Vrije Universiteit Brussel

From the SelectedWorks of Mireille Hildebrandt

Summer June, 2016

Data-gestuurde Intelligentie in het Strafrecht

Mireille Hildebrandt

Available at: http://works.bepress.com/mireille_hildebrandt/68/

SELECTEDWORKS™

DATA-GESTUURDE INTELLIGENTIE IN HET STRAFRECHT·

Mireille Hildebrandt

1 Homo digitalis in het strafrecht 2
1.1 Waar gaat dit over? 2
1.2 Nieuwe agenten in het strafrecht 3
1.3 De cyber in cyberspace 8
1.4 Homo digitalis in de onlife wereld 9

***2* Materieel strafrecht: straffer en bestrafte als *homo digitalis* 13**
2.1 Introductie: onzichtbare 'remote control' 13
2.2 De agent als rechtsubject? 15
2.3 Daderschap, wederrechtelijkheid, causaliteit en schuld 17
2.4 Data-gestuurde toerekening 21

3 Formeel strafrecht: verdachte en handhaver als *homo digitalis* 24
3.1 Introductie: het doel van de strafvordering 24
3.2 Agents van voorspelling en ondervanging 29
3.3 Aantasting van grondrechten 33
3.3.1 Het vertekende beeld van de weegschaal 33
3.3.2 De onschuldpresumptie 33
3.3.3 Gegevensbescherming, privacy, non-discriminatie en vrijheid van informatie 39
3.4 Legaliteit en legalisme: detournement de pouvoir 44

4 Naar een veilig strafrecht in een data-gestuurde samenleving 50
4.1 Reflexieve modernisering van het Wetboek van Strafvordering? 50
4.2 Legaliteit en grondrechtenbescherming 'by design' 51
4.3 We kunnen niet iedereen tegelijk verdenken, maar wel om het even wie? 55

5 Literatuur 57

· Met dank aan mijn zeer gewaardeerde meelezers Egbert Dommering, Bert-Jaap Koops, Serge Gutwirth, Bart Jacobs en John Vervaele, en de interessante gedachtewisselingen met de andere preadviseurs en het bestuur van de NJV. Uiteraard zijn alle onjuistheden geheel en al aan mijn eigen (gebrek aan) wijsheid te danken.

1 Homo digitalis in het strafrecht

We cannot doubt everything, but we should be open to doubt anything.[1]
after Putnam

We cannot suspect everybody, but should we be open to suspect anybody?[2]
Homo digitalis in het strafrecht

1.1 Waar gaat dit over?

Het recht is gebouwd op de idee dat de geest actief is en de materie passief. Dit eenvoudige schema, dat het leven overzichtelijk maakte, gaat niet meer op. Dit preadvies beperkt zich dan ook niet tot gegevensverwerking, hoe belangrijk ook. In het eerste hoofdstuk wordt besproken dat en hoe de samenleving zich beweegt van een informatiesamenleving (waar meer informatie gelijk staat aan betere kennis) naar een data-gestuurde samenleving (waar de kunst is om de relevante datapunten te vinden, te verbinden en daarop te sturen). Het centrale begrip is hier dan ook niet langer data of big data, maar *agent* (een data-gestuurde intelligent systeem). Dat betekent dat de nadruk niet ligt op gegevensverwerking maar op computersystemen die 'handelend optreden', waarbij de mate van aansturing door menselijke *agents* van geval tot geval verschilt. In het eerste hoofdstuk wordt uiteengezet hoe we ons de *homo digitalis* kunnen voorstellen in een omgeving waarin *agents* een hoofdrol spelen. Wie behoefte heeft aan een handzame introductie op data gestuurde intelligentie in combinatie met theoretische reflectie leze dus het eerste hoofdstuk. Wie liever direct naar de implicaties voor materieel en formeel strafrecht gaan kunnen door naar hoofdstukken twee en drie. Wie direct kennis wil nemen van mogelijke oplossingen begint bij hoofdstuk vier.[3]

In het tweede hoofdstuk ga ik in op enkele materieelrechtelijke implicaties van de verschuiving van informatievergaring naar data-gestuurde *agents*. In het derde hoofdstuk ga ik – na een korte bespreking van de doelen van het strafrecht – in op de aard van de *agents* die worden ingezet bij de strafrechtelijke handhaving van de rechtsorde. Daarna onderzoek ik hoe dit de aantasting van een aantal grondrechten beïnvloedt, met nadruk op de onschuldpresumptie. Daarbij zal blijken dat begrippen als verdachte en verdenking dusdanig worden opgerekt dat de combinatie van instrumentaliteit en rechtsbescherming die de kern vormt van de rechtsstaat onder hoge druk komt te staan. De opkomst van politie-*agents* dreigt dan ook de facto een einde te maken aan de bescherming die de voorwaarden voor strafbaarheid en de strafvorderlijke legaliteit zouden moeten bieden. Dit houdt verband met de onzichtbare zichtbaarheid van allerhande patronen die al dan niet correleren met strafbaar gedrag. Zichtbaar voor wie toegang hebben tot onze gedragsgegevens, onzichtbaar voor degenen die het betreft. Die (on)zichtbaarheid wordt bovendien geproduceerd door *agents* die, net als populaire zoekmachines, steeds meer bepalen welke kennis en informatie hun gebruiker (politie en justitie) 'consumeert'. De uitholling van de onschuldpresumptie is echter geen Wet van Meden en Perzen. In het vierde hoofdstuk zal ik bepleiten dat de vraag vooral is hoe zulke *agents* wel en niet worden ingekocht, afgesteld en ingezet. Dat leidt mij in de conclusie tot twee aanbevelingen die ik als stellingen hoop te verdedigen tijdens de jaarvergadering van de NJV2016.

[1] Putnam (1995:21): 'That one can be both fallibilistic and antisceptical is perhaps the basic insight of American Pragmatism. (…) Just as fallibilism does not require us to doubt everything, it only requires us to be prepared to doubt anything - if good reason to do so arises!'
[2] Zie paragraaf 3.3.2 en 4.3.
[3] Mijn moeder leerde ons vroeger dat alleen 'keukenmeiden' achterin een boek beginnen. Kennelijk was dat ook toen al een praktische benadering; bij eindnoten ook nu nog een goed begin.

1.2 Nieuwe agenten in het strafrecht

Dit preadvies richt zich dus specifiek op de gevolgen van data-gestuurde intelligentie voor het strafrecht, met nadruk op de toenemende inzet van kunstmatig intelligente *agents*, met name aan de kant van de rechtshandhaving. Het gaat daarbij niet alleen over software *agents* maar juist ook over de voortgaande vermenging van software en hardware; de opkomst van het Internet van de Dingen, cloud robotica en allerhande slimme infrastructuur. Bovendien gaat het niet alleen om *agents* die min of meer zelfstandig voorgeprogrammeerde taken uitvoeren (een eenvoudige thermostaat is in die zin al een *agent*), maar ook om *agents* die in staat zijn min of meer zelfstandig te leren op basis van de feedback die ze oppikken uit hun omgeving en die juist op basis daarvan hun gedrag aanpassen (bijvoorbeeld de zelfrijdende auto).[4] Het Nederlandse woord 'agent' heeft een andere lading dan het Engelse woord *agent*, dat zowel een term is uit de computerwetenschappen (*intelligent agent*, *multi agent systems*), [5] als de (rechts)filosofie (*human agency*),[6] als het recht (*agent-principal*).[7] Voor dit preadvies zijn alle drie betekenissen relevant. Hierna zal ik de term *agent* gebruiken voor data gestuurde systemen. Denk aan een zoekmachine, een drone, een computervirus, of een slim energiesysteem dat de levering van energie afstemt op de spanning van het energienetwerk. Meer toegespitst op de strafvordering kunnen we bijvoorbeeld denken aan een systeem van slimme sensoren (camera's en microfoons) in een smart city die detecteren of de bezoekers van een voetbalwedstrijd of uitgaansgebied op het punt staan geweld te gebruiken.

De komst van *agents* luidt de overgang in van informatiesystemen naar *agent*systemen, dat wil zeggen systemen die min of meer zelfstandig ingrijpen in de werkelijkheid.

Nu het om data-gestuurde *agents* gaat impliceert dit tegelijk een overgang van de *informatie*samenleving naar een *data-gestuurde* samenleving. Meer data staat niet (meer) gelijk aan meer informatie, integendeel. We zijn op het punt aangekomen dat een toenemende data-obesitas ons het zicht beneemt op de juistheid en de mogelijke relevantie van data; de uitdaging ligt niet meer in het verzamelen van zoveel mogelijk data maar in de slimme selectie en intelligente verwerking daarvan. In tijden van data-zwaarlijvigheid gaat het niet meer om de calorische waarde maar om de voedingswaarde en zelfs dan *niet* om meer van hetzelfde maar om de juiste verhoudingen. Zoals bekend spelen sporenelementen daarbij een cruciale rol; het ontbreken (of een teveel) van minieme hoeveelheden vitaminen en mineralen kan tot ondervoeding (of ziekelijke ontwikkeling) leiden, ondanks inname van voldoende energierijk voedsel. Zo is het ook met data; de kunst is om de juiste datapunten te vinden en dat kan niet altijd door zoveel mogelijk data te verzamelen.[8] Maar ook adequate selectie en verwerking vormen niet de kern van wat ons te wachten staat. De crux ligt in onze nieuwe – *geestloze* – huis-, land- en wereldgenoten: systemen die in staat zijn hun omgeving waar te nemen, erop in te grijpen en

[4] De software *agents* die Schermer (2007) in zijn proefschrift besprak zijn nog steeds relevant, maar de grootschalige opkomst van machinaal lerende cyberfysieke systemen gaat veel verder, met name in de mate waarin deze systemen ingrijpen in de werkelijkheid.

[5] *Agents* spelen een belangrijke rol in kunstmatige intelligentie (KI), zie Russell en Norvig (2009) en Mitchell (1997). Bij KI verwijst de term *agent* naar een systeem dat de omgeving waarneemt (via sensoren) en erop ingrijpt (via actuatoren). In de informatica wordt een software *agent* vaak gedefinieerd als een programma dat handelt in opdracht van de gebruiker of een ander programma. Zie in die laatste zin Schermer (2007: hoofdstuk 2).

[6] Over *moral* en *legal agents* Duff (2009). Bij morele of juridische *agents* gaat het om mensen die – anders dan computer systemen – bewustzijn hebben en zich – anders dan dieren – bewust zijn van dat bewustzijn. Morele *agents* zijn dankzij hun zelfbewustzijn in staat tot reflectie op de normatieve implicaties van hun eigen gedrag. Alleen *moral agents* kunnen onrechtmatig en verwijtbaar handelen.

[7] Hier gaat het om het leerstuk van vertegenwoordiging (Dowrick 1954), in Nederland geregeld in 3:60 BW (volmacht), waarbij het vertrouwensbeginsel een belangrijke rol speelt.

[8] Soms is dat overigens wel zo. Helaas generaliseren sommige auteurs ten onrechte specifieke leerstukken uit de statistiek die inderdaad aanleiding zijn om aan te nemen dat foutmarges afnemen als maar extreem veel data verzameld worden. Mayer-Schönberger en Cukier (2013) lijken in die valkuil te trappen. Zie bijvoorbeeld boyd en Crawford (2012) voor relativering.

vervolgens te leren van de feedback die zij ontwaren, zodat zij hun gedrag in lijn met te bereiken doelen kunnen aanpassen. Ik mag er alvast op wijzen dat deze *agents* zich weliswaar gedragen, maar (nog?) niet handelen. Zo zij al intenties hebben is er geen bewustzijn van die intenties, laat staan zelfbewustzijn. Zo zij al betekenis toekennen aan hun eigen of andermans gedragingen, is dat een metafoor voor hun vermogen om op basis van machinaal leren (ML) inferenties af te leiden en toe te passen. Voor deze *agents* zijn wij geen *homines sapientes*, maar *homines behaviorales*, min of meer voorzienbaar en ondervangbaar op basis van de mechanismen die uit ons gedrag worden afgeleid.[9] In dat kader passen drie caveats. Ten eerste moeten we ons niet verslikken in metaforen die termen als waarneming, betekenis, intentie en gedrag verbinden met het (zelf)bewustzijn dat ons eigen is. *Agents* nemen waar, ze 'hebben' vaak (door ons bepaalde) intenties en ze gedragen zich; bovendien kunnen ze computationele 'betekenis' toekennen aan wat ze waarnemen. Maar dat doen ze allemaal zonder enige vorm van bewustzijn, laat staan zelfbewustzijn. Wie de ontwikkelingen binnen de neurowetenschappen volgt zal zien dat steeds duidelijker wordt dat grote delen van ons gedrag gestuurd wordt door processen waar we ons niet van bewust zijn, terwijl sommigen zelfs concluderen dat ons zelfbewustzijn een zogenaamd 'epifenomeen' is – een neveneffect waar we eerder de lasten dan de lusten van smaken. We moeten echter, ten tweede – juist in het recht, en precies in het strafrecht – de verleiding weerstaan om het kind al te snel met het badwater weg te gooien door het zelfbewustzijn als een illusie bij het groot vuil te zetten.[10] Met Damasio (2011: 280, 287, 293) meen ik dat het flintertje zelfbewustzijn waarmee we zijn begiftigd er toe doet, en de grondslag vormt van het vermogen onszelf (als persoon en als samenleving) de wet te stellen. Ten derde impliceert het feit dat *agents* geen zelfbewustzijn hebben, en in die zin geestloos zijn, niet dat ze gelijkgesteld kunnen worden met om het even welk type informatiesysteem. *Agents* nemen hun omgeving waar en zijn in toenemende mate zo ontworpen dat ze in kunnen grijpen en hun gedrag vervolgens aan kunnen passen naar aanleiding van de feedback die ze ontwaren. Het zijn geen mensen (geen zelf-bewustzijn), geen dieren (geen bewustzijn), maar zijn niet noodzakelijkerwijs puur reactieve informatiesystemen.

Om de gedachten te bepalen vangen we aan met een korte bespreking enkele *agents*. Doel is niet om de daarmee opgeroepen problemen juridisch-technisch 'op te lossen', maar om de relevante vragen die *agents* oproepen scherper op het netvlies te krijgen. Pitlo zei het al: 'zoeken is ons doel. Vinden zou ons met lege handen laten staan'.[11] Hierna bespreek ik: (1) een botnet, (2) een zorgrobot die online is verbonden met de cloud, (3) slimme energienetwerken (smart grids) en (4) een smart city project in Eindhoven. Sommige *agents* zijn duidelijk herkenbaar als een identificeerbare, duurzame eenheid van actie, waarneming en reactie (bijvoorbeeld een drone), anderen vertonen waarneming en gedrag zonder dat sprake is van een eenvoudig te identificeren eenheid (denk aan een smart grid infrastructuur).[12] Interessante vraag is natuurlijk of de duurzame identificeerbaarheid een kwestie is van (1) hoe het systeem zich gedraagt (de ontologische vraag) ofwel van (2) de mate waarin wij het als eigenstandige *agent* herkennen (de kennistheoretische vraag). Mij dunkt dat dit van geval tot geval en in de loop van de tijd zal verschillen. Punt is dat systemen die zich herkenbaar als *agent* gedragen ook als zodanig geadresseerd kunnen worden, terwijl gedistribueerde systemen allerlei toerekeningsproblemen

[9] *Homo behavioralis* is het verdwijnpunt (de verzwegen premisse) van Kahneman en Tversky's (1979) cognitieve psychologie (en daarmee van de gedrageconomie). Het begrip *homo behavioralis* is gemunt door Binmore (1988) als tegenhanger van *homo economicus*. De *homo behavioralis* is volgens Binmore de 'mythische hominoide' van de gedragseconomie, volledig door genen, omgeving en evolutie gedetermineerd: 'Both species are modeled as stimulus-response machines, but *homo behavioralis* is programmed directly with behavior, like a chocolate-dispensing machine (Binmore 1988:4).'

[10] Zoals op sjabloonachtige wijze min of meer bepleit door Swaab (2010) en Lamme (2011), maar zie Slors (2015) of Van de Laar en Voerman (2011); voor het recht *NJB* (2013) special issue 'Neurolaw in Nederland'. Voor de internationale discussie Damasio (2011) en meer specifiek voor het recht Morse (2008) en Vincent (2013).

[11] Dit citaat van Pitlo e.a. (1995) hing jarenlang in mijn werkkamer bij de Erasmus Universiteit. Helaas heb ik de juiste pagina niet kunnen achterhalen. Met zijn uitspraak is niet gezegd is dat oplossingen niet interessant zijn; het gaat er meer om kortsluiting te voorkomen door oplossingen te gaan zoeken voordat de problemen verkend zijn.

[12] Over verschillende typen kunstmatige *agents* Pfeifer en Bongard (2007), Floridi en Sanders (2004) en voor de geschiedenis van kunstmatige intelligentie zie Hayles (1999), Varela, Thompson en Rosch (1991).

oproepen. Men bedenke echter dat juist de opkomst van cloud robotica impliceert dat veel herkenbare systemen feitelijk gedistribueerd zijn (de 'hersenen' van de zorgrobot 'hangen' wellicht deels in de cloud). Door consequent te spreken van *agents* wil ik het actiepotentieel van al deze systemen benadrukken. Het gaat niet alleen om gegevensverwerking.

Eerste voorbeeld. Wie kwaad wil kan haar[13] hart ophalen in de catacomben van het internet (over het zogenaamde 'darknet' zie Morozov 2011). Zij kan daar een botnet inhuren om geautomatiseerde DDOS (distributed denial of service) aanvallen te laten uitvoeren met als gevolg dat de beschikbaarheid van het doelwit ernstig te lijden heeft. Dit is zonder meer een strafbaar feit (art. 138b Sr als formeel omschreven delict),[14] en afhankelijk van het type en de distributie van de schade ook nog te kwalificeren in termen van art. 161 sexies Sr (een materieel omschreven delict dat 'gemeen gevaar voor goederen of verlening van diensten' als delictsbestanddeel heeft).[15] Zij is bij het uitvoeren van die aanval niet gebonden aan landsgrenzen en 'zij' kan ook een staat zijn, een terroristische organisatie of een bedrijf. Ze kan – in plaats van een botnet – ook een virus of andere malware aanschaffen of zelf (laten) ontwikkelen die zelfstandig een pad kiest om binnen te dringen in specifieke systemen ten einde daar informatie te kopiëren, instructies te verbergen of gewoon de werking van een of meer systemen te saboteren. Het klinkt eenvoudiger dan het is,[16] maar het kan wel en is in beginsel strafbaar ex art. 138ab WvSr (formeel omschreven delict: hacken) en eventueel ook 350a WvSr (materieel omschreven: veranderen, wissen, onbruikbaar of ontoegankelijk maken van gegevens). De mogelijkheid om dit soort aanvallen relatief eenvoudig vanuit een andere locatie en jurisdictie te organiseren roept vragen op rond extraterritoriale handhavingsjurisdictie (Koops en Goodwin 2014). In combinatie met de ernst van de gevolgen, bijvoorbeeld wanneer het om aanvallen op kritische infrastructuur gaat, roept dit alles bovendien vragen op rond het onderscheid tussen oorlog, criminaliteit, internationaal terrorisme en illegale extraterritoriale handhaving die niet als oorlogsvoering gekwalificeerd kan worden maar wellicht ook niet als strafrechtelijk optreden (Hildebrandt 2013).

Tweede voorbeeld. Het zou zomaar kunnen dat hoogbejaarden binnen 10 jaar geen verpleger van vlees en bloed aan hun zijde vinden, maar een intelligente, met emotie-detectie uitgeruste, vriendelijke maar ook robuuste zorgrobot. Deze voedt zich met data en programmatuur uit de cloud, en leert op basis van de interactie met de 'eigen' patient of cliënt. De zorgrobot kan dag en nacht doorwerken, heeft een ijzersterk geheugen en gecalculeerd inzicht in de eigenaardigheden van de cliënt, en onderhoudt directe verbindingen met apotheek, huisarts, medisch specialisten en relevante zorginstellingen (en, natuurlijk, met de verzekering die de kosten vergoedt). Deze zorgrobot is niet alleen efficiënt omdat de afgeleide gedragspatronen van de cliënt een adequate reactie op ontbrekende therapietrouw mogelijk maken, en omdat de cliënt nu veel langer 'op zichzelf' kan blijven wonen (hoewel dan toch samen met de zorgrobot), maar ook omdat deze robot humor heeft, beleefd is, het idioom van de cliënt beheerst en

---

[13] In dit advies wordt consistent met een vrouwelijk verwijswoord terugverwezen naar termen die zowel naar mannelijke als vrouwelijke personen kunnen verwijzen, zoals bijvoorbeeld persoon, gebruiker, dader, verdachte. Dit om de leesbaarheid te bevorderen (geen hij/zij of zijn/haar) en om niet te vervallen in 'hij' of 'zijn', het gebruikelijke pars pro toto. Zie bijvoorbeeld <http://taaladvies.net/taal/advies/tekst/110/verwijzingsproblemen_met_voornaamwoorden_van_de_derde_persoon_enkelvoud_algemeen/> of <http://www.learnersdictionary.com/qa/the-he-or-she-dilemma> (in Nederland valt dit waarschijnlijk onder radicaal feminisme).

[14] Een formeel omschreven delict stelt een bepaald handelen strafbaar, in dit geval het 'opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmer[en] door daaraan gegevens aan te bieden of toe te zenden'.

[15] Een materieel omschreven delict stelt het veroorzaken van een bepaald gevolg strafbaar, in dit geval gaat om het 'opzettelijk enig geautomatiseerd werk of enig werk voor telecommunicatie verniel[en], beschadig[en] of onbruikbaar ma[ken], stoornis in de gang of in de werking van zodanig werk veroorza[ken], of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdel[en], indien daarvan gemeen gevaar voor goederen of voor de verlening van diensten te duchten is', met nog een aantal strafverzwarende gevolgen (levensgevaar en de dood van een ander). Zie HR 22 februari 2011, ECLI:NL:HR:2011:BN9287.

[16] Over transnationale cybercriminaliteit Koning (2012), over cyberoorlog of spionage Hijink (2012).

voorzien is van voldoende onvoorspelbaarheid om 'echt' te lijken. Hoe nu als deze robots globaal gezien minder ongelukken veroorzaken dan verplegers, maar in specifieke gevallen de plank wel eens misslaan en bij het nemen van de pols te hard knijpen, een injectienaald in het verkeerde lichaamsdeel steken, de patiënt bij het wassen laten vallen of een verkeerde combinatie van medicijnen klaarzetten? Het is niet zo dat er bij menselijke agents nooit iets mis gaat, maar die kunnen we strafrechtelijk aanspreken. Die ervaren pijn, verdriet en spijt – de zorgrobot kan dat allemaal moeiteloos simuleren maar bij gebrek aan bewustzijn niet ervaren in onze betekenis van dat woord. De zorgrobot heeft in feite niets te verliezen. Gaan we in geval van calamiteiten de ontwerper strafrechtelijk vervolgen of de leasemaatschappij? Stel dat de zorginstelling die de robot 'in dienst heeft' de robot van een vorige – overleden – patiënt een 'harde reset' heeft gegeven zodat de fabrieksinstellingen terugkeren. En stel dat die robot toch nog wat diep verborgen algoritmes blijkt te hebben die waren getraind op de vorige patiënt, waardoor inadequaat op de nieuwe patiënt wordt gereageerd, met fatale afloop? Is hier sprake van schuld of voorwaardelijk opzet? Is denkbaar dat we de robot op enig moment zelf gaan strafrechtelijk gaan aanspreken, inspelend op de ethische regels en de synthetische emoties die zijn geconfigureerd?

Derde voorbeeld. Slimme energiesystemen (smart grid) moeten niet worden verward met een slimme meter. De laatste is slechts een onderdeel van zo'n systeem.[17] Een smart grid betekent een omwenteling in de afstemming van vraag en aanbod in de levering van energie, waarbij huishoudens, bedrijven en overheden niet alleen energie afnemen maar ook produceren, uitruilen en/of uploaden naar het distributie netwerk. De komst van de elektrische auto en de exponentieel toenemende inzet van elektronica in huis, kantoor, verkeer, sport, fabriek, gezondheidszorg, en detailhandel leidt tot een sterk wisselende energiebehoefte die zonder predictieve (voorspellende) en pre-emptieve (ondervangende) data-analyse tot een onbeheersbaar netwerk zou leiden – met voortdurende systeembreuken en uitval als gevolg. De idee is dat toegang tot gedetailleerde gebruiksgegevens redelijk nauwkeurige voorspellingen mogelijk maakt, die in samenhang met *sturing van* en zelfs *controle over* energieverbruik van de eindgebruikers tot een verantwoorde energiehuishouding kan leiden. Zo kan de netbeheerder die de juiste spanning op het net moet garanderen besluiten dat wie tijdens een veelbekeken voetbalwedstrijd ook nog een was wil draaien daar een extreem hoge prijs voor moet betalen (sturing door middel van flexibele prijsstelling) of beslissen dat bepaalde huishoudens die was niet kunnen draaien (remote control). Die laatste ingreep zal waarschijnlijk alleen mogelijk zijn als de klant korting accepteert in ruil voor een contract dat dit type ingrepen onder bepaalde voorwaarden toelaat. Het smart grid – dat in Europa op initiatief van de EU wordt uitgerold – bestaat uit een veelheid van kleine en grotere systemen, die voortdurend met elkaar in gesprek zijn middels machine-tot-machine communicatie. Sommige systemen zullen kunstmatige intelligentie (KI) toepassen, bijvoorbeeld machinaal leren, om snel inzicht te krijgen in te verwachten energieverbruik en – via simulaties – in de gevolgen van dynamische aanpassing van de prijs, dosering op afstand en andere ingrepen bedoeld om het energieverbruik te beïnvloeden. Hier is evident sprake van *agency*, nu deze systemen niet alleen hun omgeving waarnemen (zowel ons energieverbruik als weersomstandigheden, verkeerspieken, relevante evenementen, dag- en nachtritmes en zo meer) maar hun gedrag daar bovendien op aanpassen (prijsstelling, remote control, dosering) en vervolgens ook leren van de impact van het eigen gedrag op dat van de omgeving. Strafrechtelijk kan dit alles tot een nieuwe dynamiek leiden:[18] (1) deelsystemen kunnen uit de pas gaan lopen en grote schade veroorzaken nu het hier gaat om kritische infrastructuur, (2) de afstemming tussen systemen kan tot soortgelijke of nog omvangrijker problemen leiden, (3) systemen kunnen worden gehackt en gemanipuleerd door individuele personen of organisaties binnen of buiten de relevante strafrechtelijke jurisdictie, (4) bedrijven en overheden kunnen toegang krijgen tot energieverbruiksgegevens van huishoudens en daar – eventueel in samenhang met andere gegevens – conclusies uit trekken met betrekking tot religie, werkloosheid, gezondheid, feitelijke gezinssamenstelling, fraude met sociale zekerheid of belastingen en zo meer. Daarbij zij opgemerkt dat deze agents wel eens iets anders zouden kunnen doen dan de gebruiker is verteld, denk bijvoorbeeld aan

[17] Over de privacy implicaties van de slimme meter Cuijpers en Koops (2013); over de implicaties van een slimme energie infrastructuur voor een aantal grondrechten Hildebrandt (2013b).
[18] Over de kwetsbaarheid van de huidige kritische infrastructuur Nationaal Coordinator Terrorismebestrijding en Veiligheid (2015).

het voorbeeld van Volkswagen, waar volautomatisch valse informatie over vervuilingswaarden werd verstrekt. Zoals Jensma (2015) opmerkt lijkt hier sprake van strafbaar bedrog, waarbij vooral ook de oplossing die hij aandraagt tot nadenken stemt: een cyberfysieke infrastructuur die real-time monitort hoeveel vervuiling de auto produceert (en, ik voeg daar maar aan toe, gelijk de belastingdienst op de hoogte houdt van eventuele fraude met de lease auto).

Vierde voorbeeld. Hier gaat het om de inzet van predictive policing in 'Living Lab Stratumseind' in Eindhoven, waarover *NRC Handelsblad* kopte (Van Noort en Kist 2015):

> Er ontstaat een complete industrie rond technologie die met camera's, sensoren, big data en emotieherkenning misdaad voorspelt. Maar dat gaat ook wel eens mis en er is juridisch veel onduidelijk. 'Je ziet partijen de grens opzoeken.'

Volgens de krant gaat het hier om een samenwerking tussen gemeente Eindhoven, een aantal IT bedrijven (ATOS, Intel) en het Dutch Institute for Safety & Security, die een systeem ontwikkelen dat real-time de vinger aan de pols houdt binnen het geoormerkte gebied. Doel is op basis van allerlei persoons- en andere gegevens hinderlijk, gevaarlijk of anderszins onwenselijk gedrag te voorspellen. Dit alles onder de tot de verbeelding sprekende naam 'CityPulse' (een product dat wereldwijd vermarkt gaat worden; delegaties uit Florida, Roemenië en Singapore zijn al wezen kijken). Atos krijgt op deze manier de kans om haar predictieve technologie te testen op niet-laboratorium situaties, de gemeente kan CityPulse inzetten bij de handhaving van de openbare orde, de politie kan er haar voordeel mee doen. Sneller optreden om opstootjes of geweld in de kiem te smoren, overvallen of aanvallen te voorkomen, wellicht ook overlast tegengaan. Dit zou mogelijk worden gemaakt op basis van *agents* die incidenten detecteren voordat de politie ter plekke is, die escalatie van ruzies in de openbare ruimte oppikken voordat het uit de hand loopt, en meer in het algemeen, *agents* die voortdurend in kaart brengen welk gedrag in welk opzicht afwijkend is van 'normaal' en/of 'wenselijk' gedrag. In feite gaat het hier al om 'predicting the present', wat in zekere zin lastiger is dan het voorspellen van de toekomst, want bij het 'voorspellen' van het heden worden onjuiste voorspellingen onmiddellijk ontmaskerd. Het krantenartikel vermeldt nog dat het voorlopig niet duidelijk is of Stratumseind dankzij CityPulse veiliger is geworden, terwijl gegevens over hoe vaak de politie is uitgerukt naar aanleiding van signalen van CityPulse niet openbaar worden gemaakt, laat staan gegevens over hoe vaak sprake was van vals alarm. De schrijvers van het artikel merken droogjes op dat de samenwerking desondanks met drie jaar is verlengd, want, zo citeren zij de wethouder, 'waar het ons vooral om gaat is dat we Eindhoven openstellen als laboratorium voor innovatieve bedrijven (Van Noort en Kist 2015)'. Hier is evident sprake van een bijzondere vorm van privaat-publieke samenwerking, waarbij gegevensstromen vanuit de private sector worden omgelegd en afgebogen ten einde de handhaving van de openbare orde en het strafrecht van dienst te zijn.

Zoals hierboven aangestipt kan het doorsluizen van energieverbruiksgegevens vanuit de private sector (energieleveranciers, aanbieders van applicaties bij de slimme meter) naar justitie of de belastingdienst voor soortgelijke grensoverschrijdende uitwisseling leiden. Nog los van bijvoorbeeld de onschuldpresumptie roept dit de vraag op wanneer dit gaat leiden tot maatregelen die de essentie van het recht op privacy en gegevensbescherming aantasten.[19]

[19] Nog los van de proportionaliteitstoets van art. 8 EVRM kan toetsing aan art. 52 lid 1 van het Handvest van de Grondrechten in de EU (Hv) leiden tot een onrechtmatigheidsoordeel (het gaat dan om aantasting van de essentie van het recht), cf. HvJEU 8 April 2014, C-293/12 and C-594/12 (Digital Rights Ireland/Ierland), r.o. 38, 39 (geen aantasting essentie, maar wel disproportioneel en dus ongeldig) ofwel HvJEU, 6 October 2015, C-362/14 (Schrems/Data Protection Commissioner Ireland), r.o. 94-95 (wel aantasting essentie en daarmee ongeldig).

1.3 De cyber in cyberspace

Hoewel de notie 'digitaal' interessant is omdat die de aandacht vestigt op de bijzondere aard van door computers verwerkte data,[20] is van belang om digitaal te bezien in relatie tot 'cyber'. Het onderscheid tussen computer en cyber verwijst meestal naar de overgang van op zichzelf staande computersystemen naar online verbonden computersystemen en valt dus samen met de komst van het internet en het world wide web (www). Interessanter is echter dat de digitalisering van de werkelijkheid en de daarmee samenhangende informatica van begin af aan nauw was verbonden met de cybernetica, de door Wiener (1988) geïntroduceerde wetenschap van het besturen op afstand (de oud-Griekse term *kyber* kan worden vertaald met navigeren of sturen).[21]

Het is precies ook de wetenschap van de cybernetica die nauw verwant is aan die van de kunstmatige intelligentie, waar het inmiddels niet meer gaat om het na-apen van menselijke intelligentie door middel van deductieve logica maar om het bouwen van systemen die in staat zijn hun omgeving waar te nemen en erop in te grijpen. Kern van dit soort systemen is dat zij kunnen 'leren' van hun 'ervaring'.

Machinaal leren (ML) is op dit moment een van de meest gebruikte vormen van KI; het wordt bijvoorbeeld ingezet bij beeldherkenning, tekstanalyse, de ondersteuning van medische diagnostiek, cloud robotica en zelfrijdende auto's. ML valt uiteen in gecontroleerd en ongecontroleerd leren (Hildebrandt 2012:345-46). Het eerste maakt gebruik van een zogenaamde trainingset van data, bestaande uit input data (bijvoorbeeld een bepaald type tekst) en output data (bijvoorbeeld de samenvatting ervan). Het systeem meet allerlei eigenschappen van de input data om de link te kunnen leggen met de output data. Daarna krijgt het systeem nieuwe input data waarbij het zelfstandig output data genereert. De gebruiker bekijkt of het systeem het goed heeft gedaan en corrigeert eventuele fouten, waarna het systeem opnieuw het verband tussen input en output doorrekent. Op deze wijze worden algoritmes getraind, totdat het systeem voldoende goed scoort bij de omzetting van input naar output. De meest verrassende uitwerking van ML is zogenaamd Deep Learning (DL). Dat laatste combineert technieken die geïnspireerd zijn op de werking van de hersenen en bestaat uit zogenaamde kunstmatige neurale netwerken (NNs) die uit meerdere lagen zijn opgebouwd, waardoor de resultaten voortdurend verfijnd en aangepast worden. Dit maakt geavanceerde ongecontroleerd lerende systemen mogelijk die zonder veel sturing patronen detecteren op een wijze die meer overeenkomt met onbewuste leerprocessen dan met ons rationele bewustzijn. Het door IBM ontwikkelde computer systeem Watson, dat het televisiespel Jeopardy won, was mede gebaseerd op dit type DL (IBM 2011, Hildebrandt 2013a). Watson was in staat om de juiste vraag te genereren bij gegeven antwoorden, waarvoor zoeken in grote hoeveelheden ongestructureerde data noodzakelijk was. Daarvoor kan eigenlijk geen recept (algoritme) worden gegeven. DL kan daarom worden omschreven als een techniek die *zelfstandig leren* mogelijk maakt; het moet worden onderscheiden van het *aanleren* van kennis en vaardigheden (gestuurd door deductieve programmatuur of met voorbeelden getrainde algoritmes). Het begrip *agent* moet dan ook vanuit de cybernetica en ML technologie worden begrepen. De cybernetica is vooral gericht op het ontwikkelen van operationele systemen, die niet alleen informatie verwerken en gedrag voorspellen, maar ook beslissingen kunnen nemen en uitvoeren. Dat laatste is bijzonder relevant voor de inzet van *agents* in de strafvordering, nu deze beslissingen grote gevolgen kunnen hebben voor wie op het netvlies van deze *agents* komen.

