A.R. Lodder & M.B. Schuilenburg[1]

Politie-webcrawlers en Predictive policing

Computerrecht 2016/81

In artikelen, boeken en YouTube-video's over big data wordt naast commerciële, "klantgerichte" toepassingen vrijwel altijd gewezen op opsporing van strafbare feiten. In deze bijdrage gaan de auteurs in op het analyseren van big data om de inzet van politie te sturen, het zogenaamde *predictive policing*[2], alsmede op het vergaren van op het internet aanwezige informatie door zogenaamde *webcrawlers*[3] die, na analyse, gebruikt kan worden ter ondersteuning van de opsporingspraktijk.

1. Inleiding

In lijn met de traditie van de langslepende wetgevingstrajecten *Computercriminaliteit I* (1985-1993) en *Computercriminaliteit II* (1999-2006), is het in 2010[4] opgestarte *Computercriminaliteit III* na vijf en een half jaar op 22 december 2015 bij de Tweede Kamer ingediend.[5] Veel aandacht was er de afgelopen jaren voor de "hack-bevoegdheid", vreemd genoeg veelal als terug-hack aangeduid.[6] Op 2 januari 2016 meldde Inge Philips, plaatsvervangend hoofd landelijke recherche, dat door geldgebrek er geen gebruik van deze nieuwe bevoegdheden (zoals hacken door de politie) zou kunnen worden gemaakt:[7]

> "Maar er moet wel een budget zijn. We kunnen deze agenten niet zonder fatsoenlijke spullen aan het werk zetten. Dan gaan ze gehandicapt van start."

Dit citaat toont een op het oog verkeerde inschatting van de problematiek in het digitale domein. Het gaat veel minder om de spullen (de software en hardware) dan om de skills daar iets nuttigs mee te doen. Zeker in het geval van big data-technieken zal een eventuele beperking behalve op het terrein van de "spullen", in casu: de gebruikte dataverzamelingen, vooral bij de opsporingsambtenaar liggen. De ambtenaar moet de analyses uitvoeren en de uitkomsten duiden. Goede data-analisten zijn evenwel schaars en zeker data-analisten/opsporingsambtenaren.
Dat brengt ons vervolgens bij het domein van big data analytics binnen de opsporing en de rechtspraak. Een onderwerp waaraan in het WODC rapport *Big data, big consequences? Een verkenning naar privacy en big data gebruik binnen de opsporing, vervolging en rechtspraak* van Lodder e.a. uit 2014[8] in algemene zin aandacht besteed is. Een onderwerp dat ons, zeker op termijn, confronteert met de lastige vraag in hoeverre uitkomsten van data analytics als bewijs in strafzaken gebruikt kunnen worden.
In deze bijdrage gaan wij, gezien de beperkte ruimte, alleen in op de voor dit moment juridisch en technisch gezien meest interessante toepassingen op het terrein van data analytics. Om te beginnen gaan we in op de juridische aspecten van de inzet van *webcrawlers* door de politie, search bots die het internet afstruinen en indexeren. Daarnaast behandelen we *predictive policing*, het grootschalig gebruik van data dat beoogt opsporingscapaciteit meer gericht en efficiënt in te zetten en criminaliteit te voorkomen.

2. Webcrawlers

Het is haast niet voor te stellen dat men in de jaren 90 een internetpagina bij een zoekmachine moest aanmelden met het verzoek deze op te nemen in de index om te zorgen dat deze pagina vindbaar zou worden via de zoekmachine. Inmiddels worden continu grote delen van het internet geïndexeerd door autonoom opererende webcrawlers. Webcrawling houdt in dat met behulp van een computerprogramma op een methodische en geautomatiseerde manier het wereldwijde web wordt doorgebladerd. Vaak worden gegevens gekopieerd om deze te kunnen verwerken en indexeren voor bijvoorbeeld zoekmachines. Door indexering en bewerking van de verkregen en vastgelegde gegevens kan informatie worden afgeleid die niet of niet snel kenbaar zou zijn voor een willekeurige internetgebruiker. Ook de nationale politie experimenteert met webcrawlers. Dit kan de kwaliteit en snelheid van opsporing verhogen. Zo kan bijvoorbeeld door het analyseren van gecrawlde informatie snel inzicht worden verkregen in de achtergrond van een verdachte, waar dit inzicht anders niet of na langere tijd beschikbaar zou komen.

