De criminele homo digitalis

Ybo Buruma[1]

Mireille Hildebrandt heeft duidelijke opvattingen over het recht en verstand van zaken over de digitale wereld. Ze daagt uit en verveelt niet met technische uiteenzettingen of met juridische betogen over de brij van regelgeving met betrekking tot gegevens. Het preadvies zet aan tot denken en doet beseffen dat data-gestuurde intelligentie in het strafrecht gevolgen zal moeten hebben. Met name waar het automatische data-analyses betreft die geïndividualiseerde personen aanwijzen is regulering in het Wetboek van Strafvordering nodig. Dit is niet direct noodzakelijk in het geval van het gebruik van data-gestuurde intelligente systemen als gevolg waarvan algemeen beleid wordt geadviseerd of waarmee bepaalde hot spots worden aangewezen. Hildebrandt bepleit verder terecht de noodzaak om een toezichthouder in te stellen die de werking controleert van data-gestuurde systemen die bij heimelijk onderzoek worden ingezet. Dit kan zijn de Autoriteit Persoonsgegevens, maar wellicht nog beter een in het leven te roepen Commissie van Toezicht voor de Politie.

Een bespreking van het preadvies van mw. prof. mr. M. Hildebrandt, '**Data-gestuurde intelligentie in het strafrecht**' *voor de Jaarvergadering van de Nederlandse Juristen-Vereniging, 10 juni 2016 te Haarlem, Handelingen NJV, 146e jaargang/2016-1, Deventer: Wolters Kluwer 2016, p. 137-240.*

Homo digitalis is een wijds begrip. Letterlijk lijkt het te gaan om de mens die slechts aan en uit kent, zwart en wit, vriend en vijand. Dat is niet wat de preadviseurs voor ogen hebben. Maar door te spreken van de homo digitalis geven ze aan dat er meer aan de hand is dan dat de mens digitale middelen gebruikt om zijn leven te vergemakkelijken en te beveiligen.[2] De homo digitalis is niet louter wat Hannah Arendt *homo faber* noemde: de mens als maker die met vertrouwen in zijn werktuigen meent dat elk probleem kan worden opgelost.[3] De homo digitalis wantrouwt zijn digitale werktuigen vanwege de niet gemakkelijk te voorspellen effecten van het gebruik ervan op de mens zelf en op zijn samenleving. Hij vreest dat digitalisering de mens oppervlakkiger en grofkorreliger maakt.[4] En hij vraagt zich af of de samenleving er belangrijke, betekenisvolle waarden als privacy, vrijheid en zelfbeschikking voor inlevert.[5]

Het zijn onderwerpen waardoor 'digitalisering', 'internet' en 'homo digitalis' als eenduidige fenomenen worden behandeld. Het gevaar daarvan is dat we kunnen vervallen in een technologisch determinisme waarin de mens slaaf is van de technische ontwikkelingen. Als we – zo wordt vanuit dat perspectief gezegd – voortdurend in de weer zijn met Google, Amazon en Facebook en als die platforms onze keuzen richting geven op grond van wat we eerder deden, zullen we niet meer veranderen, onszelf niet meer verrassen en geen nieuwe wegen inslaan. Het is een benadering die de gemiddelde jurist niet aanspreekt. Die gaat er doorgaans vanuit dat de mens de techniek naar eigen voorkeur inzet. Volgens dit instrumentalisme bepaalt de mens zelf in hoeverre de techniek zijn leefwereld binnendringt. Terwijl in de technologisch-deterministische visie ethische en rechtsstatelijke vragen dreigen onder te sneeuwen, gaat de instrumentalistische techniekopvatting eraan voorbij dat heel wat technische uitwerkingen onverwachte en niet-bedoelde effecten in het leven roepen. De hoogleraar computerveiligheid Bart Jacobs die deze tegenstelling scherp heeft neergezet noemt als voorbeeld dat wel te voorzien was dat de mobiele telefoon tot groter gemak en snelheid van communicatie zou leiden, maar niet dat het mobieltje andere communicatiepatronen, een ander straatbeeld en een andere beleving van treinreizen zou meebrengen.[6] Digitale ontwikkelingen kunnen niet langer met de naïviteit van de determinist of de instrumentalist worden bezien, maar vergen een zorgvuldige analyse van enerzijds de ontwikkelingen die daadwerkelijk plaatsvinden en anderzijds de waarden die op het spel staan. De preadvie-

zen geven blijk van het besef dat digitalisering gevolgen heeft voor de reële werkelijkheid en dat juristen een taak hebben bij te dragen aan het tegengaan en het beheersen van ongewenste gevolgen van de digitalisering voor de vrijheid van mens en samenleving. Het is blijkens een recent WRR-rapport een actueel thema.[7]

De hoofdlijn van het preadvies

In het preadvies van Mireille Hildebrandt gaat het om de implicaties voor het strafrecht van de (automatische) bewerking van gegevens door data-gestuurde intelligente systemen. Onder deze systemen – *agents* – verstaat de preadviseur diverse fenomenen. Ze noemt als voorbeelden zoekmachines, drones, zorgrobotten, computervirussen, maar ook slimme energienetwerken (smart grids), en zelfs een systeem van slimme sensoren (camera's en microfoons) in een smart city zoals het 'Living lab Stratumseind' in Eindhoven dat detecteert of bezoekers van een uitgaansgebied op het punt staan geweld te gebruiken.[8] Het gaat haar kennelijk niet om het gebruik van *agents* om voortdurend geactualiseerde inzichten op geaggregeerd niveau te krijgen – waarop beleid kan worden gemaakt – maar om *agents* die verbanden en patronen leggen welke zich uiteindelijk vertalen in op individuen gerichte toepassingen.