Terug naar de cyber in cyberspace. Internet maakte computernetwerken mogelijk, waarop allerhande applicaties gebouwd kunnen worden, in de eerste plaats het www. De hyperconnectiviteit en het netwerkeffect die hiermee in gang werden gezet bepalen de contouren en eigenschappen van cyberspace. Op het niveau van hardware zien we een verschuiving richting de cloud, waardoor de

[20] Over de wiskundige aard van de informatietheorie die ten grondslag ligt aan informatie in het tijdperk van digitalisering, alsmede de relevantie daarvan voor het recht Hildebrandt (2016a te verschijnen).

[21] In de 19e eeuw gebruikte de natuurkundige Ampère (2012:143) de term cybernetica: 'qui est, à l'égard du gouvernement des nations, ce qu'est la stratégie relativement à la conduite d' une armée.' Men zou kunnen vertalen met administratie of bestuur, een soort bestuurskunde *avant la lettre*.

wettelijke term 'randapparatuur' opnieuw actueel is. Onze schermen (toepasselijk monitor geheten) zijn steeds meer een interface naar grootschalige, dynamische computersystemen die op servers 'draaien' die zich elders bevinden, vaak ook in andere jurisdicties. Opslag van data, software en zelfs besturingssystemen vindt plaats waar en hoe het efficiënt is, wat ook kan betekenen dat data herhaaldelijk wordt verplaatst (en uit voorzorg zowel verspreid als dubbel wordt opgeslagen). Op het niveau van software applicaties hebben sociale media en 'online gaming' een enorme vlucht genomen, waar het delen van zogenaamde 'user generated content' of spel-interactie voorop staat en het koppel van hyperconnectiviteit en netwerkeffect een geheel nieuwe betekenis heeft gegeven aan de idee van cyberspace. In eerste instantie lijkt dit koppel de beste omschrijving te bieden van cyberspace: een online wereld waar de zwaartekracht niet geldt en vooral het leggen van verbindingen langs lijnen van elkaar kruisende netwerken voorop staat. Cruciaal is dat de communicatie niet is voorbehouden aan personen, maar vaak door eenvoudige of complexe kunstmatige *agents* wordt onderhouden, hetgeen samenhangt met de computationele achterkant van cyberspace, die het mogelijk maakt om alle 'gedrag' niet het alleen te meten maar ook op te slaan, te vergelijken en daar middels data-analyse nieuwe 'kennis' uit af te leiden.

Voor zover cyberspace wordt beperkt tot de online gecreëerde ruimte geldt weliswaar niet de zwaartekracht maar gelden wel andere, algoritmisch geschapen 'wetten' die de grenzen en de logica van cyberspace bepalen. Inmiddels lijkt het echter een wat hachelijke zaak om cyberspace te beperken tot de online omgeving en blijkt het onderscheid tussen online en offline zelf steeds moeilijker vol te houden. Dat heeft te maken met vermenging van beide in smartcards (OV chipcard, betaalkaarten, toegangspasjes), in de aanleg van slimme energiesystemen, domotica, steeds autonomer functionerende auto's, zelfrijdende treinen en zo meer. Technici spreken van cyberfysieke systemen (Suh e.a. 2014), voortbouwend op wat ooit het Internet van de Dingen of Ambient Intelligence werd genoemd (toen vooral een visie, nu technisch voluit in ontwikkeling). Vanuit mijn betrokkenheid bij het Onli*f*e Initiative (een samenwerking van de Europese Commissie en een groep filosofen, neuro- en computerwetenschappers) zal ik in het vervolg van dit preadvies spreken van de onli*f*e wereld.[22] Hiermee beoog ik te benadrukken dat de leefwereld van personen en organisaties een gedaantewisseling heeft ondergaan die niet adequaat verwoord kan worden met verwijzing naar cyberspace, juist omdat die leefwereld niet meer is opgedeeld in online en offline.[23]

1.4 *Homo digitalis* in de onli*f*e wereld

Na deze preliminaire verkenningen van *agents* nu over naar de *homo digitalis*. Door te spreken van een *homo digitalis* erkent de NJV dat technologie de mens verandert die haar uitvindt en wordt de vraag opgeroepen hoe de *homo digitalis* zich verhoudt tot *homo sapiens*, *homo faber* en *homo ludens*. In hoeverre is de *homo digitalis* een ordinaire *homo economicus* of *behavioralis*, de droom van de economen en psychologen die zoeken naar de meest effectieve en efficiënte manier om mensen te beïnvloeden? Welke *huomo* ligt ten grondslag aan het mensbeeld in het strafrecht en hoe verhoudt de *homo digitalis* zich tot het – voor het strafrecht cruciale - onderscheid tussen gedrag (extern perspectief met nadruk op meetbaarheid) en handeling (gematigd intern perspectief met nadruk op betekenis)? Om

[22] Zie over het zogenaamde Onli*f*e Initiative van de Europe Commissie: <http://ec.europa.eu/digital-agenda/en/onlife-original-outcome>, en Floridi (2014). Vervaging van online en offline heeft ook consequenties voor de vervaging van publiek/privaat, bijvoorbeeld waar een smartphone in de openbare ruimte in beslag wordt genomen en vervolgens doorzocht, zie Timan en Koops (2014). Vergelijk ook de inzet van drones om gedrag in steden in de gaten te houden, een voorbeeld van 'heterdaadkrachtig' optreden in het kader van de handhaving van de openbare orde en/of de strafrechtelijke handhaving van de rechtsorde (Jensma 2013). Ik hanteer de gebruikelijke Engelse termen maar ben ook wel gecharmeerd van het voorstel van Bert-Jaap Koops om online te vertalen met 'aangelijnd', offline met 'afgelijnd' en onli*f*e met 'aangelijfd'.

[23] In mijn oratie heb ik bepleit om cyberspace ruimer op te vatten dan alleen in termen van de online wereld, maar gezien het taalgebruik is het misschien verstandiger een andere term te gebruiken om de vermenging van online en offline aan te duiden, zie Hildebrandt (2011b).

de vraag te beantwoorden welk mensbeeld ten grondslag ligt aan het strafrecht kunnen we een survey organiseren, een literatuuronderzoek doen (ideeënhistorisch, analytisch, hermeneutisch, semiotisch), een computersimulatie ontwerpen die het gedrag van kunstmatige *agent*s registreert op basis van onderscheiden mensbeelden,[24] of alle actoren in de strafrechtsketen voorzien van een daartoe ontworpen App die op slimme wijze hun reactie toetst op het ermee verweven mensbeeld.[25] We kunnen ook – met dit alles in het achterhoofd – zelf nadenken en een beargumenteerde positie innemen. Ik zal het kort houden en verwijzen naar drie filosofen die relevante gedachten ontwikkelden, die naar ik hoop verhelderen waar de schoen wringt wat betreft het onderscheid tussen gedrag en handelen.

Hegel meende in zijn *Rechtsphilosophie* dat het straffen van mensen niet gelijk mag worden gesteld met het conditioneren van een persoon op basis van psychologische dwang, zoals Feuerbach (1801:12-20) had bedacht. In zijn rechtsfilosofie merkt Hegel (1970: §99, toevoeging H) op dat dit neerkomt op het trainen van een hond en geen beroep doet op de mens als redelijk wezen, die uiteindelijk zelf beslist om zich al dan niet aan de wet te houden. De straf censureert (Duff 2001) en hoopt op inzicht en spijt, maar kan die (gelukkig) niet afdwingen; het is geen vorm van disciplinering, priming of nudging. Ik zou durven beweren dat Hegel meent dat het bij straffen gaat om een handeling en niet om gedrag, zowel aan de zijde van de verdachte of dader (dus geen disciplinering) als aan de zijde van de straffende overheid (dus geen automatisme). Wat is dan gedrag en wat handelen?

In haar *The Human Condition* onderscheidt Arendt (1958) gedrag als een automatisch proces dat onderworpen is aan de wetten van causaliteit en dus ook causaal beïnvloedbaar is.[26] Handelen, daarentegen, is verbonden met vrijheid en onzekerheid. Zij situeert handelen buiten het domein van noodzaak en voorspelbaarheid, en legt de relatie met het spreken in een publieke context en het vermogen opnieuw te beginnen (zij spreekt van nataliteit). Voor het strafrecht is dit een buitengewoon relevante benadering, die de aanspreekbaarheid van de dader benadrukt in een publieke context, op basis van de vooronderstelling dat de dader anders had kunnen en moeten handelen en vooral ook uitgaat van de gedachte dat zij in de toekomst anders kan handelen (wanneer de staf is uitgezeten mag in beginsel niet meer gestigmatiseerd worden als ex-veroordeelde). Deze vooronderstellingen zijn hachelijk en niet evident, zeker wanneer we de statistiek erbij halen om te 'bewijzen' dat het meestal of toch vaak weer mis gaat. *Gedrag benoemen als handeling* is dan ook geen vanzelfsprekendheid en vraagt een specifieke maatschappelijke ordening die voorkomt dat dader en straffer zich in hun rol verliezen en zich beperken tot wat van hen wordt verwacht (statistisch gezien dan toch). Voor de dader ligt de uitdaging erin haar gedrag toe te eigenen als haar eigen handelen, waarvoor zij ter verantwoording kan worden geroepen wanneer zij daarmee anderen heeft beschadigd (of had kunnen beschadigen).[27] Voor de straffende instantie is de uitdaging om zich te weerhouden van straffen als automatische reactie - als zou het niet anders kunnen; ook het straffen zelf is een vorm van zich gedragen die pas betekenis krijgt als de straffer zich de concrete straf als eigen handeling toe-eigent.

In haar *Giving an Account of Oneself* stelt Butler (2005:10-17) – onder verwijzing naar Nietzsche (1969: 84) – dat het morele subject als zodanig geboren wordt bij het opleggen van de eerste straf. Het gaat om het moment waarop de ander mij aanspreekt op de gevolgen van mijn gedrag en straft vanwege het leed dat ik heb veroorzaakt met *mijn* handelen. Uit die eerste straf komt mijn anticipatie voort op de gevolgen van mijn gedragingen voor anderen;[28] die anticipatie geeft betekenis aan mijn gedrag en schept vrijheid om anders te handelen. De straf verleent betekenis aan mijn gedrag *als mijn handelen* en dwingt mij alternatieve gedragingen te overwegen. Het is die overweging die de straf onderscheidt van training, disciplinering, nudging en priming. Ik word niet gedwongen om mij anders

[24] Dit zou dan een voorbeeld zijn van computationele rechtsociologie, zie Helbing (2012).
[25] Dat zou een voorbeeld zijn van sociale strafrechtsfysica, zie Pentland (2014).
[26] De discussie is ook buitengewoon relevant voor de strijd rond *homo economicus* (rationele keuzemodel, speltheorie) en *homo behavioralis* (gedragseconomie, beperkte rationaliteit, 'bias'), een strijd die niet alleen in de economische wetenschap maar ook binnen 'law and economics' speelt, zie noot 9 hierboven. Over de relevantie voor het recht Gigerenzer en Engel (2006).
[27] We onderscheiden gevaarzettings- en krenkingsdelikten.
[28] Voor de strafrechtdogmatiek is dit natuurlijk een gruwel: Nietzsche stelt dat die eerste straf vooraf gaat aan het nemen van verantwoordelijkheid, in flagrante strijd met het legaliteitsbeginsel. Punt is dat het legaliteitsbeginsel het besef van die verantwoordelijkheid vooronderstelt en dat besef moet eerst gevestigd worden. In vergelijkbare zin neurowetenschapper en filosoof Damasio (2011: 280).

te gedragen, maar om mij een voorstelling te maken van andere manieren van doen. We hebben het niet over Pavlov's hond of Pentland's sociale fysica; het gaat niet over gedrag als verklaarbaar en voorspelbaar mechanisme, maar over gedrag dat als handeling betekenis verkrijgt.

Is deze filosofische escapade achterhaald? Moet de *homo digitalis* het doen met het strafrecht als puur reguleringsmechanisme, als poging om potentiele daders te beïnvloeden door straf te bedreigen? Is het beroep op de autonomie van de dader als zelfsturend persoon een sausje om de boodschap te verhullen dat we nu eenmaal allemaal gedetermineerd zijn, hetgeen door middel van computersimulaties en data analytics kan worden aangetoond? In een hoofdstuk waarin hij Charles Taylor bekritiseert vanwege diens karikaturale visie op de natuurwetenschappen, merkt Geertz (2001: 145) op dat 'the idea of a "social physics" seems a quaint fantasy of times gone by'. Hoewel hij daar kennelijk te vroeg heeft gejuicht, is Geertz's pleidooi om geen valse tegenstellingen te creëren tussen natuur- en geesteswetenschappen hier van groot belang. Zijn punt is niet dat er geen onderscheid zou zijn, maar dat het onderscheid niet verabsoluteerd moet worden en dat geen van beiden een monopolie moeten claimen op de juiste methode. Daarbij wijst hij op de diversiteit aan theorievorming en methode *binnen* de natuurwetenschappen, waarvan fervente geesteswetenschappers vaak ten onrechte een gehomogeniseerd beeld schetsen. Met andere woorden, laten we de methodestrijd niet herhalen die in de 19e en 20e eeuw binnen de sociale wetenschappen ontstond in reactie op monopolistische aanspraken vanuit de natuurwetenschappen.[29] Laten Pentland (2014) zijn sociale fysica en Helbing (2012) zijn simulaties van sociale systemen uitproberen.[30] Wij zullen zien wat we ervan kunnen leren. Maar voorkom dat de vooronderstellingen die in dit type methodologie zijn ingebakken ongemerkt het mensbeeld in het strafrecht gaan bepalen. Laat de *homo digitalis* vooral ook een *homo ludens* zijn.[31]

Met betrekking tot de *homo digitalis* beperk ik mij verder tot enkele gedachten die relevant zijn voor *agents* in de context van het strafrecht. Onderzoek naar de eerste mensachtigen doet vermoeden dat (1) de inzet van gereedschappen, (2) gevoel voor causaal verband en (3) het spreken van een taal die tegenwoordig kan stellen wat niet aanwezig is, zich gelijktijdig hebben ontwikkeld (Ambrose 2010, Roby-Brami e.a. 2012). *Homo faber* en *homo sapiens* lijken 'gelijkoorspronkelijk', zoals de Duitsers het zo mooi kunnen zeggen. Hoewel sommige dieren wat voorhanden is in hun omgeving inzetten om een doel te bereiken (een dam te bouwen, een opening te maken) gaan ze er zelden toe over hun gereedschap zelf te maken. En hoewel sommige primaten op aandringen van hun menselijke trainers een aardige woordenschat kunnen bereiken, ontwikkelen zij geen grammatica die tot het benoemen van de verhouding tussen heden, verleden en toekomst leidt en het tegenwoordig stellen mogelijk maakt van wie of wat *voorbij* of *veraf* of zelfs *nog niet* zijn. Het vermogen om te denken (het internaliseren van de gesproken en gehoorde taal) en te weten (in de zin van het opslaan van expliciete kennis in ons geheugen of in externe dragers die het delen van kennis voorbij het hier en nu mogelijk maken) is kenmerkend voor de *homo sapiens.* Dat denkvermogen is intussen hecht verbonden met de *homo faber*, nu juist het fabriceren van dingen die inwerken op de omgeving tot leerprocessen leidt die zonder zulke feedbackmechanismen niet van de grond komen. *Homo faber* vindt technologie uit die haar toestaat zich als *homo sapiens* te heruitvinden. De technologie van het schrift is daarvan de meest evidente uiting;

[29] Ik kom hier in het kader de digitale toerekening van strafrechtelijke aansprakelijkheid nog op terug, zie paragraaf 2.4 hieronder.

[30] Kort gezegd stelt Pentland voor om zeer grote groepen mensen – op vrijwillige basis – te voorzien van smartphones die zijn uitgerust met een veelheid van sensoren, die permanent fysiek en sociaal gedrag opmeten en doormeten. Deze gegevens zouden geaggregeerd en beveiligd worden, waarna onderzoekers vragen kunnen stellen aan de database, die door algoritmische *agents* worden verwerkt. De onderzoeker krijgt geen toegang tot de gegevens, maar wel 'safe answers'. Dit zou volgens Pentland een grote vooruitgang betekenen voor de sociale wetenschappen. Helbing werkt niet met gedragdata maar met software *agents* die op basis van speltheoretische of gedragseconomische instructies met elkaar interacteren. Op basis van dergelijke simulaties probeert hij crises in complexe sociale systemen te voorspellen en te testen welke alternatieven zulke crises kunnen voorkomen.

[31] Dit is geen oproep tot 'gamification', maar een pleidooi voor het inbouwen van speelruimte in onze onli*f*e wereld, bijvoorbeeld door het mogelijk te maken om algoritmische 'waarheden' aan te vechten met behulp van alternatieve algoritmen.

het hangt direct samen met ons vermogen tot abstractie Gleick (2010:37). *Homo ludens* gaat nog een stap verder, door het spel (dat op zich niet specifiek is voor de mens) te integreren met het vermogen om te maken en te denken. Daarbij is het onderscheid tussen 'play' en 'game' van belang (Mead en Morris 1962:153-54). Het eerste is ludieker dan het tweede, speelser en meer experimenteel, de regels worden er nog gaandeweg aangepast. Het tweede veronderstelt dat men in staat is te anticiperen op alle andere spelers (en dus ook op hoe zij zich tot elkaar verhouden). Daarmee gaat het bij 'game' al snel om een spel met regels die bepalen of iets als zodanig geldt: wie de regels van het schaakspel aanpast speelt geen schaak meer, wie haar echtscheiding niet inschrijft in de burgerlijke stand blijft getrouwd voor de wet. Je zou kunnen zeggen dat Wittgenstein's (1992) inzicht in het *taalspel* als constitutief voor onderscheiden levensvormen op de grens van 'game' en 'play' staat. Taal is een spel met harde regels die we niet zonder schade kunnen negeren (dan begrijpt niemand wat we bedoelen); tegelijk wordt taal gemaakt en vermaakt steeds wanneer we haar gebruiken.[32] De regels van een taal zijn robuust maar buigzaam, en juist in taalgebruik dat zich buiten de regels stelt zonder het lijntje te breken, kunnen nieuwe paden worden ontgonnen. Zo kan ook worden geëxperimenteerd met een nieuwe benadering van de werkelijkheid.[33] Huizinga's (2010) *homo ludens* zag op de speelse mens, die zich een leefwereld schept en er tijdelijk in huist, grenzen verkent en verlegt en dan weer een ander spel verzint. Hoe belangrijk het serieuze spel ook mag zijn (bijvoorbeeld het recht als spel dat rechtsgevolg toekent aan ons handelen), de vrijheid van de mens (hoe fragiel en betwist die ook mag zijn) uit zich onder meer in de ruimte die zij neemt en schept om de zaken anders aan te pakken (de *homo faber*) en zich daartoe ook een andere werkelijkheid te denken (de *homo sapiens*). Paradoxaal maar pertinent is dat het recht (als 'game') de harde regels stelt die ruimte maken voor de vrijheid (als 'play').

Hoe nu met de *homo digitalis*? Is dat een verder doorontwikkelde *homo sapiens* (of juist een gedegenereerde versie)? Was de *homo sapiens* misschien een homo *analogus*? Voor dit preadvies gaat het vooral om de *homo digitalis* als verdachte dan wel handhaver van het strafrecht. Als we ervan uitgaan dat mensen worden wie ze zijn in het samenspel met de anderen waar ze op anticiperen, zal de intrede van *agents* gevolgen hebben voor wie wij zijn. Navigeren in de onli*f*e wereld betekent anticiperen op de ingrepen van data-gestuurde (digitale) *agents* en die anticipatie vraagt dat wij inspelen op de logica van machinaal lerende systemen. Het spel wordt dus anders gespeeld en de vraag is of deze systemen wel met zich laten spelen, of dat zij niet anders kunnen dan ons hun versie van de werkelijkheid opleggen. *Agents* opereren op basis van meetbare en doorrekenbare gedragsanalyse, zij nemen ons handelen waar als gedrag, liefst te vangen in probabilistische patronen die voorspelbaarheid genereren, en zo nodig te ondervangen door machinale *nudging* (Thaler en Sunstein 2008) en *priming* (Ariely en Berns 2010). De verdachte als *homo digitalis* zal mogelijk roepen dat zij gedwongen werd zich te *gedragen* zoals zij deed, wanneer de idee dat mensen ter verantwoording worden geroepen voor hun *handelen* als een pijnlijke – zo niet megalomane - misvatting terzijde wordt gesteld. Justitie en politie zullen als *homines digitales* mogelijk antwoorden dat hun eigen gedrag is ingegeven door accurate berekeningen van effectiviteit en efficiency, die mag blijken uit grootschalige simulaties met gedragsdata. Dat alles onder de noemer van 'sociale fysica' (Pentland 2014) of 'computationele sociale wetenschappen' (Helbing 2012).

---

[32] Hier kunnen we natuurlijk naar een stoet van geleerde werken verwijzen, met name de semiologie, de semiotiek en de taalhandelingstheorie. Ik beperk mij tot Ricoeur (1986), die ze op sublieme wijze in zijn (taal)handelingstheorie heeft verwerkt. De kunst is om evenwicht te bewaren tussen handeling en systeem, taalgebruik en –systeem. Over de relatie tussen taal, handeling en leefwereld in de wijsbegeerte van Wittgenstein, Husserl, Heidegger en Merleau-Ponty zie verder Van Brakel (1998) of Gier (1981). Zie ook Mooij (2004) vanwege zijn geniale inzichten in de relatie tussen taal, verlangen, schuld en strafrechtelijke aansprakelijkheid. Empirisch psychologisch onderzoek lijdt vaak aan gebrek aan inzicht in de eigen veronderstellingen, waardoor claims inzake *evidence based* onderzoeksresultaten met een korrel (of kruiwagen) zout moeten worden genomen, zie bijvoorbeeld over het gebrek aan herhaalbaarheid van veel psychologisch onderzoek het rapport van de Open Science Collaboration (2015).

[33] Wat juist niet betekent dat de werkelijkheid om het even hoe kan worden benaderd, wij blijven graag ver van het sociaal-constructivisme van sommige postmodernisten en volgen liever Latour (2005) in zijn idee dat het wetenschappelijk experiment vooronderstelt dat de werkelijkheid weerstand biedt.

Het mag duidelijk zijn dat dit scenario mij niet aanspreekt. De *homo digitalis* die beter aan lijkt te sluiten bij het mensbeeld van het strafrecht in een democratische rechtsstaat neemt kunstmatige intelligentie serieus en begint te 'tinkeren' met de omgeving opdat en totdat die weer een juiste balans toelaat tussen play en game; het blijft dus een *homo faber* en *homo ludens*. Dat sluit aan bij de idee van juridische bescherming by design, bedoeld om de onlife wereld zo te verbouwen dat de *homo digitalis* ook een *homo sapiens* kan blijven. Dat wil zeggen een *agent*/subject in de ethische en juridische zin, die zowel moreel als ook in rechte ter verantwoording kan worden geroepen voor gedragingen die zij (h)er-kent als haar eigen handelen. Dat laatste veronderstelt uiteraard dat de *homines digitales* aan de zijde van de strafrechtelijke wetgever, justitie en politie de rechtshandhaving niet reduceren tot automatische handhaving van de bestaande orde.[34]

2 Materieel strafrecht: straffer en bestrafte als *homo digitalis*

2.1 Introductie: onzichtbare 'remote control'

In deze inleiding eerst een korte uiteenzetting over het verschil tussen 'traditionele' criminaliteit en cybercriminaliteit, met nadruk op interventies van *agents*. Voorbeelden van strafbare interventies via *agents* zijn bijvoorbeeld DDOS aanvallen; botnets die toegang verkrijgen tot wachtwoorden, medische dossiers of vertrouwelijke emails; en ransom aanvallen waarbij de inhoud van de harde schijf wordt versleuteld en alleen tegen betaling van een 'ransom' weer vrij wordt gegeven. In deze gevallen is evident sprake van opzet. Het kan ook gaan om onverwachte of onverhoopte schade of letsel veroorzaakt door onvoorspelbaar gedrag van bona fide *agents*; strafrechtelijke aansprakelijkheid voor opzetdelicten is dan alleen aan de orde wanneer degene die het betreffende systeem heeft ontworpen, ingekocht en/of degene die het gebruikt erop bedacht zou moeten zijn dat het onverwacht gevaarlijk gedrag kan gaan vertonen en vervolgens willens en wetens de aanmerkelijke kans aanvaardt dat een strafbaar gevolg intreedt. Daarnaast kan sprake zijn van een culpoos delict, wanneer sprake is van verwijtbaarheid zonder enigerlei vorm van opzet.

Binnen het materiele strafrecht werd oorspronkelijk op pragmatische gronden onderscheiden tussen drie typen van zogenaamde computercriminaliteit: (1) strafbare feiten gepleegd *met* een computer, (2) *tegen* een computer of informatiesysteem en (3) strafbare feiten gepleegd in een omgeving van computer- of informatie- of telecommunicatiesystemen (Brenner 2007). De eerste twee vallen grotendeels samen met zogenaamde BVD criminaliteit (tegen de beschikbaarheid, vertrouwelijkheid en deugdelijkheid van computer systemen), de derde verwijst naar 'traditionele' criminaliteit, gepleegd met behulp van computer systemen (denk aan identiteitsfraude, bezit en verspreiding van kinderporno, en schending van copyright). Andere indelingen zijn mogelijk. Inmiddels wordt meestal gesproken van cybercriminaliteit (Brenner 2010, Koops 2010, Koops en Goodwin 2014), rekening houdend met de komst van het internet en allerlei applicaties (Apps) daarop – zoals het web en online sociale netwerken.

De ontwikkeling van computer- naar cybercriminaliteit hangt vooral samen met de hierboven aangegeven exponentieel gegroeide connectiviteit tussen computers, computersystemen, personen, diensten en zelfs goederen (denk aan RFID, het Internet van de Dingen en zo meer). Als gevolg daarvan kan het verschil tussen cyber- en 'traditionele' criminaliteit uit het computerloze tijdperk onder de noemer van zes factoren worden samengevat: afstand, schaal, snelheid, distributie, automatisering en onzichtbaarheid. Deze factoren veranderen de samenhang tussen gedrag en gevolg, evenals de voorzienbaarheid en de omvang van de gevolgen en het gemak waarmee schade kan worden veroorzaakt

[34] Over de gevaren van automatische handhaving Brownsword (2008), over reductie van de rechtsorde tot de concrete ordening Schmitt (1993), Hildebrandt (2015b).

op grote afstand zonder noodzakelijkerwijs veel sporen achter te laten. Het mag duidelijk zijn dat precies deze implicaties ook weer grote gevolgen hebben voor de rechtshandhaving (waarover meer in het volgende hoofdstuk).

Afstand Met enige weemoed kijken we terug naar de tijd dat een strafrechtelijk relevante handeling werd omschreven als een 'gewilde spierbeweging', en naar het leerstuk van 'functioneel daderschap' waarmee het gevolg van een handeling verricht door de een aan een ander kan worden toegerekend op basis van de samenwerking tussen beide. Wie een ander opdracht geeft een derde te doden is *doen pleger* voor zover degene die de trekker overhaalt zelf niet strafbaar is, en *medepleger* als de opdrachtnemer zelf ook strafbaar is. De opdrachtgever kan bovendien strafbaar zijn wegens uitlokking. Het oordeel dat sprake is van plegen, doen plegen, medeplegen of uitlokken is altijd een kwestie is van toerekening. De vraag of iemand een strafbaar feit heeft gepleegd volgt niet automatisch uit een fysieke gedraging maar vraagt om kwalificatie van een samenstel en/of samenspel van fysieke gedragingen, uitspraken, afspraken, houdingen en verrichtingen. Dat komt goed van pas als het gaat om cybercrime, want de afstand tussen fysiek gedrag en het strafbare gevolg kan hier extreme vormen aannemen. Niet alleen omdat de dader haar buurman in beginsel om het leven kan brengen via een *agent* die vanuit Verweggistan zijn zorgrobot hackt, maar ook omdat het mogelijk is die aanval te timen en dus ook afstand te creëren in de tijd. De vraag is of dit een fundamenteel verschil maakt, maar zolang we in verschillende jurisdicties leven met verschillende strafbaarstellingen en verschillende prioriteiten bij de handhaving zal dit soort afstand zeker tot problemen leiden. Dit houdt ook verband met de democratische component van de strafbaarstelling, die in beginsel door de wetgever als vertegenwoordiger van de rechtsgenoten binnen de eigen jurisdictie wordt vastgesteld.

Schaal, distributie, snelheid en automatisering. Deze punten laten zich goed illustreren aan de hand van de DDOS aanval. Een denial of service (DOS) aanval stuurt berichten naar de server van het target in de hoop dat de vloed aan berichten tot verstoring van de dienstverlening zal leiden. Een enkelvoudige DOS aanval zou weinig effect hebben en eindeloos herhaald moeten worden om zelfs maar enig effect te hebben. Het is natuurlijk mogelijk om een heleboel vrienden uit te nodigen (of huurlingen aan de andere kant van de wereld te betalen) om op een button te drukken, maar het kan eenvoudiger en effectiever. Men kan software ontwikkelen (of kant en klaar kopen) die binnendringt in andere computersystemen en vanuit die verspreide positie volautomatisch een massief bombardement van berichten naar het target stuurt. Daarmee kan een enkel individu vanaf willekeurige afstand een aanval inzetten op grote schaal, gedistribueerd, razendsnel en geautomatiseerd. Dit noemen we een distributed denial of service (DDOS) aanval. Voor het slachtoffer zal de aanval in eerste instantie bovendien onzichtbaar zijn.

DDOS aanvallen zijn een perfect voorbeeld van de manier waarop de cybernetica kan worden ingezet als handzame methode om de omgeving op sluwe wijze onder controle te krijgen via de inzet van tamelijk domme *agents*. Nu ook cybercriminelen zich gaan bekwamen in ML en DL zal het nog lastiger worden om vat te krijgen op cybercriminaliteit, omdat dat soort *agents* zich op basis van hun 'ervaringen' aan kunnen passen en van tactiek kunnen veranderen. Dat houdt verband met het zesde kenmerk van cybercriminaliteit, te weten de onzichtbaarheid van de betrokken *agents*, waarachter daders zich kunnen verschuilen.

Onzichtbaarheid Fysieke gedragingen zijn zichtbaar voor zover ze in nabijheid van anderen plaatsvinden, of middels CCTV camera's of drones worden opgenomen. Of een fysieke gedraging gekwalificeerd kan worden als deel uitmakend van een strafbare handeling hangt van velerlei factoren af. Het is zeker niet zo dat voor de komst van de computer strafbare feiten altijd in het volle zicht werden gepleegd of als zodanig herkend. Neem het onderscheid tussen heterdaad en niet-heterdaad; vaak worden heimelijk verrichte misdrijven als ernstiger aantasting van de rechtsorde gezien en dus zwaarder bestraft. Cybercriminaliteit beweegt zich echter in een leefwereld die in toenemende mate wordt bepaald door een computationele achterkant die voor de 'gebruiker' of liever 'bewoner' van die onli*f*e wereld niet gemakkelijk kenbaar is. Dat heeft te maken met bedrijfsgeheimen en intellectuele rechten op software, maar ook los daarvan is de architectuur of grammatica van die achterkant lastig te doorgronden. Zelfs al zou iemand de algoritmes aanreiken en verklaren, dan zouden we daar waarschijnlijk vooral moe van worden, zonder dat duidelijk is hoe die algoritmes onze onli*f*e wereld

configureren. Dat maakt cybercriminaliteit bij uitstek ondoorzichtig en onbegrijpelijk. Wie haar voordeur niet op slot draait mag niet verbaasd staan als ze wordt bestolen, we kunnen ons onmiddellijk een voorstelling maken van de dief die binnentreedt en waardevolle spullen meeneemt. Bij diefstal van wachtwoorden en identiteitsfraude is het al veel moeilijker te achterhalen wat er nu precies gebeurt en hoe we dat het beste kunnen voorkomen. Wanneer ML en DL hun intrede doen bij het fabriceren van kant-en-klare malware zal het echter nog veel lastiger worden om te doorzien tegen welke aanvallen of systeembreuken we ons moeten beschermen.

De onli*f*e wereld ziet op een wereld waarin het onderscheid tussen online en offline steeds kunstmatiger wordt, en waarin deze zes factoren eigenlijk over de hele linie meespelen. Strafbare interventies via data-gestuurde intelligentie roepen aldus nieuwe problemen op rond daderschap, causaliteit, wederrechtelijkheid en schuld.