2.1 *Bevoegdheid*

De eerste vraag die wij stellen is of de politie bevoegd is informatie op internet te verzamelen.[9] Hierbij moet een onderscheid worden gemaakt tussen bestuursrechtelijke handhaving en strafrechtelijke opsporing. In een (vertrouwelijk) onderzoeksrapport van Lodder, Borgers en Neerhof

1 A.R. Lodder is hoogleraar Internetrecht aan de Vrije Universiteit Amsterdam en Of Counsel bij SOLV Advocaten. M.B. Schuilenburg is verbonden aan de afdeling Strafrecht en Criminologie van de Vrije Universiteit Amsterdam.
2 D. Willems & R. Doeleman, 'Predictive policing – wens of werkelijkheid?', *Tijdschrift voor de Politie*, jr. 76, nr. 4/5.
3 Web crawler, Wikipedia, https://en.wikipedia.org/wiki/Web_crawler.
4 Computercriminaliteit III, *Kamerstukken II* 2015/16, 34372.
5 Wetsvoorstel Computercriminaliteit bij Tweede Kamer ingediend, Rijksoverheid.nl, 22 december 2015.
6 Terug hacken impliceert een reactie, maar het gaat om inbreken in computers, niet per se computers waarvandaan ook gehackt is.
7 H. Modderkolk, 'Politie krijgt hackbevoegheden 'maar kan ze niet gebruiken' *Volkskrant* 2 januari 2016.
8 Afgerond en gedrukt zomer 2014 en online beschikbaar op: http://dare.ubvu.vu.nl/handle/1871/51919. Op de site van het WODC bleef dit onderzoek *Big Data privacy* als 'lopend' vermeld, vanwege het feit dat een parallel onderzoek naar big data en techniek nog niet was afgerond. Inmiddels, begin 2016, wordt het technische onderzoek als afgerond vermeld http://wodc.nl/onderzoeksdatabase/2394a-big-data-techniek.aspx maar het privacyonderzoek nog altijd als opend! http://wodc.nl/onderzoeksdatabase/2394-big-data.aspx.
9 J. Oerlemans & B.J. Koops, 'Surveilleren en opsporen in een internetomgeving', *Justitiële Verkenningen* 2012, nr. 5, p. 46-47 stellen een afzonderlijke wettelijke regeling voor observatie in een internetomgeving voor.