Het bijzondere van deze *agents* is dat ze niet alleen informatie verwerken en gedrag voorspellen, maar dat ze beslissingen nemen en uitvoeren. En juist dan kunnen de ongewenste effecten ontstaan. Een simpel voorbeeld is de OV-chipkaart die het mogelijk maakt op een treinperron te komen – zoals op Amsterdam Zuid. De elders in het systeem met voldoende saldo digitaal geladen kaart maakt een fysieke beweging mogelijk. Je kunt die chipkaart natuurlijk zien als een digitale sleutel, maar je kunt hem ook opvatten als deel van een zelfbeslissend systeem – een systeem dat kwetsbaar is en kan falen. Omdat de leefwereld aldus niet meer helder is opgedeeld in online en offline introduceert Hildebrandt het woord 'onlife wereld'.

Materieel strafrecht

Naar huidig recht kunnen *agents* niet worden aangemerkt als rechtssubject, al kunnen ze wel leren hun gedrag te veranderen en zelfstandig in te grijpen. Zo kan een zorgrobot eenvoudige huishoudelijke taken doen. Wat nu als de zorgrobot een kop gloeiend hete thee aan een demente bejaarde geeft die zich daardoor lelijk verbrandt? Kan het gedrag van de robot gelden als handeling van een rechtssubject? Kan de schuld aan de fabrikant of de gebruiker (bijvoorbeeld een zorginstelling) worden toegerekend? Hildebrandt laat het antwoord op deze vragen in het midden en kiest voor de pragmatische oplossing om in lijn met het verkeersstrafrecht een nieuw artikel in te voeren waarin wordt bestraft 'een ieder die zich bedient van *agents* die zich zodanig gedragen dat gevaar voor personen, goederen of diensten wordt veroorzaakt of kan worden veroorzaakt of die zich zodanig gedragen dat het maatschappelijk verkeer wordt gehinderd of kan worden gehinderd'. Het lijkt mij gelet op de ruime betekenis van het woord agent een al te onbepaalde omschrijving,

Urgenter is de aandacht die de preadviseur vraagt voor de mogelijkheden van een nieuwe vorm van anticiperend straffen

omdat mijns inziens niet voorzienbaar is welk computersysteem het maatschappelijk verkeer kan hinderen en ik ook daarom tenminste opzettelijk of culpoos gevaar veroorzaken zou verlangen. Juist bij lerende *agents* zal degene die zich van de agent bedient, zich immers verweren met de stelling dat de leverancier een beter lerende agent had beloofd en hij niet wist dat gebruik van de agent zo gevaarlijk zou zijn. Maar dat is een kwestie van uitwerking: het idee dat hier materieel-strafrechtelijke vragen liggen overtuigt mij wel, al lijkt het erop dat de praktijk ook in het bestaande recht aanknopingspunten vindt.[9]

Urgenter is de aandacht die de preadviseur vraagt voor de mogelijkheden van een nieuwe vorm van anticiperend straffen. *Agents* opereren op basis van meetbare en doorrekenbare analyses van (objectief) gedrag. Maar 'The map is not the territory', oftewel een abstractie die ergens van is afgeleid is niet het ding zelf.[10] En de door

Auteur

1. Prof. mr. Y. Buruma is raadsheer in de Hoge Raad, als CPO-hoogleraar 'Rechtsstaat, rechtsvorming en democratie' verbonden aan het Centrum voor Postacademisch Juridisch Onderwijs, Radboud Universiteit en redacteur van dit blad.

Noten

2. De preadviseurs Zwenne & Schmidt geven een voorzichtige definitie: 'Een homo digitalis is een homo sapiens (mens) die zich in meer of mindere mate laat vertegenwoordigen of laat leiden door een of meer gedigitaliseerde processen, en die dus leeft en moet leven en overleven in een wereld of omgeving die dat mogelijk maakt', (p. 312) en ze gaan uitgebreid op de term in (p. 366-373).

3. H. Arendt, *The Human Condition,* University of Chicago Press, 1958, p. 305-306.

4. N. Carr, *What the Internet is Doing to Our Brains,* Norton, 2010.

5. E. Morozov, *The Net Delusion. The Dark Side of Internet Freedom,* Public Affairs, 2011; E. Morozov, *To Save Everything, Click Here*, Allen Lane, 2013.

6. B. Jacobs, 'Voorwoord', in: M. Becker, *Ethiek van de digitale media,* Amsterdam: Boom 2015.

7. E. Hirsch Ballin, E. Schrijvers, D. Broeders, *Big Data in een vrije en veilige samenleving,* WRR-rapport nr. 95, Den Haag 2016.

8. Daarmee wijkt ze af van de wijze waarop bijvoorbeeld W.I. Koelewijn, *Privacy en politiegegevens. Over geautomatiseerde normatieve informatie-uitwisseling*, Leiden University Press, 2009 spreekt over softwareagents. De agents van de preadviseur lijkt Koelewijn aan te duiden als Multi Agent Systems, maar ook hij gaat uit van agenten die zonder onderbreking en autonoom handelen waarbij ze reageren op veranderingen in de omgeving, communiceren met andere agenten (en mensen) en het vermogen hebben om te leren.

9. Vergelijk Hof Den Haag 16 december 2015, ECLI:NL:GDHA:2015:3466 over het laten vliegen van een drone/quadcopter door een journalist waarbij toepassing wordt gegeven aan de Wet luchtvaart, het Luchtverkeersreglement en de Regeling modelvliegen.