2.2 De *agent* als rechtsubject?

Onder huidig recht kan een *agent* niet worden aangemerkt als een rechtssubject; het kan uitsluitend object zijn van rechten. Juridisch-technisch is het niet meer en niet minder dan een instrument waarvan een dader zich bedient of waarvoor zij verantwoordelijk is. Zo kan zij bijvoorbeeld als hoteleigenaar een domotica systeem beheren dat onvoldoende is beveiligd en wordt gehackt met desastreuze gevolgen: diefstal van eigendommen omdat anderen toegang hebben tot de kamers, ontregeling van de warmwatervoorziening waardoor gasten brandwonden oplopen. In beginsel lijkt dat niet revolutionair, nu ernstig letsel sinds jaar en dag door allerlei technologie wordt veroorzaakt (denk aan auto's, treinen, vliegtuigen en allerhande elektrische en elektronische apparatuur). Verkeerd gebruik, verzuimd onderhoud, onverwachte samenloop van omstandigheden, bezuiniging op fabricage, en onjuiste of onvoldoende uitleg kunnen stuk voor stuk leiden tot schade of letsel en in een beperkt aantal gevallen zal dat naast privaatrechtelijke aansprakelijkheid aanleiding zijn voor strafvervolging. Ook doleuze delicten zullen vaak gepleegd worden met gebruik van technologie, bijvoorbeeld een mes, vuurwapen, gif of explosieven. Kortom, de inzet van apparaten en systemen kan al dan niet opzettelijk schade of letsel veroorzaken waarvoor enigerlei rechtssubject strafrechtelijk aansprakelijk is. Data-gestuurde *agents* onderscheiden zich echter van andere instrumenten doordat zij niet alleen instrument zijn maar daarnaast in staat zijn om op grond van hun leervermogen zelfstandig in te grijpen, hun gedrag te veranderen en daarbij rekening te houden met de manier waarop het mogelijke slachtoffer zich gedraagt. Daarmee dringt de vergelijking met een dier zich op, dat zoals dat zo mooi heet 'een eigen energie heeft' die in het privaatrecht tot risicoaansprakelijkheid leidt.[35] Strafrechtelijk is dat laatste niet aan de orde, nu daar behalve vervulling van de bestanddelen van een delictsomschrijving en wederrechtelijkheid altijd sprake moet zijn van verwijtbaar handelen (inclusief eventueel nalaten) van het rechtssubject. Het OM zal dus moeten aantonen dat de eigenaar of houder van een dier met opzet of in ieder geval verwijtbaar heeft gehandeld, bijvoorbeeld door het dier geen muilkorf te laten dragen, een hek niet te repareren of een giftige slang zonder toezicht buiten de kooi te laten. Hoewel wij niet precies kunnen voorzien hoe en wanneer een dier derden in gevaar zou kunnen brengen of verwonden, hebben we wel voldoende zicht op hoe de dieren die we 'houden' zich in het algemeen gedragen en wat van de houder verwacht mag worden om letsel of schade te voorkomen.
Dat ligt bij *agents* anders. Enerzijds omdat het ontwerp en de inzet van *agents* relatief nieuw en volop in ontwikkeling zijn, anderzijds omdat zij een aantal eigenschappen hebben waaraan wij niet gewend zijn, noch bij onze apparaten en machines, noch bij dieren en mensen. Het gaat daarbij om de bovengenoemde punten, te weten afstand, schaal, snelheid, distributie, automatisering, en onzichtbaarheid. Ik leid daar nog twee opvolgende punten uit af, die het bijzonder lastig maken om het gedrag van *agents* en de implicaties daarvan te voorzien: hun mobiliteit en polymorfe hoedanigheid.

[35] Zie omtrent de vraag of we *agents* rechtssubjectiviteit zouden moeten toekennen Teubner (2007), Solum (1992), Chopra en White (2011), Pagallo (2013), Karnow (1997). Het gaat daarbij vooral om privaatrechtelijke aansprakelijkheid, waarbij zowel de vergelijking met dieren als die met de slaaf in het Romeinse recht regelmatig terugkeren. Meer specifiek over het strafrecht Hildebrandt (2005, 2008, 2011), Gless en Weigend (2014).

Karnow (1997) voorzag eind vorige eeuw al dat *agents* vaak over verschillende servers gedistribueerd zijn (denk ook aan cloud computing) en zich snel en voortdurend verplaatsen in functie van hun taken, waarbij ze dankzij hun vermogen om te leren bovendien in staat zijn hun eigen systeem opnieuw te configureren waardoor ook hun waarneembare vorm kan veranderen. Malware wordt niet voor niets betiteld als virus, worm of Trojaans paard. De combinatie van remote control, schaalvergroting, snelheid, decentrale opslag, automatisering, onzichtbaarheid, mobiliteit en morfologische veranderlijkheid kan het bijzonder lastig maken om een *agent* als zodanig te identificeren, blijvend te traceren en te adresseren. Karnow stelt dan ook de vraag of hier nog wel sprake is van een herkenbare eenheid die het mogelijk maakt een agent als oorzaak van wat voor gevolg ook te identificeren, nog los van de vraag of de *agent* als instrument of subject wordt gekwalificeerd.

In dat kader is het nuttig om een zijstap te maken naar de idee van *moral agency*. Vanwege de eis van verwijtbaarheid lijkt *moral agency* een mogelijkheidsvoorwaarde te zijn voor rechtssubjectiviteit binnen het domein van het strafrecht, ook al vallen beide zeker niet samen. Rechtssubjectiviteit wordt toegekend door het positieve recht, het is geen van nature gegeven categorie maar een kunstmatige constructie, die het toekennen van rechten en plichten mogelijk maakt. Morele subjectiviteit is evenmin een natuurlijk gegeven, maar staat los van juridische attributie en heeft op zichzelf genomen geen rechtsgevolg. In zijn bespreking van kunstmatige *agents* stelt informatiefilosoof en –ethicus Floridi, in navolging van Aristoteles, de idee van een *moral agent* tegenover die van een *moral patient*.[36] Terwijl de *agent* de relatief interactieve, autonome en adaptieve entiteit is die actief ingrijpt en daarmee bijvoorbeeld nadeel (schade of letsel) veroorzaakt, is de *patient* de entititeit die het gevolg van die ingrepen ondergaat en aldus schade of letsel bekomt. Floridi abstraheert daarbij van de aanwezigheid van een innerlijk bewustzijn; zijn *agents* kunnen heel wel geestloze entiteiten zijn die desondanks het vermogen hebben om 'kwaad' te doen door het beschadigen van *patients*. Ook een *patient* is bij Floridi niet noodzakelijk een met gevoel uitgerust wezen; het is minstens een identificeerbare entiteit met een zekere complexiteit die in staat is te reageren op de ingrepen van de *agent*. Floridi wijst erop dat onder invloed van milieuprotagonisten de categorie van morele *patients* enorm is uitgebreid (van dieren en planten tot hele ecosystemen), terwijl de categorie van morele *agents* afhankelijk blijft van vrije wilsvorming en intenties. Tegelijkertijd is de invloed van kunstmatige systemen die zich als geestloze *agents* gedragen exponentieel toe aan het nemen, waarbij – geheel los van intenties of bewustzijn – het vermogen van deze *agents* om nadeel, schade, leed of letsel toe te brengen aan levende maar ook aan waardevolle niet-levende systemen evenredig toeneemt. Hij beargumenteert dat het erkennen van de morele relevantie van het gedrag van deze *agents* pertinent is, willen wij tot een redelijke en ook veilige omgang met kunstmatige agenten komen. Daarbij spreekt hij zelf van moreel gedrag, waar ik toch graag van moreel relevant gedrag zou blijven spreken, vasthoudend aan de idee dat de kwalificatie 'moreel' tenminste een handelende *agent* eist die tot oordeelsvorming in staat is. Interessant is dat Floridi bepleit dat ook vernietiging van of schade aan een niet-levende entititeit door een niet-menselijke *agent* moreel relevant is en moet worden afgewezen en indien mogelijk voorkomen – voor zover mogelijk. Floridi lijkt te claimen dat ook wanneer het niet mogelijk was om zoiets te voorkomen toch sprake is van moreel kwaad, puur en alleen vanwege de vernietiging of beschadiging van een *patient*.

Ik zou twee dingen op het netvlies willen houden. Ten eerste vraagt de onli*f*e wereld erkenning van de ingrijpende invloed van *agents*, gezien de desastreuze gevolgen voor onze leefwereld in de brede zin van *agent*-gedrag dat tot vernietiging van of schade aan die leefwereld leidt. Dit heeft direct te maken met onze exponentieel toenemende afhankelijkheid van *agents*, die de onli*f*e wereld configureren en bevolken. Ten tweede moet helder zijn dat het strafrechtelijk aansprakelijk stellen van geestloze *agents* onzinnig is zolang het strafrecht is geënt op wederrechtelijkheid en schuld en daarmee op het zelfbewustzijn dat reflectie en betekenisvolle anticipatie mogelijk maken. Wij zullen ons dus moeten bezinnen op de rol van *agents* binnen het strafrecht, nu zij noch met mensen, noch met levenloze dingen, noch met dieren gelijk kunnen worden gesteld maar zich wel degelijk *gedragen* op een wijze die strafbare gevolgen kan veroorzaken.

[36] Zie Floridi en Sanders (2001, 2004), Hildebrandt (2011b, 2015a).

2.3 Daderschap, wederrechtelijkheid, causaliteit en schuld

De doctrine van het materiele strafrecht in Nederland gaat uit van de leer van het strafbare feit, die de voorwaarden voor strafbaarheid bevat.[37] Voor strafbaarheid is vereist: (1) een handeling, die kan bestaan uit een niet-handelen waar dat wel geboden was; die (2) valt onder de delictsomschrijving en dus gekwalificeerd kan worden als een strafbaar feit; die (3) wederrechtelijk is en waarvoor geen rechtvaardigingsgrond kan worden aangewezen; en die, tenslotte, (4) aan schuld te wijten is, bij gebreke van een schulduitsluitingsgrond. Wanneer in de delictsomschrijving het woord 'wederrechtelijk' of de zinsnede 'aan schuld te wijten' (of terminologie van gelijke strekking) is opgenomen moet dit worden bewezen, anders volgt uit het voldoen aan de delictsomschrijving in beginsel dat het handelen onrechtmatig en/of verwijtbaar is. Alleen wanneer een verweer wordt gevoerd (maar nu bevinden we ons in het formeel strafrecht, art. 350 WSv en verder), moet de rechter naar aanleiding daarvan zelfstandig vaststellen dat sprake is van wederrechtelijk en/of verwijtbaar handelen.

In dit preadvies gaat het met name om de vraag in hoeverre strafrechtelijke aansprakelijkheid voor gedragingen van *agents* aan een natuurlijk of rechtspersoon kunnen worden toegerekend, in viervoudige zin: (1) kan het gedrag van een *agent* als handeling van een rechtssubject aan het rechtssubject worden toegerekend en valt het onder een delictsomschrijving? (daderschap en kwalificatie), (2) kan het strafrechtelijk relevante gevolg aan het gedrag van een *agent* worden toegerekend? (causaliteit), (3) welke rol speelt het gedrag van *agents* bij het vaststellen van de wederrechtelijkheid en de onrechtmatigheid? (met name bij een beroep op noodweer of noodtoestand) en, (4) kan de schuld aan de dader worden toegerekend wanneer het betreffende rechtssubject geen weet had van de gedraging van de *agent(s)* en/of geen zicht had op de mogelijke verwerkelijking van een strafbaar gevolg (hier gaat het vooral om de ex ante voorzienbaarheid)?

De eerste vraag is of het *gedrag* van een *agent* als *handeling* aan een rechtssubject kan worden toegerekend en of het onder een delictsomschrijving valt. Met andere woorden, is sprake van daderschap en kan de handeling worden gekwalificeerd als een strafbaar feit? Normaliter is dat deels een feitelijke en deels een rechtsvraag, nu het gaat om de constellatie van feiten en omstandigheden die mede bepalen of het ontwikkelen, verkopen of gebruiken van een gereedschap, apparaat of systeem in een specifiek geval heeft te gelden als hetgeen in de diverse bestanddelen van de delictsomschrijving wordt beschreven. Het zal dus afhangen van allerlei factoren, waarbij het strafrechtelijk analogieverbod en prudentie ten aanzien van extensieve interpretatie van belang zijn (het binnendringen van een computer door een *agent* is geen huisvredebreuk en kan door de rechter niet naar analogie als computervredebreuk worden gekwalificeerd; daarvoor is wetgeving nodig).[38] Interessant is dat het hier uiteindelijk gaat om de vraag of het gedrag van een *agent* mag gelden als onderdeel van het handelen van een rechtssubject. Kennelijk moet aan het gedrag van de agent betekenis worden verleend die het mogelijk maakt de verbinding te leggen met een handeling – en die betekenis wordt in laatste instantie niet door het rechtssubject verleend, maar door het recht en uiteindelijk door de spreekbuis van het recht, de rechter. Als *agents* rechtspersoonlijkheid zouden hebben, zou hun opdrachtgever als doen-pleger kunnen worden vervolgd, nu doen-plegen ziet op een strafrechtelijke figuur waarbij degene die de strafbare gedraging uitvoert zelf niet strafbaar is, bijvoorbeeld vanwege dwang, minderjarigheid of een strafuitsluitingsgrond. Indien de wetgever zou besluiten dat *agents* rechtssubject kunnen zijn en onder bepaalde voorwaarden ook strafbaar, zouden zij als medeplegers kunnen gelden, uitgelokt door een natuurlijk persoon of andere rechtspersoon of zelfs omgekeerd (de *agent* verleidt natuurlijke personen

[37] De leer is overgenomen uit de Duitse doctrine en met name ten aanzien van de elementen wederrechtelijkheid en schuld lastig om te zetten naar Anglo-Amerikaanse doctrine (die onderscheidt een 'wrongful act' (*actus reus),* en het mentale element (*mens rea*). Mens rea ziet zonder meer op verwijtbaarheid, maar het verweer 'excuse' lijkt zowel op wederrechtelijk als op schuld te kunnen zien.

[38] Zie MvT Computercriminaliteit I, Kamerstukken II 1989-1990, 21551, nr. 3, t.a.v. de invoering van art. 138a (computervredebreuk) p. 15-17. Inmiddels vernummerd tot 138ab Sr.

of rechtspersonen door te wijzen op gedragingen die een gewenst gevolg hebben ook al zijn ze strafrechtelijk verboden). Positiefrechtelijk is dit vooralsnog onzin want de agent is geen rechtssubject, maar het gedachtenexperiment is juridisch wel relevant. Het zou goed zijn eens na te denken in hoeverre nieuwe deelnemingsvormen ontwikkeld kunnen worden die rechtssubjecten als dader kwalificeren op basis van de specifieke relatie met een *agent* wiens gedrag de bestanddelen van een delictsomschrijving vervult (afgezien van eventuele wederrechtelijkheid en schuld). Een ander belangrijk punt betreft de specifieke voorwaarden van doleuze dan wel culpoze delicten. Wanneer kan het kleurloos opzet van een *agent* aan de dader worden toegerekend,[39] hoe ver mag het leerstuk van voorwaardelijk opzet worden opgerekt bij opzet op de wederrechtelijkheid en hoe verhoudt het bestanddeel 'aan schuld te wijten' zich tot het gedrag van de *agent* en de kennis van de dader? Kleurloos opzet en onbewuste schuld lijken hier op het lijf geschreven van de geestloze *agents*. Het doet er niet toe wat de bedoeling was en of de *agent* zich ergens van bewust was, het gedrag heeft in het maatschappelijk verkeer als opzet dan wel schuld te gelden. Althans, ten aanzien van de dader. Dat de *agent* geen bedoelingen had en geen schuldbewustzijn is dan niet relevant; het gaat erom dat ook in het reguliere commune strafrecht sprake kan zijn van kleurloos opzet en onbewuste schuld die tot strafbaarheid leiden.[40]

De tweede vraag was of het strafrechtelijk relevante gevolg aan het gedrag van een *agent* kan worden toegerekend. Hier gaat het om de causaliteit in geval van een materieel omschreven delict. Uitgaande van het feit dat het gedrag van de *agent* aan de dader kan worden toegerekend is de vraag of hier sprake is van causaal verband tussen het handelen van de dader en het ingetreden strafbare gevolg. Causaliteit wordt in beginsel toegerekend op basis van conditio sine qua non, maar in geval van dubbele causaliteit (meerdere handelingen kunnen ieder voor zich als oorzaak van het strafbare gevolg worden aangewezen), alternatieve causaliteit (een van meerdere handelingen heeft als oorzaak te gelden, maar onduidelijk is welke), of eigen schuld (het gevolg was niet ingetreden als het slachtoffer niet causaal had bijgedragen), wordt ook naar andere factoren gekeken. Daar komt bij dat de conditio sine qua non een te groot net over de werkelijkheid gooit nu bijvoorbeeld ook de geboorte van het slachtoffer als conditio sine qua non kan worden aangemerkt. Dit wordt enigszins ondervangen door de leer van de causa proximus, die de aandacht richt op de – in tijd en ruimte - meest nabije oorzaak. Zo kennen we ook nog de nova causa interveniens (niet toe te rekenen aan de dader) die de causale keten doorbreekt (hoewel het strafbare gevolg mogelijk had kunnen optreden zonder deze interventie moet worden aangenomen dat de interventie de meest voor de hand liggende oorzaak is, die de eerdere als het ware uitwist). Tenslotte kan het zijn dat een handeling moet worden aangemerkt als conditio sine qua non, terwijl het gevolg voor de veroorzaker niet of nauwelijks voorzienbaar was. Hoewel de voorzienbaarheid pas aan de orde komt bij de vraag naar de verwijtbaarheid, kan die desondanks meespelen bij de causaliteitsvraag, met name bij culpose gevolgsdelicten (bijvoorbeeld dood door schuld). Wanneer *agents* worden ingezet met het doel een delict te plegen, zal wanneer het strafbare gevolg intreedt toerekening van causaal verband meestal geen probleem zijn (hooguit een bewijsprobleem dat wordt veroorzaakt door de hierboven genoemde onzichtbaarheid van cybercriminaliteit en door de snelheid waarmee sporen kunnen worden uitgewist). Wanneer *agent*gedrag zonder opzet leidt tot strafbare gevolgen ligt dat anders, met name in geval van culpoze delicten. Hier worden we geconfronteerd met het feit dat ML gebaseerd is op probabilistische aannamen, die werken met foutmarges en – in geval van distributieve profielen – met profielen die wellicht helemaal niet van toepassing zijn op het voorliggende geval.[41] Meestal is er een trade-off tussen de foutmarges voor fout-positieven en fout-negatieven. Het instellen van de drempel waaronder de *agent* moet blijven lijkt een relevante eis die al bij de causaliteitsvraag getoetst moet worden: welk

[39] Kleurloos opzet betekent opzet op het strafbare gevolg, niet op de wederrechtelijkheid daarvan.

[40] Mij dunkt dat de theorie van Chopra en White (2011) hier van pas kan komen. Zij richten zich voornamelijk op de privaatrechtelijke aansprakelijkheid van *agents* zelf. In de context van het strafrecht gaat het erom of bepaalde kennis bij de ontwikkelaar, verkoper en/of gebruiker van een *agent* verondersteld mag worden, zodat zij strafrechtelijk aansprakelijk kan worden gesteld als dader met kleurloos opzet of onbewuste schuld.

[41] Over non-distributieve profielen zie Vedder (1999), Custers (2004), Hildebrandt (2008b). Probleem is dat probabilistische modellen die personen matchen met een profiel dat gemiddeld genomen van toepassing is (dus op geaggregeerd niveau), niet noodzakelijk klopt op individueel niveau.

voorzienbaar risico nam de dader, gezien de inzet van de *agent*? Gezien de potentieel desastreuze gevolgen van op elkaar inwerkende *agents* en de complexe keten van oorzaken die daarmee – ingevolge het netwerkeffect – gegeven is, lijkt de vaststelling van causaliteit zowel ex ante (door de ontwikkelaar, verkoper of gebruiker van de *agent*s) als ex post (door de rechter) een Herculeaanse opdracht.

De derde vraag was welke rol het gedrag van *agents* speelt bij het vaststellen van de wederrechtelijkheid (als bestanddeel van een delictsomschrijving) en de onrechtmatigheid (als element van het strafbare feit), met bijzondere aandacht voor het beroep op noodweer of noodtoestand. Wanneer de wederrechtelijkheid is opgenomen in de delictsomschrijving gaat het meestal om handelen zonder toestemming of andere juridische grondslag. Zo valt het gebruik van penetratiesoftware waarmee de security van een systeem kan worden getest in beginsel onder art. 138ab WvSr (hacking), ware het niet dat de eis van wederrechtelijkheid deel uitmaakt van de delictsomschrijving. In gelijke zin zal een wettelijke bevoegdheid voor het op afstand binnendringen van computersystemen voor politieagenten de wederrechtelijkheid wegnemen. Ten aanzien van *agents* is dan bijvoorbeeld de vraag van belang wanneer het gebruik van bepaalde *agents* toestemming impliceert om bepaalde formeel omschreven delicten te plegen. Als ik applicaties gebruik die mijn computer binnendringen om daar gegevens te kopiëren op basis van toestemming zal het niet eenvoudig zijn om tot veroordeling wegens hacking te komen. Het zou overigens interessant kunnen zijn om eens een proefproces te voeren wanneer duidelijk is dat de gegevens voor een ander – niet verenigbaar – doel worden gebruikt, waarvoor dan ook geen toestemming is gegeven. In dat geval kan – lijkt mij - wel degelijk sprake zijn van schending van art. 138ab lid 1 Sv.[42]

Kan de inzet van een *agent* die een strafbaar gevolg veroorzaakt gerechtvaardigd worden op basis van noodtoestand? Denk aan het inschakelen van een automatische piloot op het moment dat het systeem aangeeft dat de piloot het 'roer' moet overnemen. Het is goed denkbaar dat de piloot zich niet in staat acht het toestel onder controle te krijgen, en moet kiezen uit twee kwaden. Dat kan echter bijzonder gevaarlijk zijn, zie mijn beschrijving in ander werk (Hildebrandt 2011a). Het is niet ondenkbaar dat een onli*f*e wereld mensen bij herhaling voor de keuze stelt om hetzij de ene hetzij de andere *agent* (of nog een derde of vierde *agent*) in te schakelen, hetzij zelf in te grijpen (waarbij dat laatste vaak behoorlijk risicovol zal zijn). In dat kader kan zich ook de situatie voordoen dat personen zich moeten verweren tegen *agents* die zich gedragen op een manier die onmiddellijk gevaarlijk is 'voor eigen of eens anders lijf, eerbaarheid of goed'. Ik heb de eerbaarheid niet uit het rijtje weggelaten, want ik zou de mogelijkheid van verkrachting door bijvoorbeeld een avatar of zorgrobot niet op voorhand willen uitsluiten. Vergelijk de virtuele verkrachting,[43] die juridisch interessante vragen oproept inzake wat hier nog onder noodweer zou kunnen vallen (gebruik van software die het systeem van de provider plat legt als enige effectieve mogelijkheid om de aanranding te voorkomen?).

De vierde vraag was of de schuld aan de dader kan worden toegerekend wanneer het betreffende rechtssubject geen weet had van de gedraging van de *agent(s)* en/of geen zicht had op de mogelijke

[42] Maar zie Gerechtshof Den Haag, 15 november 2002, ECLI:NL:GHSGR:2002:AF0684. In r.o. 5 stelt het hof vast dat '[g]een sprake [is] van 138a Sr ("computervredebreuk"). (…) De getuige heeft immers geen beveiliging doorbroken en is evenmin door een bijzondere technische ingreep binnengedrongen in de computer van de verdachte.' In TK 1989-1990 nr. 21551 nr. 3 (de MvT bij de Wet Computercriminaliteit) p. 15 meent de Minister echter: 'Het [artikel 138 Sr] beschermt degeen die blijkens feitelijke beveiliging heeft duidelijk gemaakt dat hij zijn gegevens heeft willen afschermen tegen nieuwsgierige blikken.' Daarmee lijkt de eis dat sprake is van beveiliging een indicatie te zijn van ontbrekende toestemming. Sinds 2006 is die eis weliswaar vervallen, maar geldt het installeren van beveiliging nog steeds als teken dat geen toestemming bestaat voor binnendringen. In lijn daarmee moet duidelijk zijn dat wie toestemming geeft voor de verwerking van persoonsgegevens voor een specifiek doel dat dus niet doet voor een ander, incompatibel doel; dit zou dan ook kwalificeren als wederrechtelijk binnendringen.

[43] Materieelrechtelijk is de vraag interessant of virtuele verkrachting (van een avatar door een avatar) strafbaar moet worden geacht onder de huidige wetgeving en – indien dat niet het geval is – aparte strafbaarstelling behoeft, zie Strikwerda (2014) die dat laatste bepleit en daarbij voorop stelt dat sprake moet zijn van gevolgen in de niet-virtuele wereld. Zij beschrijft de effecten op de 'gebruiker' van de avatar, die tonen dat daadwerkelijk leed wordt veroorzaakt. Over de relatie tussen online gamers en 'hun' avatar ook Ganesh (2013).

verwerkelijking van een strafbaar gevolg. Meer concreet is de vraag of we mogen eisen dat het rechtssubject vanwege de onkenbaarheid of de onvoorspelbaarheid van bepaalde *agents* van gebruik afziet. Dit hangt samen met het feit dat ML *agents* mogelijk maakt die problemen oplossen die de ontwerper zelf niet kon voorzien. ML 'denkt' niet in deterministische algoritmes waar vooraf alle denkbare scenario's moeten worden ingeprogrammeerd, maar in systemen die leren vergelijkbare problemen zelfstandig op te lossen, al dan niet op basis van instructies (gecontroleerd leren). Bij gecontroleerd lerende *agents* kan de gebruiker worden verweten dat zij de algoritmes niet goed heeft getraind, zoals de eigenaar van een hond die het bijten niet afleert. Wanneer het gaat om complexe systemen die in voortdurend gesprek zijn met andere complexe systemen, wordt deze eis een hachelijke zaak. Daarom niet minder pertinent, want indien het inderdaad vrijwel onmogelijk is om systeembreuken of onverwacht gevaarlijk gedrag uit te sluiten doemt de vraag op of het maatschappelijk wel verantwoord is onszelf van afhankelijk te maken van dergelijke systemen. Nog lastiger wordt het als we kijken naar ongecontroleerd lerende systemen, zoals DL. Daarbij wordt de onvoorspelbaarheid zelf onvoorspelbaar en dat is – hoe vreemd dat ook moge klinken – nu juist ook het voordeel van dit type intelligentie. Maar ieder voordeel heeft zijn nadeel. Bij DL wordt de vraag of het geen tijd wordt de *agent* zelf aan te spreken wel heel prangend. Maar dat zal dan alleen privaatrechtelijk interessant zijn, nu ook DL *agents* geen bewustzijn, laat staan zelfbewustzijn hebben.

Gless en Weigend (2014:565-6, 590-1) suggereren dat we misschien moeten accepteren dat de voordelen van het op grote schaal gebruiken van dit soort technologie opwegen tegen het feit dat we in veel gevallen geen strafbare handeling aan een rechtssubject kunnen toerekenen, dan wel in de knoop komen bij de causaliteit, de wederrechtelijkheid/onrechtmatigheid of de schuld. Dit zou dan met name opgaan voor zelflerende systemen, die zowel onvoorspelbaar als – juist daarom - bijzonder nuttig kunnen zijn. Zij stellen voor de zorgplicht in te perken vanwege het ontwikkelingsrisico en/of een rechtvaardigingsgrond in te voeren onder de noemer van 'sociaal-adequate inzet' van *agents* (idem:591). De vergelijking met verkeersstrafrecht dringt zich op. Ook daar accepteren we schade en letsel vanwege het veronderstelde maatschappelijke nut van de auto, en beperken de strafbaarheid van de eindgebruiker (de automobilist) tot hetgeen voorzienbaar en vermijdbaar was, terwijl vage normen zoals die van art. 5 WVW de weggebruiker aanmanen om zowel soepel als vlot en veilig te anticiperen op andere weggebruikers.[44] Het zou kunnen dat de zelfrijdende auto veel van die problemen oplost en tegelijkertijd een heel nieuw type problemen met zich meebrengt. Misschien een nieuw artikel invoeren in het commune strafrecht:[45]

> Met hechtenis van maximaal x maanden of een boete van de ye categorie wordt gestraft 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.

[44] Art. 5 WVW: 'Het is een ieder verboden zich zodanig te gedragen dat gevaar op de weg wordt veroorzaakt of kan worden veroorzaakt of dat het verkeer op de weg wordt gehinderd of kan worden gehinderd.' Overtreding is strafbaar gesteld in art. 177 WVW. Het gaat om een overtreding, niet om een misdrijf (art. 178 WVW). Uiteraard kan het veroorzaken van dood of ernstig letsel door schuld in het verkeer op basis van het commune delict worden vervolgd (art. 307, 308 Sr).

[45] Ik ga ervan uit dat de lezer voldoende ironisch is onderlegd om in te schatten dat de problemen hiermee niet zijn opgelost. Interessant is desondanks het feit dat art. 179 lid 2 WVW de mogelijkheid opent een bijkomende straf op te leggen: ontzegging van de rijbevoegdheid. Het zou niet verkeerd zijn natuurlijke personen of juist rechtspersonen naar aanleiding van overtreding de bevoegdheid te ontzeggen nog langer gebruik te maken van *agents*.

2.4 Data-gestuurde toerekening

De inzet van data-gestuurde intelligentie aan de zijde van politie en justitie komt uiteraard aan de orde onder het kopje formeel strafrecht, bij de bespreking van *police intelligence*.[46] Het vermogen om correlatieve patronen te detecteren die biometrische, locatie, surf en vooral ook sociale media datapunten verbinden met gewelddadig gedrag, pedofilie of fraude in de sociale zekerheid en belastingen roept echter ook vragen op omtrent strafrechtelijke aansprakelijkheid. Het is van cruciaal belang om de uitbreiding van strafbaarheid in het vizier te krijgen waartoe predictieve data analyse kan uitlokken. Het gaat dan met name om de rol van profielen die worden verkregen bij smart policing, fenomeenonderzoek, grootschalig onderzoek van informatiesystemen, en bij de koppeling van allerlei gegevensbestanden uit de publieke en private sector.

Kunnen we er wel zeker van zijn dat we als samenleving weerstand gaan bieden aan de verleiding om punitieve maatregelen op te leggen aan degenen wiens datapunten matchen met gewelddadig of frauduleus gedrag? Het feit dat de strafrechtelijke dogmatiek, de wet, de Grondwet en mensenrechtenverdragen dit niet toestaan vormt een belangrijke hindernis, maar het zou een gevaarlijke illusie zijn te menen dat de huidige betekenis van de straf niet radicaal kan veranderen onder druk van vermeende inzichten uit de neurowetenschappen, de gedragseconomie, de sociale fysica en de computationele sociologie.

Het zou zomaar kunnen dat het voorkomen van ongewenst gedrag een daad van goedertierenheid wordt die op enig moment onder de noemer van de humanisering van de straf aanvaardbaar wordt als een nieuwe vorm van anticiperend straffen (pre-crime punishment). *La Defense Sociale revisited*.[47] Juist dan is van belang dat juristen zich emanciperen van de mechanistische en probabilistische narratieven die delen van de sociale wetenschappen in de greep houden.[48] Met name vanuit de bestuurskunde, de rechtssociologie en de criminologie mag nog wel eens gesuggereerd worden dat rechten geen wetenschap is en dat de rechtsgeleerdheid zich nu eindelijk eens moet bekeren tot de enig zaligmakende methode van de empirische sociale wetenschappen (op gemankeerde wijze gekopieerd van 'de' natuurwetenschappen).[49] Het gaat dan meestal om methodologieën die geënt zijn op het zogenaamde methodologisch individualisme, dat *homo sapiens* reduceert tot een rationalistisch beslismechanisme dan wel tot een *homo behavioralis* die kan worden aangestuurd dank zij kennis van haar neiging tot irrationeel gedrag. *Der Methodenstreit revisited*.[50]

---

[46] Nederlandse vertaling met 'politie intelligentie' is niet gebruikelijk, het kan bovendien worden uitgelegd als een inschatting van de gemiddelde intelligentie van politieagenten. Vertaling met 'inlichtingen' of de 'vergaring' daarvan stamt uit een vorig tijdperk en zag ook toen over het hoofd dat het gaat om het detecteren van relevante verbanden. Over smart policing, police intelligence enzomeer Bob Hoogenboom (2009).

[47] *La Defense Sociale* was een stroming binnen de strafrechtswetenschappen rond het begin van de 20e eeuw, die de functie van de straf terugbracht tot 'sociaal verweer' tegen sociaal onwenselijk gedrag en ertoe neigde het strafrecht om te vormen tot een sociale wetenschap, cf. de grondleggers Ancel (1981), Van Hamel (1907); zie de analyse in Foqué en 't Hart (1990: hoofdstuk 7).

[48] Of, 'positivistische' narratieven, cf. Wendt (2015).

[49] Van Delft (2003), De Geest (2004), zie verder het uitstekende vakblad *Law and Method*, <http://www.bjutijdschriften.nl/tijdschrift/lawandmethod/detail>.

[50] De methodestrijd tussen de natuurwetenschappen en de geesteswetenschappen barstte los in de 19e eeuw, waarbij de geesteswetenschappen een eigen positie en methode claimden. De idee was dat natuurwetenschappen streven naar verklaringen (causaliteit), terwijl de geesteswetenschappen gericht zijn op begrip (betekenis), cf. Leezenberg en De Vries (2012). In de 20e eeuw deed zich een hernieuwde strijd voor, nu met name binnen de sociale wetenschappen die bang waren de status van wetenschap te verliezen als zij de methoden en technieken van de natuurwetenschappen niet overnamen, cf. Schuyt (1986). Over de relativering van de tegenstelling de reeds aangehaalde Geertz (2001) en bijvoorbeeld ook Prigogine en Stengers (1984), die op basis van de transformaties van de natuurwetenschappen zelf het positivistische beeld van de natuurwetenschappen als achterhaald dogmatisme afwijzen. Over de 'science wars' tussen de postmodernisten en laat 20e eeuwse positivisten Stengers (2010), Latour (1998). Met het oog op het recht Loth en Gaakeer (2005), Hildebrandt (2004).

De rechtswetenschap moet weer een normatieve wetenschap durven zijn en zich bezinnen op de betekenis van die normativiteit. Normatief kan immers niet betekenen dat de jurist zich als moraalridder gaat gedragen. Het verschil tussen recht en moraal zetelt onder meer in de positiviteit van het recht,[51] die het mogelijk maakt om op juridische gronden knopen door te hakken waar dat op grond van de moraal niet kan (nu we het over die moraal meestal niet eens zijn). De jurist in functie is dus gebonden aan het recht, zij mag haar persoonlijke morele inzichten niet opleggen aan anderen.[52] Dat betekent echter niet dat het recht geen normatieve kaders schept die onderhouden moeten worden. De jurist moet haar rug recht houden als het gaat om het recht als systeem van checks en balances dat ongelijkheid compenseert om rechtsgenoten de mogelijkheid – zo men wil capability – te bieden zich zelfstandig tot anderen te verhouden en zichzelf daarbij steeds opnieuw uit te vinden. Dat speelt bij de uitleg van geldend recht,[53] maar uiteraard ook bij het adviseren van de wetgever. De vrijheid waar het om gaat mag dan weer niet in naïef voluntaristische zin als een natuurverschijnsel worden begrepen, maar speelt in die zin dat het recht de institutionele architectuur meebepaalt waarbinnen persoonlijke vrijheid en verantwoordelijkheid vorm kunnen krijgen. Vrijheid kan niet verondersteld worden, het moet worden bevochten – als het ware tegen de tweede wet van de thermodynamica in.[54]

De explosie van data-gestuurde *agents* in de onli*f*e wereld impliceert dat het recht die taak niet meer uitsluitend op basis van het uitvaardigen en interpreteren van tekst kan vervullen en zich zal moeten wenden tot die andere architecten van onze gedeelde wereld: de computerwetenschappers en de data scientists. In plaats van opnieuw een methodenstrijd te beginnen, nu tegen de informatici, of ons de les te laten lezen door externe – kwantitatief georiënteerde - perspectieven op de zijnsmodus van het recht, zouden wij het gesprek aan moeten gaan. En wel op zo'n wijze dat ieder vanuit eigen taken en verantwoordelijkheden de onli*f*e wereld mee verder opbouwt en inricht.