uit juni 2015 is in opdracht van de nationale politie daarnaar gekeken.[10]
Binnen het bestuursrecht kan informatie over de naleving van wettelijke voorschriften worden verkregen via uitoefening van de bevoegdheden die een toezichthouder op grond van de Algemene wet bestuursrecht (Awb) of de bijzondere wet heeft, maar kan ook op andere wijze verkregen informatie, zoals via webcrawling, in beginsel worden gebruikt bij besluitvorming over oplegging van een bestuurlijke sanctie. Webcrawling kan als feitelijk handelen van een bestuursorgaan worden gekwalificeerd, waarbij het zorgvuldigheidsbeginsel (artikel 3:2 Awb) en het evenredigheidsbeginsel (artikel 3:4 lid 2 Awb) in acht moet worden genomen.[11]Webcrawling is echter geen toezichthandeling als bedoeld in titel 5.2 Awb. Het gaat niet om uitoefening van één van de in die titel of in een andere wet neergelegde bevoegdheden, zoals inlichtingen vorderen, het betreden van plaatsen, en dergelijke. Artikel 5:13 (gebruik bevoegdheden toezichthouder) is dus hierop niet van toepassing.
Bij het opstellen van de bevoegdheden in het Wetboek van Stafvordering en bijzondere wetten kon een technologie als webcrawling niet worden voorzien. Vooralsnog heeft de ontwikkeling van die technologie niet de aandacht van de wetgever genoten, hoewel er momenteel wel initiatieven ter modernisering van strafvordering lopen. Het onderbrengen van webcrawling bij bestaande bevoegdheden is niet eenvoudig. Algemene taakstellende bepalingen van een verkennend onderzoek bieden een fragiele grondslag, omdat deze niet toereikend zijn indien de resultaten van webcrawling te zeer ingrijpen in de persoonlijke levenssfeer van de betrokkene. In de specifiek wettelijk geregelde opsporingsbevoegdheden kan een grondslag nog het beste worden gevonden in een combinatie van de bevoegdheden tot stelselmatige observatie en stelselmatige inwinning van informatie. Uitgaande van een dergelijke grondslag is de inzet van webcrawlers echter aan beperkingen onderhevig.
Het verdient daarom voorkeur in de wet een specifieke bevoegdheid op te nemen voor webcrawling-activiteiten, hoewel het binnen het huidige kader dus niet op voorhand ontoelaatbaar is dergelijke activiteiten uit te voeren.

2.2 *Dataretentie, webcrawling en privacy*

Vanuit privacyperspectief kan verschillend worden gedacht over de wenselijkheid van grootschalige, ongerichte verzameling van informatie. Het uitgangspunt "select before you collect" is in beginsel leidend. Echter, een probleem is dat je pas weet nadat je informatie verzameld hebt of deze relevant is. Daarnaast kan informatie op het moment van verzamelen irrelevant zijn, maar enkele dagen, weken, maanden later alsnog relevantie krijgen. McGowan verwoordt mooi de verschillende perspectieven:[12]

> "The government deems all these records "relevant" based on the fact that they are used to find patterns and connections in preventing terrorist activity. Critics of the program, however, assert that billions of records cannot possibly be relevant when a negligible portion of those records are actually linked to terrorist activity."

De Digital Rights Ireland-uitspraak uit 2014[13] biedt interessante aanknopingspunten voor het beoordelen van de rechtmatigheid van de inzet van webcrawlers. Alvorens deze te bespreken, gaan wij kort in op de verschillen en overeenkomsten tussen webcrawling en dataretentie.
Een eerste verschil is de partij die de gegevens opslaat. Bij dataretentie is dat een private partij, de telecomprovider. Bij webcrawlers is dat de politie zelf, althans wordt in opdracht van de politie gewerkt. Dit geldt overigens niet voor alle webcrawling-activiteiten. De integrale kopie die van sociaal mediaverkeer wordt bijgehouden door het commerciële bedrijf Coosto wordt gebruikt door politie en andere overheidsinstanties.[14] Fabrini gaf in dit licht terecht aan:[15]

> "the distinction between retention of meta-data by private companies rather than by government agencies does not make a real difference, since it is the retention itself that alters the relationship between citizen and government in a way that is inimical [= harmful in effect] to democratic society."

Een tweede verschil tussen webcrawling en dataretentie is de aard van de informatie. Van internet afkomstige informatie ziet op de inhoud en verkeersgegevens zonderen de inhoud juist uit. Daarmee is van internet afkomstige informatie vanuit een privacyperspectief in beginsel gevoeliger, hoewel de aan metadata (zoals verkeersgegevens) te ontlenen privacygevoelige informatie niet onderschat kan worden. Clayton & Tennis stellen in dit verband:[16]

> "metadata can be highly intrusive to personal privacy – even more revealing in certain regards than the contents of our communications in some cases."

