling niet nodig is om tot de verdenking te komen.[3] Een directe en concrete strafrechtelijke aanleiding om kritisch naar de kwaliteit van de voorspelling te kijken, zoals het gebruik van de voorspelling ter rechtvaardiging van de inzet van een specifieke strafvorderlijke bevoegdheid, ontbreekt in de meeste zaken. De relevantie van een onderzoek naar de gebruikte data voor rechterlijke beslissingen in het strafproces is dus allerminst vanzelfsprekend. Dit kan zelfs rechtvaardigen dat de opsporingsautoriteiten informatie met betrekking tot de voorspelling uit het procesdossier van de strafzaak laten.[4]

In de praktijk zullen de gevallen waarin de strafrechter als filter aan de achterkant functioneert zich beperken tot de gevallen waarin het de verdediging lukt de rechter te overtuigen de gebruikte datasets op vuile data te controleren. Hiervoor zal de verdediging de strafrechtelijke relevantie van dit onderzoek moeten concretiseren. Zo kan de verdediging betogen dat de voorspelling noodzakelijk was om tot een verdenking tegen de verdachte te komen, waardoor het gebruik van bijvoorbeeld onjuiste gegevens in de voorspellende data-analyse tot gevolg heeft dat de aanhouding van de verdachte onvoldoende op feiten was gestoeld. Ook kan de verdediging betogen dat de taak van de rechter om over de rechtmatigheid van het opsporingsonderzoek te waken reeds op zichzelf noopt tot het verbinden van rechtsgevolgen aan het gebruik van vuile data, ook al vindt deze onrechtmatigheid plaats nog voordat sprake is van een verdenking tegen een bepaalde burger (Das & Schuilenburg, 2018).[5] Deze opvatting vindt steun in de bereidheid van de Hoge Raad (1 november 2016, ECLI:NL:HR:2016:2454) om bijvoorbeeld discriminatoire verkeerscontroles binnen het kader van de strafzaak te sanctioneren. Wanneer de rechter oordeelt dat de opsporingsautoriteiten onrechtmatig verkregen materieel hebben gebruikt in een dataset, zou het gevolg hiervan kunnen zijn dat het Openbaar Ministerie niet-ontvankelijk wordt verklaard in de strafzaak of dat de verdachte strafkorting krijgt bij een eventuele veroordeling.

De eerste, zeer verreikende, sanctie komt slechts in beeld wanneer een fundamenteel rechtsbeginsel wordt geschonden. Door deze rechterlijke sanctie wordt achteraf de voorspelling die mede berustte op vuile data buiten de deur gehouden, of het toekomstige gebruik hiervan wordt in ieder geval ontmoedigd. In de praktijk komen dergelijke rechterlijke sancties nauwelijks voor. De taakopvatting van de strafrechter is, eufemistisch uitgedrukt, bepaald niet gericht op een welwillende houding met betrekking tot het identificeren van laakbaar overheidsoptreden (Corstens, 2018, 885; Pitcher & Samadi, 2018; Brinkhoff, 2016). De vervolging van de dader wordt vaak belangrijker gevonden dan de wijze waarop het onderzoek is verricht. Om de rechter te overtuigen van de noodzaak om in de strafzaak

de datasets te controleren op de aanwezigheid van vuile data (en dus van de noodzaak om inzicht te hebben in deze data), zal de verdediging met zeer indringende argumenten moeten komen. Voor de verdediging is het zonder over de datasets te beschikken echter vrijwel onmogelijk te concretiseren waarom de gebruikte datasets mogelijk problematisch zijn. Een verzoek van de verdediging om inzicht te krijgen in de gebruikte datasets zal daarom algauw als een *fishing expedition* worden afgedaan. Wanneer de verdediging het mogelijke gebruik van onrechtmatige data aan de kaak wil stellen, lijkt met andere woorden sprake van een *catch 22*-situatie.