Ook als uitbreiding van strafbaarheid niet aan de orde is, kunnen police intelligence en profiling desondanks leiden tot uitbreiding van de inzet van *maatregelen*,[55] op te leggen naar aanleiding van het begaan van een strafbaar feit. Stel dat uit inzage van historische gedragsgegevens (bijvoorbeeld metadata van telecommunicatie, postings op sociale media, energieverbruiksgegevens) blijkt dat datapunten van de verdachte correleren met recidive of juist met 'vatbaarheid voor' of 'geneigdheid tot' geheel andere strafbare feiten of zelfs met andere vormen van ongewenst gedrag. Mag dit aanleiding zijn om maatregelen op te leggen die – losgekoppeld van de ernst van het feit en de mate van schuld – veel ingrijpender zijn dan hun punitieve tegenhangers? In juridische zin is dit niet zonder meer verboden.[56] Wat nu als politie of andere *agents* correlaties ontdekken tussen een reductie van agressie

[51] Niet te verwarren met rechtspositivisme, dat de positiviteit verabsoluteert ten koste van de instrumentaliteit en de rechtvaardigheid. Zie Radbruch (1950:173), Hildebrandt (2015b:52-54).

[52] De rechter moet geldend recht dat zij onrechtvaardig acht in beginsel desondanks toepassen, tenzij de betreffende normen niet meer kunnen worden begrepen als *gericht op* rechtvaardigheid, aldus Radbruch (1950, 1945). In dat geval is eigenlijk geen sprake meer van recht, maar van bestuur.

[53] Overigens niet alleen bij het strafrecht. Zie over de doorwerking van grondrechten in het privaatrecht Sieburgh (2015).

[54] Over de relatie tussen entropie, onzekerheid en vrijheid, vanuit een informatietheoretisch perspectief Leydesdorff (2010); relevantie voor het recht Hildebrandt (2016a te verschijnen).

[55] Maatregelen zijn niet punitief van aard en dus ook niet gebonden aan de evenredigheidseis ten aanzien van de ernst van het feit of de mate van schuld. Zie Titel IIa WvSr. Het gaat om onttrekking aan het verkeer, ontneming van wederrechtelijk verkregen voordeel, schadevergoeding, plaatsing in een psychiatrisch ziekenhuis of in een inrichting voor stelselmatige daders (ISD), ofwel oplegging van een vrijheidsbeperkende maatregel. Over grondslag en normering Kooijmans (2002). In het kader van pre-emptieve maatregelen zie Struijk (2015) over de ISD.

[56] Zie bijvoorbeeld art. 36e WSr waar een ontnemingsmaatregel mogelijk wordt gemaakt voor voordeel behaald door 'andere strafbare feiten, waaromtrent voldoende aanwijzingen bestaan dat zij door de veroordeelde zijn begaan', wanneer 'aannemelijk is dat of dat misdrijf of andere strafbare feiten op enigerlei wijze ertoe hebben geleid dat de veroordeelde wederrechtelijk voordeel heeft verkregen' en bij de vaststelling van het voordeel mag worden uitgegaan van een aantal vermoedens (art. 36e lid 3 onder a en b WvSr). Bij plaatsing in een psychiatrische inrichting, ter beschikkingstelling, dwangverpleging en plaatsing in een ISD wordt vooral gelet op het gevaar dat

in gevangenissen en de inname van voedingssupplementen? Kunnen we ons voorstellen dat een maatregel wordt opgelegd die eist dat de veroordeelde haar bloed laat controleren ten einde vast te stellen dat zij haar supplementen heeft ingenomen, bijvoorbeeld in het kader van een voorwaardelijke straf? Als zij haar pillen niet braaf inneemt wordt de straf alsnog ten uitvoer gelegd. Dit is geen science fiction, ook al bestaat die maatregel nog niet.[57]

De vraag is of het strafrecht zich daartoe moet lenen. Of is het wellicht zo dat juist het strafrecht vanuit een scherp gevoel voor de constitutieve samenhang van instrumentaliteit en rechtsbescherming weerstand kan bieden aan weer een nieuwe versie van wat Foqué en 't Hart (1990) begin jaren '90 'beheersingsdenken' noemden. Zij benoemden daarmee wat inmiddels het reguleringsparadigma mag heten, dat wil zeggen de behoefte om het recht te reduceren tot een instrument om mensen te beïnvloeden, in plaats van een instrument dat mensen aanspreekt. Voor zover de strafrechter – eerder dan het OM of het bestuur - weerstand weet te bieden aan zulk beheersingsdenken, zou dat ervoor kunnen pleiten om maatregelen naar aanleiding van een strafbaar feit zoveel mogelijk binnen het strafrecht te houden en dus bij de strafrechter te laten. De inzet van politie-*agents*[58] om beslissingen te genereren die pre-emptief ingrijpen ter voorkoming van nog te plegen misdrijven of overtredingen mag intussen niet gelijk worden gesteld met het beheersingsdenken van eind 20ste, begin 21ste eeuw. Dat was gebaseerd op een hiërarchisch soort systeemdenken waarbij de overheid een centrale rol had. Het nieuwe beheersingsdenken is niet meer systeemgerelateerd maar 'denkt' in termen van netwerken; het richt zich niet meer op *government* maar op *governance*, wijst *command and control* af en verschuilt zich achter de objectieve feiten die zouden blijken uit 'harde' data analyse. Bovendien is niet ondenkbaar dat de straffende overheid haar controletaken steeds meer moet delen met politie-*agents* die zij niet volledig in de hand heeft, terwijl zij er wel steeds meer van afhankelijk wordt. Dat laatste zal de grootste verandering worden; data analytics en daaruit afgeleide voorspellingen zijn van een andere orde dan machinaal lerende systemen die ingrijpen in de maatschappelijke orde. De ambtenaren die de uitvoerende macht handen en voeten geven, zullen mogelijk deels worden vervangen door *agents* en de ambtenaar van de toekomst zal in dat geval worden gerekruteerd op haar vermogen om daarmee samen te werken. Dat is niet slecht of fout, maar het maakt wel degelijk uit. *Agents* die hun eigen programmatuur bijstellen met het oog op het verwezenlijken van de doelen van strafrechtelijk beleid, kunnen op de loop gaan met de methodologie – en daarmee ook met de doelstellingen - van hun opdrachtgevers.[59]

Het is, kortom, niet ondenkbaar dat de inzet van politie-*agents* er op den duur toe gaat leiden dat de grens tussen straf en maatregel irrelevant wordt (wanneer de uitbreiding van strafbaarheid van poging en voorbereiding doorschiet naar door *agents* afgeleide inclinaties). Ik zou bovendien niet willen uitsluiten dat de inzet van *agents* door politie en justitie gaat leiden tot uitholling van de voorwaarden van strafbaarheid. Een nieuw type 'voorzienigheid', gebaseerd op geavanceerde vormen van bijvoorbeeld machinaal leren in gebruik bij politie en justitie, kan zomaar leiden tot 'strafbaarheid' vanwege gedragingen die niet hebben plaatsgevonden maar waartoe de verdachte kennelijk neigt.

De schuld ligt dan bijvoorbeeld in afwijzing van hulp bij het bevechten van zulke neigingen. 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

---

de verdachte zou kunnen veroorzaken (art. 37, 37a, 37b, 38m WvSr); ook bij de vrijheidsbeperkende maatregel staat beveiliging van de samenleving en het voorkomen van strafbare feiten voorop (art. 38v WvSr). Het mag duidelijk zijn dat de strafrechtelijke maatregel voortkomt uit de idee van het sociaal verweer, zie hierboven noot 47.

[57] Op dit moment loopt een experiment met dergelijke supplementen naar aanleiding van positieve resultaten bij een eerder experiment, zie de Visser (2015). Daarbij is op dit moment geen sprake van dwang.

[58] A*gents* die door de politie (onder gezag van het OM) worden ingezet duid ik hieronder aan als politie-*agents*, wanneer dat het leesgemak en de herkenbaarheid bevordert.

[59] De ervaring leert dat wie de middelen beheert daarmee deels ook de doelen in de hand heeft. Wijsgerig heeft met name Dewey (1967) het constitutieve verband tussen middel en doel verder uitgewerkt.

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 onli*f*e wereld zo in kunnen richten dat dit soort machinale toerekening kan worden voorkomen. Voorkomen is hier zeker beter dan genezen; de kans dat dergelijke informatie gebruikt gaat worden tegen degenen die ermee 'getarget' kunnen worden is niet onaanzienlijk.[60]

3 Formeel strafrecht: verdachte en handhaver als *homo digitalis*

3.1 Introductie: het doel van de strafvordering

In de MvT van de Wet BOB sprak de Minister van – toen nog slechts – Justitie de onsterfelijke woorden:[61]

> Bijzondere opsporingsmethoden zijn in het verleden te vaak ingezet ten behoeve van vage doelstellingen, zoals het ontmantelen van een criminele organisatie of het verbeteren van de informatiepositie van de rechtshandhavende autoriteiten.

Ik vrees dat de behoefte om de eigen informatiepositie te verbeteren niet alleen in het verleden maar ook in heden en toekomst doorslaggevend zal zijn.[62] Het woordje 'positie' doet vermoeden dat het vooral ook gaat om informatieoverwicht ten opzichte van anderen, zoals bijvoorbeeld verdachten of mogelijke verdachten. Zo'n informatieoverwicht leidt echter gemakkelijk tot informatieover*ge*wicht, hetgeen om een veelheid van redenen niet wenselijk is. De behoefte om de beschikking te hebben over heel veel informatie, en liefst ook heel veel 'big en open data', hangt samen met de verzelfstandiging van het vooronderzoek ten opzichte van het hoofdonderzoek ter terechtzitting. Het doel van de strafvordering was enerzijds, ingevolge het procesbeginsel, de voorbereiding van het onderzoek ter terechtzitting ten einde in een openbaar proces bij een onpartijdige en onafhankelijke rechter op tegenspraak vast te stellen of de verdachte het tenlastegelegde strafbare feit heeft gepleegd, en anderzijds, in het verlengde daarvan de voorbereiding van het straffen zelf ingeval de verdachte wordt veroordeeld. De voortgaande relativering van het procesbeginsel betekent dat in de meeste gevallen de straf niet door de strafrechter wordt opgelegd, maar door het Openbaar Ministerie wordt opgelegd of overeengekomen (in de vorm van een strafbeschikking of transactie).[63] Daarmee blijft echter overeind dat de strafvordering de *voorbereiding* is van een straf die alleen mag worden opgelegd op voorwaarde van een aantal processuele waarborgen. Een daarvan is toegang tot de rechter. De voorbereiding mag niet worden verward met de straf zelf; de strafvordering zelf heeft geen punitief karakter.

---

[60] Inmiddels is in de VS software ontwikkeld die de kans op recidive berekent met de bedoeling die ter beschikking te stellen aan rechters, ten einde een meer objectieve maatstaf te bieden bij het vaststellen van de straf, zie Tokmetzis (2015) en Barry-Jester, Casselman en Goldstein (2015). Algoritmische straftoemeting is overigens beslist niet objectief, zie voor een interessante analyse Aas (2005).

[61] Handelingen Tweede Kamer 1996-97, 25 403, nr. 3, Memorie van Toelichting Wetsvoorstel tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), p. 3.

[62] Het 'discours' over de informatiepositie van overheden wordt vaak gevoerd onder de noemer van 'surveillance'. Na afronding van de eerste versie van dit preadvies zag ik dat ik het woord 'surveillance' helemaal niet gebruik. De term is inmiddels beladen met een keten van associaties die mijns inziens in de weg kunnen staan aan een open discussie over (1) de bevoegdheden die overactieve overheden wel en niet nodig hebben, (2) de precieze waarborgen die deze bevoegdheden inperken en legitimeren en (3) de manier waarop we kunnen voorkomen dat overheden voortdurend de grenzen opzoeken van hun bevoegdheden.

[63] Materieel gezien is een transactie een straf in de zin van art. 6 EVRM. Ook de bestuurlijke sancties met een punitief karakter, zoals bijvoorbeeld de bestuurlijke boete, zijn materieel gezien straffen en bevestigen dat de meeste straffen niet door de strafrechter worden opgelegd. Zie ook Crijns (2014). Over het procesbeginsel Hildebrandt (2002).

Intussen heeft het Ministerie van Veiligheid & Justitie ingezet op een integrale 'Modernisering van het Wetboek van Strafvordering',[64] waarbij de nadruk van de strafvordering nog verder verschuift naar het voorbereidend onderzoek. Het gevolg hiervan is minstens dat allerhande vormen van monitoring en ander onderzoek, al dan niet gebaseerd op data-gestuurde risico-analyses, de rechter niet zullen bereiken en dus door anderen getoetst moeten worden.[65] Juist bij toenemende inzet van politie-*agents* moet in een rechtsstaat de aanvechtbaarheid worden gekoesterd en veilig gesteld van de beslissingen die – grotendeels onder de radar – door (of op basis van) dergelijke systemen worden genomen.

Voordat ik de risico's van de verdere verzelfstandiging van het voorbereidend onderzoek aankaart, roep ik in herinnering wat wij in een rechtsstatelijke democratie beogen met straf en strafrecht. Het is gebruikelijk om de doelen van de overheidsstraf te onderscheiden in termen van generale en specifieke preventie door middel van afschrikking enerzijds en vergelding door leedtoevoeging anderzijds. De verenigingstheorie brengt beide samen door te eisen dat straffen zowel binnen de maat van de vergelding blijven (proportionaliteit ten opzichte van de ernst van het feit en de mate van schuld) als binnen die van het algemeen belang (er moet sprake zijn van enig nut, in het bijzonder specifieke of generale preventie en wellicht ook genoegdoening van slachtoffer en/of samenleving). In mijn proefschrift (Hildebrandt 2002) heb ik de stelling verdedigd dat preventie en vergelding twee kanten van dezelfde medaille zijn; de straf vormt de negatie van een normschending (in het verleden) *waardoor* het gezag van de norm (in de toekomst) wordt hersteld. Hoe het ook zij, de inzet van *agents* in de strafvordering, de opsporing, het verkennend onderzoek en wat daar eventueel nog aan vooraf gaat, sluit aan bij een verschuiving in de richting van preventie en risicomanagement die duidelijk zichtbaar is in de stroom van aanpassingen in het huidige wetboek van strafvordering. Sinds ik begin jaren '90 van de vorige eeuw strafprocesrecht doceerde in Leiden is het wetboek veranderd in een labyrint van aanvullingen en uitbreidingen, waar alleen de specialist de weg terug nog kan vinden. Het gaat dan met name om de Wet Bijzondere Opsporingsbevoegdheden (2000), die een wettelijke grondslag (en dus ook inzichtelijke beperking) van in de praktijk reeds gebruikte onderzoeksmethodieken voorzag,[66] de Wetten Computercriminaliteit I (1993) en II (2006), en III (ligt nu voor),[67] en de Wet ter verruiming van de mogelijkheden tot opsporing

[64] Contourennota Modernisering Wetboek van Strafvordering, aangeboden aan de Tweede Kamer op 3 februari 2015, <http://www.rijksoverheid.nl/documenten-en-publicaties/brieven/2015/02/03/brief-concept-contourennota-modernisering-wetboek-van-strafvordering.html>, hierna aangehaald als Contourennota 2015. Vergelijk ook het preadvies van Knigge (1994), en de bespreking van de in 2014 door het Ministerie van Veiligheid en Justitie voorgestelde discussienota door Keulen (2014) Zie inmiddels het advies van de Raad voor de Rechtspraak (2015), onder meer verwijzend naar het rapport van de PG bij de Hoge Raad inzake de naleving van het recht bij strafbeschikkingen (Fokkens 2014).

[65] Daaraan kleven grote risico's, zie bijvoorbeeld, over de omgang met bijzondere persoonsgegevens in het kader van de strafvordering: zie CBP (2015).

[66] De Wet BOB van 2000. Het ging met name om de invoering van de volgende bevoegdheden: observatie, infiltratie, pseudokoop, pseudodienst-verlening, stelselmatige informatie-inwinning, het betreden van een besloten plaats en het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel; de wettelijke regeling van de informant, de burgerinfiltrant en de burgerpseudokoop- of dienstverlening; een aangepaste regeling van de bevoegdheid tot het opnemen van telecommunicatie en het vorderen van inlichtingen; een nieuwe grondslag voor de toepassing van specifieke opsporingsbevoegdheden, te weten 'aanwijzingen' dat in georganiseerd verband ernstige misdrijven worden 'beraamd' of gepleegd en de regeling van het verkennend onderzoek. Wat betreft dat laatste is nieuw dat onder de opsporing worden gebracht: (1) bevoegdheden waarvoor geen redelijke verdenking wordt vereist en (2) bevoegdheden inzake strafbare feiten die nog niet gepleegd zijn en waar geen sprake is van een poging of voorbereidingshandeling.

[67] Computercriminaliteit III beoogt te regelen: heimelijk onderzoek op afstand in een computer systeem (hacken), aanpassing regeling ontoegankelijk maken gegevens, decryptiebevel aan verdachte bij verdenking enkele zeer ernstige delicten (in de definitieve versie geschrapt), strafbaarstelling wederrechtelijk overnemen en 'helen' van gegevens. Het wetsvoorstel is op 22 december 2015 ingediend bij de Tweede Kamer, het is beschikbaar via < https://www.rijksoverheid.nl/actueel/nieuws/2015/12/22/wetsvoorstel-computercriminaliteit-bij-tweede-kamer-ingediend>.

en vervolging van terroristische misdrijven (2007).[68] De voorgenomen modernisering van het wetboek moet worden toegejuicht voor zover het gaat om hernieuwde inzichtelijkheid, toegankelijkheid en systematische integratie van de eisen van effectiviteit en rechtsstatelijkheid.[69] Modernisering lijkt inmiddels een wat ouderwetse term.[70] 'Upgrade' zou meer bij deze tijd passen en expliciteren dat het gaat om een reconfiguratie die inspeelt op de veranderende omgeving en de eigen functionaliteit verbetert (en dus meer is dan een 'update'). Bovendien gaat het niet om een upgrade van de software maar van de 'firmware', dat wil zeggen van het meest stabiele onderdeel van het 'operating system' van het strafrecht, dat nauw verbonden is met de 'hardware' (de institutionele ondergrond, inclusief de Grondwet, en de organieke wetgeving inzake rechterlijke macht, advocatuur) en daarmee feitelijk de mogelijkheden bepaalt van de te implementeren software (nadere regelgeving, beleidsregels en protocollen voor de uitvoering).[71] De functionaliteit van het Wetboek van Strafvordering is genesteld in de constitutieve samenhang tussen de instrumentaliteit en de rechtsbescherming van het strafrecht als rechtsstatelijk georiënteerde omgang met criminaliteit. Dat betekent bijvoorbeeld dat 'modernisering' niet kan betekenen dat de wirwar van bestaande bevoegdheden op toegankelijke wijze gerangschikt worden, liefst hier en daar uitgebreid,[72] en voorzien van wat algemene clausules die zouden moeten waarborgen dat de hele zaak 'Straatsburg en Luxemburg proof' is.[73] Met name het voorstel om de proportionaliteit en de subsidiariteit als een bijkans magische formule toe te voegen in de hoop dat de praktijk daar wel weg mee weet, is problematisch en onzorgvuldig.[74] Het lijkt op een achteraf toegevoegde 'add-on' (in termen van de onlife wereld) en we weten dat een 'add-on' meestal niet goed werkt omdat die de werking van een systeem vertraagt. Wie rechtsbescherming als onderdeel van de functionaliteit van het strafrecht ziet (dus niet als een bijkomende gedachte) moet die inbouwen in de diepste lagen van het systeem, zodat het deel uitmaakt van ieder onderdeel. *The devil is in the details*, dat geldt ook voor het strafrecht.

Zo'n add-on is des te hachelijker wanneer in beleidskringen de neiging bestaat om punitieve aspecten van de rechtshandhaving op te nemen in strafvordering, door het benadrukken van de

---

[68] In zijn Contourennota (2015:3) noemt de Minister ook nog de aanpassingen die zijn ingevoerd naar aanleiding van de resultaten van het Onderzoeksproject Strafvordering 2001, onder leiding van Knigge en Groenhuijzen: Wet OM-afdoening (Stb. 2006, 330), de regeling van de versterking van de positie van het slachtoffer (Stb. 2010, 1) en die van de deskundige (Stb. 2009, 33), Wet herziening regels betreffende de processtukken in strafzaken (Stb. 2011, 601) en de Wet versterking positie rechter-commissaris (Stb. 2011, 600).

[69] Contourennota 2015. Voor commentaar op het eerder rondgestuurde discussiestuk zie bijvoorbeeld Keulen (2014) en het advies van de Raad voor de Rechtspraak (2015).

[70] Het begrip modernisering kan verwijzen naar de transformaties die plaatsvonden na de industriële revolutie, en hangt dan samen met een bepaald soort vooruitgangsgeloof. In dat kader zou Beck's (1986) reflexieve modernisering ook hier van nut kunnen zijn. Beck richtte zich op het besef dat technologische vooruitgang inmiddels niet alleen problemen oplost maar ook nieuwe schept, waarbij catastrofale gevolgen niet zijn uitgesloten.

[71] Ach, 'update', 'upgrade', 'software', 'hardware' en 'operating system' zijn hier 'maar' metaforen. Uiteindelijk denken wij echter onvermijdelijk en steeds in metaforen (zij het vaak zo versleten dat we het metaforisch karakter niet meer herkennen, zie Ricoeur (1975) die de zaken naar mijn mening scherper en fundamenteler formuleert dan Lakoff en Johnson (2003). Daarom is het verstandig wanneer het om de inrichting van de samenleving gaat ons permanent te bezinnen op de inzet van metaforen. Het gebruik van metaforen als 'upgrade', 'firmware' etc. is er niet op gericht de werking van de samenleving gelijk te stellen aan die van de digitale infrastructuur (het blijven metaforen); het is wel gericht op erkenning van de transformaties van de ICT-infrastructuur die het recht mede vormt (zie hieronder hoofdstuk 4).

[72] Met name ten aanzien van de inzet van 'heimelijke bevoegdheden' (de term 'bijzondere opsporingsbevoegdheden' wordt geschrapt). Het gaat bijvoorbeeld om de regeling van 'de stelselmatige vastlegging van persoonsgegevens op het internet, de inzet van een 'stille sms' of IMSI-catcher ter plaatsbepaling of een tijdslot voor de uitvoering van een bevel tot het opnemen van vertrouwelijke communicatie (Contourennota 2015: 56)'.

[73] Zo keert de eis van proportionaliteit en subsidiariteit in de Contourennota op een wel heel hoog abstractieniveau steeds weer terug, als een soort van bezweringsformule, die het stroomlijnen van de voorwaarden voor de inzet van bevoegdheden van een mensenrechtelijk vernisje moet voorzien. Zie Contourennota (2015:27-28, 42-45), met name in verband met voorlopige hechtenis en wat de Minister verdenkingscriteria noemt. De idee is dat deze beginselen in het tweede Boek, dat betrekking heeft op het Voorbereidend Onderzoek, worden gecodificeerd.

[74] Zie ook: Raad voor de Rechtspraak (2015:10).

preventieve werking van *strafvorderlijke* bevoegdheden. Het lijkt er soms op neer te komen dat het afdoen van zaken ter terechtzitting een uitzondering zou moeten blijven, omdat het duur is en veel gedoe geeft; alles wat in het voorveld van de zitting meegenomen kan worden is winst en dat houdt ook in dat de meeste zaken nooit ter zitting verschijnen. Denk aan de strafbeschikking,[75] aan het verkennend onderzoek dat zich onderscheidt doordat het niet is gericht op strafvorderlijke beslissingen, en denk alvast aan de inzet van politie-*agents* die op geaggregeerd niveau voorspellend en zo mogelijk op individueel niveau ondervangend zullen functioneren. In de bespreking van de eerste ervaringen met de nieuwe strafvorderlijke bevoegdheden in geval van aanwijzingen van het beramen of plegen van terroristische misdrijven, lezen wij dat (De Poot e.a. 2008:6):

> De grote nadruk op de preventieve functie van het strafrechtelijke optreden vloeit enerzijds voort uit de redenering dat terrorisme moeilijk te bestrijden is met klassiek strafrechtelijke middelen. Terroristen lijken zich immers niet te laten weerhouden door de dreiging van een hoge straf. Anderzijds gaat het bij terrorisme vaak om zeer ernstige destructieve misdrijven. Daarom wordt voorkóming juist bij terrorisme van zeer groot belang geacht. Om de preventieve functie van het strafprocesrecht te kunnen verbeteren, is een aantal wetswijzigingen doorgevoerd die de politie en het OM de mogelijkheid geven om in geval van een mogelijk terroristisch misdrijf in een vroeg stadium opsporingsmethoden in te zetten en bewijs te vergaren.

Hier wordt onomwonden gesproken van de preventieve werking van dwangmiddelen en andere onderzoeksbevoegdheden. Gesteld wordt dat de afschrikkende werking van de straf geen indruk maakt op terroristen en dat de ernst van terroristische misdrijven niet toelaat te wachten tot het misdrijf is voltooid. Het gaat dus niet om de gebruikelijke doelen van de straf zelf, maar om de preventieve werking van vroegtijdig onderzoeken, bewijs verzamelen en ingrijpen – voordat sprake is van veroordeling en strafoplegging. Daarmee worden aspecten van de punitieve rechtshandhaving naar voren geschoven. Wanneer dat samenvalt met de inzet van *agents* raakt de punitieve rechtshandhaving gemakkelijk ingebed in de logica van semi-actuariële risico-instrumenten die zich met het voortschrijden der techniek ontpoppen als geavanceerde predictie- en mogelijk ook als pre-emptiemachines.[76]

Het is belangrijk om die vlucht naar voren te duiden in samenhang met verschuivingen in het opsporingsbegrip en complexe aanvullingen daarop in de vorm van het verkennend onderzoek.[77] Uit de aanpassing van de definitie van het opsporingsbegrip (in 2007) volgt dat de eis van een verdenking (redelijk vermoeden) ten aanzien van een bepaalde persoon of een bepaald strafbaar feit niet meer noodzakelijk is om van opsporing te spreken (art. 132a WSv):[78]

> Onder opsporing wordt verstaan het onderzoek in verband met strafbare feiten onder gezag van de officier van justitie met als doel het nemen van strafvorderlijke beslissingen.

Ook de bevoegdheden die mogen worden uitgeoefend op basis van aanwijzingen vallen kennelijk onder opsporing, hoewel zij wettelijk geregeld zijn als verkennend onderzoek ter voorbereiding van de

[75] Zeer kritisch daarover Fokkens (2014). In de Contourennota (2015: 57) wordt nader onderzoek en aanpassing van de wettelijke regeling aangekondigd.
[76] De Nederlandse vertaling zou luiden: voorspel- en ondervangingsmachines.
[77] Zie ook, zeer genuanceerd, de oratie van Borgers (2007).
[78] Aangepast bij de invoering van de Wet ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven, in 2007. De oude definitie (ingevoerd bij de Wet BOB in 2000) luidde: 'Onder het opsporingsonderzoek wordt verstaan het onderzoek onder leiding van de officier van justitie naar aanleiding van een redelijk vermoeden dat een strafbaar feit is begaan of dat in georganiseerd verband misdrijven worden beraamd of gepleegd, als omschreven in artikel 67, eerste lid, die gezien hun aard of samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren, met als doel het nemen van strafvorderlijke beslissingen.'

opsporing.[79] Het verkennend onderzoek was overigens van begin af aan (in 2000) al mogelijk op basis aanwijzingen voor het *beramen* van misdrijven in georganiseerd verband (art. 126gg WSv).[80] Wie zich mijn zorg over de strafbaarstelling van een neiging tot strafbaar - of zelfs ongewenst - gedrag herinnert uit het voorgaande hoofdstuk over materieel strafrecht, zal begrijpen dat ik hier een bevestiging zie van de neiging om de strafvordering te richten op het voorkomen van strafbare feiten. Niet door met een straf op een reeds gepleegd strafbaar feit te reageren, maar door bepaalde gedragingen zoveel mogelijk te ondervangen. Hierdoor worden niet alleen de rechter en alle waarborgen waar die voor staat in vergaande mate buiten spel gezet, maar wordt de straf zelf schijnbaar vermeden. Enerzijds wordt de straf in formele zin (opgelegd door de strafrechter na het geding ter terechtzitting) steeds meer een uitzondering, anderzijds duiken de punitieve aspecten van de straf in materiele zin op in het voorveld van de bestraffing met name waar het gaat om afschrikking (preventie). Nog ernstiger is de tendens om de straf te vervangen door de ondervanging van ongewenst gedrag, hetgeen impliceert dat de categorie van de verdachte wordt opgerekt tot zo ongeveer alle burgers. Daarmee wordt de categorie van strafbaar gedrag gerelativeerd zodat die zo ongeveer alle ongewenst gedrag gaat omvatten, terwijl tegelijkertijd de idee van een aanspreekbaar rechtssubject samen met de idee van de straf als gedateerde, illusoire instituties kunnen worden vergeten.

Het is intussen niet mijn bedoeling om af te dingen op de preventieve werking van het strafrecht. Ik kan mij bovendien vele situaties voorstellen waarbij het ondervangen van strafbaar of ook ongewenst gedrag een publiek belang is. Dat gaat op bij terroristische aanvallen, maar ook bij belastingontduiking, pesten op het werk en het veel te vroeg buiten zetten van afval (dat vervolgens door meeuwen over de hele straat wordt verspreid). Dat wil echter niet zeggen dat het strafrecht het meest geëigende systeem is om het betreffende publieke belang te beschermen. De preventieve werking van het strafrecht zetelt in een specifieke samenhang van norm en handeling. Ten eerste de handeling waarbij een normschending strafbaar wordt gesteld, vervolgens de handeling waarbij diezelfde norm wordt geschonden, tenslotte de handeling waarbij die normschending wordt bestraft. Op het moment dat normschendingen die niet strafbaar zijn gesteld (zoals beraming van een strafbaar feit), of dermate vaag zijn dat zij geen duidelijkheid verschaffen over welk handelen een schending vormt, toch voorwerp van opsporing lijken te worden, wordt de samenhang tussen strafrechtelijk beschermde normen en de gerechtvaardigde verwachtingen van de burger doorbroken. Hetzelfde geldt wanneer de reactie op een vermeende normschending bestaat uit opsporingshandelingen die geen duidelijke publieke bestraffing

[79] In de Memorie van Toelichting bij het Wetsvoorstel Wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven (Tweede Kamer, 2004-2005, 30 164, nr. 3:17) meldt de Minister dat het onderscheid is gelegen in het feit dat het verkennend onderzoek nog niet is gericht op het nemen van strafvorderlijke beslissingen, maar op de voorbereiding daarvan. Cleiren (2015) noemt als reden voor de uitbreiding van het bereik van art. 132a WSv de destijds nieuwe bevoegdheid van het preventief fouilleren in veiligheidsrisicogebieden met het oog op terroristische aanslagen. Over de inmiddels hallucinante verhouding tussen opsporingsonderzoek, voorbereidend en verkennend onderzoek, ook in relatie tot de strafvordering (het legaliteitsbeginsel van art. 1 WSv) en de strafrechtelijke handhaving van de rechtsorde (art. 13 Pw) zie Blom (2015a) De wijze waarop Van der Meij (2015) art. 132a WSv bespreekt lijkt mij niet te sporen met de manier waarop Cleiren en Blom de verhouding tussen verkennend onderzoek en opsporingsonderzoek bezien, nu deze laatsten anders dan Van der Meij menen dat het verkennend onderzoek niet onder de opsporing valt (maar onder de voorbereiding van de opsporing en voorbehouden aan opsporingsambtenaren). We zien uit naar verheldering.

[80] De uitbreiding van strafbaarheid ten aanzien van voorbereidingshandelingen leek het beramen van dergelijke misdrijven zelf strafbaar te stellen (art. 46 WvSr), waardoor zodra sprake is van een verdenking van dergelijke handelingen al dwangmiddelen kunnen worden toegepast. Kennelijk werd het desondanks noodzakelijk geacht ook het gebruik van dwangmiddelen mogelijk te maken wanneer wel sprake is van het beramen van dergelijk misdrijven maar nog geen verdenking van voorbereidingshandelingen hard kan worden gemaakt. Het beramen is nog niet strafbaar maar wel aanleiding voor nader onderzoek. We komen hier onmiskenbaar bij de strafvorderlijke variant van 'intentiestrafrecht'. Zie ook Kuitenbrouwer (2007) naar aanleiding van Gerechtshof Amsterdam 19 september 2007, ECLI:NL:GHAMS:2007:BB3756, die volgde op HR 20 februari 2007, ECLI:NL:HR:2007:AZ0213. Overigens niet onbegrijpelijk wanneer de voorbereiding zich heeft geopenbaard in een afgeluisterd gesprek waarin onmiskenbaar sprake is van gedetailleerde planning van het betreffende misdrijf, zie HR 9 juni 2015, ECLI:NL:HR:2015:1503.

naar aanleiding van een publiek strafproces vormen, maar al dan niet succesvolle pogingen om normschendingen in kaart te brengen, te ondervangen en eventueel via een besloten procedure te bestraffen (Crijns 2014).

De preventieve werking van dat samenspel heeft niet zoveel van doen met de preventieve doelen van het strafrecht; het is meer een poging tot disciplinering (*nudging* en *priming*) dan een strafrechtelijk appel. Of daarmee het publieke belang van het terugdringen van bepaald handelen gediend is kan niet gemakkelijk worden vastgesteld. Handelen wordt hier namelijk als gedrag bezien; het krijgt niet de aandacht maar wordt afgedaan.[81] Uiteindelijk zal dit niet effectief zijn en strategisch gedrag oproepen van de burger, die zich immers niet serieus aangesproken voelt door een automatisch afgeschreven boete.[82]

Ik beperk mij in dit hoofdstuk verder tot de inzet van *agents* in het kader van de strafrechtelijke rechtshandhaving die voorafgaat aan de behandeling ter terechtzitting. In 3.2 bespreek ik de stand van zaken met betrekking tot de inzet van agents in de strafvordering, de opsporing in zeer brede zin en wat daar nog aan vooraf gaat. In 3.3. zal ik ingaan op de mate waarin en de wijze waarop die inzet kan leiden tot schending van grondrechten. Ik zal dat tenslotte verbinden met een bespreking van doelbinding in het kader van het strafvorderlijk legaliteitsbeginsel in 3.4.