10 Een zeer algemene analyse van het zoeken in open internet bronnen is te vinden in het voor het FP7 project *Versatile Information Toolkit for End-Users Oriented Open-Sources Exploitation* geschreven rapport *D 3.2 ANALYSIS OF THE LEGAL AND ETHICAL FRAMEWORK IN OPEN SOURCE INTELLIGENCE*.
11 Zie ook PG Awb III, p. 338.
12 C.J. McGowan, The Relevance of Relevance: Section 215 of the USA PATRIOT Act and the NSA Metadata Collection Program, 82 *Fordham L. Rev.* 2399 (2014). Available at: http://ir.lawnet.fordham.edu/flr/vol82/iss5/15.
13 Hof van Justitie EU 8 april 2014 (Digital Rights Ireland), ECLI:EU:C:2014:238, vgl. ook Nederlandse vervolg: Rechtbank Den Haag 15 maart 2015, ECLI:NL:RBDHA:2015:2498.
14 Minister Blok in antwoord op Kamervragen op 5 november 2013 (met kenmerk 2013Z17854): "De politie en negen ministeries (Algemene Zaken, Binnenlandse Zaken en Koninkrijksrelaties, Defensie, Economische Zaken, Financiën, Infrastructuur en Milieu, Onderwijs, Cultuur en Wetenschap, Veiligheid en Justitie en Volksgezondheid, Welzijn en Sport) hebben Coosto als leverancier."
15 F. Fabbrini (2015): Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S. *Harvard Human Rights Journal*, forthcoming.
16 Newell, B. C., & Tennis, J. T. (2014). Me, My Metadata, and the NSA: Privacy and Government Metadata Surveillance Programs. In *iConference 2014 Proceedings* (p. 345-355).

Verkeersgegevens leggen locatie-informatie bloot (waar was iemand, althans een tot hem/haar behorend apparaat) en communicatie-informatie (met wie, wordt hoe vaak en hoe lang gecommuniceerd). Bij verkeersgegevens kunnen zo verbanden worden gelegd tussen (vermeende) deelnemers aan de communicatie. Er wordt immers vanuit het ene punt informatie uitgewisseld (zoals tekst, spraak) met een ander punt.

De op internet aanwezige informatie is zeer divers, zowel qua vorm (beeld, geluid, tekst, etc.) als wat betreft de inhoud. Niet altijd zal informatie aan een bepaalde persoon te koppelen zijn en verbanden tussen personen zijn doorgaans minder expliciet dan bij verkeersgegevens. Door analyse van op het internet aanwezige informatie kunnen echter toch verbanden worden afgeleid, ook als die dieper verborgen zijn. Een analysetool is immers iets anders dan Google.

Ten slotte kan de oorsprong van de informatie worden genoemd. Anders dan bij verkeersgegevens maakt door webcrawlers verzamelde informatie al onderdeel van het openbare leven uit. Hierbij moet echter de kanttekening worden gemaakt dat het feit dat iedereen praktisch de mogelijkheid heeft de informatie te raadplegen niet noodzakelijkerwijze volgt dat dit ook juridisch toelaatbaar is. Dit geldt met name vanwege mogelijke analysehandelingen. Het raadplegen van 20-25 afzonderlijke informatiebronnen over een persoon is wat anders, dan deze met elkaar in verband te brengen. Zo kan immers een beeld worden opgebouwd wat onder omstandigheden zelfs meer over iemand kan vertellen dan deze over zichzelf weet.

Bovenstaande verschillen brengen enige nuancering aan in de vergelijkbaarheid van dataretentie met webcrawling. De massaliteit van de verzamelde informatie is echter vergelijkbaar. Gezien de onuitputtelijke informatiebron die het internet is, zal bij webcrawling de mogelijke inbreuk in de persoonlijke levenssfeer in beginsel groter zijn.