10. De uitspraak is van Alfred Korzybski, aangehaald in P.A.M.G. de Kock, *Anticipating Criminal Behaviour,* Wolf, 2014, p. 123-128, maar het is een soundbite die de opvattingen van preadviseur vast correct weergeeft.

een agent geschapen homo digitalis – in de zin van digitaal gevormd beeld van de mens – is niet de mens zelf. Als mensen in het strafrecht ter verantwoording worden geroepen voor hun handelen krijgen ze in het kader van het hoor en wederhoor altijd de gelegenheid een volledig beeld van zichzelf te presenteren. Dat verschil is van belang. De preadviseur schrijft puntig: 'De idee dat mensen strafrechtelijk aansprakelijk zouden worden gesteld voor het feit dat hun gedrag correleert met een neiging tot geweldpleging, tot pedofilie, tot fraude met belastingen of sociale zekerheid of tot fundamentalistisch radicalisme lijkt – misschien – absurd. Tegelijkertijd worden systemen ontwikkeld waarmee dergelijke neigingen kunnen worden berekend. Het is verstandig, zo niet pertinent, om al in dit stadium te bedenken hoe wij de architectuur van de onlife wereld zo in kunnen richten dat dit soort machinale toerekening kan worden voorkomen.' Met reden spreekt ze van 'La Defense Sociale revisited'. De kans op bestraffing (louter) op deze gronden is, dunkt me, nu nog beperkt (al is er door de strafbaarheid van voorbereidingshandelingen heel veel mogelijk). Maar de kans dat na een gepleegd feit specifieke maatregelen (bijzondere voorwaarden e.d.) worden opgelegd op grond van *police intelligence* en profilering is inderdaad niet ondenkbaar.[11]

Strafprocesrecht

In de paragraaf over het formele strafrecht ligt het zwaartepunt van het preadvies. Hildebrandt wijst erop dat in het project 'Modernisering van het Wetboek van Strafvordering' de nadruk van de strafvordering nog verder dan al het geval is verschuift naar het voorbereidend onderzoek. De auteur heeft daar fundamentele bedenkingen bij. Zeker in het kader van de antiterrorismewetgeving wordt volgens haar onomwonden gesproken van de preventieve werking van dwangmiddelen en andere onderzoeksbevoegdheden. Zo worden volgens de auteur de rechter en alle waarborgen waar die voor staat in vergaande mate buiten spel gezet.

Het zijn misschien wel erg grote woorden, maar dat er een verschuiving naar het vooronderzoek plaatsvindt is ontegenzeggelijk het geval en dat onderstreept inderdaad de urgentie van het nadenken over de ontwikkeling van gedragvoorspellende en -beïnvloedende *agents.* Het is evenwel kennelijk moeilijk scherp zicht te krijgen op wat er feitelijk gebeurt. De preadviseur vermeldt het iColumbo platform dat is gebouwd met als doel het analyseren van 'open en big data' ten einde inzicht te verkrijgen in specifieke criminaliteitspatronen dan wel het monitoren en profileren van een specifiek persoon of een specifieke groep personen in verband met gepleegde of mogelijk te plegen strafbare feiten.[12] Verder haalt ze een TNO-rapport uit 2010 aan, maar de feiten blijven wat schimmig. Toch durft ze de conclusie aan dat het gebruik van *agents* op dit moment nog niet aan de orde is binnen de opsporing.[13] Maar '(h)et punt is dat alles erop wijst dat het binnenkort wel aan de orde is'.

Op deze feitelijk ietwat wankele bodem waagt de preadviseur zich aan een bespreking van de impact van politie-*agents* op relevante grondrechten onder de krachtige noemer 'aantasting van grondrechten'. Het eerste onderwerp betreft de gevolgen van de inzet van *agents* op de reikwijdte van de onschuldpresumptie. Volgens de onschuldpresumptie berust de bewijslast voor de vaststelling van schuld op de vervolgende instantie. Een bewijslastverschuiving moet – zo schrijft de concept-Richtlijn Onschuldpresumptie (COM (2013) 821 final) voor – te rechtvaardigen en weerlegbaar zijn. Dat uitgangspunt komt onder druk als de *agents* op basis van 'big en open data' (zoals te verkrijgen via Facebook) categorieën personen detecteren die een grote kans maken een specifiek

Is de opname in zo'n vergelijkingsbestand te rechtvaardigen en is de vergelijking en de daarop gebaseerde extra controle te rechtvaardigen?

type strafbare feiten te zullen plegen, pogen, voorbereiden of beramen. Hildebrandt gaat specifiek in op als gevolg van de inzet van *agents* gerezen verdenkingen of gesuggereerde controles. Ze haalt het voorbeeld aan van een geval waarin met automatische nummerplaatherkenning (ANPR) kentekens van passerende personenauto's werden gescand en vergeleken met een vergelijkingsbestand waarin de politie kentekens had verzameld wegens eerdere betrokkenheid bij druggerelateerde criminaliteit. Los van de lastige kwesties van détournement de pouvoir (in welk kader de preadviseur de zaak bespreekt) en privacy (in het bijzonder doelbinding) is deze zaak illustratief voor de vraag hoever we gaan met het controleren van mensen die volgens de bestanden eerder betrokken waren bij een vorm van criminaliteit. Is de opname in zo'n vergelijkingsbestand te rechtvaardigen en is de vergelijking en de daarop gebaseerde extra controle te rechtvaardigen? Ik kom op dit niet alleen voor de preadviseur belangrijke punt terug.