3.2 *Agents* van voorspelling en ondervanging

Het Wetsontwerp Computercriminaliteit III omvat onder meer een nieuwe bevoegdheid die het voor de politie mogelijk maakt om onder specifieke voorwaarden rechtmatig op afstand binnen te dringen in computersystemen. Dit heeft – onder meer – te maken met de toenemende versleuteling van communicatie, die ertoe kan leiden dat alleen toegang tot gegevens voor en na de versleuteling (op de 'randapparatuur' van de gebruiker) de inhoud van communicatie beschikbaar maakt.[83] Uiteraard heeft het ook te maken de noodzaak om botnets te ontmantelen, gegevens en programma's ontoegankelijk te maken ten einde algemeen gevaar voor personen, goederen, diensten en infrastructuur te weren. Bij de ontmanteling van het Bredolab botnet werd reeds geëxperimenteerd met dit type remote control.[84] Mede dankzij aanhoudende maatschappelijke bevraging van de rechtmatigheid hiervan ligt nu een regeling voor die de betreffende bevoegdheid in het leven roept en normeert (art. 126nba WSv). Vooralsnog geldt deze regeling 'alleen' in geval van art. 67 WSv delicten (waarbij voor terroristische misdrijven de eis van een ernstige verdenking vervalt), mits sprake is van een ernstige inbreuk op de rechtsorde (een eis die in het nieuwe WSv zou moeten vervallen). Doel is het bepalen van de aanwezigheid van gegevens of van de identiteit of locatie van het geautomatiseerde werk of de gebruiker; het overnemen van gegevens die in het geautomatiseerde werk of een daarmee in verbinding staande gegevensdrager zijn of worden verwerkt;[85] of ook de ontoegankelijkmaking van gegevens. De bevoegdheid vereist een bevel

[81] In zijn Nijmeegse oratie wijst Buruma (1996) op het belang van de aandacht van de strafrechter, die niet mag worden gedwongen haar aandacht dusdanig te verdelen dat die wordt afgeleid van de hoofdtaak (vaststellen van de strafbaarheid en de oplegging van straf). Aandacht is iets waar we zuinig op moeten zijn; het is een schaars goed, ook in het strafrecht. In de onlife wereld is onze (machinaal leesbare) aandacht inmiddels een te verhandelen gedragsmodus, die tijdens online veilingen aan de hoogstbiedende adverteerder wordt doorverkocht. Hier dringt zich het onderscheid op tussen aandacht als meetbaar gedrag en aandacht als handeling.
[82] Dat was de conclusie van mijn proefschrift (Hildebrandt 2002).
[83] Zie hierover – in relatie tot de veiligheids- en inlichtingendiensten Jacobs (2015).
[84] Zie Koning (2012) en Oerlemans (2011).
[85] Wat betreft de MvT sluit deze formulering niet uit dat onderzoek zal worden gedaan in servers die zich de facto buiten Nederland bevinden. Deze heikele kwestie roept veel vragen op, onder meer betreffende het raakvlak tussen cybercriminaliteit en cyberoorlog, die ik – gezien de 'beperkte' omvang van dit preadvies – buiten beschouwing moet laten. Zie bijvoorbeeld B.-J. Koops en Goodwin (2014), Klip en Massa (2010), Hildebrandt en Koning (2012), Hildebrandt (2013c).

van de OvJ na machtiging van de RC (die in noodgevallen mondeling mogen worden gegeven, met schriftelijke vastlegging achteraf, binnen drie dagen). In het nu voorgestelde art. 126uba WSv wordt vervolgens bepaald dat binnen mag worden gedrongen 'bij een persoon ten aanzien van wie uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat hij betrokken is bij het in georganiseerd verband beramen of plegen van misdrijven'. Hier vervalt de eis van ernstige verdenking eveneens en is 'betrokkenheid bij' voldoende, waarbij het bovendien kan gaan om het – in georganiseerd verband – 'beramen' van misdrijven (zonder verdere inperking). Wat betekent 'betrokkenheid bij het beramen van misdrijven in georganiseerd verband' (stoute jongens die zich voornemen gezamenlijk een supermarkt te beroven)? Bij wege van het nu voorgestelde art. 126zpa WSv wordt bovendien 'in geval van aanwijzingen van een terroristisch misdrijf' onderzoek op afstand mogelijk 'in een geautomatiseerd werk dat in gebruik is bij een persoon' (die dus zelfs geen verdachte hoeft te zijn). Rekening houdend met de voorgestelde ruime definitie van 'geautomatiseerd werk' in art. 80sexies WSr,[86] lijkt deze bevoegdheid minst genomen 'overinclusive' zoals de Engelsen het zo mooi zeggen. Dat politie en justitie deze bevoegdheid wensen is begrijpelijk en de regeling lijkt voorzien van keurige waarborgen. Mijn punt is echter vooral dat we de omvang van de implicaties van toepassing van 'remote hacking' door politie-*agents* pas kunnen beoordelen als we beseffen dat de 'opgehaalde' gegevens bij zullen dragen aan voortgaande data-gestuurde interventies, net als bij via interceptie verkregen gegevens. Daarbij ligt voor de hand dat op enig moment uitbreiding van de hackbevoegdheid zal worden bepleit voor misdrijven die met een zekere waarschijnlijkheid beraamd zullen worden. Dat laatste zou betekenen dat de functionaliteiten van politie-agents de toepassing van dit type bevoegdheden in vergaande mate zullen bepalen.[87]

De ontwikkeling van data-gestuurde systemen met het oog op de opsporing vindt – voor zover bekend - plaats in de context van het Internet Recherche & Onderzoek Netwerk (iRN),[88] een onderdeel van de Nationale Politie, waarin naast de politie onder meer ook de Belastingdienst, de Nationaal Coördinator Terrorisme Bestrijding en Veiligheid, de UVW, de Nederlandsche Bank, en diverse Nederlandse Gemeentes samenwerken met gespecialiseerde private IT bedrijven.[89] Het iRN functioneert als een beveiligde Internet Service Provider voor en van de overheid. Het biedt de mogelijkheid om platformen in te richten waarbinnen verschillende modules (deelprogramma's) kunnen worden ontwikkeld en uitgeprobeerd. Meer specifiek voor politie en justitie is binnen iRN het iColumbo platform gebouwd met als doel het analyseren van 'open en big data' ten einde inzicht te verkrijgen in specifieke criminaliteitspatronen (bijvoorbeeld witwassen, mensensmokkel, drugssmokkel, geweld, terrorisme)[90] dan wel het monitoren en profileren van een specifiek persoon of een specifieke groep personen, in

[86] 'Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken.' Zie ook paragraaf 3.4.

[87] Van Noort en Kist (2015) beschrijven predictieve politie technologie, die bijvoorbeeld volgens IBM aan de Nederlandse politie wordt verkocht. Het is precies dat type technologie dat aanwijzingen van het beramen van een terroristisch misdrijf kan opleveren, op basis van gegevens verkregen uit interceptie en binnendringen op afstand.

[88] Uiteraard wordt ook en juist binnen de veiligheidsdiensten gewerkt aan data-gestuurde systemen, bijvoorbeeld ARGO II, zie bijvoorbeeld <https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/inhoud/inlichtingen-en-veiligheid/gegevens-verwerken-met-argo-ii>. Uitwisseling tussen de diensten enerzijds en politie en justitie anderzijds vindt plaats in het kader van een ambtsbericht (op basis van art. 36 en 38 Wiv 2002, en de *Handleiding informatieverstrekking van en door de AIVD en de MIVD*), zie Brinkhof (2014), en Vervaele (2005).

[89] Over iRN bijvoorbeeld de websites van Committ (een private publieke samenwerking die naar eigen zeggen 'unites academic research and (non-)profit organizations in ICT. It is a use-inspired fundamental ICT-research in well-being and well-working, in public safety, in science, in information services and search, and with applications in culture, agriculture, and health care.'): <http://www.commit-nl.nl/universities/politie-gelderland-zuid> en Flusso (naar eigen zeggen: 'een maatwerk applicatieontwikkelaar en ICT dienstverlener die meedenkt en adviseert over de architectuur van applicaties.'): <http://www.flusso.nl/Werk/big_data-nationalepolitie/>. Tevens Roessingh (2013), Bert-Jaap Koops e.a. (2012).

[90] Dit is mijn inschatting, ik heb geen expliciete informatie kunnen detecteren vanwege de overheid waarin uit de doeken wordt gedaan wat precies wordt onderzocht. Maar dat laat zich tot op zekere hoogte raden.

verband met gepleegde of mogelijk te plegen strafbare feiten. Het mag duidelijk zijn dat steeds wanneer onderzoek plaats vindt dat een min of meer ernstige inbreuk impliceert op een of meer grondrechten, hiervoor min of meer specifieke, wettelijk bevoegdheden, voorzien van proportionele waarborgen noodzakelijk zijn. Ik kom daarop terug in paragraaf 3.3 en hoofstuk 4.

In het – oorspronkelijk kennelijk geheime – TNO rapport *Herkenning van digitale informatie* uit 2010 worden een aantal toepassingen beschreven voor het automatisch detecteren van specifieke informatie: (bijna)-identieke bestanden of delen daarvan; verborgen boodschappen; personen; verdacht gedrag; objecten, zoals logo's of auto's; tekst in beeld/video; opvallend internet-/netwerkverkeer; netwerken van personen (sociale netwerken); taaluitingen.[91] Het onderzoek was gericht op de beschikbaarheid en geschiktheid van bestaande en nieuw te ontwikkelen software modules die op basis van machinaal leren en andere vormen van data analyse relatief snel en relatief betrouwbaar relevante informatie afleiden uit grote gegevensbestanden (zowel tekst, geluid, als plaatjes, internetverkeer en sociale netwerken). De uitkomsten van het onderzoek zijn niet opzienbarend, de beschreven applicaties lijken trouwhartig de stand der techniek te volgen. De onderzoekers signaleren daarbij allerlei praktische incompatibiliteiten, bijvoorbeeld wijzend op het feit dat bestaande commerciële producten niet noodzakelijkerwijs aansluiten bij de onderzoeksbehoeften van de opsporende of inlichtingen verzamelende overheden.[92] Dat wil niet zeggen dat met dit type technieken geen verrassende voorspellingen kunnen worden gedaan en patronen kunnen worden blootgelegd. Het lijkt erop alsof de besproken toepassingen niet meer doen dan automatisch doorzoeken wat anders met de hand was doorzocht, maar dat is zeker niet het geval. Enerzijds omdat de mankracht om de voortdurend exponentieel toenemende datastromen te doorzoeken ontbreekt, hetgeen individuele datapunten - zelfs wanneer overheden ze verzamelen en opslaan - nog steeds redelijk onvindbaar maakt. Met dit soort software wordt die onvindbaarheid echter op zijn minst gerelativeerd. Het is belangrijk dat burgers zich daarvan bewust zijn. Anderzijds is het mogelijk om via machinaal leren nieuwe patronen te ontdekken; om als het ware nieuwe hypothesen te ontwikkelen over de samenhang tussen criminaliteit, gedrag, gebouwde omgeving, weersomstandigheden, bestedingscapaciteit, buurt, leeftijd, huwelijkse staat, genetisch profiel, energieverbruik, opleiding van de ouders, kinderziektes, reisgedrag en zo meer. Waar dit soort hypotheses vroeger door sociale wetenschappers werden bedacht, ontwikkeld en vervolgens getest aan de hand van een of meer steekproeven, is het nu mogelijk om toepassingen te bouwen die op basis van mathematische en statistische technieken zelfstandig verbanden leggen en aldus hypotheses genereren waar wij wellicht nooit op waren gekomen. Door de beschikbaarheid van schier eindeloze hoeveelheden gedragsdata (deels vrijwillig in de vorm van postings door gebruikers van sociale media vrijgegeven) is het nu bovendien mogelijk de betrouwbaarheid van die hypotheses te testen, en bijvoorbeeld irrelevante correlaties weg te filteren. We zijn hier terug bij Pentland's sociale fysica. Er is namelijk geen sprake van een theorie die verklaart waar deze correlaties op zijn gebaseerd; het gaat hier niet om oorzaken of redenen voor gedrag maar om statistische samenhang. Het gaat niet om handelen maar om gedrag, niet om *homo sapiens* maar om *homo behavioralis*. Dat is interessant, maar niet meer dan een beginpunt van nader onderzoek dat zich wel degelijk zou moeten bekommeren om de betekenis van het gedrag als handeling van een individueel persoon. Binnen het strafrecht is die persoon een rechtssubject en als zodanig ook aanspreekbaar; niet alleen maar een object van onderzoek dat gelaten moet afwachten welke correlaties haar status als verdachte of mogelijk verdachte, potentieel mogelijk verdachte of eventueel potentieel mogelijk verdachte zullen bepalen.[93] Naast dit type bezwaren

[91] TNO (2010: 3), dit rapport werd kennelijk pas openbaar gemaakt op de website van de NCTB na een beroep op de Wob van Rejo Zengers, zie <https://rejo.zenger.nl/inzicht/herkenning-digitale-informatie-en-fingerprinting-episode-2/> en <https://www.nctv.nl/onderwerpen-a-z/herkenning-digitale-informatie-en-fingerprinting.aspx>.

[92] TNO (2010:109-11) met een bijzonder nuttige samenvatting van wat de onderzochte technologieën nu wel en niet vermogen, en een serie aanbevelingen.

[93] In zijn Contourennota (2015:41-2) wil de Minister de verdenkingscriteria terugbrengen van 10 naar 4. Hij verwart daarbij overigens de voorwaarden voor de toepassing van bepaalde dwangmiddelen (zoals dat sprake moet zijn van een verdenking van een strafbaar feit waarvoor voorlopige hechtenis is toegelaten of dat sprake moet zijn van een ernstige inbreuk op de rechtsorde) met de graad van verdenking (aanwijzingen, vermoeden, redelijk vermoeden, ernstige bezwaren). Het is opmerkelijk dat daarbij de voorwaarden en criteria vooral naar beneden

roep ik in herinnering dat 'de wet van de grote aantallen' niet overal en altijd opgaat, en dat op eenzelfde dataset verschillende algoritmes getraind kunnen worden met heel verschillende uitkomsten.[94]

We zullen moeten leren – als jurist, als rechter, als wetgever, als bestuur – dat het betwisten van de uitkomsten van machinaal lerende systemen tot de kern van het aloude hoor en wederhoor moet gaan behoren. We zullen immuun moeten worden voor de suggestie dat de uitkomsten van computationele technieken noodzakelijkerwijs juist, volledig of zelfs maar relevant zijn in relatie tot verdachten, potentieel verdachten, mogelijk potentieel verdachten en eventueel mogelijk potentieel verdachten. De 'equality of arms' van art. 6 van het EVRM moet opnieuw worden uitgevonden op het moment dat noch de OvJ, noch de rechter, noch de advocaat kunnen narekenen hoe deze nieuw politie-*agents* tot hun 'conclusies' komen. Het zou goed zijn om daarbij het aloude proces-verbaal opnieuw uit te vinden door te eisen dat deze *agents* in toegankelijke logfiles bijhouden wat zij doen, met welk doel, en hoe zij tot resultaat komen.

Uit de informatie die beschikbaar is over het iRN en iColumbo leid ik af dat het in kaart brengen van geaggregeerde en gepersonaliseerde patronen plaats vindt (of zal vinden) op basis van daarmee gelieerde metadata (locatie, telecommunicatie verkeersgegevens), openbaar beschikbare gegevens (gepost op sociale media of anderszins op internet gepubliceerd), in combinatie met gegevens uit andere bestanden (GBA, energieverbruik, sociale zekerheid, belastingaangifte, meldpunt witwassen en zo meer). In hoeverre de bevoegdheid bestaat om gegevensbestanden te koppelen hangt af van de vraag of daarvoor een wettelijke grondslag is,[95] en of is voldaan aan het doelbindingsbeginsel. Dat laatste is binnen het strafrecht bekend als het verbod van *detournement de pouvoir*, dat in beginsel uitsluit dat resultaten verkregen op basis van een specifieke bevoegdheid worden gebruikt voor een doel waarvoor die bevoegdheid niet was verleend. Ik kom daarop terug in paragraaf 3.4.

Het iRN is geen uitvinding van Google of DARPA, zoveel is duidelijk.[96] In het licht van hetgeen grote technologiebedrijven en financieel goed bedeelde onderzoeksinstituten van defensie in de VS intussen uitvinden en ontwikkelen moeten we aannemen dat de overgang van informatie systemen naar data-gestuurde beslissystemen ook binnen de Nederlandse opsporing tot initiatieven in die richting zal leiden. Ik breng in herinnering dat het mij in dit preadvies niet zozeer gaat om informatieverwerking maar om *agents*, dat wil zeggen systemen die hun omgeving niet alleen waarnemen maar daarin ook ingrijpen en in toenemende maat ook kunnen leren van de feedback. Dat is op dit moment – zo lijkt het althans[97] – nog niet aan de orde binnen de opsporing. Het punt is dat alles erop wijst dat het binnenkort wel aan de orde is en dat het in dit geval niet verstandig is om af te wachten en de put te dempen als het kalf verdronken is. Wanneer *agents* eenmaal ontworpen, getest en in omloop zijn gebracht zal het niet eenvoudig zijn om de specifieke combinatie van instrumentaliteit en rechtsbescherming in te bouwen die noodzakelijk is voor een verantwoorde strafvordering. Vandaar het belang van juridische bescherming by design, nader te bespreken in hoofdstuk 4.

---

worden bijgesteld. Zo wenst hij de eis dat sprake moet zijn van een ernstige inbreuk op de rechtsorde maar gewoon af te schaffen omdat hij die eis vaag acht.

[94] Zie hierboven noot 8 en par. 5.

[95] Bijvoorbeeld in het kader van het verkennend onderzoek, waar art. 126hh WSv de bevoegdheid toekent om gegevensbestanden te vorderen van private of publieke partijen en deze te koppelen en bewerken, waarbij lid 2 eventuele beperkingen uit de WPg buiten toepassing verklaart, zie Blom (2015b). Hiervoor is dan wel een machtiging nodig van de rechter-commissaris.

[96] DARPA staat voor Defense Advances Research Projects Agency (onderdeel van Defensie in de VS), die de voorganger van het internet (ARPA-net) uitvond, en in het kader van de 'robotics challenges' aan de wieg stond van de zelfrijdende auto is het gevolg van wedstrijden die werden uitgeschreven door DARPA, cf. Markoff (2015, 2015a). Zie <http://www.darpa.mil>. Google investeert in de high speed ontwikkeling van intuïtieve herkenning van objecten en concepten op basis van ongecontroleerd machinaal leren, met spectaculaire resultaten, zie Hern (2015) en <http://googleresearch.blogspot.co.uk/2015/06/inceptionism-going-deeper-into-neural.html>.

[97] Justitie is niet geneigd inzicht te geven in de gebruikte technologie, zie Van Noort en Kist (2015).

3.3 Aantasting van grondrechten

3.3.1 Het vertekende beeld van de weegschaal

Het beeld van de weegschaal keert altijd weer terug in het recht. En te-recht. Over de misleidende retoriek van de weegschaal wordt intussen regelmatig de klok geluid.[98] Ook dat is terecht. In de strafvordering keert de noodzaak tot afweging voortdurend terug. Ten eerste een afweging van de belangen van derden tegen die van de verdachte en die van 'de maatschappij'; denk aan getuigen, maar ook aan eventueel potentieel verdachten of aan iedereen[99] die op enig moment kan worden gemonitord omdat politie-*agents* ergens een mogelijk verband ontwaren. Ten tweede een afweging van de belangen van de verdachte tegen die van 'de maatschappij'; denk aan vrijheidsbenemende maatregelen in het kader van de maatschappelijke veiligheid. Ten derde het belang van het strafrechtelijk onderzoek tegen de belangen van de verdachte; denk aan vluchtgevaar, of vernietiging van bewijsmateriaal. Ten vierde moeten vaak belangen worden afgewogen tegen een of meer fundamentele rechten; denk aan het belang van de opsporing tegen het belang van privacy, het belang van een redelijk zicht op in de toekomst te plegen strafbare feiten tegen belangen als privacy, non-discriminatie en vrijheid van informatie. Ten vijfde en ten laatste blijken onderscheiden fundamentele rechten in concrete situaties vaak met elkaar te botsen en dus alweer om afweging te vragen.

Hier wil ik kort vijf punten maken, om aan te geven dat een juridische afweging complex is en vooringenomenheid of ongerechtvaardigde ongelijkheid kan verhullen (Waldron 2003, Hildebrandt 2013d). Allereerst is de mogelijkheid om belangen af te wegen tegen rechten niet evident; zij kunnen niet zomaar vergeleken worden. Daarnaast wordt vaak gesuggereerd dat vrijheid een *individuee*l recht of belang zou zijn, terwijl veiligheid een *collectief* recht of *publiek* belang is; dit is evident een verkeerde manier om het debat over afwegingen te 'framen', nu beiden zowel individuele als collectieve, publieke dimensies hebben. In de derde plaats wordt de vrijheid van de ene groep vaak afgewogen tegen de veiligheid van andere groepen; de vrijheid van migranten wordt bijvoorbeeld ingeperkt opdat autochtonen zich veilig voelen. Ten vierde ziet de weegschaal op evenwicht, niet op een trade-off; een trade-off is alleen aan de orde als *noodzakelijkerwijs* vrijheid moet worden ingeleverd om veiligheid te bekomen. Tenslotte, wanneer een trade-off onvermijdelijk is moet de daarmee gemoeide schending van grondrechten worden gecompenseerd (de weegschaal!) door het toekennen van effectieve rechten aan degene wiens grondrecht wordt geschonden. Bij de mogelijke aantasting van of inbreuken op grondrechten speelt de proportionaliteit een prominente rol.[100] Het lijkt er wel eens op dat het invoegen van de spreuk 'rekening houdend met proportionaliteit en subsidiariteit' voldoende is om inbreuken en mogelijke inbreuken bij voorbaat en achteraf te bezweren als zijnde redelijk, zo niet onvermijdelijk. Bij de analyse van de impact van politie-*agents* op relevante grondrechten moeten deze vijf punten in het achterhoofd worden gehouden; het gaat zelden of nooit om een simpele afweging van het ene belang of recht tegen het andere.

3.3.2 De onschuldpresumptie

Geïnspireerd op het Amerikaanse pragmatisme zou ik ten aanzien van de waarheidsvinding in wetenschap en recht willen stellen dat we weliswaar niet aan alles tegelijk kunnen twijfelen, maar in beginsel bereid moeten zijn om het even wat te betwijfelen – en dus, nader te onderzoeken. Dit gaat in het bijzonder op ten aanzien van de bewijslast bij de vaststelling van schuld aan een strafbaar feit, oftewel 'het gedaan hebben'. Dit is een aspect van de onschuldpresumptie, inhoudende dat de bewijslast rust op de Officier van Justitie en dat veroordeling niet mogelijk is wanneer gerede twijfel blijft bestaan over de schuld van de verdachte.

---

[98] Zie bijvoorbeeld de verzuchting van Leyten (1997) die het woord afweging niet meer wilde horen. En de meesterlijke wijze waarop Waldron (2003) de retorische kunstgrepen fileert waarmee de weegschaal allerhande onrecht rechtvaardigt.

[99] Iedereen moet hier worden gelezen als het Engelse *anybody*, niet als *everybody*.

[100] Zie bijvoorbeeld, ten aanzien van de jurisprudentie van het EHRM De Vries e.a. (2011).

Een ander aspect van de onschuldpresumptie betreft de rechtsgevolgen die zijn verbonden met de status van 'verdachte'. Het gaat daarbij om de wijze waarop deze wel en niet bejegend mag worden. In het verlengde daarvan gaat het ook om de status van niet-verdachten die in het kader van de strafvordering in zeer brede zin op het netvlies van politie en justitie verschijnen. Daarbij doet zich de vraag voor of het verstandig is daarbij uit te gaan van de stelling dat we weliswaar niet iedereen tegelijk kunnen verdenken maar ten minste bereid moeten zijn om in beginsel om het even wie te verdenken. De stelling zou kunnen verwijzen naar het beginsel dat bij de opsporing en vervolging van strafbare feiten geen sprake mag zijn van vooringenomenheid, ook en juist wanneer de verleiding daartoe groot is. De stelling kan ook anders worden gelezen, namelijk dat de inzet van politie-*agents* het mogelijk maakt om iedere burger in beginsel te bezien als een potentiele verdachte. In paragraaf 3.2 sprak ik van een status als verdachte of mogelijk verdachte, potentieel mogelijk verdachte of eventueel potentieel mogelijk verdachte. In juridische zin is dat een hachelijke zaak, want alleen de verdachte heeft een juridische status, nu de kwalificatie van 'verdachte' een aantal rechtsgevolgen heeft die haar vaak in een betere positie brengen dan bijvoorbeeld een getuige of zelfs een slachtoffer (bijvoorbeeld het zwijgrecht en andere rechten die voortvloeien uit het *nemo tenetur* beginsel, en de inzage in processtukken die samenhangt met de interne openbaarheid en de vereiste *equality of arms*). Dergelijke rechtsgevolgen zijn niet toegekend aan degene die op basis van data-analyse tot een risicogroep behoort die bijzondere aandacht krijgt, dat wil zeggen nadere observatie of verdergaand onderzoek naar reisgedrag, sociale media netwerk-analyse, energieverbruiksgedrag en zo meer. Het is wel zo dat op basis van de Wet politiegegevens (Wpg) een aantal rechten en plichten zijn verbonden aan het verwerken van de persoonsgegevens van zo'n mogelijk, potentieel mogelijk of eventueel potentieel mogelijk verdachte.[101] De Wpg onderscheidt volgens de *Aanwijzing Wet Politiegegevens en de rol van de Officier van Justitie* 'twee verschillende vormen van doorzoeken van politiegegevens: geautomatiseerd vergelijken (art. 8 lid 2, 11 lid 1, 11 lid 2 en 12 lid 4 Wpg) en in combinatie verwerken (art. 8 lid 3 en 11 lid 4)'.[102] Terwijl de Wpg niet uitlegt wat hieronder moet worden verstaan gaat de *Aanwijzing* uit van het volgende:[103]

> Geautomatiseerd vergelijken: het met een binaire zoeksleutel van (een)trefwoord(en) zoeken van bepaalde politiegegevens. Het resultaat van deze gerichte zoekslag is een uitkomst van hit / no hit. Gecombineerd verwerken: zonder binaire zoeksleutel binnen (een selectie van) beschikbare politiegegevens zoeken naar verbanden. Het resultaat van deze vrije zoekslag is een verzameling van gegevens die voldoen aan bepaalde gemeenschappelijke kenmerken. Deze gemeenschappelijke kenmerken kunnen een profiel van indicatoren of bepaalde kenmerken (trefwoorden) inhouden. Het zoeken met een complex en/of uitgebreid profiel met indicatoren of kenmerken dat is verkregen met een gecombineerde verwerking dient weer gezien te worden als een geautomatiseerde vergelijking. [H]et zoeken met gemeenschappelijke kenmerken [kan] een grote inbreuk op de privacy opleveren en deze verwerking [valt] daarmee snel onder de verwerkingsdoeleinden van art. 9 en 10 Wpg, [w]aaruit veelal nog grotere inbreuken op de privacy voortvloeien.

Hieruit vloeien volgens de *Aanwijzing* dan weer strafprocessuele consequenties voort, met name het begin van verdenking, die reden zijn om deze verwerking te kwalificeren als vallend onder verantwoordelijkheid van de OvJ. De ingewikkelde beschrijving in de *Aanwijzing* ziet op het verschil tussen clustering (ongecontroleerd leren) en classificatie (gecontroleerd leren), waarbij het vaak zo is dat de bij clustering gevonden patronen worden ingezet als classifiers bij een nieuwe ronde gecontroleerd leren.

Ik zou hier dan ook wel van *agents* durven spreken, voor zover deze systemen zelfstandig beslissen welke personen in aanmerking komen voor stelselmatige gegevensverwerking (dan wel bepalende invloed hebben op een bijna-automatische beslissing hieromtrent van een opsporingsambtenaar).

[101] Een politiegegeven is volgens art. 1 sub a Wpg: elk persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt.
[102] Punt 9.1 van de *Aanwijzing Wet Politiegegevens en de rol van de Officier van Justitie* Staatscourant, nr. 24124, 2 september 2013.
[103] Idem.

Dankzij dit soort machinaal leren kan iemand op basis van slimme algoritmes ingedeeld raken in een categorie van nader te monitoren personen. Hoewel het belang van het onderzoek zich wel zal verzetten tegen het verstrekken van profieltransparantie aan specifieke individuen is het toch zaak om inzicht te geven in de vraag of en zo ja, in welk opzicht *men* kan worden geprofileerd.

Verzoeken om transparantie over hoe men zelf wordt geprofileerd (art. 25 Wpg) kunnen inderdaad worden geweigerd, bijvoorbeeld wanneer het onthouden van kennisneming noodzakelijk is in het belang van een goede uitvoering van de politietaak (art. 27 lid 1 sub a Wpg). Hoewel dit begrijpelijk is, zou dit niet in de weg mogen staan aan inzicht in het *type* profilering dat plaatsvindt op een meer abstract niveau, zodat burgers zicht hebben op hoe ze eventueel geprofiled kunnen worden. Het feit dat de Minister in de Contourennota (2015:55) spreekt van heimelijke bevoegdheden indiceert dat het hier gaat om bevoegdheden met 'het kenmerk dat zij heimelijk worden toegepast, hetgeen wil zeggen dat de persoon ten aanzien van wie de bevoegdheid wordt uitgeoefend vooraf van deze toepassing geen kennis heeft en dat hem daarvan pas later in het voorbereidend onderzoek mededeling wordt gedaan.' In dit geval zal het echter vaak gaan om heimelijke plaatsing in een categorie personen ten aanzien van wie min of meer stelselmatig persoonsgegevens zullen worden verwerkt, terwijl dit bij de meesten van hen niet tot een verdenking of een voorbereidend onderzoek zal leiden. Zij zullen hier dus niet achter komen. Op de mogelijkheden om informatie te bekomen inzake het type *agents* waarmee politie en justitie boeven hoopt te vangen kom ik in paragraaf 3.3 terug, bij de bespreking van vrijheid van informatie.

Hoe verhouden deze – merendeels heimelijke – operaties zich nu tot de onschuldpresumptie?[104] Om te beginnen is het goed om de verhouding tussen de onschuldpresumptie als *vermoeden van onschuld* en de verdenking als redelijk *vermoeden van schuld* te bezien.[105] De eerste betreft een regel die het handelen van overheidsdienaren normeert, de tweede betreft een voorwaarde voor het uitoefenen van een aantal bevoegdheden die mogelijk inbreuk maken op grondrechten. In die zin zijn beide niet met elkaar in strijd; het is eerder zo dat de onschuldpresumptie het complement of tegenwicht vormt van de verdenking. Omdat *een ieder* in strafrechtelijke zin voor onschuldig moet worden gehouden totdat de schuld aan een strafbaar feit in rechte is vastgesteld, zal een redelijk vermoeden de presumptie als het ware relevant maken en de gevolgen van dat vermoeden normeren. Dat hangt samen met het feit dat het redelijk vermoeden van schuld lange tijd de enige ingang was voor het toepassen van dwangmiddelen, die niet met punitieve interventies verward mogen worden. Precies vanwege de onschuldpresumptie mogen strafvorderlijke bevoegdheden uitsluitend worden uitgeoefend met het oog op de bewijsvergaring, de onttrekking aan het verkeer, het voorkomen van beïnvloeding van getuigen, vluchtgevaar, en het voorkomen van nog te plegen strafbare feiten. Dwangmiddelen dienen niet de specifieke of generale preventie die uitgaat van de afschrikkende werking van de straf, noch de vergelding of de genoegdoening die immers allemaal inherent zijn aan de punitieve werking van de straf.

De vraag is hoe de onschuldpresumptie zich verhoudt tot veel lichtere graden van verdenking, die niet onder het opsporingsbegrip van art. 132a WSv vallen. Het gaat dan met name om handelingen en beslissingen die (nog) niet met het oog op strafvorderlijke beslissingen worden genomen, maar met het oog op de voorbereiding daarvan (het verkennend onderzoek). De vraag is met name in hoeverre *police intelligence* in zijn algemeenheid en het geautomatiseerd en gecombineerd verwerken van

[104] Zie voor een overzicht van argumenten omtrent de inhoud en reikwijdte van de onschuldpresumptie in juridische en ethische zin Mackor en Geeraets (2013). Ik spits hier toe op de relevantie voor de toepassing van dwangmiddelen en de inzet van agents en laat de andere aspecten van de presumptie grotendeels buiten beschouwing (bijvoorbeeld de strafrechtelijke bewijslastverdeling en het verbod op publiekelijk uitspraken te doen over de schuld van een verdacht die ter zake (nog) niet is veroordeeld of is vrijgesproken (bijvoorbeeld wegens gebrek aan bewijs). Zie ook (Vitkauskas 2012) voor de relevante jurisprudentie van het EHRM.

[105] Vergelijk ook Packer (1968):161-162 en 167), die onderscheidt tussen *factual guilt* ('het gedaan hebben') en *legal guilt* ('aan alle voorwaarden voor strafbaarheid hebben voldaan, zoals vastgesteld door de rechter na een eerlijk proces'), cf. Hildebrandt (2002:341-342).

politiegegevens in het bijzonder, de toepassing van de onschuldpresumptie noodzakelijk maken, evenals de vraag wat zo'n toepassing dan zou inhouden. Uit de jurisprudentie van het EHRM blijkt dat de onschuldpresumptie ook geldt voordat sprake is van een 'criminal charge',[106] ook al lijkt daarover geen overeenstemming te zijn binnen de doctrine.[107] Daarbij gaat het echter vaak om uitspraken inzake de schuld van een verdachte of vrijgesprokene,[108] en niet om de beslissing dat een bepaald persoon 'mogelijk betrokken' is bij een of meer reeds gepleegde, beraamde of nog te plegen strafbare feiten op basis van onderzoek van politiegegevens.

Wanneer politie-*agents* worden gebruikt om te bepalen welke type personen nader worden gemonitord herleeft de prangende vraag naar de reikwijdte van de onschuldpresumptie. Is die van toepassing: (a) als sprake is van enigerlei handeling die mogelijk verband houdt met strafvordering, dus ook onderzoek zoals in de Wpg aangeduid als geautomatiseerd of gecombineerd zoeken, en/of (b) in geval van enigerlei handeling die punitief uitgelegd kan worden, of (c) pas wanneer sprake is van een redelijke verdenking van een strafbaar feit, of (d) uitsluitend in geval van een tenlastelegging?