2.3 *Waarborgen*

Bij dataretentie is er een duidelijke wettelijke grondslag voor het verzamelen en vastleggen van de gegevens. Bij webcrawling is zo'n grondslag voor zover aanwezig veel minder concreet. Bij dataretentie gaat het in zekere zin om de vervolgvraag: hoe verhoudt het verzamelen, opslaan en gebruiken van de gegevens zich tot het recht op privacy. Ook als er een wettelijke basis voor het verzamelen en/of webcrawlen bestaat, rijzen privacyvragen met betrekking tot het opslaan en gebruiken van de gegevens. In Digital Rights Ireland kwam naar voren dat de opslag op zichzelf, hoe ingrijpend ook, gerechtvaardigd kan zijn, mits er voldoende waarborgen in acht worden genomen.

De bij dataretentie noodzakelijke waarborgen zoals geformuleerd in Digital Rights Ireland lenen zich voor toepassing op webcrawlers. In meer specifiek op gegevensverwerking toegesneden regelgeving zijn duidelijke waarborgen voor webcrawling en data analytics niet te vinden. Artikel 8 en 9 Wet politiegegevens en de parallel aan de Algemene Privacy verordening voorgestelde en behandelde Richtlijn gegevensbescherming bij justitiële samenwerking in strafzaken en politionele samenwerking bieden weinig soelaas. De beginselen die daarin zijn opgenomen zijn algemeen van aard en niet bijzonder toegespitst, zeker niet voor big data-toepassingen als webcrawling.

Een belangrijke waarborg is het loggen van het informatiegebruik. Hiermee moet onrechtmatige raadpleging of gebruik van gegevens worden voorkomen (Digital Rights Ireland r.o. 54). Er moeten "objectieve criteria [zijn] ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan met het oog op het voorkomen, opsporen of strafrechtelijk vervolgen" (r.o. 60). Daarnaast moeten er "materiële en procedurele voorwaarden betreffende de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan" (r.o. 61), alsmede "objectieve criteria op basis waarvan het aantal personen dat de bewaarde gegevens mag raadplegen en vervolgens gebruiken, kan worden beperkt tot wat strikt noodzakelijk is voor de verwezenlijking van het nagestreefde doel" (r.o. 62) en ten slotte moeten er voldoende garanties zijn "dat de bewaarde gegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik ervan" (r.o. 66). In aanvulling op deze overwegingen is van cruciaal belang dat de gegevens en de uitkomsten van de analyses worden gebruikt door data-analisten die niet betrokken zijn bij de zaak waar de informatie voor geanalyseerd wordt. Dit om inopportuun gebruik van uitkomsten te voorkomen.

In overweging 58 van Digital Rights Ireland[17] wordt ingegaan op het feit dat er ook van onschuldige informatie wordt bewaard. De opslag van de gegevens op zichzelf wordt pas van betekenis als er wat met deze gegevens gebeurt.[18] Een mogelijkheid is te trachten een procedure te ontwikkelen die garandeert dat verstrekte gegevens alleen bij specifieke verdenkingen mogen worden opgevraagd en moeten worden vernietigd zodra de verdenking eindigt. In dat geval zal er, eventuele fouten daargelaten, vrijwel nooit informatie over een onschuldige burger worden geraadpleegd.

2.4 *Chilling effect*

Er zijn veel technische toepassingen te verzinnen die in theorie een bijdrage leveren aan de criminaliteitsbestrijding, maar in de praktijk niet. In dergelijk gevallen kan een maatregel beter in zijn geheel achterwege gelaten worden. In de eerste plaats moet het *chilling effect* dat kan uitgaan van grote dataverzamelingen niet onderschat worden. Mensen gaan zich anders gedragen als ze zich bespied wanen, ongeacht of dit ook daadwerkelijk het geval is (vgl. de