Het tweede onderwerp dat in het kader van aantasting van grondrechten wordt besproken is de brede categorie van gegevensbescherming, privacy, non-discriminatie en vrijheid van informatie. De auteur houdt het beperkt omdat het haar gaat om de rol van de *agents* in plaats van gegevensbescherming an sich en de afweging tussen het fundamentele recht op privacy en het belang van de opsporing al herhaaldelijk goed is beschreven. Die *agents* vergen dat de eis van voorzienbaarheid opnieuw moet worden doordacht. Daarbij denkt ze in de eerste plaats aan het 'grondrecht op non-discriminatie'. Het profileren van mogelijk betrokkenen bij eventueel nog te plegen strafbare feiten leidt volgens de preadviseur gemakkelijk tot het categoriseren van groepen van personen die zouden neigen tot strafbaar gedrag. Dankzij slimme *agents* kun je datapunten vinden die redelijk betrouwbaar correleren met gegevens die (op grond van artikel 5 Wpg) niet zelf zijn opgeslagen maar die indirect uitnodigen te discrimineren op ras, geloof, seksueel leven, enz. De preadviseur signaleert het bestaan van specifieke technieken, zoals 'discrimination awareness data mining'. Daarmee

Het orakel © Carol and Mike Werner / Alamy Stock Photo

zou worden tegemoetgekomen aan de eis om te ondervangen dat niet te lichtvaardig als resultaat van de inzet van de agent wordt aanvaard dat potentiële daders gezocht moeten worden in kringen die worden gedefinieerd door hun ras, geloof of seksueel leven. Ze neemt dan ook 'een diametraal tegenovergestelde positie' in ten opzichte van die van Moerel & Prins die menen dat het speciale regiem voor bijzondere persoonsgegevens niet meer nodig is. Bespeuren we in die tegengestelde posities de echo van de technische determinist (het is niet realistisch om te denken dat etnische afkomst niet uit de data naar voren komt) versus de instrumentalist (maar we kunnen oplossingen zoeken zolang we het doel van nondiscriminatie voortdurend en scherp voor ogen houden)?

Tot slot vraagt Hildebrandt aandacht voor legaliteit en détournement de pouvoir. In dat verband gaat ze in op het doelbindingsbeginsel en ook hier gaat ze het debat aan met Moerel & Prins. Deze andere preadviseurs stellen voor dit beginsel af te schaffen omdat het achterhaald is ('gegevensverwerking en -analyse zijn zelf het doel') en ineffectief (mensen geven met een muisklik blind toestemming voor van alles) en te vervangen ware door het criterium van het gerechtvaardigde belang van het datasubject. Hildebrandt vindt dat – net als ik – een verfrissend voorstel, maar zij is niet overtuigd. Ze voert aan dat het niet duidelijk is waarom het weglaten van de eis van doelbinding bedrijven ertoe zou verleiden zich nu ineens wel iets aan te trekken van de rechten en belangen van het datasubject en dat er zo onduidelijkheid ontstaat voor de datacontroller die het belangcriterium per geval moet toepassen. Zelf heb ik er weinig tegen om meer verantwoordelijkheid bij de fabrikanten en de datacontrollers te leggen – in plaats van bij de dataconsumenten – maar Hildebrandts reactie roept wel de vraag op of bij de analyse in Big Data ten behoeve van politiedoeleinden de op het spel staande 'gerechtvaardigde belangen' niet logischerwijs scherper moeten worden geformuleerd (met speciaal regime en met doelbinding) dan in het gewone dataverkeer. Beantwoording van die vraag vergt overigens wel – zoals Hildebrandt aangeeft – dat men oog heeft voor de gestage uitbreiding van publiek-private samenwerking en de komst van het Internet van de Dingen. Gegevensverwerking in de private sector wordt een schatkamer voor overheden die in het kader van de strafvordering werken aan het verbeteren van hun informatiepositie. Hildebrandt houdt dus vast aan het belang van

11. Vergelijk bijv. HR 12 juli 2011, ECLI:NL:HR:2011:BQ4676 (Behandelprogramma Seks en Grenzen).

12. Daarover S. Brinkhoff, 'Big datamining door de politie', *NJB* 2016/994, afl. 20, p. 1400-1407.

13. Tot een vergelijkbare conclusie komt het WRR-rapport dat nog noemt de Infobox Crimineel en Onverklaard Vermogen en de innovatieve technieken waarmee de Inspectie SZW met het oog op fraude risicovolle bedrijven selecteert.

doelbinding en bespreekt in het perspectief daarvan de détournement de pouvoir. Vanwege het ingrijpende karakter van dwangmiddelen en heimelijke bevoegdheden moeten burgers een goed beeld hebben van de gevallen waarin zij daaraan mogen worden onderworpen. Daarom wijst ze een 'creatieve omgang' met bevoegdheden door de opsporing in ronde bewoordingen af. Dat is een pleitbaar standpunt, waarvoor overigens weinig aanknopingspunten in de strafrechtelijke jurisprudentie bestaan.[14]

Naar een veilig strafrecht in een data-gestuurde samenleving

In haar conclusie wijst Hildebrandt erop dat allerhande vormen van monitoring en ander onderzoek, al dan niet gebaseerd op data-gestuurde risicoanalyses, de rechter niet zullen bereiken en dus door anderen getoetst moeten worden. Vandaar haar pleidooi in het eerste vraagpunt om een wettelijke bepaling op te nemen die het ontwerp en de inrichting van data-gestuurde systemen normeert en dat in het tweede vraagpunt om een toezichthouder in te stellen die de werking van die data-