In dat verband is het goed kennis te nemen van de concept Richtlijn Onschuldpresumptie,[109] die onder 'Toepassingsgebied' stelt:

> De richtlijn is van toepassing op verdachten of beklaagden in strafprocedures vanaf het eerste begin van de strafprocedure, zelfs vóór het moment waarop de verdachten door de bevoegde autoriteiten in kennis worden gesteld van het feit dat ze van een strafbaar feit worden verdacht of beschuldigd. Zij is van toepassing tot het afsluiten van de procedure, dat wil zeggen tot de definitieve beslissing is gegeven.

Zolang strafvorderlijke bevoegdheden zich beperken tot verdachten of personen ten aanzien van wie een vervolgingsbeslissing is genomen lijkt dit een zinnige inperking van de reikwijdte van de onschuldpresumptie. Wanneer echter op grote schaal risicoanalyses worden uitgevoerd op 'big en open data' om zicht te krijgen op criminaliteitspatronen die vervolgens worden toegepast op niet-verdachten, ten einde te beslissen wie in aanmerking komen voor stelselmatige gegevensverwerking,[110] lijkt het moment gekomen om de relevantie van de onschuldpresumptie voor alle burgers wier gegevens worden verwerkt te benadrukken. Dit roept de interessante vraag op of de onschuldpresumptie niet voor alle burgers geldt of hoort te gelden, zoals ik hierboven eigenlijk al formuleerde door te spreken van *een*

---

[106] Het Hof hanteert daarbij een materieel verdenkingscriterium, cf. EHRM, 21 december 2000, nr. 34720/97 (Heaney and McGuinness v. Ireland), r.o. 41; EHRM, 27 november 2008, nr. 36391/02 (Salduz v Turkey) r.o. 50 en 52; EHRM, 14 oktober 2010, nr. 1466/07 (Brusco v. France) r.o. 47; het is niet doorslaggevend of justitie iemand formeel als verdachte kwalificeert, maar of zij de persoon de facto verdenkt.

[107] Zie bijvoorbeeld Weigend (2013:196) over de traditionele betekenis van de onschuldpresumptie: 'a person charged with a crime is to be treated as if he had not committed that crime until the court has found him guilty.' In de Nederlandse context zou het betekenen dat de onschuldpresumptie pas relevant wordt vanaf het moment dat een vervolgingsbeslissing is genomen.

[108] Bijvoorbeeld EHRM 25 maart 1983, nr. 8660/79 (Minelli v. Switzerland) r.o. 25-41; EHRM, 10 februari 1995, nr. 15175/89 (Allenet de Ribemont v. France) r.o. 39-41.

[109] Brussel, 27.11.2013, COM(2013) 821 final, Voorstel voor een Richtlijn van het Europees Parlement en de Raad inzake de versterking van bepaalde aspecten van het vermoeden van onschuld en van het recht om in strafprocedures bij het proces aanwezig te zijn, p. 6 punt 15, (zie ook art. 2 van de concept Richtlijn).

[110] Die beslissing wordt in de Contourennota (2015:56) aangemerkt als een nieuw in te voeren en te normeren strafvorderlijke bevoegdheid, naar analogie van de stelselmatige observatie, waarbij de Contourennota spreekt van 'stelselmatige vastlegging van persoonsgegevens op het internet' zonder aan te geven wat daaronder precies moet worden verstaan en hoe normering plaats vindt. Zie bijvoorbeeld Oerlemans en Koops (2012), die overigens van mening verschillen over de vraag of gegevens die zich achter een wachtwoord of registratie bevinden onder openbaar toegankelijke gegevens mogen worden begrepen.

ieder, geheel los van enigerlei onderzoek of verdenking.[111] In dat geval vallen a t/m d zonder meer binnen het bereik van de presumptie en gaat het er meer om wat deze in onderscheiden omstandigheden betekent. Of nog concreter, welke rechtsgevolgen de presumptie in ieder van de genoemde gevallen heeft. Ik breng in dat verband de articulatie van de strafrechtelijke bewijslastverdeling onder de aandacht, zoals in de concept Richtlijn Onschuldpresumptie geformuleerd als uitvloeisel van de presumptie (art. 5, inzake bewijslast en vereiste bewijsstandaard):[112]

> 1. De lidstaten zorgen ervoor dat de bewijslast voor de vaststelling van de schuld van verdachten of beklaagden op de vervolgende instantie rust. Dit doet geen afbreuk aan enige ambtshalve bevoegdheid van de procesrechter om feitenonderzoek te doen.
> 2. De lidstaten zorgen ervoor dat elk vermoeden dat de bewijslast naar de verdachten of beklaagden verschuift, van voldoende belang is om een afwijking van dit beginsel te rechtvaardigen en weerlegbaar is. Om een dergelijk vermoeden te weerleggen, volstaat het dat de verdediging voldoende bewijs aanvoert om gegronde twijfel te doen ontstaan over de schuld van de verdachte of beklaagde.
> 3. De lidstaten zorgen ervoor dat, wanneer de procesrechter de schuld van een verdachte of beklaagde onderzoekt en er gegronde twijfel bestaat over de schuld van de betrokkene, deze wordt vrijgesproken.

Mij dunkt dat deze verwoording van de bewijslastverdeling, als volgend uit de onschuldpresumptie, op zichzelf genomen niet opzienbarend is, maar in het licht van de inzet van politie-*agents* opnieuw relevant wordt. De onschuldpresumptie betreft traditioneel verdenking van reeds gepleegde strafbare feiten, de poging daartoe en de voorbereiding daarvan (voor zover die ook strafbaar zijn). Het is alvast pertinent om bovenstaande definitie uit te breiden naar personen ten aanzien waarvan *aanwijzingen voor* of *verdenking van* reeds beraamde strafbare feiten aanleiding zijn om opsporingsbevoegdheden uit te oefenen, ook wanneer die beraming zelf niet strafbaar is. Ingevolge het verkennend onderzoek is die beraming immers aanleiding voor de inzet van heimelijke dwangmiddelen. Het gaat dan echter nog steeds om reeds gepleegde, gepoogde, voorbereide of beraamde strafbare feiten. Wat nu als semi-strafvorderlijke bevoegdheden ontstaan ten aanzien van verdenking van of aanwijzingen voor strafbare feiten die gepleegd, gepoogd, voorbereid en beraamd *gaan worden*? Dit zal immers kunnen volgen uit de verwerking van politiegegevens. Wat nu als daarbij ook categorieën personen worden gedetecteerd die een grote kans maken een specifiek type strafbare feiten te *zullen* plegen, pogen, voorbereiden of beramen? Die kans is berekend door *agents* en ik heb de stille hoop dat de lezer inmiddels wil aannemen dat we hier niet over science fiction spreken. Geldt de onschuldpresumptie ook ten aanzien van verdenking van of aanwijzingen voor nog te plegen, nog te pogen, nog voor te bereiden en nog te beramen misdrijven? Of sluit het feit dat er nog niets is gepleegd, gepoogd, voorbereid of beraamd de toepassing van strafvorderlijke bevoegdheden uit en dus ook de onschuldpresumptie? Ik denk dat het in dit geval verstandig is om vooruit te lopen op het moment dat zulke semi-strafvorderlijke bevoegdheden worden ingevoerd door vast te stellen dat ten aanzien van mogelijk betrokkenen in ieder geval de onschuldpresumptie geldt.

Bijkomende vraag is of die grotere kans op schending van een strafrechtelijk beschermde norm in geval van *overtredingen* mag leiden tot een omkering van de bewijslast in de zin van art. 5 lid 2 van de concept Richtlijn ten aanzien van de oplegging van een boete? Of kan het zijn dat dit toch te ver gaat, maar dat op enig moment wel degelijk strafvorderlijke bevoegdheden kunnen worden uitgeoefend in

---

[111] Zie Duff (2013:171) over verschillende varianten van de presumptie: 'Some argue that the PoI [presumption of innocence, mh] operates only within the trial, as a rule that lays the burden of proof on the prosecution. Others argue that it applies more broadly: for instance that it incorporates all the demands of due process; that it applies to pre-trial detention as well as to the trial; that it is implicated if samples of DNA are retained even from those who have not been convicted; that it might have implications for the process of criminalization; that it is an aspect of a broad "principle of civility" that governs our civic dealings with each other.'

[112] Sinds jaar en dag, maar zeker sinds Salabiaku (EHRM 7 oktober 1988, Serie A, no. 141-A) wordt een objectieve delictsomschrijving bij minder ernstige strafbare feiten geduld, mits de verdediging de kans heeft het daarmee gegeven schuldvermoeden te weerleggen.

het kader van een verder uitgebreid verkennend onderzoek – ook al is geen sprake van een reeds gepleegd, gepoogd, voorbereid of beraamd strafbaar feit? Absurd? Gezien de gestage verzelfstandiging van het voorbereidend onderzoek, de reeds bestaande mogelijkheid in te grijpen ingevolge aanwijzingen dat misdrijven worden beraamd en de inzet van politie-*agents* lijkt me deze wending niet ondenkbaar. Maar wel evident in strijd met de onschuldpresumptie.

Het rechtsgevolg van de toepassing van de onschuldpresumptie op de uitbreiding (van strafbaarheid of van heimelijke bevoegdheden) tot bijvoorbeeld het voornemen of zelfs de neiging om strafbare feiten te beramen, voor te bereiden, te pogen of te plegen, zou moeten zijn dat zulk een bestraffing en de uitoefening van dergelijk bevoegdheden – ook al zou de wetgever ze invoeren – onrechtmatig zijn. Hoe sneller en grondiger we ons bezinnen op dit soort 'pre-crime punishment' des te beter.

Een laatste punt. Schending van de onschuldpresumptie door het stelselmatig verwerken van persoonsgegevens van iemand die niet verdacht is, en waartegen geen aanwijzingen bestaan, zal vaak nauw samenhangen met mogelijke discriminatie en aantasting van de privacy van degenen die – zonder dit te weten - onder verscherpt toezicht komen te staan. De betreffende schending wordt vanwege de relativiteitsleer (*Schutznorm*) echter niet binnen het strafrecht afgerekend wanneer het niet de privacy (of het recht op non-discriminatie) van de verdachte betreft,[113] of wanneer het überhaupt niet tot een tenlastelegging komt. Schending van de onschuldpresumptie is dan ook bijzonder relevant in dit nieuwe voorveld van de strafvordering en de opsporing, omdat het grenzen stelt aan het handelen van de overheid. Met name wanneer de mogelijkheden om over te gaan tot automatische punitieve handhaving nog verder worden uitgebreid, en wanneer ze bijvoorbeeld pro-actief en zelfs pre-emptief kunnen worden uitgevoerd is het zaak de onschuldpresumptie in te roepen om de onrechtmatigheid vast te stellen. In het bijzonder strafrecht en in het bestuursstrafrecht is geautomatiseerde handhaving al sinds jaar en dag aan de orde, denk aan boetes voor verkeersovertredingen. Op het moment dat burgers met dank aan voortdurende monitoring steeds vaker te maken krijgen met een veelheid van buitengerechtelijke boetes en andere 'punitieve maatregelen' biedt de theoretische mogelijkheid om naar de rechter te stappen geen bescherming meer. De toetsingsvrijheid van de rechter is sowieso vaak sterk ingeperkt,[114] en wie heeft de tijd en de middelen om bij voortduring de gang naar de rechter te

[113] Over de *Schutznorm*, zie HR 16 september 2014, ECLI:NL:HR:2014:2749, NJ 2014/462, m. nt. Schalken, r.o. 2.5.2 waar de Hoge Raad in lijn met eerdere jurisprudentie vaststelt dat 'Indien het niet de verdachte is die door de niet-naleving van het voorschrift is getroffen in het belang dat de overtreden norm beoogt te beschermen, geldt bovendien dat in de te berechten zaak als regel geen rechtsgevolg zal behoeven te worden verbonden aan het verzuim (vgl. HR 19 februari 2013, ECLI:NL:HR:2013:BY5321, NJ 2013/308).'

[114] Art. 8 Wet administratiefrechtelijke handhaving verkeersvoorschriften biedt zeer beperkte gronden voor vernietiging van de administratieve sanctie wegens *gedragingen* die steeds vaker op geautomatiseerde wijze worden vastgesteld (het gaat dan ook niet over handelingen). In het verlengde hiervan wordt door het OM regelmatig om machtiging verzocht voor toepassing van het dwangmiddel van de gijzeling. Kantonrechters lijken zich tegen het automatisme te verzetten door een zware bewijslast op het OM te leggen inzake de eis van proportionaliteit en subsidiariteit (zie bijvoorbeeld de afwijzing van het verzoek door Rechtbank Zeeland-West-Brabant, 11 december 2014, ECLI:NL:RBZWB:2014:9017). In 2013 werd door 37.000 maal een verzoek tot gijzeling wegens niet voldoen van boetes ingevolge de WAHV aangevraagd, (Redactie AD 2014). Inmiddels hebben we ook rechtspraak over geautomatiseerde verhoging van opgelegde boetes (een verhoging van niet-betaalde administratiekosten van 6 euro naar 711 euro), waarbij de rechter zich afvraagt waar het CJIB mee bezig denkt te zijn, zie Rechtbank Zeeland-West-Brabant, 28 maart 2013, ECLI:NL:RBZWB:2013:CA0211. Zie ook (Jensma, Barkhuysen en Hulskamp 2013). Tenslotte nog de vraag of een volledig geautomatiseerde boetebeschikking nog wel in overeenstemming is met art. 3.2 WAHV als het feitelijk de computer is die de boete vaststelt. Na een eerdere beslissing dat de boete onrechtmatig was opgelegd (Gerechtshof Arnhem-Leeuwarden 20 februari 2014, ECLI:NL:GHARL:2014:1236), meent het hof in een latere zaak 'dat het verwerkingsproces bij de op geautomatiseerde wijze vastgestelde gedraging "niet de vereiste verzekering afsluiten en in stand houden" zodanig is ingericht dat het opleggen van de boetes aan een bevoegde ambtenaar kan worden toegerekend,' (Gerechtshof Arnhem-Leeuwarden 5 juni 2014, ECLI:NL:GHARL:2014:4324). Kennelijk acht het hof voldoende dat de *agent* die boetes oplegt onder verantwoordelijkheid van een bevoegde ambtenaar valt.

bewandelen voor allerlei lichte straffen.[115] Ook daarom is het zaak de onschuldpresumptie in herinnering te roepen en te erkennen dat met de voortgaande verzelfstandiging van het voorbereidend onderzoek de rechtsgevolgen van de toepassing van de onschuldpresumptie een belangrijk tegenwicht kunnen gaan vormen als het gaat om buitengerechtelijk onderzoek en buitengerechtelijke bestraffing. Cruciale vraag is dan wel wie de naleving van strafvorderlijke normen kan toetsen als de rechter hier niet aan te pas komt.

3.3.3 Gegevensbescherming, privacy, non-discriminatie en vrijheid van informatie

De rechten in data, bestanden en methoden bestaan uit de fundamentele rechten op gegevensbescherming, privacy, vrijheid van informatie, het auteursrecht (op software en op databanken), het sui generis recht op databanken en soms wellicht het patentenrecht (op software en hardware). Al deze rechten zijn in beginsel absolute rechten in die zin dat ze tegenover een ieder kunnen worden gehandhaafd.[116] Dat betekent uiteraard niet dat deze rechten absoluut zijn in de zin van onbeperkt. Het feit dat het om absolute rechten gaat impliceert ook niet noodzakelijkerwijs dat het exclusieve rechten zijn in de zin dat de rechthebbende in beginsel het exclusieve recht heeft om het uitsluiting van alle anderen over de data, bestanden en methoden te beschikken. Dat is overigens wel het geval bij de IP-rechten, maar dat komt dus niet omdat het absolute rechten zijn in bovengenoemde zin: handhaafbaar tegenover een ieder. Wanneer de rechthebbende haar beschikkingsrecht door middel van een overeenkomst inperkt kan daar overigens een relatief recht uit voortvloeien, bijvoorbeeld een licentie om een ebook te downloaden of een licentie om persoonsgegevens voor een specifiek doel te gaan verwerken.[117]

Met name het recht op gegevensbescherming wordt ten onrechte vaak gekwalificeerd als een soort van eigendomsrecht, alsof het recht om gegevens te verwerken exclusief zou toekomen aan het data subject.[118] Dat is volkomen onzinnig. Het zou betekenen dat het verwerken van een gegeven zoals mijn naam een exclusief recht van mijzelf zou zijn, terwijl de naam nu juist een manier is om mij aan te spreken en aan te duiden binnen enigerlei vorm van gezelschap. Robinson Crusoë had geen naam (nodig) voordat Vrijdag arriveerde.

Het grondrecht op gegevensbescherming is een bundel rechten die onder meer de verhouding regelt tussen een data subject (de identificeerbare natuurlijke persoon naar wie een data verwijst) en een of meer data controller(s) (degene die het doel en de middelen van een verwerking bepaalt).[119] Binnen die verhouding *kan* het fundamentele recht op gegevensbescherming (van het data subject) ook beschikkingsrechten omvatten, namelijk daar waar het data subject het verwerken van haar gegevens kan toestaan (en dus ook kan weigeren) of een overeenkomst kan sluiten omtrent het gebruik van de gegevens (dataverwerkingslicentie), zolang die verwerking aan de overige eisen van het gegevensbeschermingrecht voldoet.[120]

---

[115] Wie tijd heeft zou weleens geen geld kunnen hebben, terwijl wie het geld hebben weleens geen tijd zouden kunnen hebben.

[116] Pitlo e.a. (1995). Het complement van absolute rechten zijn relatieve rechten, die niet tegenover een ieder maar alleen tegenover specifieke rechtssubjecten kunnen worden ingeroepen (bijvoorbeeld rechten uit overeenkomst of onrechtmatige daad).

[117] Binnen het KP7 EU project USEMP hebben wij daartoe een zogenaamde data licensing agreement (DLA) ontwikkeld. Zie <http://www.usemp-project.eu>.

[118] Novotny en Spiekermann (2013) pleiten op grond van gedragseconomische argumenten voor een soort eigendomsrecht in persoonsgegevens. Voor een gedegen analyse van de zin en onzin van eigendomsrechten op persoonsgegevens zie bijvoorbeeld Purtova (2012).

[119] De Nederlandse vertaling van 'betrokkene' en 'verantwoordelijke' vind ik minder gelukkig dan de Engelse termen 'data subject' en 'data controller'. Betrokkene is mij te vaag en te bestuursrechtelijk en geeft minder direct aan dat het om het subject van een data gaat (de verwijzing naar het begrip persoonsgegeven gaat verloren bij gebruik van de term 'betrokkene'); verantwoordelijke verwijst niet expliciet naar degene die controle heeft over de data.

[120] In ieder geval heeft het data subject een aantal transparantierechten – ook wanneer haar toestemming of contractuele instemming niet nodig zijn.

Als het gaat om de verwerking van persoonsgegevens in het kader van politie en justitie geldt een ander regiem, nu de reguliere gegevensbescherming niet van toepassing is. In Nederland is die verwerking geregeld in de hierboven al besproken Wpg, die impliceert dat het data subject tegenover politie en justitie niet kan beschikken over de verwerking in het kader van de politietaak. Niet omdat politie of justitie nu ineens eigenaar zijn geworden van de data, maar omdat zij een wettelijke grondslag hebben om – ook als het data subject dat niet zo prettig vindt – haar gegevens te verwerken. In specifieke gevallen en onder specifieke voorwaarden. Het zal dan vaak gaan om gedragsgegevens en metadata, die data subjecten niet zelf aanleveren maar die door de ICT infrastructuur waarvan zij gebruik maken mogelijk worden gemaakt (locatie en verkeersgegevens van mobiele telefonie, IP adressen en metadata van email verkeer, de graaf van het sociale netwerk, of het surfgedrag dat bij de provider van de browser en het zoekgedrag dat bij de provider van de zoekmachine kan worden opgevraagd).

Het feit dat de betreffende telecomproviders, 'content' providers en andere dienstverleners beschikkingsrechten hebben in deze gegevens (verwerking voor een specifiek en tevoren geëxpliciteerd doel, art. 7 en 9 Wbp, op een van de juridische gronden uit art. 8 WBP) sluit niet uit dat politie en justitie ook beschikkingsrechten hebben in de data – onder bepaalde voorwaarden en met het oog op specifieke doelen, conform de Wpg. Die rechten en bevoegdheden sluiten bovendien niet uit dat ook het data subject rechten heeft in deze persoonsgegevens (met name transparantierechten, correctie- en verzetsrechten, art. 16-20 Kaderbesluit gegevensbescherming inzake politiële en justitiële samenwerking, art. 25-28 Wpg).[121]

Anders dan IP rechten is het dataverwerkingsrecht in beginsel dus geen exclusief recht. Terwijl het recht om te beslissen over publicatie, verspreiding en vermenigvuldiging van een werk uitsluitend toekomt aan de auteur, is de bundel van rechten die voortvloeien uit het gegevensbeschermingsrecht niet per se exclusief. Wanneer de overheid een wettelijke verwerkingsgrond heeft en binnen de bandbreedte van een geëxpliciteerd, specifiek en legitiem doel blijft, heeft diezelfde overheid een specifiek beschikkingsrecht ten aanzien van de betreffende data. Datzelfde geldt in beginsel dus ook voor een bedrijf dat persoonsgegevens nodig heeft om aan haar contractuele verplichtingen te voldoen en zelfs voor een bedrijf dat de gegevens moet verwerken in het kader van haar legitieme belang (cf. art. 8 sub f Wbp). In dat laatste geval eist het recht echter dat daarmee de fundamentele rechten van het data subject niet overruled mogen worden; hier wordt een afweging vereist. De rechten die personen en rechtspersonen hebben in data, bestanden en methoden kunnen dus botsen, zelfs *binnen* het kader van het gegevensbeschermingsrecht.

De inzet van data-gestuurde *agents* in het kader van de strafvordering vormt al snel een aantasting van diverse grondrechten die verband houden met de verwerking van persoonsgegevens. Ten aanzien van het grondrecht op gegevensbescherming (art. 8 Handvest Grondrechten van de Europese Unie, dat deels doorwerkt in art. 8 EVRM)[122] heb ik hierboven al specifiek gekeken naar de wijze waarop de inzet van politie-*agents* in de Wpg wordt genormeerd. Het grondrecht op gegevensbescherming is vaak een instrument om andere grondrechten te beschermen, toegespitst op de specifieke implicaties van de verwerking van persoonsgegevens. Ik beperk mij hier dan ook tot een verwijzing naar de paragraaf over de onschuldpresumptie en de nog te bespreken grondrechten van non-discriminatie en vrijheid van informatie. Tenslotte zal ik er in de paragraaf over legaliteit en doelbinding nog eens op terugkomen. Het lijkt me bovendien verstandig om weerstand te bieden aan de wijdverbreide neiging om de problemen die door de inzet van *agents* worden gegenereerd zoveel mogelijk onder de noemer van

[121] Het feit dat het fundamentele recht op gegevensbescherming absoluut is in die zin dat het tegenover eenieder gehandhaafd kan worden sluit niet uit dat daarop uitzonderingen bestaan, waardoor de uitwerking van genoemd recht bijvoorbeeld niet in Richtlijn 95/46 EG maar in Kaderbesluit 2008/977/JBZ van de Raad moet worden gezocht. Ook het eigendomsrecht wordt ingeperkt, bijvoorbeeld door onteigening, inbeslagname, onttrekking aan het verkeer en door het leerstuk van misbruik van bevoegdheid.

[122] Zie bijvoorbeeld paragraaf 2 in Koning (2015) en hoofdstuk 4 in González Fuster (2014).

privacy 'af te handelen'. Daarmee bedoel ik zeker niet te stellen dat privacy niet aan de orde is, maar ik ga de mij toegemeten ruimte niet besteden aan de reeds goed beschreven afweging tussen het fundamentele recht op privacy enerzijds en het belang van het opsporingsonderzoek, van de geschokte rechtsorde, van het voorkomen van gevaar en het veiligstellen van mogelijk bewijsmateriaal anderzijds.[123] Ik merk daarbij op dat het mij hier vooral ook gaat om het verruimen van het blikveld door scherp te stellen op *agents* in plaats van gegevensbescherming *an sich*. Dat betekent vooral dat de eis van voorzienbaarheid opnieuw doordacht moet worden, nu met name *agents* die opereren op basis van ML geacht worden problemen oplossen juist omdat zij enigszins onvoorspelbaar zijn.

Het grondrecht op non-discriminatie speelt in het strafrecht een grote rol, omdat het profileren van 'mogelijke betrokkenen' bij eventueel nog te plegen strafbare feiten gemakkelijk leidt tot het categoriseren van groepen van personen die zouden neigen tot strafbaar gedrag. Zoals bijvoorbeeld Zedner (2008) opmerkt zijn er belangrijke morele – en ik zou zeggen ook politieke[124] - gronden om het systematisch monitoren van specifieke groepen te verwerpen, enerzijds vanwege de stigmatiserende werking en anderzijds vanwege het effect van een self-fulfilling prophesy. Harcourt (2007) heeft intussen mooi aangetoond dat de statistiek die het voorspellen van crimineel gedrag onderbouwt geen goede raadgever is als het gaat om het verdelen van de aandacht van de politie.[125] Hij wijst erop dat de hoge verwachtingen van pre-emptief politie optreden gebaseerd zijn op de elasticiteit van de 'vraag naar' criminaliteit.[126] Zo'n elasticiteit zou betekenen dat criminaliteit meer en beter kan worden teruggedrongen wanneer politie en justitie zich bij de inzet van middelen concentreert op personen die voorspelbaar meer crimineel gedrag zullen vertonen. Die veronderstelling gaat volgens Harcourt niet op omdat de vraag niet noodzakelijk elastisch is. Ten eerste omdat zelfs wanneer de voorspellingen zouden kloppen dit niet betekent dat de motivatie om strafbare feiten te plegen afneemt door extra inzet (afschrikking werkt niet bij alle vormen van criminaliteit). Ten tweede omdat herverdeling van middelen

[123] Over de complexe interactie tussen beide Europese constitutionele hoven De Hert en Gutwirth (2009); over de relevante afwegingen vanuit het perspectief van de Nederlandse Grondwet Koops (2011). In EHRM, 29 juni 2006, nr. 54934/00 (Weber en Saravia/Duitsland) heeft het EHRM de eisen samengevat die gesteld moeten worden aan interceptie van en toegang tot informatie die een inbreuk vormt op art. 8.1 EVRM. In r.o. 95 overweegt het Straatsburgse Hof dat de volgende waarborgen wettelijk geregeld moeten zijn: de aard van de strafbare feiten die aanleiding kunnen zijn voor interceptie; duidelijke afbakening van de categorieën personen wiens telefoon mag worden afgetapt; afbakening van de periode gedurende welke mag wordt afgetapt; de te volgen procedure bij analyse, gebruik en opslag van verkregen data; te nemen voorzorgsmaatregelen bij het doorgeven van de data aan andere partijen; en de voorwaarden waaronder opgeslagen informatie kan of moet worden vernietigd, eventueel inclusief de informatiedragers). Zie ook EHRM 1 juli 2008, 58243/00 (Liberty e.a./Verenigd Koninkrijk). Ten aanzien van de analyse van metadata is het nu interessanter te verwijzen naar de interpretatie van het HJEU, 8 april 2014, C-293/12 en C-594/12 (Digital Rights Ireland/Ierland), dat – in lijn met de jurisprudentie van het EHRM – oordeelde over de Richtlijn Data Retentie (24/2006/EG) en deze wegens een gebrek aan noodzakelijke waarborgen nietig verklaarde (zie r.o. 62-68). Het Luxemburgse Hof baseert zich daarbij op de onderling verbonden maar niet met elkaar gelijk te stellen grondrechten op privacy en gegevensbescherming (art. 7 en 8 Handvest Fundamentele Rechten van de Europese Unie). Bij data-gestuurde opsporing is het probleem vooral (r.o. 27): 'Uit deze gegevens, in hun geheel beschouwd, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren'.

[124] Het opdelen van de samenleving in allerlei data-gestuurde 'groepen' die meer of minder neigen tot crimineel gedrag leidt tot problematische fragmentering en gebrek aan nadruk op wat mensen bindt en zou moeten binden (het slaat de bodem weg onder het democratisch debat over wat ons zou moeten binden); vergelijk de argumenten die Sunstein (2001) aanvoert tegen het gepersonaliseerd filteren van online nieuws.

[125] Over de inzet van crime mapping Coldren, Huntoon en Medaris (2013), en bijvoorbeeld Cope (2004). Zie ook Hoogenboom (2010) en Hildebrandt (2016b te verschijnen).

[126] Elasticiteit is een begrip uit de micro economie en wordt gebruikt om de afstemming van vraag en aanbod via het prijsmechanisme te beschrijven. Normaliter neemt de vraag toe als de prijs daalt (dat heet prijselasticiteit). Er zijn echter allerlei omstandigheden waarin deze correlatie niet opgaat. Harcourt beargumenteert dat die elasticiteit bij het begaan van strafbare feiten vaak niet opgaat, omdat de motieven voor het plegen van bijvoorbeeld geweldsdelicten niet noodzakelijk samenhangen met angst voor straf (die hier als te betalen prijs wordt gezien).

op basis van statistiek zal leiden tot minder oog voor degenen die voorspelbaar minder strafbare feiten plegen. Volgens Harcourt mogen we echter niet veronderstellen dat dit *niet* zal leiden tot meer strafbaar handelen bij die specifieke groep. Dat laatste is ook problematisch omdat een eventuele toename minder zichtbaar zal zijn juist omdat er minder op wordt gelet. Ten derde is er het verschijnsel van 'overfitting' dat ertoe kan leiden dat politie-*agents* gaandeweg minder goed in staat zijn om 'outliers' waar te nemen die buiten het model vallen. Dit is een bekend probleem in ML en kan op allerlei manieren worden ondervangen, maar dat vraagt dan wel een waakzaam oog op de vooroordelen die zich in toepassingen van ML nestelen.[127]

Wanneer de opsporing in toenemende mate gebruik gaat maken van politie-*agents*, moet de rechter in staat zijn contra-expertise te beoordelen die de ML van deze *agents* kan aanvechten of evalueren.[128] Heikel punt blijft echter dat de meeste implicaties van de inzet van deze *agents* door de verzelfstandiging van het vooronderzoek buiten de aandacht van de rechter blijven. Cruciale vraag is dan ook wie de inzet van deze agents wel kan toetsen.

De inzet van politie-*agents* zal steeds berusten op de verwerking van politiegegevens,[129] daarmee is ook enige bescherming tegen verboden discriminatie gegeven. Artikel 5 Wpg stipuleert dat verwerking van gegevens met betrekking tot iemands 'godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging, slechts plaats [vindt] in aanvulling op de verwerking van andere politiegegevens en voor zover dit voor het doel van de verwerking onvermijdelijk is.' De grote vraag is wat dat betekent voor geautomatiseerd zoeken en in combinatie zoeken, waarbij immers al gauw sprake is van aanvullende gegevens. Sterker nog, dankzij slimme *agents* kun je datapunten vinden die redelijk betrouwbaar correleren met genoemde gegevens, zodat je zonder deze gegevens direct te verwerken, toch in staat bent om indirect op ras, geloof of vakbondslidmaatschap te discrimineren. Naar analogie van de anti-discriminatie wetgeving zou indirecte discriminatie op basis van dit type gegevens eveneens onder het verzwaard regiem moeten komen.[130] Dat wil zeggen dat naast deze - of ermee correlerende - datapunten altijd aanvullende gegevens in de analyse moeten worden betrokken, en dat er altijd sprake moet zijn van een verzwaarde noodzakelijkheidseis (onvermijdelijkheid).

Om te achterhalen of bepaalde politie-*agents* tot indirecte discriminatie leiden, doordat zij selecteren op kenmerken die bij nader inzien correleren met art. 5 Wpg gegevens, kunnen daarvoor ontwikkelende technieken worden ingezet, zoals 'discrimination aware data mining' (Pedreshi, Ruggieri en Turini 2008). Ik kom dan ook tot een diametraal tegenovergestelde positie dan die van de Moerel en Prins, die menen dat het speciaal regiem voor bijzondere persoonsgegevens beter afgeschaft kan worden.[131]

---

[127] Over machinaal leren Russell en Norvig (2009:693-859). Bias kan voortkomen uit overfitting (idem:705, 736), maar natuurlijk ook uit vooroordelen die verdisconteerd zijn in de input data. In dezelfde zin Mitchell (1997:42-45), die expliciteert dat machinaal leren bias veronderstelt om van nut te kunnen zijn, een inzicht dat de hermeneutici onder ons niet zal verbazen, cf. Gadamer (1990).

[128] Over de catch-22 die hiermee gemoeid is Hildebrandt (2004).

[129] Die zijn immers terecht tautologisch gedefinieerd als: elk persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt (art. 1 sub a Wpg). Dat een gegeven een politiegegeven is mag dus niet worden begrepen als een intrinsieke eigenschap van een bepaald type gegeven; ieder persoonsgegeven kan – indien noodzakelijk voor de uitoefening van de politietaak – een politiegegeven worden. Sterker nog, ook als het niet noodzakelijk was, valt het onder de Wpg (die niet-noodzakelijke verwerking als onrechtmatig kwalificeert, art. 3.1 Wpg).

[130] Art. 1 sub c Algemene Wet Gelijke Behandeling definieert indirect onderscheid als: 'indien een ogenschijnlijk neutrale bepaling, maatstaf of handelwijze personen met een bepaalde godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht, nationaliteit, hetero- of homoseksuele gerichtheid of burgerlijke staat in vergelijking met andere personen bijzonder treft.' Dit is een objectieve maatstaf. Zie bijvoorbeeld EHRM, 13 november 2007, 57325/00 (D.H. e.a./Tsjechië).