17 Hof van Justitie EU 8 april 2014 (Digital Rights Ireland), ECLI:EU:C:2014:238.

18 De opslag vormt wel een inbreuk op artikel 8 EVRM, maar kan gelegitimeerd zijn op basis van artikel 8 lid 2 bijvoorbeeld als de verwerking cf. Wbp of Wpg is.Vgl. EHRM 16 januari 2000 (Amann vs. Zwitserland), o.v. 69 "the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding" en vervolgens o.v. 71 "Such interference breaches Article 8 unless it is "in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 and, in addition, is "necessary in a democratic society" to achieve those aims."

werking van het panopticon).[19] Zo kan er een verstikkende werking uitgaan van het ongebreideld opslaan.[20] Effectiviteit is moeilijk aantoonbaar. In een uitgebreid overzicht van Ferdinandusse, Laheij en Hendriks getiteld *De bewaarplicht telecomgegevens en de opsporing. Het belang van historische telecommunicatie gegevens voor de opsporing* wordt weliswaar van een groot aantal zaken aangeven dat verkeersgegevens een rol hebben gespeeld, maar noch hoe snel de verkeersgegevens na het misdrijf zijn gevraagd (wat om een bewaarplicht te rechtvaardigen belangrijke informatie is) noch hoe essentieel de gegevens waren. Dit is niet de plaats om dieper in te gaan op de nut en noodzaak van verkeersgegevens, maar een noodzakelijke voorwaarde voor de inzet van webcrawlers is dat dit aantoonbaar tot resultaten leidt. Naast aantoonbare resultaten is er nog een andere vraag relevant, en dat is tot welke dilemma's het gebruik van big data leidt in de opsporing. Een antwoord hierop zoeken we in het zogenoemde *predictive policing*.

3. Predictive policing

Predictive policing is het voorspellen van crimineel en normoverschrijdend gedrag door middel van grootschalige monitoring en data-analyse. De term wordt toegeschreven aan politiecommissaris William Bratton van de Los Angeles Police Department die haar in 2008 introduceerde.[21] Het idee hierachter is dat de politie kan ingrijpen voordat de misdaad is gepleegd. Ter illustratie hiervan wordt vaak verwezen naar de film 'Minority Report' (2002) van Steven Spielberg.[22] De film speelt zich af in het Washington D.C. van 2054. In die stad vinden al zes jaar geen moorden meer plaats. De sleutel tot dit succes zijn drie paranormale 'pre-cogs' die in hun dromen moorden zien gebeuren. Op basis van hun denkbeelden kunnen de dader, het slachtoffer en de locatie van het misdrijf worden geïdentificeerd. Vervolgens arresteert de speciale politie-eenheid *PreCrime* de dader voordat hij of zij kan toeslaan. Relevant in dit alles is dat een van de kernelementen van schuld en straf wordt verlaten. Niet de daad, maar de intentie is strafbaar. *PreCrime, it works!*, zo luidt de campagneslogan.

Predictive policing ligt in het verlengde van criminologische noties als *actuarial justice* en risicojustitie.[23] Hierbij gaat het om een denken in termen van risicomanagement, het voorkomen van criminaliteit en het verminderen van angst voor criminaliteit door het identificeren en classificeren (en *de facto* onschadelijk maken) van handelingen of gedragingen die onveiligheid kunnen veroorzaken. Feeley en Simon hebben laten zien dat de technieken die hiervoor worden gebruikt een basis hebben in het verzekeringswezen.[24] Hierin worden premies en uitkeringen berekend op grond van uitgebreide risicotaxaties.[25] Aan de basis hiervan liggen grootschalige dataverzamelingen die door middel van verfijnde algoritmen worden ontsloten.