In de tweede plaats zijn er mogelijkheden om achteraf vuile data te filteren *buiten* het strafproces om. Zo moet bij geautomatiseerde profilering in principe aan de 'betrokkene' informatie worden verschaft over de logica van de besluitvorming (artikel 7a Wpg). Logica lijkt echter hier over iets anders te gaan dan de rechtmatigheid en juistheid van de data zelf. Op basis van bijvoorbeeld onrechtmatig verkregen data door de Nationale Politie kan best een logisch in orde zijnd besluitvormingsproces worden vormgegeven. Bovendien hoeft, wanneer het om de opsporing van strafbare feiten gaat, slechts in zeer beperkte mate met de verdachte of andere betrokkenen informatie te worden gedeeld, waardoor de mogelijkheid zeer beperkt is om de kwaliteit van de data aan te vechten (Custers & Lesier, 2019; Hildebrandt, 2016).

Kortom, de effectiviteit van de filtermogelijkheden aan de achterkant lijkt nog beperkter dan die aan de voorkant van het proces van predictive policing. Van een sluitend en transparant mechanisme om vuile data in de gebruikte datasets van CAS te identificeren en te verwijderen, is daarom nog geen sprake.

Conclusie en reflectie

Op verschillende terreinen waar de overheid een verantwoordelijkheid voor beleid en uitvoering draagt, worden steeds meer digitale applicaties en technologische hulpmiddelen ingezet om de kans op criminaliteit of ander risicovol gedrag te voorspellen. De Nationale Politie, de Belastingdienst en de Algemene Inlichtingen- en Veiligheidsdienst, maar ook gemeenten, maken gebruik van grote hoeveelheden datasets uit verschillende bronnen om 'risicovolle' personen of groepen in kaart te brengen, met als doel de opsporing van criminelen, fraudeurs en terroristen te vergemakkelijken. CAS en SyRI, het opsporingssysteem voor uitkeringsfraude, zijn tot de verbeelding sprekende voorbeelden hiervan. Maar denk ook aan de algoritmische systemen van de Belastingdienst bij de opsporing van mogelijke fraude met toeslagen.

Opvallend is dat er nauwelijks passende kaders zijn voor hoe voorspellende analyses optimaal kunnen worden ingezet in overheidsvraagstukken én op zo'n manier dat het juridisch en ethisch verantwoord is. Daarom is het een belangrijke vraag hoe het overheidsdomein zo veel mogelijk kan profiteren van voorspellende analyses en hoe tegelijk ethiek en de rechtsstaat deze nieuwe voorspellingstechnieken beheersbaar en controleerbaar kunnen houden (*rule of law*). Voorspellende analyses bieden niet alleen nieuwe kansen voor het voorkomen en opsporen van

criminaliteit en ander ongewenst gedrag, maar leiden ook tot risico's voor de rechten en vrijheden van burgers en het gevaar van willekeur. Onderzoek hoe de regulering van voorspellende analyses optimaal kan worden gewaarborgd, is om die redenen van groot belang. Veiligheid houdt namelijk ook in dat de burger wordt beschermd tegen de overheid, tegen de mogelijke willekeur van de machtsuitoefening door de politie bijvoorbeeld.

In dit artikel zijn we ingegaan op het probleem van vuile data en hoe op een juridisch verantwoorde manier kan worden omgegaan met de risico's die hieraan zijn verbonden. We hebben hierbij een onderscheid gemaakt tussen onjuiste en onrechtmatig verkregen data die komen uit of zijn afgeleid van politieoptreden, waaronder corruptie en discriminatie van bepaalde groepen of personen. Kern van de strafvorderlijke rechtsbescherming is dat de burger tegen beide vormen van vervuiling in de datasets van voorspellende analyses moet worden beschermd. In het geval van CAS hebben we laten zien dat de filters om vuile data te weren uit de gebruikte datasets beperkt zijn. Hoewel er in theorie mogelijkheden bestaan vuile data te weren, en in bepaalde gevallen evident vuile data ook daadwerkelijk geïdentificeerd zullen worden, zijn de filters aan zowel de voor- als de achterkant onvoldoende transparant en fijnmazig om een effectieve bescherming tegen vuile data te kunnen bieden. Alleen in uitzonderlijke, zeer specifieke situaties zou de rechter een rol kunnen spelen bij de bescherming van de burger tegen het gebruik van vuile data.