[131] Verboden discriminatie speelt immers niet alleen binnen het strafrecht, maar ook binnen de private sector. De niet-haalbaarheid van het speciale regiem is in de huidige situatie inderdaad evident. Dat moet echter niet leiden

Het grondrecht op vrijheid van informatie verwijst in dit verband naar het grondrecht om overheidsinformatie op te vragen en te ontvangen.[132] In Nederland gaat het dan om de reeds besproken Wpg, de Wet Openbaarheid van Bestuur 1991 (Wob), en de Wet hergebruik van overheidsinformatie 2015 (Who).[133] We moeten daarbij onderscheid maken tussen drie situaties: (1) een persoon die verzoekt om inzage (of correctie) van op haarzelf betrekking hebbende persoonsgegevens; (2) een persoon of instantie die verzoekt om specifieke overheidsinformatie openbaar te maken, of (3) te mogen hergebruiken. In het tweede of derde geval zal het vaak niet om persoonsgegevens gaan, hoewel evident complicaties optreden als dat wel het geval is.[134] Het opvragen van persoonsgegevens die door de politie worden verwerkt valt bij uitsluiting onder de Wpg, die - naast regels voor de verstrekking aan degene die het betreft - een eigen regiem kent voor de verstrekking van politiegegevens aan andere instanties.[135] Met betrekking tot de inzet van *agents* is het echter belangrijk om te kunnen voorzien welke type verbanden worden gezocht in welk type gegevensbestanden, en met welke technologie dit gebeurt. Het vrijgeven van het geheime TNO rapport over digitale herkenningstechnieken is een mooi voorbeeld van wat vrijheid van informatie kan betekenen als het gaat om politie-*agents*.[136] Dit rapport is echter evident achterhaald. Zowel het voorbeeld van CityPulse als een blik op de technologie die op de markt is voor politie, veiligheids- en inlichtingendiensten maken duidelijk dat ook wordt geëxperimenteerd met meer geavanceerde patroonherkenning.[137] In dat kader zou het interessant kunnen zijn om te zijner tijd een verzoek in te dienen op grond van de Who om onderzoek te mogen doen via Pentland's Safe Answers

---

tot afschaffing, maar tot het inbouwen van adequate bescherming in de cyberfysieke infrastructuur, waarbij met name het doormeten van indirecte discriminatie van groot maatschappelijk belang zal zijn. Dat zal alleen gebeuren als de bescherming van deze gegevens onder de komende Avg daadwerkelijk gehandhaafd wordt. Gezien de boetebepalingen in de Avg (tot aan 4% van de wereldomzet) ben ik daarover optimistischer dan Moerel en Prins. Dat het speciaal regiem tot onnodige bescherming leidt lijkt mij gezien de uitzonderingen niet houdbaar, tenzij daarmee wordt bedoeld dat het onwenselijk is dat data controllers moeten onderzoeken of een uitzondering van toepassing is. Dat onderzoek zal echter terugkeren in het kader van de door Moerel en Prins voorgestane toets aan het 'gerechtvaardigd belang', maar nu als minder zichtbaar en nog casuistischer criterium voor de afweging.

[132] Andere implicaties van de vrijheid van informatie zijn hier niet direct relevant, zoals de vrijheid van betoging en de vrijheid van meningsuiting, zie art. 7 Grondwet, art. 10 EHRM en art. 11 Hv (vrijheid van meningsuiting), dat naar vaste jurisprudentie ook het recht op het ontvangen van informatie omvat (als zodanig ook geformuleerd in 10 EVRM en 11 Hv). Dit gaat echter om het recht om kennis te nemen van informatie die door om het even welke partij wordt geuit; het betreft een verbod op overheidscensuur. In Nederland is het recht op openbaarheid van bestuur apart geregeld in art. 110 Grondwet. Een ander relevant aspect van de vrijheid van informatie betreft het 'chilling effect' dat uitgaat van het besef dat politie en justitie steeds meer toegang claimen tot telecommunicatie. Dit kan indirect leiden tot deuken in de vrijheid van meningsuiting.

[133] De Who is in feite een rib uit het lijf van de Wob (hoofdstuk V-A wordt uit de Wob gelicht). De Wob betreft toegang tot overheidsinformatie, de Who gaat om hergebruik en stipuleert dat deze informatie zo mogelijk in elektronisch formaat wordt aangeleverd. De invoering is vooral het resultaat van de aanpassingen van de Richtlijn inzake hergebruik overheidsinformatie 2013/37/EU, die nu een verplichting bevat tot het ter beschikking stellen van alle overheidsinformatie, behoudens een aantal uitzonderingen.

[134] Art. 10.1 sub d Wob sluit verstrekking van persoonsgegevens op basis van de Wob uit 'tenzij de verstrekking kennelijk geen inbreuk op de persoonlijke levenssfeer maakt.' Dit is interessant omdat het aansluit bij het recht op privacy dat met de ontsluiting van persoonsgegevens gemoeid kan zijn. Het enkele feit dat het om een persoonsgegeven gaat is dus niet doorslaggevend. Zie ook art. 2.1 sub g Who, die hergebruik uitsluit van 'informatie die betrekking heeft op openbare persoonsgegevens waarvan hergebruik onverenigbaar is met de doeleinden waarvoor ze zijn verkregen'. Hier wordt aangesloten bij het doelbindingsbeginsel uit het gegevensbeschermingsrecht, met name voor openbare persoonsgegevens (bijvoorbeeld informatie die gebruikers zelf op openbaar beschikbare delen van het web zetten).

[135] Zie paragraaf 3 van de Wpg inzake verstrekking aan anderen dan politie en marechaussee. De regeling van de Wpg sluit toepasselijkheid van de Wob uit, zie Afdeling Bestuursrechtspraak Raad van State, 4 februari 2015, 201309828/1/A3, r.o. 3.1.

[136] Zie hierboven noot 91. Vergelijk ook het onderzoek naar audits inzake uitvoering van de Wpg (Bits of Freedom 2012), dat beschikbaar kwam na vele Wob verzoeken om de resultaten van de audits boven water te krijgen.

[137] Zie Van Noort en Kist (2015) die wijzen op marktleider IBM die zelf aangeeft zaken te doen met Nederlandse politiekorpsen. Zie verder hoofdstuk 4 inzake het 'Living Labs' experiment in Eindhoven, met predictieve policing technologie van ATOS.

technologie, waarbij geen toegang wordt gegeven tot de politiegegevens zelf, maar wel inzicht kan worden verkregen omtrent, bijvoorbeeld, criminaliteitspatronen.[138] Dat is niet alleen interessant voor hen die overwegen strafbare feiten te plegen maar ook voor wetenschappelijk onderzoekers, security bedrijven, en voor potentieel verdachte burgers. De politie zal zich hier uiteraard tegen verzetten, onder het mom van: 'Dat zou te veel prijsgeven over onze tactiek bij politiewerk. Dat zou door kwaadwillenden verkeerd gebruikt kunnen'.[139]

Om vergelijkbare redenen werd verdachten vroeger de tenlastelegging zo laat mogelijk (of helemaal niet) meegedeeld; dat zou er maar toe leiden dat ze zich daartegen konden verdedigen. Waarschijnlijk zal de rechter menen dat de Wpg de toepasselijkheid van de Who uitsluit, maar mij dunkt dat in het tijdperk van politie-*agents* daar opnieuw over moet worden nagedacht.

Het brengt mij ook weer terug bij Holmes (1996:991) die meende dat het belang van het recht schuilt in het voorspelbaar maken van overheidsoptreden dat volgt op het handelen van rechtsgenoten:

> People want to know under what circumstances and how far they will run the risk of coming against what is so much stronger than themselves, and hence it becomes a business to find out when this danger is to be feared. The object of our study [of law, mh], then, is prediction, the prediction of the incidence of the public force through the instrumentality of the courts.

3.4 Legaliteit en legalisme: detournement de pouvoir

Legaliteit verwijst naar de inperking van het overheidshandelen door het recht. Het onderscheidt de verlichte despotie van de rechtsstaat. De eerste maakt zowel het algemeen belang als de rechten en vrijheden van individuen afhankelijk van de inzichten van degene die de feitelijke macht uitoefent, van *le bon plaisir du prince*, zoals het absolutistische soevereiniteitsdenken wel wordt aangeduid (Chevallier 1994:18). De rechtsstaat betekent dat de soevereiniteit intern zodanig wordt verdeeld dat de ene overheidsmacht de andere binnen de perken houdt. Legaliteit mag niet worden verward met legalisme, een rigide vorm van regelgeleid denken, waarbij de overheid alleen mag handelen ter uitvoering van vooraf vastgestelde wettelijke of jurisprudentiële regels en geen discretionaire bevoegdheid toekomt. Met name in de uitvoeringspraktijk, bijvoorbeeld van politie en justitie, is dat een onhoudbare en onwenselijke benadering, die tot sluipwegen en verborgen wangedrag leidt. Legaliteit is hecht verbonden met zowel instrumentaliteit als rechtsbescherming, het is gericht op effectief, legitiem recht. Discretionaire bevoegdheden zijn bepalend voor legaliteit. Zoals Evans en Harris (2004:881-2) onder verwijzing naar Dworkin (1978:31) hebben beargumenteerd, verwijst de term discretie dus niet naar willekeur maar naar een genormeerde vrije ruimte die enerzijds mogelijkheden biedt om taken naar beste inzicht en toegesneden op concrete omstandigheden uit te voeren en anderzijds wel degelijk eisen stelt aan de rechtmatigheid van die uitvoering.[140] Een van die eisen vinden we terug in het

[138] De aangepaste Richtlijn hergebruik overheidsinformatie, specificeert in art. 1.4: 'Deze richtlijn laat het niveau van de bescherming van individuen met betrekking tot het verwerken van persoonsgegevens krachtens de bepalingen van het Gemeenschapsrecht en de nationale wetgeving intact en heeft daar geen enkele invloed op, en houdt met name geen wijziging in van de verplichtingen en rechten in Richtlijn 95/46/EG.' Dit is van groot belang omdat de in 2013 aangepaste richtlijn een *verplichting* bevat tot het verstrekken van overheidsinformatie voor hergebruik. Persoonsgegevens vormen daarop ingevolge art. 1.4 een uitzondering (zie ook Art. 29 Werkgroep in haar advies 06/2013 over open gegevens en hergebruik van overheidsinformatie). Het verstrekken van de mogelijkheid om zonder toegang tot de data onderzoek te doen naar relevante verbanden kan niet op grond van Richtlijn 95/46/EG worden uitgesloten. Interessant is dan ook de relatie tussen Wpg en de Who: sluit het eigen verstrekkingsregiem ook de toepasselijkheid van de Who uit?

[139] Aldus een woordvoerder van de Nationale Politie, volgens Van Noort en Kist (2015).

[140] In gelijke zin Muller, Dubelaar en Cleiren (2007: 596-8) over 'beleidsvrijheid' en de normering die uitgaat van 'algemene beginselen van behoorlijke politiezorg). Ik zie dan ook niets in de idee dat creatieve omgang met

doelbindingsbeginsel: bevoegdheden mogen alleen worden gebruikt voor het legitieme doel waarvoor zij zijn toegekend. Discretionaire bevoegdheden worden aldus genormeerd door het doel waarvoor zij zijn gegeven; op die manier dient het doel zowel de instrumentaliteit (het maakt overheidsoptreden mogelijk) als de rechtsbescherming (het begrenst datzelfde optreden).

Het doelbindingsbeginsel bevestigt dat instrumentaliteit en rechtsbescherming niet tegen elkaar moeten worden afgewogen, maar elkaar bepalen.

Gezien de grote economische belangen die gemoeid zijn met gegevensbescherming in de private sector en de mogelijke inbreuken op grondrechten is het doelbindingsbeginsel van meet af aan richtinggevend geweest voor de juridische normering van de verwerking van persoonsgegevens. Zo is het legitieme belang van de data controller sinds jaar en dag een rechtmatige *grond* van verwerking (art. 8 Wbp), maar wordt daarnaast bij iedere grond de *voorwaarde* gesteld dat het betreffende data subject weet voor welk doel haar gegevens wel en niet gebruikt worden (art. 7 en 9 Wbp). Door naast een juridische bevoegdheidsgrondslag (toestemming, contract, vitaal belang van het data subject, publieke taak of het legitieme belang van de data controller) steeds te eisen dat de controller duidelijk maakt met welk doel of welke doelen de verwerking plaatsvindt, wordt voorkomen dat de grondslag een *carte blanche* wordt voor om het even welke verwerking. In het verlengde hiervan is het verwerken van persoonsgegevens voor een ander doel dan waarvoor ze zijn verkregen onrechtmatig voor zover het nieuwe doel onverenigbaar is met het oorspronkelijke doel. Deze benadering sluit aan bij Nissenbaum's nadruk op contextuele integriteit, die rechtstreeks samenhangt met de redelijke verwachting van degene wiens gegevens worden verwerkt.[141] Nadeel van 'context' is dat niet duidelijk is wie op welk moment bepaalt welke context aan de orde is. Dit wringt met name omdat gegevensverwerking in de onli*f*e wereld vaak plaatsvindt in een veelvoud van contexten, waarbij de economische context bijna altijd een voorname rol speelt. Voordeel van doelbinding is de attributie van verantwoordelijkheid en aansprakelijkheid die ermee gegeven is (Hildebrandt 2014, 2015a). De data controller moet een legitiem doel specificeren en expliciteren, ten laatste op het moment dat de gegevens worden verwerkt en is daar vervolgens aan gebonden.

In het preadvies van Moerel en Prins wordt voorgesteld om binnen de private sector, waar horizontale verhoudingen de boventoon voeren, doelbinding als een achterhaald en ineffectief beginsel af te schaffen. Zij stellen voor in plaats daarvan de bescherming van het gerechtvaardigde belang van het data subject als ijkpunt en toetssteen te nemen. Een verfrissend voorstel dat het aandurft de zaken op een radicaal andere wijze te bekijken, ongehinderd door blinde navolging van de huidige systematiek van de gegevensbescherming. Het voorstel lijkt – in termen van het gegevensbeschermingsrecht – gronden en voorwaarden te verwarren. Van verwarring is bij de preadviseurs echter geen sprake, integendeel, zij constateren dat doelbinding in het tijdperk van big data en IoT vaak een wassen neus is, omdat de data controller daarmee zelf bepaalt waartoe zij is gehouden en zich bij het vaststellen van het doel weinig of niets aantrekt van het gerechtvaardigde belang van het data subject. Precies om die reden stellen zij vervolgens voorop dat gegevensverwerking altijd legitiem moet zijn in het licht van de fundamentele rechten en vrijheden van het data subject. Dit sluit aan bij de huidige juridische grondslag van art. 8.f Wbp die een afweging eist van het legitieme belang van de data controller tegen de rechten en belangen van het data subject. Hoewel verfrissend, is het voorstel wat mij betreft niet overtuigend. Het is mij

bevoegdheden onder het 'stoere' kopje van 'het opzoeken van de grenzen van wet- en regelgeving' illegaal overheidshandelen met zich meebrengt, zie bijvoorbeeld Halderen en Lasthuizen (2013:17), die dat benoemen als 'noble cause corruption' (ibid). Vergelijk bijvoorbeeld Schuyt (2009) die in geval van burgerlijke ongehoorzaamheid veronderstelt dat men bereid is de consequenties van het negeren van democratisch gelegitimeerde normen te aanvaarden, waaronder met name ook strafbaarheid. Juist in geval van ambtelijke ongehoorzaamheid moet helder zijn dat onrechtmatige experimenten tot strafvervolging van de betreffende ambtenaar en diens leidinggevende kunnen leiden.

[141] Bij het bepalen van de rechtmatigheid van de verwerking speelt bij het oordeel over de verenigbaarheid van een nieuw doel met het oorspronkelijke doel de vraag of het nieuwe doel binnen een andere context speelt een belangrijke rol. Zie Opinie 03/2013 inzake doelbinding van de Art. 29 Werkgroep, p. 3, 13, 24-25.

bijvoorbeeld niet duidelijk 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 data subject, nu zij daartoe ook op dit moment verplicht zijn. Het criterium van het gerechtvaardigde belang heeft overigens dezelfde nadelen als dat van contextuele integriteit, wanneer het toetssteen en ijkpunt van legitieme gegevensverwerking wordt. Anders dan bij doelbinding is mij vooralsnog onduidelijk wie de inhoud en reikwijdte ervan bepaalt, op welk moment, en hoe dit kenbaar moet worden gemaakt aan data subjecten. Door het perspectief te verhuizen naar dat van het data subject, maar de data controller verantwoordelijk te houden ontstaat voor de data controller bovendien grote onzekerheid, want de betekenis van de fundamentele rechten en belangen zal per persoon, context en applicatie verschillen. Zo keert de complexiteit die met de voorgestelde vereenvoudiging moet worden teruggedrongen langs de achterdeur terug.[142] Dat heeft ook van doen met het feit dat de keuze voor het gerechtvaardigde belang – anders dan doelbinding – hecht verbonden is met een belangenafweging, die allerlei vragen oproept rond de vergelijkbaarheid van de belangen, de distributie van kosten en baten en de kwalificatie van belangen als individueel dan wel publiek belang.[143] Moerel en Prins wijzen er overigens terecht op dat onder omstandigheden het uitblijven van een belangenafweging tot minder bescherming leidt. Dat pleit ervoor om die belangenafweging *ook* verplicht te stellen in geval van toestemming. Mijn punt is dat ook in dat geval doelbinding een voorwaarde is om tot een juiste afweging te komen, namelijk een afweging binnen de bandbreedte van het verenigbare, legitieme doel.

Het is op dit moment evident zo dat de gegevensbescherming niet of nauwelijks gehandhaafd kan worden vanwege de beperkte handhavingsbevoegdheden; dat heeft echter weinig te maken met de vraag aan welke criteria gegevensverwerking zou moeten voldoen als er wel gehandhaafd kan worden.

De op mededingingsrecht geïnspireerde boete van maximaal 4% van de wereldomzet voor schending van de bepalingen van de komende Algemene Verordening Gegevensbescherming (Avg) zal een 'game changer' zijn, die het speelveld voor alle partijen opnieuw zal structureren.[144] Door doelbinding daadwerkelijk te handhaven wordt de data controller terecht gedwongen zich de vraag te stellen waartoe hij de gegevens nodig heeft en dat in heldere taal mee te delen aan degene wiens data worden verwerkt. Dat levert een vorm van rechtzekerheid op die bij het legitiem belang als enig criterium niet eenvoudig te realiseren is. De gebruiker kan immers niet voorzien welke gegevensverwerking het toekomstige economische belang van de controller kan rechtvaardigen.

Moerel en Prins menen intussen dat ook 'informed consent' een zinloze voorwaarde is, die in de praktijk hooguit leidt tot het afvinken van allerlei vakjes om maar zo snel mogelijk toegang te krijgen tot de gewenste applicatie. Dat is op dit moment zeker het geval en ik ben het eens met de idee dat *voordat* sprake kan zijn van 'informed consent' een 'level playing field' moet worden geschapen zodat de gebruiker default instellingen kan kiezen die het leven gemakkelijk maken en tegelijk bescherming bieden. Een mooi voorbeeld van het creëren van zo'n level playing field was art. 7 lid 4 van de concept Avg, zoals vastgesteld door het Europees Parlement:

[142] Uit de overwegingen van Moerel en Prins maak ik op dat zij zelf constateren dat (1) enerzijds niet steeds op voorhand duidelijk *kan* zijn wat het gerechtvaardigde belang in specifieke situaties eist en dat (2) anderzijds de afweging die beslissend zal zijn voor de vraag of de belangen, rechten en vrijheden van het data subject zich tegen verwerking verzetten minstens zo complex is als de huidige afwegingen.
[143] Cf. paragraaf 3.3.1 hierboven.
[144] Op 17 december 2015 is de definitieve tekst vastgesteld van de komende Avg en van de komende Richtlijn gegevensbescherming opsporing en vervolging, justitiële samenwerking, opsporings- doeleinden. Zie: <http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-1739884>.

> The execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of data that is *not necessary for the execution of the contract or the provision of the service* pursuant to Article 6(1), point (b) (mijn nadruk).[145]

Met deze eenvoudige clausule worden heel veel problemen opgelost. Bovendien kunnen ook nu vrijwel alle legitieme verwerkingen plaats vinden op basis van andere gronden dan toestemming, met name contract, een wettelijke verplichting en het legitieme belang van de data controller. In die zin is 'informed consent' sowieso de minst interessante rechtsgrond, die vanwege de mogelijkheid om consent te allen tijde in te trekken sowieso niet erg aantrekkelijk is voor data controllers. Met name degenen wier verdienmodel vooral over de band van de verwerking van persoonsgegevens loopt zullen zich op de rechtsgrond van art. 8 lid 7 Wbp verlaten, zelfs als zij voor alle zekerheid om toestemming vragen. Ik meen dan ook dat doelbinding betere bescherming en tevens rechtszekerheid voor beide partijen biedt, juist omdat doelbinding ook richting geeft aan de legitieme verwachtingen van het data subject als diens toestemming niet nodig is. Precies in het kader van de rechtszekerheid, het vertrouwensbeginsel en het voorkomen van misbruik van bevoegdheid blijft doelbinding daarom prioritair.

Is dit relevant voor de strafvordering? Gezien de gestage uitbreiding van publiek-private samenwerking, met name in de context van het bestrijden van (internationale) cybercriminaliteit moeten we ervan uitgaan dat alle gegevens die op enig moment worden verzameld door private partijen, niet alleen in theorie maar ook in de praktijk beschikbaar kunnen komen voor politie en justitie (de inlichtingen- en veiligheidsdiensten laat ik er dan nog buiten). Zeker wanneer de voorgestelde definitie van computers ('geautomatiseerde werken') als onderdeel van het wetsvoorstel Computercriminaliteit III kracht van wet krijgt: Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken (art. 80sexies WSr). De komst van het Internet van de Dingen leidt ertoe dat zo ongeveer alle 'dingen' die online verbonden zijn ofwel op afstand uitgelezen kunnen worden onder het bereik van de term 'geautomatiseerd werk' komen te vallen.[146] Dat alles betekent dat alle burgers bij het delen van – vaak onbewust vergeven - gedragsgegevens zouden moeten beseffen dat zij als eventueel mogelijk potentieel verdachte in beeld komen. Ook wanneer hun gegevens worden verwerkt in de private context. Dat is nu al het geval, op basis van art. 125i en verder (doorzoeking ter vastlegging van gegevens), art. 126l (plaatsing technisch hulpmiddel om vertrouwelijke informatie op te nemen), art. 126m en verder (interceptie telecommunicatie), art. 126nc Sv en verder (vordering gegevens), art. 126q lid 1 sub b (het overnemen van gegevens van computers) en zo voort en zo verder, maar het besef van de gevolgen van het opvragen en uitlezen van metadata, inhoud en profielen bij private partijen lijkt nauwelijks aanwezig.

De beperking van de verwerking van persoonsgegevens in de private sector is evident van groot belang voor de bescherming die het strafrecht kan bieden; niet verzamelde gegevens en niet-afgeleide profielen kunnen ook niet door justitie worden gevorderd of uitgelezen. Het is naïef te denken dat zolang we in een rechtsstaat leven de osmose tussen private en publieke sectoren geen reden tot zorg is. Integendeel, de rechtsstaat eist dat we de gegevensverwerking in de private sector niet inrichten als een schatkamer voor overheden die in het kader van de strafvordering werken aan het 'verbeteren van hun informatiepositie'.

In de strafvordering zelf geldt – net als in het bestuursrecht - het constitutionele beginsel van *detournement de pouvoir* (ddp), dat stipuleert dat overheden, en zeker de straffende overheid, een bevoegdheid alleen mag gebruiken voor het doel waarvoor die bevoegdheid is gegeven. Het gaat hier

[145] Art. 6(1) sub b betreft doelbinding. In de inmiddels definitief vastgestelde tekst is dit punt iets afgezwakt: 'When assessing whether consent is freely given, utmost account shall be taken of the fact whether, among others, the performance of a contract, including the provision of a service, is made conditional on the consent to the processing of data that is not necessary for the performance of this contract.'

[146] Zie ook De Graaff (2015) – met het oog op de nieuwe voorgestelde Wet op de Inlichtingen- en Veiligheidsdiensten - over de hoeveelheid en soort gegevens die dankzij het Internet van de Dingen beschikbaar kunnen komen voor overheden die deze kunnen opvragen of zelfs real-time toegang kunnen eisen.

dus niet om *doelbinding als zelfbinding*. Dat is wel het geval als private partijen, zonder daartoe verplicht te zijn, diensten aanbieden waarbij het noodzakelijk is om persoonsgegevens te verwerken. Zij zijn dan gehouden een voldoende specifiek legitiem doel te communiceren en zichzelf daardoor te binden. Die noodzaak kan heel praktisch zijn, zo zal bijvoorbeeld een adres nodig zijn om goederen af te kunnen leveren. Het kan ook om een economische noodzaak gaan, wanneer het verdienmodel gratis dienstverlening combineert met gepersonaliseerde advertentie-inkomsten. Doelbinding is echter niet altijd een kwestie van zelfbinding; ook private partijen zijn vaak verplicht persoonsgegevens te verwerken in het kader van een publieke taak, ten behoeve van het vitale belang van het data subject of op grond van een wettelijke verplichting (belastingwetgeving). Daarmee is het doel van de verwerking meestal ook gegeven. Bij de strafvordering bepaalt de wetgever per definitie het doel. Het gaat dan bovendien om bijzonder ingrijpende bevoegdheden, niet voor niets dwangmiddelen genoemd, en nog los daarvan gaat het vaak om heimelijke bevoegdheden. Het ingrijpende karakter eist dat burgers een goed beeld hebben van de gevallen waarin zij onderworpen mogen worden aan dwangmiddelen, juist ook wanneer de toepassing voor hen verborgen wordt. Daar hoort niet bij dat dwangmiddelen die met het oog op een specifiek doel wettelijk zijn toegestaan worden gebruikt voor een ander doel, waartoe de wettelijke bevoegdheid in het voorliggende geval ontbreekt. Dat heet misbruik van bevoegdheid en – in het Frans – machtsmisbruik.[147] Het feit dat de strafvordering vaak heimelijke interventies vereist, maakt de doelbepaling in het kader van de rechtszekerheid en het vertrouwensbeginsel nog pregnanter. Het doel is immers zowel constitutief als limitatief voor de toe te passen bevoegdheid (Cleiren 1992:15), Hildebrandt 2014:26). Dat komt verder tot uiting in het feit dat schending van ddp kan leiden tot bewijsuitsluiting (art. 359a WSv). Doelbinding vloeit dan ook voort uit het rechtsstatelijk legaliteitsbeginsel, niet te verwarren met het legalisme van de 19e eeuw.

Legaliteit betekent hier dat overheidsorganen gehouden zijn te handelen in overeenstemming met hun wettelijke opdracht, binnen de grenzen van het recht, terwijl hun handelen gericht moet zijn op het algemeen belang en de bescherming van individuen. Daarmee normeert de legaliteit ook onderhandelende en netwerkende overheden en stelt grenzen aan wat een legitieme overheid wel en niet vermag. Het loslaten van ddp in het strafrecht in het kader van het accorderen van 'creatieve omgang' met bevoegdheden door de opsporing klinkt sommigen misschien als muziek in de oren (veelbelovend, adaptief, onvermijdelijk),[148] het is een teken aan de wand en moet naar mijn mening in ronde bewoordingen af worden gewezen.

Dat ddp zonder daar veel woorden aan vuil te maken als een ouderwetse hinderpaal terzijde wordt gesteld – dus ook in het strafrecht – mag worden opgemaakt uit een arrest van het Hof in Den Bosch van 5 oktober 2010.[149] Hoewel hierbij geen politie-*agents* zijn ingezet raakt het arrest aan de kern van de problematiek die met *agents* aan de orde is. Kort gezegd werd door de politie in Limburg een verkeerscontrole georganiseerd op de A2, waarbij het eigenlijke doel een drugscontrole was, gericht op

[147] We kunnen natuurlijk neuzelen over de vraag of *abus de pouvoir* en *detournement de pouvoir* niet heel verschillende zaken benoemen. Ook misbruik van bevoegdheid door bevoegdheden weliswaar voor het juiste doel maar disproportioneel in te zetten is in de strafvordering onrechtmatig, maar dat valt niet onder het inzetten voor een ander doel. Het gaat mij hier dus uitsluitend om het gebruik van een strafvorderlijke bevoegdheid voor een ander doel dan waarvoor die is gegeven. Verdere categorisering is altijd mogelijk, zie Halderen en Lasthuizen (2013: 22), die onderscheiden tussen niet inzetten, misbruik, oneigenlijk gebruik en selectief inzetten van bevoegdheden.

[148] Onderzoek van Halderen en Lasthuizen (2013) laat zien hoe groot de verleiding is om 'creatief' om te gaan met bevoegdheden en hoe belangrijk het is om juist dan binnen de grenzen van ddp te blijven. Zie idem p. 26 over het informeel delen van informatie over een bewoner met een woningcorporatie die uitzetting overweegt. Creatieve omgang is echter niet per definitie in strijd met de legaliteit. Ik zou, in tegendeel, willen beargumenteren dat de discretionaire ruimte voor politie en justitie cruciaal zijn bij het vervullen van de hen toegemeten taken. Zie hierboven noot 140 en Hildebrandt (2016b te verschijnen).

[149] Hof 's-Hertogenbosch, 5 oktober 2010, ECLI:NL:GHSHE:2010:BN9352, waarin opgenomen het vonnis van Rechtbank Maastricht, 17 februari 2010.

het 'vangen' van drugskoeriers. Dit alles onder de noemer van het Project Waakzaam 2,[150] dat – zo lezen wij in het vonnis van rechtbank Maastricht – is gericht op 'verhoging van de veiligheid in de regio Limburg-Zuid - in het bijzonder door het bestrijden van de overlast die wordt veroorzaakt door uit Frankrijk afkomstige zogenaamde drugkoeriers'. Het verhogen van de veiligheid vindt plaats door (opnieuw volgens de rechtbank) 'controleacties (…) op en rond de verkeersstromen in het gebied Limburg-Zuid.' In plaats van het aanhouden van alle weggebruikers in hoop om daarbij toestemming te bekomen de auto te mogen doorzoeken, maakte de politie gebruik van slimme camera's met automatische nummerplaatherkenning (ANPR: Automatic Number Plate Recognition). De rechtbank vervolgt: 'Hierbij werden kentekens van passerende personenauto's gescand en vervolgens telkens vergeleken met een vergelijkingsbestand waarin kentekens zijn verzameld die bij de politie bekend zijn wegens eerdere betrokkenheid bij druggerelateerde criminaliteit. Indien een gescand kenteken overeenkwam met een kenteken in het vergelijkingsbestand, een zogenaamde 'hit', werd deze personenauto door de politie naar een controleplaats geleid, alwaar een controle plaatsvond.' Het voertuig in kwestie werd na selectie via genoemde ANPR-apparatuur 'na een volgteken te hebben gekregen, door een motoragent naar de controleplaats te Gronsveld geleid. De selectie uit de verkeersstroom, het geven van aanwijzingen om te volgen en het feitelijk tot stilstand doen brengen van het voertuig op de controleplaats levert een stopteken op als bedoeld in artikel 160 van de Wegenverkeerswet 1994. Nadat [het voertuig, mh] op de controleplaats stopte, vorderde verbalisant [verbalisant] het rijbewijs van medeverdachte [medeverdachte], die de auto bestuurde. Nadat [medeverdachte] hem de autopapieren had overhandigd vroeg verbalisant [verbalisant] in de Franse taal aan [medeverdachte] of hij drugs in zijn bezit had, wat door [medeverdachte] werd ontkend. Vervolgens vroeg verbalisant [verbalisant] in de Franse taal aan [medeverdachte] of hij het voertuig mocht onderzoeken op de aanwezigheid van drugs. Met toestemming van [medeverdachte] werd het voertuig onderzocht. In het voertuig werd in de kofferbakruimte 633,5 gram heroïne en 4,8 gram cocaïne aangetroffen.' De rechtbank spreekt de verdachte vrij wegens schending van ddp, waarna Hof Den Bosch de verdachte veroordeelt omdat er geen sprake is van ddp. De verdachte is immers gevraagd naar zijn papieren hetgeen duidelijk maakt dat het wel degelijk ging om uitoefening van een bevoegdheid op basis van de WVW (aldus het hof), en het bewijsmateriaal is gevonden dankzij toestemming, zodat geen bevoegdheid nodig was (aldus het hof).[151] Hof Den Bosch maakt er niet veel woorden aan vuil. Ook de Hoge Raad spreekt zich uit, maar tegen die tijd gaat het alleen nog maar om een foutje in de betekening. Ybo Buruma merkte in de NRC op:[152]

> Dat we de boeven niet meer om elke individuele vormfout van de politie vrijuit laten gaan, is natuurlijk prima. Maar het Hof heeft volgens mij onvoldoende aandacht besteed aan het feit dat er hier niet zomaar een foutje, maar een geheel nieuwe methode aan de orde was.

Volgens Buruma, toen nog hoogleraar Strafrecht aan de Radboud Universiteit, staat die nieuwe methode op gespannen voet met de onschuldpresumptie en had het Hof zich er om die reden niet zomaar vanaf mogen maken. Weliswaar is het inmiddels vaste rechtspraak dat geen sprake is van misbruik van de controlebevoegdheid van de WVW als het stopteken mede wordt gebruikt ter controle van kenteken en/of rijbewijs,[153] hier is overduidelijk sprake van geautomatiseerd voorsorteren van personen ten

[150] Interessante vraag is of wij ooit hadden vernomen over dit boeiende voorbeeld van 'smart policing' als hierover geen uitspraak was gedaan.

[151] Cruciale vraag is of een opsporingsambtenaar om toestemming mag vragen om datgene te verrichten waarvoor zij geen wettelijke bevoegdheid heeft. Mij dunkt dat gezien de ingrijpende gevolgen van strafvorderlijke interventies die toestemming op gespannen voet kan staan met de ratio van *nemo tenetur*.

[152] Het gaat om een commentaar dat Buruma op uitnodiging schreef bij een artikel van Jensma, Buruma en De Swart (2010).

[153] Hoge Raad, 21 november 2006, ECLI:NL:PHR:2006:AY9670. De problematiek van het inzetten van bevoegdheden uit de ene context (verkeersveiligheid) in een andere context (drugscriminaliteit) houdt ook verband met de vraag naar de rechtmatigheid van de voortgezette toepassing van bevoegdheden die speelt in de verhouding tussen bijzonder en commuun strafrecht. Zie Cleiren (2015).

aanzien waarvan geen sprake is van een *redelijk vermoeden van* of zelfs maar *aanwijzingen voor* schuld aan een strafbaar feit. Het is niet ondenkbaar dat sommigen uit deze rechtspraak afleiden dat ook in het strafrecht doelbinding een wassen neus is geworden. Dat is niet onaannemelijk,[154] maar dat is geen argument dat pleit tegen ddp. Integendeel, het verfrommelen van de onschuldpresumptie en het verkwanselen van ddp door de strafrechter zijn niet onbegrijpelijk maar wel hachelijk en onaanvaardbaar in het licht van de inzet van *agents*. Niet onbegrijpelijk voor zover ook de rechter een steentje bij wil dragen aan de slagvaardigheid van de strafvordering; hachelijk en onaanvaardbaar omdat deze verfrommeling en verkwanseling in flagrante strijd zijn met de voorzienbaarheid van het *ius puniendi* en van de daartoe noodzakelijke strafvorderlijke bevoegdheden.