Over het gebruik en het nut van predictive policing in het veiligheidsbeleid is al het nodige geschreven.[26] Vaak wordt erop gewezen dat de aandacht van politie voor meer preventie op zichzelf niet nieuw is. Uit het werk van politiecommissaris Patrick Colquhoun blijkt dat de politie vanaf het begin van de negentiende eeuw al sterk was gericht op het voorkomen van criminaliteit. In *A Treatise on the Police of the Metropolis* schrijft Colquhoun dat de essentie van de politie "the prevention of crimes and misdemeanors" is.[27] Ook wordt erop gewezen dat commerciële bedrijven als Amazon, Facebook en Google op dezelfde manier werken. Zo doet Amazon suggesties voor nieuwe boeken op basis van vorige aankopen. Tot slot is er veel twijfel of predictive policing wel nieuwe voorspellingen kan doen. Zo werkt het systeem op basis van historische gegevens. Dit betekent dat het systeem niet zozeer voorspelt alswel de kans extrapoleert waar iets kan gebeuren.
Veel minder is bekend tot welke dilemma's deze manier van vroegtijdig ingrijpen en signaleren kan leiden. In hoeverre leidt bij predictive policing het hebben van een detentieverleden bijvoorbeeld tot een verhoogd risico? Hoe voorkomt de politie dat ze onjuiste voorspellingen doet? Kan een persoon worden opgepakt voor een daad die hij of zij nog niet heeft gepleegd?
Deze vragen zijn actueel omdat ook de nationale politie een groot geloof heeft in predictive policing. Zo wordt in het boek *Predictive policing, kansen voor een veiligere toekomst* gesteld dat "predictive policingeen volgende stap is in het politiewerk waarbij analyses, beschrijvend, verklarend – en dus ook steeds meer voorspellend – aan de basis staan van het nemen van beslissingen over het politiewerk".[28] Inmiddels werkt de nationale politie ook samen met het Nationaal

19 Jeremy Bentham, The Works of Jeremy Bentham, vol. 4 (Panopticon, Constitution, Colonies, Codification) [1843].

20 Vgl. ook overweging 37 in Digital Rights Ireland: "bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden".

21 W.L. Perry, B. McInnis, C.C. Price, S.C. Smith, J.S. Hollywood (2013). *Predictive policing, the role of crime forecasting in law enforcement operations*. Rand Corporation, Safety and Justice Program.

22 M. Schuilenburg (2006) 'It's the Protocol, Stupid!'. *Monu. Magazine on Urbanism*, 5, p. 53-58; M. Schuilenburg (2006). 'De codes van de openbare ruimte'. *In de Marge*, 3, p. 2-10; L. Zedner (2007). 'Pre-Crime and Post-Criminology?' *Theoretical Criminology*, 11(2), p. 261-281.

23 M. Feeley & J. Simon (1992). 'The new penology. Notes on the emerging strategy of corrections and its implications'. *Criminology*, 30(4), p. 449-474; M. Feeley & J. Simon (1994). 'Actuarial justice. The emerging new criminal law'. D. Nelken (ed.), *The futures of criminology*. London: *Sage*, p. 173-201;

24 J. Simon (1988). 'The ideological effects of actuarial practices'. *Law and Society Review* 22(4), p. 771-800; J. Simon & M. Feeley (2003). 'The form and limits of the new penology'. T.G. Blomberg & S. Cohen (eds.), *Punishment and social control*. New Brunswick: *Transaction Publishers*, p. 75-116.

25 N. Reichman. 'Managing crime risks. Towards an insurance bases model of social control'. *Research In Law Deviance and Social Control*, 1986/8, p. 151-172.

26 Zie bijvoorbeeld: R. van Swaaningen. 'Justitie als verzekeringsmaatschappij. "Actuarial justice" in Nederland'. *Justitiële verkenningen*,1996/5, p. 80-97; M. Schuilenburg (2012). Orde in veiligheid. Een dynamisch perspectief. Boom Lemma: Den Haag.