Willen voorspellende data-analyses zoals CAS en SyRI zich tot volwaardige en integere opsporingsmethoden voor de overheid ontwikkelen, dan zal onder ogen moeten worden gezien dat een voorwaarde hiervoor is dat de data die worden gebruikt op een basaal niveau 'schoon' zijn, en ook dat de zuiverheid van de data controleerbaar moet zijn. Hierdoor kan zowel de effectiviteit als de positieve perceptie van voorspellende methoden als predictive policing in de samenleving worden versterkt. Een fundamenteel uitgangspunt van de rechtsstaat is immers dat ook de overheid zich aan de wet dient te houden. In een rechtsstaat is het bovendien niet zo dat burgers er maar op moeten vertrouwen dat de spelregels eerlijk zijn en dat deze automatisch worden nageleefd. Er moet met andere woorden kunnen worden gecontroleerd of de overheid zuiver handelt en als dit niet het geval is, moet de burger hiervan een punt kunnen maken. Dit is zeker het geval wanneer het gaat om gegevens die een hoog risico voor de rechten en vrijheden van personen met zich brengen, zoals gegevens met betrekking tot ras en etnische afkomst. Het filteren van vuile data op een overzichtelijke, transparante en zo waterdicht mogelijke manier is daarom een onderwerp dat meer aandacht behoeft.

Noten

1 Deze verplichting is omslachtig vormgegeven: de verplichting bestaat in haar algemeenheid om de rechterlijke beslissing, sepot of strafbeschikking aan de verwerkingsverantwoordelijke te verschaffen. Uit de wetshistorie blijkt dat een belangrijk doel

hiervan is de genoemde categorieën zaken onder de aandacht van de verwerkingsverantwoordelijke te brengen.

2 Stel dat de enige informatie die de verwerkingsverantwoordelijke van de Nationale Politie tot zijn beschikking krijgt het aantal verkeerscontroles is dat in een wijk heeft plaatsgevonden en dat een bepaald deel hiervan een 'resultaat' heeft opgeleverd. Dit kan relevante informatie zijn voor een voorspellende data-analyse als CAS. Het is echter onmogelijk op basis van deze informatie per controle de rechtmatigheid te beoordelen. Hiertoe zou de verwerkingsverantwoordelijke over de stukken met betrekking tot elk van deze controles moeten beschikken. Mocht de verantwoordelijke al van alle relevante informatie worden voorzien, dan is het nog altijd de vraag of het redelijkerwijs te verwachten is dat hij alle informatie verwerkt. Het gaat hier om de beoordeling van een juridisch complexe en bovendien tijdrovende vraag. Zo is zelfs binnen de rechtspraak niet goed duidelijk wanneer een verkeerscontrole al dan niet rechtmatig is (Noyon & Trapman, 2017; Reijntjes, 2019).

3 Als er op basis van een voorspelling een verhoogd risico wordt vastgesteld op overvallen op nachtwinkels in een bepaalde wijk én in deze wijk rijdt een auto midden in de nacht ogenschijnlijk doelloos met gedoofde lichten een aantal keer de nachtwinkel voorbij, dan kan bijvoorbeeld de voorspelling een bijdrage (maar ook niet meer dan dat) leveren aan het ontstaan van de verdenking.