Gegevensverwerking in de private sector wordt een schatkamer voor overheden die in het kader van de strafvordering werken aan het verbeteren van hun informatiepositie

gestuurde systemen – eventueel, zoals de Commissie van Toezicht voor de Inlichtingen- en Veiligheidsdiensten (CTIVD) al heeft gesuggereerd, geautomatiseerd – controleert. Hildebrandt wijst er in dat verband terecht op dat het belangrijk is dat juridische bescherming wordt gearticuleerd in de technische systemen die we gebruiken – de bescherming moet zo diep mogelijk in de architectuur, het ontwerp, de technische inrichting en de default instellingen worden ingebouwd. Een voorbeeld is de in de Europese Algemene Verordening Gegevensbescherming (Vo (EU) 2016/679) neergelegde plicht om bij de inzet van technologie die het risico op schending van gegevensbescherming verhoogt een 'data protection assessment' uit te voeren. Voor het strafrecht zou als opmaat naar juridische bescherming by design een 'presumption of innocence-assessment' kunnen worden ingevoerd. Ze concludeert: 'Data-gestuurde intelligentie is veelbelovend maar geen panacee, en er zijn kosten verbonden aan de uitholling van de onschuldpresumptie, aan de kans dat verfijnde onzichtbare discriminatie de regel wordt in plaats van de uitzondering en aan de permanente invasie van ons privéleven.'

Waardering en kritiek

Mireille Hildebrandt heeft duidelijke opvattingen over het recht en kennelijk verstand van zaken over de digitale wereld. Ze daagt uit en verveelt niet met technische uiteenzettingen of met juridische betogen over de brij van regelgeving met betrekking tot gegevens. Het is een bewonderenswaardig preadvies over een voor velen weinig vertrouwde materie. Het is evenwel ook een lastig preadvies omdat de preadviseur de abstractie niet schuwt en niet altijd even scherp redeneert. Dat doet aan mijn waardering voor de gereleveerde inzichten echter niet af.

Ik wil in mijn reflectie op het preadvies ingaan op de vraag of een iets verdergaande feitelijke precisering niet had geholpen om nog wat nadere nuances aan te brengen en ik ga nader in op de aan de NJV voorgelegde vragen.

De feiten

In 2006 las ik voor het eerst over 'Agenten voor agenten'.[15] Dat betekent dat tien jaar geleden al sprake was van de hier besproken technieken. Toch lijkt de kennelijke opvatting van Hildebrandt dat innovatieve digitale informatietechnieken in de opsporing nog weinig toepassing vinden wel juist.[16] Dat roept de vraag op hoe dat komt. De WRR wijst op het geheime en experimentele karakter van dergelijke toepassingen, maar daar is wel wat meer over te zeggen. Ik doe dat door me wat nader te verdiepen in de vraag wat voor kennis dergelijke *agents* kunnen genereren.

In de VS is er veel aandacht voor 'predictive policing software'. Onder meer de korpsen van Los Angeles en Atlanta gebruiken dergelijke software van het bedrijf PredPol die statistische analyses maakt van gegevens over vermogensdelicten (inbraak, autodiefstal), waaruit de gebleken – steeds geactualiseerde – historische verdeling en frequenties worden weergegeven op stedelijke kaarten in blokjes van nog geen 50 m2. Op grond daarvan intensiveert de politie daar op bepaalde – door de berekeningen aangedragen – tijdstippen het toezicht.[17] Een ander voorbeeld. In onze steden hangen steeds meer camera's. Blijkens een studie van TNO bestaan er intelligente sensornetwerken die bepaalde gebeurtenissen en incidenten begrijpen, ook al kijkt er niet een mens naar de opnames. Het kan dan gaan om algemeen afwijkend gedrag, gedrag dat afwijkt vanwege de locatie (schreeuwen in een voetbalstadion is anders dan op Schiphol) en zeer specifiek afwijkend gedrag (lang op een plaats rondhangen op Schiphol).[18] Het gaat in beide voorbeelden dus niet om voorspellingen over mensen, maar over gebeurtenissen respectievelijk aan anonieme mensen gerelateerde gebeurtenissen. Het wordt persoonlijker als we denken aan het werk van de Financial Intelligence Unit Nederland. De FIU onderwerpt door de banken e.d. aangeleverde meldingen van ongebruikelijke transacties aan diverse analyse- en onderzoeksprocessen. Alle gemelde transacties worden gemonitord aan de hand van gerichte query's en wekelijkse matches met de Verwijzingsindex Recherche Onderzoeken en Subjecten, waarin zijn opgenomen personen die voorkomen in lopende opsporingsonderzoeken of die om intelligenceredenen in verhoogde belangstelling van opsporingsdiensten staan. Aldus kunnen ongebruikelijke transacties worden opgewaardeerd naar verdachte transacties. In hoeverre hier nu smart *agents* worden gebruikt is eigenlijk niet zo relevant: dankzij digitale bewerkingen van grote bestanden wordt de aandacht op concrete homines digitales gericht. En dan zijn er nog de

De politie is zich onvoldoende bewust van de waarde van de (rest-) informatie die door haar eigen handelen is verkregen maar die niet onmiddellijk bruikbaar is voor het eigen onderhanden onderzoek

zogenaamde sociale netwerkanalyses waarbij de relaties tussen verdachten en anderen met mathematische technieken in kaart worden gebracht door onderzoek in gesloten bronnen (tapverslagen, telecomgegevens, getuigenverklaringen) en open bronnen (social media). Ook hiermee komen individuen in beeld die aanvankelijk 'slechts' als familielid, geliefde of kennis werden aangeduid.[19]