27 P. Colquhoun (1806). *A treatise on the police of the metropolis*. London: Printed for J. Mawman.

28 R. Rienks (2015). *Predictive policing, kansen voor een veiligere toekomst*. Apeldoorn: Politieacademie.

Forensisch Instituut aan zo'n tien projecten inzake predictive policing.[29]

In de literatuur worden verschillende argumenten genoemd tot welke ongewenste effecten predictive policing kan leiden. Een van de effecten hiervan is een nog vroegtijdiger inzetten van methoden en technieken van opsporing en een toename van het aantal controles zonder dat een rechter hier toezicht op heeft.[30] Opsporingsonderzoeken breiden zich namelijk uit tot personen die zelf niet onder verdenking staan, en zonder dat ze er zelf weet van hebben. De consequentie hiervan is dat predictive policing kan leiden tot een willekeurige en moeilijk controleerbare inzet van strafrechtelijke opsporingsmiddelen.

Een ander ongewenst effect is het feit dat het voornemen van een dader niet altijd zal leiden tot een concrete handeling, hij of zij kan ten slotte tot inkeer komen. Je zou zelfs kunnen beweren dat met vroegtijdig ingrijpen door de politie het klassieke daadstrafrecht langzaam wordt uitgebreid met een intentiestrafrecht: niet alleen de handeling zelf wordt strafbaar, maar ook de intentie om iets crimineels te doen.[31]

Dit alles stemt tot nadenken of predictive policing eenvoudig kan worden ingezet door de nationale politie. Schuilenburg heeft er in dit verband op gewezen dat de inzet van dergelijke vormen van proactieve handhaving vergaande consequenties heeft voor de vrijheidssfeer van burgers, aangezien bij al deze wijzigingen de formele strafrechtelijke werkelijkheid nauwelijks is mee veranderd.[32]

4. Slot

Big data-technieken bieden veel nieuwe mogelijkheden, maar voordat hiervan op grote schaal gebruik wordt gemaakt door de overheid is het belangrijk dat de werking inzichtelijk wordt gemaakt en wordt vastgesteld of de techniek ook daadwerkelijk resultaten oplevert. Zeker bij bijzonder in de levens van burgers ingrijpende domeinen als politieopsporing is voorzichtigheid geboden. Dat bewijst predictive policing, de techniek waarmee de politie op basis van grootschalige dataverzamelingen toekomstige misdaden wil voorspellen. Het is aan juristen voorwaarden te stellen aan het gebruik van de techniek, iets wat op dit moment in regelgeving in onvoldoende mate gebeurt. In een meer breder perspectief dient de samenleving zich te bezinnen op het vertrouwen in uitkomsten van analyses van gegevens zonder dat deze uitkomsten inzichtelijk zijn. Dit laatste is met steeds ingewikkelder algoritmen niet altijd eenvoudig, reden te meer dat waarborgen moeten worden geformuleerd voor een zorgvuldige toepassing ervan. Hiertoe is in deze bijdrage een eerste aanzet gegeven, maar er is nog veel werk te verzetten door technici, ethici en juristen. Ongeacht de schoonheid van de techniek, voorkomen moet worden dat we geregeerd worden door techniek zonder dat we begrip hebben over de werking ervan of waarborgen aan het gebruik hebben gesteld.

29 'De politie van de toekomst houdt iedere burger in de gaten', *De Correspondent*, 7 juli 2015.

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

31 M. Schuilenburg (2007). 'Bidden is goed, verzekeren beter'. I. Devisch & M. De Kesel (red.), *Fundamentalisme face to face*. Kampen: Klement, p. 90-108; M.J. Borgers, (2005). 'Strafbaarstellingen in de strijd tegen het terrorisme: werving ten behoeve van de gewapende strijd en samenspanning tot terroristische misdrijven'. A.H.E.C. Jordaans, P.A.M. Mevis & J. Wöretshofer (red.), *Praktisch strafrecht. Liber amicorum J.M. Reijntjes*, Nijmegen: Wolf Legal Publishers.

32 M. Schuilenburg (2012). *Orde in veiligheid. Een dynamisch perspectief*. Den Haag: Boom Lemma.