4 In principe moeten alle relevante handelingen van de opsporingsambtenaren voorafgaand aan de verdenking die uiteindelijk tot de strafzaak leidt, worden geverbaliseerd (artikel 152 Wetboek van Strafvordering (Sv); Corstens, 2018, 310 e.v.). Slechts stukken die relevant zijn voor de beslissingen die de strafrechter moet nemen hoeven echter in het procesdossier te worden opgenomen, zo valt te lezen in artikel 149a lid 2 Sv (Corstens, 2018, 259 e.v.). Het is daarom denkbaar dat door het gebrek aan directe concrete relevantie voor de rechterlijke beslissing, informatie met betrekking tot de voorspelling in het geheel niet in het procesdossier wordt opgenomen.

5 Het opsporingsonderzoek vangt al aan voordat er sprake is van een verdenking, namelijk wanneer sprake is van een onderzoek in verband met strafbare feiten met als doel het nemen van strafvorderlijke beslissingen (artikel 132a Sv). Hier kan bijvoorbeeld sprake van zijn wanneer datasets worden samengesteld en een analyse wordt uitgevoerd om potentiële woninginbrekers in kaart te brengen ter bestrijding van een toegenomen aantal inbraken in woonwijk X. Wil de rechter aan het gebruik van vuile data in dit kader een rechtsgevolg verbinden, dan zal deze onrechtmatigheid wel moeten hebben plaatsgevonden in het opsporingsonderzoek naar het feit waar de verdachte voor wordt vervolgd. Dit laatste, wat technische, punt is vanwege het bereik van artikel 359a Sv, de bepaling die het mogelijk maakt rechterlijke sancties te verbinden aan onrechtmatigheden. In het zojuist gegeven voorbeeld kan de rechter dus alleen een sanctie verbinden aan een onrechtmatige voorspelling wanneer de verdachte wordt vervolgd vanwege een woninginbraak in woonwijk X. Wanneer echter naar aanleiding van deze voorspelling de burger die nader in de gaten werd gehouden wordt betrapt bij het sluiten van een drugsdeal, kan de rechter in de vervolging vanwege de drugsdeal geen gevolgen verbinden aan de eventuele onrechtmatigheid van de voorspelling. In deze laatste situatie kunnen alleen in zeer uitzonderlijke gevallen, wanneer het gaat om uiterst ernstige onrechtmatigheden, gevolgen worden verbonden aan de onrechtmatigheid.

Literatuur

Amnesty International (2013). *Proactief politieoptreden vormt risico voor mensenrechten. Etnisch profileren onderkennen en aanpakken*. Amsterdam: Amnesty International.

Andrejevic, M. (2017). Digital Citizenship and Surveillance: To Pre-Empt A Thief. *International Journal of Communication*, 11: 879-896.

Bennett Moses, L., & Chan, J. (2018). Algorithmic prediction in policing: assumptions, evaluation, and accountability. *Policing and Society*, 28 (7): 806-822.

Borgers, M.J. (2007). *De vlucht naar voren*. Den Haag: Boom.

Brinkhoff, S. (2016). De toepassing van artikel 359a Sv anno 2016. Een pleidooi voor herstel van balans en de terugkeer naar echte rechterlijke vrijheid. *Delikt & Delinkwent*, 8 (2): 101-116.

Buruma, Y. (2010). Opvragen, beweren en kennisnemen van gegevens voor de opsporing. *Delikt & Delinkwent*, 57 (7): 923-953.

Buruma, Y. (2016). De criminele homo digitalis. *Nederlands Juristenblad*, 1073 (22): 1534-1541.

Çankaya, S. (2012). *De controle van marsmannetjes en ander schorriemorrie: het beslissingsproces tijdens proactief politiewerk.* Den Haag: Boom Lemma uitgevers.

Christin, A., Rosenblat, A., & Boyd, D. (2015). *Courts and Predictive Algorithms. Data & Civil Rights: A New Era of Policing and Justice*.https://datasociety.net/output/data-civil-rights-courts-and-predictive-algorithms/, geraadpleegd op 28 oktober 2019.

Cohen, S. (1972 [2002]). *Folk Devils and Moral Panics*. Londen/New York: Routledge.