Een en ander suggereert dat de gevallen waarin algoritmes uitwijzen tegen wie preëmptieve actie moet worden ondernomen niet de enige vorm van het gebruik van *agents* door de politie zijn. Maar er is ook een verklaring waarom dat gebruik voorlopig minder talrijk is dan je op grond van andere toepassingen van smart *agents* zou verwachten. Terwijl bol.com, credit card maatschappijen en datingsites aardig in staat zijn ons goed in te schatten zijn er drie kritische punten die het voor de politie moeilijk maken dezelfde technieken ook toe te passen. Data-mining – met smart *agents* – werkt het best als je op zoek bent naar een precies gedefinieerd profiel, er veel regelmatig ververste – ook ogenschijnlijk irrelevante – gegevens in de te onderzoeken bestanden zijn en de kosten van vals alarm laag zijn.[20]

Mijn precieze uitgavenprofiel is bij de credit cardmaatschappij bekend en het is voor een smart *agent* niet een al te complexe opgave om te zien wanneer ik gedrag vertoon dat niet in mijn gedragspatroon past. Zo'n precies profiel van de onbekende individuele bankrover of terrorist bestaat niet. We kunnen wantrouwig worden als iemand zijn mobieltje uitzet of tijdens een reis naar Pakistan geen credit cards gebruikt, en zouden deze kenmerken daarom als aan te leren zoekgedrag in de Big Data aan smart *agents* kunnen meegeven. Maar dat zijn geen kenmerken van alle bankrovers en terroristen en evenmin kenmerken die alleen bankrovers en terroristen hebben. Profilering op dit soort kenmerken levert een te grote groep op. Omdat de politie niet – zoals marketeers en credit cardmaatschappijen – kan zoeken op individuele voorkeuren of afwijkingen van individuele patronen gebaseerd op individuele histories in vergelijking met grote groepen, maar op individuele voorkeuren of afwijkingen van algemeen veel voorkomende patronen louter gebaseerd op die vergelijking, is de precisie van de uitkomst onvoldoende. Dat wil zeggen dat de kans op een fout-positieve uitkomst van data-mining – het achteraf onterecht gebleken vermoeden dat iemand bankrover of terrorist is – groter is dan bij de klant van de credit card maatschappij. Overigens blijken bestanden die vanwege de ernst van de zaak toch worden aangelegd weinig bruikbaar te zijn voor individu-gerichte predictive policing. Zo werden alleen al in 2013 in de VS 468 749 mensen voorgedragen voor de watch-list van de National Counterterrorism Center. Slechts 1% van de voordrachten werd verworpen.[21] De Boston Marathon aanslag van 2013 is echter niet voorkomen, hoewel een van de daders op de terroristenlijst stond en zij beiden te veel hadden gekletst op de sociale media: de gegevens waren bekend maar niemand had ze opgemerkt.

De tweede factor waarom we weinig over predictive policing horen is dat de politie natuurlijk wel beschikt over gegevensbestanden maar dat deze tot nu toe niet zo zijn samengesteld en gestructureerd (gecategoriseerd) dat *agents* in staat zijn relevante en toepasbare patronen te leggen: psychiatrische, psychologische en sociale kenmerken zijn soms wel bekend maar worden elders opgeslagen. Sterker nog: de politie is zich onvoldoende bewust van de waarde van de (rest-)informatie die door haar eigen handelen is verkregen maar die niet onmiddellijk bruikbaar is voor het eigen onderhanden onderzoek.[22] Het proefschrift van Peter de Kock waarin verslag wordt gedaan van data-mining met behulp van scenario's in grote verzamelingen van bestanden met gegevens over terroristische aanslagen is overigens een voorbeeld dat dergelijke verzamelingen van bestanden wel zijn aan te leggen en nuttige gegevens kunnen opleveren met het oog op toekomstige gebeurtenissen.[23]

Ten slotte is een verkeerde inschatting van de credit cardmaatschappij – net als het geval waarin de politie ten onrechte naar een hot spot gaat – minder erg dan een verkeerde inschatting die leidt tot het ten onrechte binnenvallen van een huis. Hoe erg men dat laatste vindt, hangt van de omstandigheden af. In landen waar men wat minder op heeft met de rechten van onschuldige burgers

14. Zie bijv. HR 22 september 2015, ECLI:NL:HR:2015:2775.

15. W.I. Koelewijn & H.H. Kielman, 'Agenten voor agenten', in W. Huismans, L.M. Moerings, G. Suurmond (red.), *Veiligheid en recht*, Boom, 2006, p. 231-253.

16. S. Hulsman, M. Princen, P. Klerks & N. Kop, *Handelen naar waarheid. Sterkte- en zwakteanalyse van de opsporing,* Amsterdam, 6 mei 2016, noemen nog 'de Raffinaderij', een business intelligence-voorziening die bij liquidaties en terrorismezaken wordt gebruikt, maar ondersteunen verder wel het beeld.

17. Zie www.predpol.com. Een van de weinige onafhankelijke onderzoeken – van de RAND Corporation: P. Hunt, J. Saunders, J.S. Hollywood, *Evaluation of the Shreveport Predictive Policing Experiment,* www.rand.org/pubs/research_reports/RR531.html – wees uit dat er geen statistisch significante afname van vermogenscriminaliteit was, maar dat politieambtenaren er wel veel voordelen in zien vermoedelijk omdat de politie wel efficiënter zijn tijd besteedde.