Corstens (2018). *Het Nederlands Strafprocesrecht* (bewerkt door M.J. Borgers en T. Kooijmans). Deventer: Wolters Kluwer.

Custers, B.H.M. (2016). Big data in wetenschappelijk onderzoek. *Justitiële verkenningen*, 1: 8-21.

Custer, B.H.M., & Lesier, M.R. (2019). Persoonsgegevens in het strafrecht. *Nederlands Juristenblad*, 2107 (34): 2490-2497.

Danaher, J. (2016). The threat of algocracy: reality, resistance and accommodation. *Philosophy & Technology*, 29: 245-268.

Das, A., & Schuilenburg, M. (2018). Predictive policing: waarom bestrijding van criminaliteit op basis van algoritmen vraagt om aanpassing van het strafprocesrecht. *Strafblad. Tijdschrift voor wetenschap en praktijk*, 33 (4): 19-26.

Dubbelaar, M.J. (2009). Betrouwbaarheid versus rechtmatigheid in strafzaken. *RM Themis*, 170 (3): 93-105.

Ericson, R.V. (2007). *Crime in an insecure world*. Cambridge: Polity Press.

Eterno, J., & Silverman, E. (2012). *The crime numbers game. Management by manipulation*. New York: Taylor & Francis Group.

Ewald, F. (2002). The return of Descartes's malicious demon: An outline of a philosophy of precaution. In: T. Baker & J. Simon (red.), *Embracing risk. The changing culture of insurance and responsibility.* Chicago/Londen: The University of Chicago Press, 273-301.

Ferguson, A.G. (2017). *The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement*. New York: NUY-Press.

Garland, D. (1990). *Punishment and modern society. A study in social theory*. Chicago: Chicago University Press.

Goode. E., & Ben-Yehuda, N. (2009). *Moral Panics: The Social Construction of Deviance*. Oxford/Cambridge, MA: Blackwell.

Graham, S. (2010). *Cities under siege: the new military urbanism*. Londen: Verso.

Groenhart, N.W. (2019). Commentaar op Wet Politiegegevens. In: E.R. Muller, E.T. Brainich, J.G. Brouwer & A.E. Schilder (red), *Tekst & Commentaar Openbare orde en veiligheid.* Deventer: Wolters Kluwer, 439-523.

Hildebrandt, M. (2016). Data-gestuurde intelligentie in het strafrecht. In: E.M.L. Moerel, J.E.J. Prins, M. Hildebrandt, T.F.E. Tjong Tjin Tai, G-J. Zwenne & A.H.J. Schmidt, *Homo Digitalis* (Handelingen 146e NJV vergadering 2016). Deventer: Kluwer, 137-240.

Hoving, R.A. (2019). Verdacht door een algoritme. Kan predictive policing leiden tot een redelijke verdenking? *Delikt & Delinkwent*, 41 (7): 530-546.

Hunt, P., Saunders, J., & Hollywood, J.S. (2014). *Evaluation of the Shreveport predictive policing experiment*. Santa Monica, CA: Rand.

Keulen, B.F., & Knigge, G. (2016). *Strafprocesrecht.* Deventer: Wolters Kluwer.

Kuiper, R. (2014). *Vormfouten* (Staat en Recht, nr. 19). Deventer: Kluwer.

Lub, V. (2013). Buurtwachten in Nederland: ontwikkeling, mechanismen en morele implicaties. *Justitiële verkenningen*, 42 (5): 27-44.

Lyon, D. (red.) (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. New York: Routledge.

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

Marx, G.T. (1984). Notes on the Discovery, Collection, and Assessment of Hidden and Dirty Data. In: J.W. Schneider & J.I. Kitsuse (red.), *Studies in the Sociology of Social Problems*. Ablex: Norwood, 78-113.

Mayer-Schönberger, V., & Cukier, V. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think.* Boston: Houghton Mifflin Harcourt.

Mohler, G., Short, M., Malinowski, S., Johnson, M., Tita, G., Bertozzi, A., & Brantingham, P. (2015). Randomized Controlled Field Trials of Predictive Policing. *Journal of the American Statistical Association*, 110 (512): 1399-1411.

Mutsaers, P. (2013). *A Public Anthropology of Policing. Law Enforcement and Migrants in the Netherlands* (diss. Tilburg). Tilburg University.

Noyon, L., & Trapman, L.S.A (2017). Het boekje te buiten? *Ars Aequi*, 66 (2): 83.

Oerlemans, J.J. (2018). Beschouwing rapport Commissie-Koops: strafvordering in het digitale tijdperk. *Platform Modernisering Strafvordering*, 18 (2): 92-105.

Pearsall, B. (2010). Predictive Policing: The future of law enforcement. *National Institute of Justice Journal*, (266): 16-19.

Peeters, R., & Schuilenburg, M. (2018). Machine Justice: Governing Security Through the Bureaucracy of Algorithms. *Information Polity. An International Journal*, 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.

Pieterman, R. (2008). *De voorzorgcultuur. Streven naar veiligheid in een wereld vol risico en onzekerheid*. Den Haag: Boom Juridische uitgevers.

Pitcher, K.M., & Samadi, M. (2018). Integriteit als perspectief bij de rechterlijke reactie op vormverzuimen. *Delikt & Delinkwent*, 59 (8): 731-746.

Reijntjes, J.M. (2019). Annotatie bij HR 9 oktober 2018, ECLI:NL:HR:2018:1872. *Nederlandse Jurisprudentie*, 24 (3/4): 350-358.

Richardson, R., Schultz, J., & Crawdford, K. (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.

Rienks, R., & Schuilenburg, M. (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.* Oud-Turnhout: Gompel & Svacian, 39-54.

Rodrigues, P.R., & Wouden, M.A.H. van der (2016). Proactieve politiecontrole en onderscheid naar etniciteit of nationaliteit. *Nederlands Juristenblad*, 1650 (32): 2294-2302.

Schermer, B.W. (2011). The limits of privacy in automated profiling and data mining. *Computer law & security review*, 27 (1): 45-52.

Schermer, B.W. (2017). Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens. *Tijdschrift voor Bijzonder Strafrecht & Handhaving*, 3 (4): 207-216.

Schuilenburg, M. (2015). *The Securitization of Society: Crime, Risk, and Social Order*. New York: New York University Press.

Schuilenburg, M. (2016). Predictive policing: De opkomst van een gedachtenpolitie?. *Ars Aequi*, 65 (12): 931-936.

Schuilenburg, M. (2018). Opgeruimd staat netjes: over de sociologie van gebiedsverboden en de praktijk van het Collectief Winkelverbod. *Justitiële Verkenningen*, 44 (2): 27-40.

Schuilenburg, M. (2019). *Hysterie. Een cultuurdiagnose*. Amsterdam: Boom filosofie.

Schuilenburg, M., & Swaaningen, R. van (2013). Veiligheid in een laatmoderne cultuur. *Tijdschrift over Cultuur & Criminaliteit*, 3 (2): 109-122.

Simon, J. (2007). *Governing through crime. How the war on crime transformed American democracy and created a culture of fear*. Oxford: Oxford University Press.

Smith, G.J.D., Bennett Moses, L., & Chan, J. (2017). 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.

Willems, D., & Doeleman, R. (2014). *Predictive Policing* – wens of werkelijkheid? *Tijdschrift voor de Politie*, 4/5 (76): 39-42.

Willis, J.J., & Mastrofski, S.D. (2014). Pulling together: integrating craft and science. *Policing*, 8 (4): 321-329.

WRR (2016). *Big Data in een veilige samenleving*. Amsterdam: Amsterdam University Press.

Završnik, A. (2019). Algorithmic justice: Algorithms and big data in criminal justice settings. *European Journal of Criminology*. doi:10.1177/1477370819876762.

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