18. J. Dijk e.a., 'Intelligent Sensor Networks for surveillance', *Cahiers Politiestudies* 2011-3, nr. 20, p. 109-125.

19. P. Duijn & P. Klerks, 'De brug tussen wetenschap en opsporingspraktijk', *Tijdschrift voor Criminologie* 2014 (56) 4, p. 39-70.

20. B. Schneier, *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World,* London: Norton 2015, p. 136-137.

21. De court filing van 28 maart 2014 (in de zaak *Gulet Mohamed vs. Holder*) waarop deze cijfers zijn gebaseerd is gepubliceerd door J. Scahill & R. Devereaux, 'Blacklisted', *The Intercept* 23 juli 2014.

22. Laatstelijk Hulsman e.a., 2016, p. 60.

23. P.A.M.G. de Kock, *Anticipating Criminal Behaviour*, Wolf, 2014.

is dit minder een belemmering. Maar ook een rechtsstaat kan uit angst voor oorlog of terrorisme tot andere afwegingen komen. Niettemin verklaart ook deze derde factor waarom we nog niet zo veel van individu-gerichte predictive policing door slimme *agents* horen.

De vraagpunten

Dit laatste brengt me bij de normatieve vragen die het preadvies opwerpt en de vragen die aan de vergadering van de NJV worden voorgelegd.

Het eerste vraagpunt stelt aan de orde dat in het nieuwe Wetboek van Strafvordering een bepaling moet worden opgenomen die het ontwerp en de inrichting van data-gestuurde systemen normeert. Daarover het volgende. Het wettelijk regelen van opsporingsactiviteiten waardoor niet rechtstreeks en onweerlegbaar inbreuk op individuele mensenrechten wordt gemaakt is mijns inziens niet noodzakelijk, tenzij er (politiek-bestuurlijke) institutionele redenen zijn om nadere regels te stellen. Het verbod op doorlating van drugs en personen die voorwerp zijn van mensensmokkel is een voorbeeld van dit laatste. Dat verbod is niet ingegeven door de rechten – laat staan de fundamentele rechten – van de verdachte, maar door diverse maatschappelijke redenen (de kans dat de drugs toch op de markt komen, de rechten van de gesmokkelde illegalen, het gevaar van corruptie bij politie en douane). Daarom is het (bij amendement) in de wet opgenomen en ontstaat er politiek-bestuurlijk gedoe als het in strijd met de wet toch gebeurt. Maar in het strafproces tegen de verdachte heeft het verbod nauwelijks betekenis.

Welnu, het gebruik van *agents* zonder meer lijkt mij niet in strijd met enig fundamenteel recht en in zoverre is er geen grondwettelijke of verdragsrechtelijke plicht tot wetgeving. Ik kan ook geen institutionele redenen verzinnen voor wettelijke regeling van het gebruik van *agents* als gevolg waarvan algemeen beleid wordt geadviseerd of waarmee bepaalde hot spots worden aangewezen.

Dat is misschien anders bij het gebruik van *agents* die tot de identificatie van (groepen) personen leidt. Het lijkt mij politiek-bestuurlijk belangrijk om een technische waarborg – bijvoorbeeld een impact assessment – in te bouwen waardoor vormen van verborgen discriminatie door de *agents* actief worden tegengegaan. De vraag is dan of (aanpassing van) de Wet politiegegevens een afdoende basis is. Dat is een wet waarvan de naleving een politiek-bestuurlijke eis is die door de Autoriteit Persoonsgegevens kan worden gecontroleerd maar waarvan overtreding in het strafproces tegen een individuele verdachte niet zonder meer gevolgen zal hebben.[24]

Als de *agents* concrete individuen aanwijzen, biedt de mensenrechtelijke invalshoek vooral vanwege de mogelijke gevolgen voor de onschuldpresumptie wellicht toch wel reden om in het Wetboek van Strafvordering specifieke wetgeving op te nemen. Ik denk daarbij – anders dan de preadviseur – niet het eerst aan de gevallen waarin de inzet van smart *agents* startinformatie oplevert doordat de politie ertoe wordt bewogen nadere controles uit te voeren. Mijns inziens is op door smart *agents* ontdekte gronden gebaseerde controle te prefereren boven controle gebaseerd op ongereflecteerde vooroordelen: uit Amerikaans onderzoek bleek ook dat firma's die *online* background checks doen bij sollicitaties met 8.4% meer waarschijnlijkheid zwarte sollicitanten aannemen dan firma's die dan niet doen.[25] Bovendien staat controle niet gelijk aan schuldig verklaring en is het nadeel – mits de controle niet disproportioneel wordt uitgevoerd – beperkt.

Wat voor mij de doorslag geeft om automatische data-analyses die geïndividualiseerde personen aanwijzen wel wettelijk te regelen in het Wetboek van Strafvordering, is dat het Wetboek van Strafrecht door de – soms de 'overinclusiveness rakende' – vormgeving van strafbaarheid (zoals bij voorbereidingshandelingen, witwassen en terrorismebestrijding) van de rechter een zware verantwoordelijkheid eist om vast te blijven houden aan de onschuldpresumptie. Of uit de feiten het vereiste voornemen kan worden afgeleid, of de omkering van de bewijslast van de wetenschap van criminele herkomst van geld niet te overtrokken is en of opgewonden meningsuitingen als bijdragen aan een terroristische organisatie hebben te gelden zijn vragen die de rechter serieus onder ogen moet blijven zien. De omstandigheid dat de computer iemand als potentiële voorbereider, witwasser of terrorist neerzet kan bij de beantwoording van die vragen een rol spelen – terwijl het maar de vraag is of de computer dat niet te gemakkelijk heeft aangenomen. Opname op zo'n lijst zou de effectieve betekenis van de onschuldpresumptie – en daarmee de eerlijkheid van het proces – kunnen beïnvloeden. Daarom zal ik – ondanks mijn bemerkingen – voor het vraagpunt stemmen.

Opname op zo'n lijst zou de effectieve betekenis van de onschuldpresumptie – en daarmee de eerlijkheid van het proces – kunnen beïnvloeden

Het tweede vraagpunt stelt aan de orde of het noodzakelijk is een toezichthouder in te stellen. Die gedachte spreekt aan in het licht van het voorgaande en ik zal ook voor dit vraagpunt stemmen. Laat ik nog een extra argument noemen. Hildebrandt wijst er terecht op dat de 'informationele zelfbeschikking' niet zover gaat dat het recht om gegevens te verwerken exclusief zou toekomen aan het datasubject. Maar er zijn grenzen. Het recht op vergetelheid is zo'n grens – in die zin dat opgeslagen gegevens in bepaalde gevallen niet meer ter beschikking mogen worden gesteld van het grote publiek.[26] En hoewel dat recht in de wereld van het strafrecht wellicht wat anders werkt, moet het nationale recht ervoor zorgen dat opgeslagen persoonlijke data daadwerkelijk en effectief worden beschermd tegen misbruik en fouten.[27] Dat geldt natuurlijk ook voor door *agents* geschapen beelden die zelf weer worden opgeslagen. Dat effectieve remedies dienaangaande op dit moment mogelijk zijn, lijkt niet het

geval. Een toezichthouder zou zich ook daarom moeten buigen over de kwaliteitseisen die te stellen zijn aan een door een smart *agent* te vormen beeld van de individuele 'criminele homo digitalis'.

De preadviseur laat in het midden wie de toezichthouder moet zijn. Natuurlijk kan dan worden gedacht aan de Autoriteit Persoonsgegevens,[28] maar ik heb zelf een voorkeur voor het in het leven roepen van een Commissie van Toezicht voor de Politie met taken en bevoegdheden die vergelijkbaar zijn met die van de Commissie van Toezicht voor de Inlichtingen- en Veiligheidsdiensten. Het voordeel daarvan is dat die commissie dan ook achteraf onderzoek zou kunnen gaan doen naar (andere) inbreuken op de privacy door de politie (taps, hacken, stelselmatig controleren e.d.) en/of andere heimelijke bevoegdheden. Die commissie zal de toepassing van deze (in beginsel inbreuk makende) bevoegdheden in de praktijk beoordelen waarbij ook het voorkomen van onrechtmatige toepassingen aan het licht kan komen. Daarbij kan de commissie juist het oog hebben op structureel relevante toepassingen, zoals bijvoorbeeld het effect van sluipende discriminatie. Dat is van belang als we denken aan de al eerder gesignaleerde terughoudendheid in de rechtspraak van de Hoge Raad met betrekking tot het verbinden van gevolgen aan vormverzuimen die niet onmiddellijk de eerlijkheid van het proces raken.[29] De commissie zal kunnen beoordelen of digitale vergelijkingen (vanwege het doelbindingsbeginsel, of vanwege de niet-noodzakelijkheid van de lijstvorming) of nog zelfstandiger optreden van smart *agents* in databestanden onrechtmatig zijn en of de betreffende methode structureel voorkomt. Wellicht – maar dat is een lastig onderwerp waarover de toekomst nog in nevelen is gehuld – zou zo'n vaststelling onder omstandigheden zelfs in individuele gevallen bij het oordeel van de strafrechter in een concreet geval kunnen worden betrokken.

Slot

Het preadvies van Mireille Hildebrandt betreft een urgent en belangrijk onderwerp. De visionaire aanpak ervan zet aan tot denken. Ze doet beseffen dat datagestuurde intelligentie in het strafrecht gevolgen zal moeten hebben. De bal ligt nu bij de wetgever, de politiepraktijk en de rechtspraak. •

24. HR 19 februari 2013, ECLI:NL:HR:2013:5321 (*Examenarrest*), *NJ* 2013/308; HR 3 juli 2012, ECLI:NL:HR:2012:BV1800 (*ANPR*); HR 7 juli 20109, ECLI:NL:HR:2009:BH8889 (*Niet-vernietigde foto's*), *NJ* 2009/399.

25. H.J. Holzer, S. Raphael & M.A. Stoll, 'Perceived Criminality, Criminal Background Checks, and the Racial Hiring Practices of Employers', *Journal of Law and Economics* 2006, 49, nr. 2 , p. 451-480 aangehaald in Morozov, 2013, p. 210.

26. HvJ EU 13 mei 2014 C-131/12 (*Google Spain vs. Costeja*), *NJ* 2014/385. Zie ook H. de Jong & T. de Wit, 'Vergeet het maar, Wat is er gebeurd na het Costeja-arrest?', *Tijdschrift voor Internetrecht* 2015 (2), p. 40-46.

27. EHRM 4 december 2008 (*S. and Marper vs. UK*).

28. Ik laat de begeleidingscommissie op grond van art. 21 Wwft in verband met de FIU-activiteiten onbesproken.

29. Zie het hiervoor genoemde *Examenarrest alsmede R. Kuiper, Vormfouten,* Kluwer, 2014 en kritisch over die terughoudendheid S. Brinkhoff, *Startinformatie in het strafproces*, Kluwer, 2014.