4 Naar een veilig strafrecht in een data-gestuurde samenleving

4.1 Reflexieve modernisering van het Wetboek van Strafvordering?

In de Contourennota (2015:4) voor een nieuw Wetboek van Strafvordering wordt als een van de doelstellingen van de modernisering van het Wetboek de 'facilitering van de digitalisering' genoemd. Dat is de omgekeerde wereld. Digitalisering zou bij moeten dragen aan een legitieme en effectieve strafvordering, niet omgekeerd. Als gezegd, gaat het bij deze modernisering om een 'upgrade' van de 'firmware', dat wil zeggen van het meest stabiele onderdeel van het 'operating system' van het strafrecht, dat nauw verbonden is met de 'hardware' (de institutionele ondergrond, inclusief de Grondwet, en de organieke wetgeving inzake rechterlijke macht, advocatuur). Deze 'firmware' bepaalt feitelijk de mogelijkheden van de te implementeren software (nadere regelgeving, beleidsregels en protocollen voor de uitvoering).[155]

Het zou een goede zaak zijn als in de 'upgrade' van het Wetboek van Strafvordering het inzicht wordt meegenomen dat juridische instrumentaliteit en rechtsbescherming van vooraf aan in moet worden gebouwd in het ontwerp van de onlife wereld, met name als het gaat om politie-*agents* en wat dies meer zij.

Zo kan het wetboek aansluiten bij een minder naïeve opvatting van modernisering, die zich bewust is van de gevaren van een blind geloof in technologische vooruitgang en bereid is te reflecteren op de – vaak niet direct in het oog springende - kosten van de inzet van technologie.

De vraag is allereerst *of* nieuwe technologie moet worden ingezet. Die vraag kan echter maar beantwoord worden wanneer duidelijk is hoe, wanneer, ten koste dan wel ten bate van welke groepen, machtsevenwichten, waarden en normen de nieuwe technologie zou worden geïntroduceerd. Het besef moet doordringen dat keuzes in het ontwerp van de technologie mede doorslaggevend zullen zijn voor

[154] Zie immers ook HR 12 november 2002, ECLI:NL:HR:2002:AE9028, r.o. 4.2 en 4.3. Hier ging het overigens om de vraag of het is toegestaan een verdachte op grond van art. 52 WSv staande te houden door een stopteken te geven dat kan worden opgevat als een stopteken in de zin van art. 160 WVW. Het Hof schrijft, met instemming van de HR: 'Uit de vaststelling dat artikel 52 van het Wetboek van Strafvordering de staandehouding legitimeert, en het hof de wijze waarop die bevoegdheid is gehanteerd niet onrechtmatig oordeelt, volgt bovendien, dat zich hier niet het geval voordoet waarbij de opsporing uitsluitend mogelijk is gemaakt door het oneigenlijk gebruik van een aan de Wegenverkeerswet 1994 te ontlenen bevoegdheid tot controle.' Het woordje 'uitsluitend' doet vermoeden dat het er niet toe doet of wie dan ook het stopteken – mede – baseerde op de WVW, zolang maar sprake is van een verdenking die staande houden rechtvaardigt.

[155] Zie hierboven paragraaf 3.1.

de mate waarin legaliteit, doelbinding, onschuldpresumptie, privacy en non-discriminatie realiseerbaar zijn dan wel onmogelijk of onwaarschijnlijk worden.

Als Roessingh (2013) in Trouw schrijft 'iColumbo kan meer dan hij mag', duidt hij een van de grootste uitdagingen van de stuwende kracht van technologie in de onlife wereld. Politie-*agents* kunnen vrijwel altijd meer dan is toegestaan. Dat vraagt een dubbele bezinning. Ten eerste moet bij de introductie van data-gestuurde technologie steeds onder ogen worden gezien of, en zo ja in hoeverre het onvermijdelijk is dat de investering in nieuwe systemen leidt tot *agents* die meer kunnen dan zij mogen.[156] Hier geldt dat voorkomen beter is dan genezen; door de aanmaak, het opslaan, uitlezen of koppelen van gegevens technisch lastig te maken is de kans dat bevoegdheden op grote schaal worden overtreden kleiner, evenals de kans dat criminelen zich toegang verschaffen tot opgeslagen gegevens. Daarbij moet worden bedacht dat de aanzwellende data-obesitas in de private sector niet alleen zal leiden tot het dichtslibben van allerhande informatiesystemen en tot lekkage en diefstal van persoonsgegevens, maar dat het politie en justitie kan verleiden hun heil te zoeken in verdere ondergraving van de onschuldpresumptie door zich toegang te verschaffen tot steeds meer gegevens over steeds grotere groepen personen.[157] Ten tweede is het zaak om – voor zover systemen inderdaad meer kunnen dan mag – technisch controleerbaar te maken of, hoe en door wie bevoegdheden worden overschreden. Met name wanneer het gaat om *agents* die eraan bijdragen dat personen heimelijk in een categorie worden geplaatst van wie stelselmatig persoonsgegevens zullen worden verwerkt is die controle cruciaal. We kunnen er juist dan niet van uitgaan dat de strafrechter er überhaupt aan te pas zal komen en zullen dus van meet af aan 'auditability' en 'accountability' in moeten bouwen.

Dat vraagt om een toezichthouder die - niet in individuele gevallen maar op een meer generiek niveau - in staat is om dankzij die 'auditability' de schending van bevoegdheden en effectieve bescherming van de onschuldpresumptie te toetsen. Niet in plaats van de strafrechter, die immers oordeelt in individuele gevallen, maar toch wel als een onmisbare aanvulling van het systeem van checks en balances.

4.2 Legaliteit en grondrechtenbescherming 'by design'

Voortbouwend op inzichten uit de techniekfilosofie en de studie van de inbedding van waarden en normen in apparaten, technische systemen, architectuur en infrastructuur (Verbeek 2011, Flanagan, Howe en Nissenbaum 2007), wordt inmiddels in verschillende contexten gewerkt aan het vertalen van juridische bescherming naar technische specificaties, standaarden en protocollen. Denk aan de nieuwe verplichting tot gegevensbescherming by design in de komende Avg (art. 23), de in Duitsland

[156] Een voorbeeld van technologie die meer kan dan mag zijn de zogenaamde IMSI catchers, die volgens het Besluit bijzondere vergaring nummergegevens telecommunicatie (gebaseerd op art. 3.10.4a en 13.4.2 Telecommunicatiewet) kunnen worden ingezet om nummergegevens uit de ether te vissen door middel van afwijkend frequentiegebruik, en bestandsanalyse mogelijk te maken met het oog op het onderzoek van telecommunicatie. De betreffende bevoegdheden zijn geregeld in art. 126nb WSv. Omdat deze apparatuur inmiddels ook kan afluisteren en opnemen stipuleert art. 4.2.a van het Besluit dat in het proces-verbaal moet worden opgenomen of de apparatuur vergrendeld is om dit onmogelijk te maken. De Hoge Raad heeft echter vastgesteld dat de apparatuur ook gebruikt mag worden voor locatiebepaling, ook al is dit niet in art. 126bn WSv geregeld. Redengevend is dat sprake zou zijn van een beperkte inbreuk op de persoonlijke levenssfeer, zie HR 1 juli 2014, ECLI:NL:HR:2014:1562,

[157] Denk aan de gestage uitbreiding van bevoegdheden in het kader van fraude-detectie inzake sociale zekerheid en belastingen, bijvoorbeeld art. 54 Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI) en de jurisprudentie naar aanleiding van het opvragen van parkeergedragsgegevens bij commerciële partijen, Hof 's Hertogenbosch, 19 augustus 2014, ECLI:NL:GHSHE:2014:2803 en Rechtbank Oost-Brabant, 26 november 2013, <http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBOBR:2013:6553>.

ontwikkelde methode KORA (*Konkretisierung rechtlicher Anforderungen*), en het idee van Ambient Law dat technische bescherming zou moeten bieden in een omgeving geënt op Ambient Intelligence.[158]

Zelf spreek ik inmiddels van juridische bescherming 'by design'. Daarmee wil ik in de eerste plaats benadrukken dat we als juristen niet alle heil van juridische teksten kunnen blijven verwachten. Tekst is gebaseerd op een specifieke informatie en communicatietechnologie (ICT), te weten die van het schrift (of liever, de drukpers). Het moderne, positieve recht is gearticuleerd in die specifieke ICT, waaraan het zowel zijn effectiviteit als zijn beschermende werking dankt. Zolang de samenleving is ingericht op basis van een ICT-infrastructuur waarin schrift en drukpers de hoofdrol spelen, voldoet het geschreven recht. Het is echter een illusie te denken dat we een samenleving die is geënt op een andere ICT-infrastructuur kunnen blijven normeren vanuit enkel de vorige.

We kunnen dus wel een regel opschrijven en uitvaardigen die stipuleert dat we een recht hebben om voor onschuldig gehouden te worden tot onze schuld in rechte is vastgesteld, maar daarmee zijn we er nog niet. Als we tegelijkertijd systemen ontwerpen die het gemakkelijk maken om mensen op afstand te volgen en hun gedrag te voorspellen en te ondervangen, wordt het zaak de inzet van die systemen door politie en justitie aan banden te leggen. De Pavlov reflex is om daartoe weer regeltjes op te schrijven en uit te vaardigen en zo voort en zo verder. Daar gaan we de oorlog niet mee winnen. Juridische bescherming by design gaat er daarom van uit dat rechtsstatelijk waarborgen moeten worden gearticuleerd in de technische systemen die we gebruiken.

Net zoals de paradox van de rechtsstaat erin bestaat dat we ons tegen de staat (de wetgever, het bestuur) kunnen verzetten dankzij diezelfde staat (de rechter), moeten we leren de technische systemen waaraan we onze veiligheid en ons welzijn danken te gebruiken om ons tegen diezelfde systemen te beschermen. Die bescherming moet dus zo diep mogelijk in de architectuur, het ontwerp, de technische inrichting en de default instellingen worden ingebouwd. Door te spreken van juridische bescherming by design, in plaats van techno-regulering, wil ik in de tweede plaats benadrukken dat het *niet* gaat om het afdwingen van de naleving van bestuurlijke normen met technische middelen (Hildebrandt 2010). Dat zou een kwestie zijn van nudging of van technoregulering, waarbij burgers en bedrijven met technische middelen in plaats van juridische normen tot zogenaamd 'compliant' gedrag worden verleid of gedwongen.[159] Technoregulering gaat uit van een bestuurskundig reguleringsparadigma, waar recht een beleidsinstrument is, bedoeld om gedrag te beïnvloeden.[160] De idee van technoregulering is gebaseerd is op een sociaal-wetenschappelijk, extern perspectief op het recht. Dat leidt gemakkelijk tot het afwegen van de instrumentaliteit tegen de rechtsbescherming, in plaats van beiden als wederzijds constitutief samen te denken.[161] Bescherming en effectiviteit moeten in een rechtsstaat twee kanten van dezelfde medaille zijn; ze moeten als het ware afhankelijk zijn van elkaar en dus niet tegen elkaar worden uitgespeeld.

Juridische bescherming by design stelt bovendien drie eisen aan het articuleren van rechtsnormen in technische systemen. Ten eerste moet die articulatie zijn gebaseerd op geschreven normen die met het

[158] Over de methode KORA zie Geminn (2014): 336-368), Neumann en Volkamer (2014: 78-81). Over Ambient Law zie Hildebrandt (2008), Hildebrandt en Koops (2010).

[159] Zie bijvoorbeeld Berkhout en Engers (2012: 827) over informatiegestuurd fiscaal toezicht op basis van de *homo behavioralis*: 'een theorie over de mechanismen die aan fiscaal non-compliant gedrag ten grondslag liggen'.

[160] Probleem van het sociaal-wetenschappelijk perspectief dat ten grondslag ligt aan het reguleringsparadigma is een onhoudbaar methodologisch individualisme dat geen inzicht kan geven in de constitutieve samenhang van instrumentaliteit en rechtsbescherming, en zich noodzakelijkerwijs moet beperken tot speltheoretisch, gedragseconomisch en kwantitatief georiënteerd empirisch onderzoek. In dat verband is het nuttig te wijzen op de nutteloosheid van theorieloos kwantiatief onderzoek, waarvan onduidelijk is welke theorie nu eigenlijk gefalsificeerd kan worden. Misschien is dat probleem nog dringender dan het feit dat veel onderzoek niet gerepliceerd kan worden (bv Open Science Collaboration 2015), zie ook hierboven voetnoot 50.

[161] Zie hierover de discussie tussen Leenes (2011) en Hildebrandt (2011c). Over de gevaren van technoregulering en de onmogelijkheid om juridische normen restloos te vertalen in technische specificaties Leenes (2010, 1998). Sceptisch over de vertaling van rechtsnormen in technische systemen (juist omdat hij geen onderscheid maakt tussen technoregularing en juridische bescherming by design) Koops (2013).

oog op die articulatie door de democratische wetgever zijn vastgesteld, zodat we niet achter onze rug om in een bepaalde richting worden gedwongen door technische defaults. Het gaat dus niet om bestuurlijke implementatie. Ten tweede moeten die defaults ten gronde de verhouding tussen transparantie en opaciteit installeren die aan de orde is bij een rechtsstaat: overheidshandelen hoort in beginsel transparant te zijn, het handelen van de burger hoort daarentegen in beginsel afgeschermd te zijn tegen overheidsbemoeienis. Dat betekent dat technische systemen die worden ingezet aan de kant van justitie en politie transparant maken in hoeverre hun gebruikers bevoegdheden overschrijden en hoe zij burgers in het kader van de strafvordering transparant kunnen maken. Ten derde is het zaak dat technische dwang of defaults in rechte kunnen worden aangevochten als zijnde in strijd met het recht, zeker wanneer zij de onschuldpresumptie raken.

Kort gezegd gaat het bij juridische bescherming by design om de *noodzaak* om in specifieke gevallen het geschreven en ongeschreven recht tevens in de cyberfysieke infrastructuur te articuleren. Juist bij het gebruik van *agents* in de opsporing, die uiteindelijk zien op de toepassing van het geweldmonopolie en het ius puniendi is de verankering van bescherming in technische systemen pertinent. Het gaat er eigenlijk om de normatieve neutraliteit van het recht te bewaken door compenserende juridische normering door te voeren, steeds wanneer technologische ontwikkelingen de effectieve bescherming van grondrechten frustreert (Hildebrandt 2010, Hildebrandt en Tielemans 2013). Een analyse van de gevolgen van de inzet van specifieke politie-*agents* voor het beschermde rechtsgoed van bestaande grondrechten zou inspiratie kunnen vinden in Nissenbaums' (2010) beslissingsheuristiek inzake contextuele integriteit, die toestaat om volgens een stappenplan zulke gevolgen in kaart te brengen en daarmee een proportionaliteitstoets voor te bereiden.[162] Meer specifiek valt te denken aan de nieuwe juridische verplichting om bij de inzet van technologie die het risico op schending van gegevensbescherming verhoogt een 'data protection impact assessment' (DPIA) uit te voeren (art. 33 Avg).

Voor het strafrecht zou als opmaat naar juridische bescherming by design een 'presumption of innocence-assessment' (POIA) aangewezen kunnen zijn, die zich richt op de risico's voor de effectieve bescherming van de onschuldpresumptie, het verbod van niet-gerechtvaardigde discriminatie, de privacy en de gegevensbescherming, en het recht op vrijheid van informatie. Daarbij gaat het dan niet alleen om schending van de rechten van de verdachte, maar ook van degene ten aanzien van wie aanwijzingen bestaan van betrokkenheid bij het beramen van strafbare feiten en ook van de burger die op basis van risicoprofielen in aanmerking komt voor stelselmatige observatie, waarbij dan ook weer diens sociale netwerk in beeld zal komen. De hierboven gesignaleerde tendens om het zwaartepunt van de strafvordering nog verder te verschuiven naar het vooronderzoek, naar het verkennend onderzoek en meer in het algemeen richting predictive policing leidt zoals aangegeven tot een steeds groter aandeel van heimelijke observaties die niet door de strafrechter worden getoetst, en in dat opzicht vergelijkbaar zijn met heimelijke operaties van de inlichtingen- en veiligheidsdiensten. Daarmee wordt relevant om kennis te nemen van de reactie van de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD) op het concept Wetsvoorstel Wet Inlichtingen- en Veiligheidsdiensten 20xx, met name waar de CTIVD aandacht besteedt aan toezicht op heimelijke bevoegdheden die niet aan de rechter worden voorgelegd, en het belang van organisatorische en technische functionele scheiding van systemen die grote databestanden beschikbaar maken voor data-analyse.[163] De CTIVD (2015:36) adviseert:

> in de memorie van toelichting bij het concept-wetsvoorstel te beschrijven dat een systeemtechnische scheiding onderdeel zal uitmaken van de wettelijke functiescheiding.

[162] De proportionaliteitstoets betreft bij Nissenbaum de vraag of de aantasting van bestaande ethische waarden en normen, die wordt veroorzaakt door de inzet van nieuw technologie, noodzakelijk is in het licht van het maatschappelijk tegoed dat mogelijk wordt gemaakt.

[163] CTIVD (2015: 35-37). Zie ook het onderzoek van Loof e.a. (2015) naar het mensenrechtelijk kader voor toezicht op de diensten.

De toezichthouder spreekt ook van geautomatiseerd toezicht.[164] Hoewel dit niet wordt gedefinieerd vermeldt het rapport wel een viertal randvoorwaarden die onder meer verwijzen naar functiescheiding, compartimentering en transparant gegevensbeheer, automatische rapportage en digitale ontsluiting van gegevensbestanden. In de komende Avg worden naast de voorgeschreven DPIA nog andere verplichtingen opgelegd die functionele scheiding van gegevensverwerkingssystemen en automatisch toezicht aantrekkelijk kunnen maken, met name in art. 28 (documentatie van type dataverwerking, doel, doorgifte aan derde partijen en zo meer, welke documentatie op verzoek beschikbaar moet worden gemaakt voor de autoriteit gegevensbescherming).

Zeer relevant is art. 14.1a(h) van de komende Avg die stipuleert dat ten aanzien van profiling drie zaken moeten worden gecommuniceerd aan het betreffende data subject: (1) het feit dat sprake is van profiling, (2) begrijpelijke informatie over de onderliggende logica en (3) de voorziene gevolgen.[165] Ook al is de concept Avg niet van toepassing op gegevensverwerking door politie-*agents*, dit type profieltransparantie zou op geaggregeerd niveau beschikbaar moeten komen voor alle burgers ten einde voorzienbaar te maken welk type gedrag tot stelselmatige observatie kan leiden – zodat de burger haar gedrag aan kan passen. Niet om dan heimelijk strafbare feiten te plegen, buiten het zicht van justitie (ook al zal dat zeker ook een gevolg zijn), maar om ervoor te kiezen geen strafbare feiten te plegen dan wel het risico te nemen dat men tegen de lamp loopt.[166]

Uitgangspunt is dat een *veilig* strafrecht (1) voorkomt dat de bewijslast ten aanzien van strafbaar handelen op basis van machinale gedragsanalyse wordt omgedraaid, (2) voorzienbaar maakt dat en hoe bepaalde handelingen tot strafbaarheid leiden en (3) transparantie biedt ten aanzien van de manier waarop politie en justitie burgers voorzienbaar maken door het verzamelen en vernetwerken van gegevens en de inzet van data-gestuurde intelligentie.

Zowel op het niveau van de wetgever als op dat van het bestuur en de rechter zullen afwegingen moeten worden gemaakt tussen het algemene belang van profieltransparantie en het algemene belang van criminaliteitsbestrijding.[167] Dit is op zichzelf niets nieuws. In een onlife wereld kan die afweging echter niet beperkt blijven tot het geschreven of ongeschreven recht. Daar zal, ook bij het ontwerp van de architectuur van de communicatie en informatie infrastructuur, moeten worden onderzocht hoe de schending van grondrechten die in de architectuur zit ingebakken (bijvoorbeeld: backdoors die justitie toegang moeten geven tot communicatie via internet) kan worden voorkomen of gecompenseerd (bijvoorbeeld door eventuele interceptie zo lastig te maken dat die technisch alleen per geval kan worden geeffectueerd).

Het is bovendien zaak dat de proportionaliteit die moet worden ingebouwd in de technische systemen door een onafhankelijke toezichthouder wordt getoetst, juist omdat de rechter in te veel gevallen buiten

[164] CTIVD (2015), die op p. 21 opmerkt 'Naar de mogelijkheden van deze vormen van toezicht verricht de CTIVD momenteel onderzoek'.

[165] Art. 14 lid 1a sub h: 'the existence of automated decision making including profiling referred to in Article 20(1) and (3) and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.'

[166] De komende Richtlijn gegevensbescherming opsporing en vervolging, justitiële samenwerking, opsporingsdoeleinden stipuleert in art. 9: 'Article 9 Measures based on profiling and automated processing. (1) Member States shall provide that measures which produce an adverse legal effect for the data subject or significantly affect them and which are based solely on automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall be prohibited unless authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.' In de Richtlijn is echter, anders dan in de Avg, geen transparantierecht opgenomen ten aanzien van profielen. Hoe begrijpelijk ook, in een rechtsstaat kan het niet zo zijn dat we geen idee hebben hoe we door justitie en politie kunnen worden getarget. Hier is slimme wetgeving nodig, die niet alleen beschermt tegen criminaliteit maar ook tegen 'overijverige' overheden.
2. Automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall not be based solely on special categories of personal data referred to in Article 8.

[167] Met in achtneming van de caveats uit sectie 3.3.1.

spel staat (ten eerste vanwege buitengerechtelijke afdoening en bestraffing, ten tweede vanwege de inzet van heimelijke bevoegdheden die niet tot strafzaken leiden, en ten derde vanwege de inzet van heimelijke bevoegdheden die niet bijdragen aan het bewijs en om die reden buiten het geding ter terechtzitting blijven).

Dat het toepassen van ingrijpende bevoegdheden in beginsel vooraf getoetst moet worden door de rechter-commissaris doet daar niet aan af. Het gaat er integendeel om te bekijken in hoeverre de technische infrastructuur het mogelijk maakt om onder de radar allerhande gedragspatronen zichtbaar te maken – en toe te passen - zonder dat wij dit weten.

4.3 We kunnen niet iedereen tegelijk verdenken, maar wel om het even wie?

Een volledig data-gestuurde samenleving kan eigenlijk niet veilig zijn, voor zover daarin alle vormen van sturing afhankelijk zijn geworden van machinaal lerende systemen. We zijn dan de macht over het stuur kwijtgeraakt. Interessant is dat juist uit de hoek van de 'voormannen' van de kunstmatige intelligentie waarschuwingen klinken tegen de toenemende afhankelijkheid van *agents*, vanwege hun toenemend vermogen om zelfstandig in te grijpen en zich daarbij ook steeds zelfstandiger te ontwikkelen.[168] Die waarschuwingen betreffen vooral de snelheid waarmee wij ons over lijken te geven aan systemen die we steeds minder in de hand hebben. Die snelheid ontneemt ons de kans om sturend te blijven bij het ontwerp van de architectuur die bepalend zal zijn voor de speelruimte van de *homo digitalis*. Tegelijk gaan stemmen op om de werkelijkheid onder ogen te zien en de onl*i*fe wereld met open vizier te betreden in het besef dat die wereld deels bevolkt wordt door entiteiten die 'handelend' optreden, allerlei 'intenties' bemiddelen en zowel de dingen als de mensen in hun omgeving voortdurend statistisch 'uitlezen'.[169] In mijn recente boek (Hildebrandt 2015) bepleit ik zo'n open vizier, inclusief het besef dat data-gestuurde *agents* weliswaar hun omgeving waarnemen, erop ingrijpen en ons gedrag proberen te ondervangen maar vooralsnog geen bewustzijn, geen zelfbewustzijn en geen gevoel ontwikkelen. Data, data-modellen en 'data lakes' (ongestructureerde datasets) moeten niet verward worden met datgene waarnaar ze verwijzen of waarvan ze de sporen of inferenties vastleggen. Zo is het ook met *agents* die aardig lijken, intelligent, zelfs humorvol. Zij kunnen uitstekend simuleren en dat kan niet alleen heel nuttig maar ook heel prettig zijn. Ze hebben echter niets te verliezen.

Voor het strafrecht betekent dit dat we de opbrengst van de inzet van politie-*agents* niet moeten overschatten en de kosten niet mogen onderschatten. 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. Die invasie vindt weliswaar plaats door middel van *agents* en in eerste instantie dus niet door personen, maar die *agents* zullen de afgeleide kennis op enig moment delen met wie daartoe bevoegd zijn. Bovendien, als we de betreffende *agents* niet slim ontwerpen, delen ze die informatie ook en voortdurend met wie daartoe niet bevoegd zijn.

We kunnen niet iedereen tegelijk verdenken, maar zouden wel om het even wie moeten kunnen verdenken. Deze stelling kan op twee manier gelezen worden. Ten eerste vanuit een eenzijdig beveiligingsperspectief. Dan gaat het erom in tijden van hyperconnectiviteit, remote control, en geautomatiseerde aanvallen te waarborgen dat iedereen voortdurend in de gaten wordt gehouden ten einde om het even wie onder verdenking te kunnen plaatsen – liefst nog voor zij zelfs maar een strafbaar feit heeft beraamd. Ten tweede vanuit het driedubbelperspectief van beveiliging, democratisch samenleven en individuele vrijheid. Dan gaat het erom te *voorkomen* dat politie-*agents* iedereen voortdurend in de gaten houden, en personen voorsorteren op basis van (voor hen zelf) onleesbare patronen, die uitmaken wie in aanmerking komen voor straffen en/of maatregelen. De bereidheid om 'om het even wie' te verdenken, *als feiten en omstandigheden daar aanleiding toe geven*, sluit in deze

[168] Gibbs (2015).
[169] Markoff (2015b), Kool en van Est (2015).

interpretatie juist uit dat we worden opgesloten in de gedragsprofielen van de *homo behaviouralis*. Dat zal alleen lukken als juristen zich niet alleen bezighouden met de vraag of de toedeling en de uitoefening van bevoegdheden in overeenstemming is met het strafvorderlijk legaliteitsbeginsel en de mensenrechten, maar zich ook actief gaan bezighouden met de vraag of politie-*agents* zo zijn ontworpen dat zij alleen mogelijk maken wat *niet* mag als dit *strikt noodzakelijk* is, en zichtbaar en controleerbaar maken wanneer welke bevoegdheden door wie worden overschreden. Voorwaar, geen sinecure.

5 Literatuur

Aas, K.F. 2005. *Sentencing in the Age of Information: From Faust to Macintosh*. London: Routledge-Cavendish.

Ambrose, S.H. 2010. "Coevolution of Composite-Tool Technology, Constructive Memory, and Language: Implications for the Evolution of Modern Human Behavior". *Current Anthropology* 51 (1): 135–47.

Ampère, A.-M. 2012. *Essai sur la philosophie des sciences.* Parijs: Hachette.

Ancel, M. 1981. *La défense sociale nouvelle*. 3e ed. Parijs: Editions Cujas.

Arendt, H. 1958. *The Human Condition*. Chicago, London: University Press of Chicago.

Ariely, D. en G.S. Berns. 2010. "Neuromarketing: the hope and hype of neuroimaging in business". *Nature reviews. Neuroscience* 11 (4): 284–92.

Barry-Jester, A.M., B. Casselman en D. Goldstein. 2015. "Should Prison Sentences Be Based On Crimes That Haven't Been Committed Yet?" *FiveThirtyEight*, zie <http://fivethirtyeight.com/features/prison-reform-risk-assessment/>.

Beck, U. 1986. *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt am Main: Suhrkamp.

Berkhout, T.M. en T.M. van Engers. 2012. "Onderzoeksmethodologie voor informatiegestuurd fiscaal toezicht". *Weekblad Fiscaal Recht* 6958: 824–32.

Binmore, K. 1988. "Social Contract III: Evolution and Utilitarianism". CREST Working Paper. <http://deepblue.lib.umich.edu/handle/2027.42/100628>.

Bits of Freedom. 2012. "Gegevens burgers niet veilig bij politie. Onderzoek naar de audits Wet Politiegegevens". <https://www.bof.nl/live/wp-content/uploads/politie-privacy-audits-2012/20120704-onderzoek-politie-privacy-audits-2012.pdf>.

Blom, T. 2015a. "Verkennend onderzoek bij: Wetboek van Strafvordering, Artikel 126gg [Ter voorbereiding van de opsporing. Voorwaarden]". In *Tekst & Commentaar Strafvordering*. Online versie (bijgewerkt tot 1 juli 2015).

Blom, T. 2015b. "Vorderen gegevens t.b.v. verkennend onderzoek, bij: Wetboek van Strafvordering, Artikel 126hh [Vorderen en bewerken gegevens]". In *Tekst & Commentaar Strafvordering*. Online versie (bijgewerkt tot 1 juli 2015).

Borgers, M. 2007. *De vlucht naar voren door Oratie Vrije Universiteit Amsterdam*. Den Haag: Boom Juridische Uitgevers.

boyd, d. en K. Crawford. 2012. "Critical Questions for Big Data". *Information, Communication & Society* 15 (5): 662–79.

Van Brakel, J. 1998. *Interculturele communicatie en multiculturalisme*. Leuven: Universitaire Pers Leuven.

Brenner, S.W. 2007. *Law in an era of "smart" technology*. New York: Oxford University Press.

———. 2010. *Cybercrime Criminal Threats from Cyberspace*. Santa Barbara, CA: Praeger.

Brinkhof, S. 2014. "Ambtsberichten van de AIVD. Belangrijke maar met risico's omgeven schakel in de strafrechtelijke aanpak van jihadisme". *Nederlands Juristen Blad* (37), 2633–39.

Brownsword, R. 2008. *Rights, Regulation, and the Technological Revolution*. Oxford: Oxford University Press.

Buruma, Y. 1996. *De aandacht van de strafrechter (oratie Nijmegen)*. Deventer: Gouda Quint.

Butler, J. 2005. *Giving an account of oneself*. New York: Fordham University Press.

College Bescherming Persoonsgegevens. 2015. "CBP: Databestanden Justitie niet actueel". Den Haag.

Chevallier, J. 1994. *L'Etat de droit*. Parijs: Montchrestien.

Chopra, S. en L.F. White. 2011. *A Legal Theory for Autonomous Artificial Agents*. Michigan: University of Michigan Press.

Cleiren, C. P. M. 1992. *De Openheid van de Wet, de Geslotenheid van Het Recht*. Arnhem: Gouda Quint.

———. 2015. "Legaliteit bij: Wetboek van Strafvordering, Artikel 1 [Legaliteitsbeginsel]". In *Tekst & Commentaar Strafvordering* Online versie (bijgewerkt tot 1 juli 2015).

Coldren, J.R., A. Huntoon en M. Medaris. 2013. "Introducing Smart Policing: Foundations, Principles, and Practice". *Police Quarterly* 16 (3): 275–86.

Commissie van Toezicht Inlichtingen- en Veiligheidsdiensten. 2015. "Reactie CTIVD op concept-wetsvoorstel Wiv 20XX". Den Haag: CTIVD. <http://www.ctivd.nl/actueel/nieuws/2015/09/03/reactie-ctivd-concept-wetsvoorstel>.

Cope, N. 2004. "'Intelligence Led Policing or Policing Led Intelligence?' Integrating Volume Crime Analysis into Policing". *British Journal of Criminology* 44 (2): 188–203.

Crijns, J.H. 2014. “Op zoek naar consistentie - Bestraffing buiten de rechter om in strafrecht en bestuursrecht”. *Rechtsgeleerd Magazijn Themis* 6: 263–74.

Cuijpers, C. en B.-J. Koops. 2013. “Smart Metering and Privacy in Europe: Lessons from the Dutch Case”. In S. Gutwirth, R. Leenes, P. de Hert en Y. Poullet (red.) *European Data Protection: Coming of Age*. Dordrecht: Springer, 269–93.

Custers, B. 2004. *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*. Nijmegen: Wolf Legal Publishers.

Damasio, A.R. 2011. *Self comes to mind: constructing the conscious brain*. New York: Pantheon Books.

Dewey, John. 1916. “The Logic of Judgements of Practice”. In *Essays in Experimental Logic.* Chicago: University of Chicago Press: 214-281.

Dowrick, F. E. 1954. “The Relationship of Principal and Agent”. *The Modern Law Review* 17 (1): 24–40.

Duff, R.A. 2001. *Punishment, Communication, and Community*. Oxford: Oxford University Press.

———. 2009. “Legal and Moral Responsibility”. *Philosophy Compass* 4 (6): 978–86.

———. 2013. “Who Must Presume Whom to Be Innocent of What?” *Netherlands Journal of Legal Philosophy*, 42 (3), 170-192.

Dworkin, R. 1978. *Taking Rights Seriously*. Cambridge: Harvard University Press.

Evans, T. en J. Harris. 2004. “Street-Level Bureaucracy, Social Work and the (Exaggerated) Death of Discretion”. *British Journal of Social Work* 34 (6): 871–95.

Von Feuerbach, P.J.A. 1801. *Lehrbuch des gemeinen in Deutschland gültigen Peinlichen Rechts: mit vielen Anmerkungen und Zusatzparagraphen und mit einer vergleichenden Darstellung der Fortbildung des Strafrechts durch die neuen Gesetzgebungen*. Giessen: Georg Friedrich Heyers Verlag.

Flanagan, M., D. Howe en H. Nissenbaum. 2007. “Values in Design: Theory and Practice”. In J. van den Hoven en J. Weckert (red.) *Information Technology and Moral Philosophy*. Cambridge: Cambridge University Press.

Floridi, L. (red.). 2014. *The Onlife Manifesto. Being Human in a Hyperconnected Era*. Dordrecht: Springer.

Floridi, L. en J.T. Sanders. 2001. “Artificial Evil and the Foundation of Computer Ethics”. *Ethics and Information Technoogy.* 3 (1): 55–66.

Floridi, L. en J.W. Sanders. 2004. “On the Morality of Artificial Agents”. *Minds and Machines* 14 (3): 349–79.

Foqué, R. en A.C. ’t Hart. 1990. *Instrumentaliteit en rechtsbescherming*. Arnhem Antwerpen: Gouda Quint Kluwer Rechtswetenschappen.

Gadamer, H.G. 1990. *Gesammelte Werke Bd.1: Hermeneutik I: Wahrheit und Methode: Grundzüge einer philosophischen Hermeneutik*. Tubingen: Mohr Siebeck.

Ganesh, S. 2013. *How avatars become of the flesh and blood*. Proefschrift Radboud Universiteit Nijmegen. Uitgegeven in eigen beheer.

Geertz, C. 2001. *Available Light: Anthropological Reflections on Philosophical Topics.* Princeton NJ: Princeton University Press.

de Geest, G. 2004. “Hoe maken we van de rechtswetenschap een volwaardige wetenschap?” *Nederlands Juristenblad* 79: 58–66.

Geminn, Ch. L. 2014. *Rechtsverträglicher Einsatz von Sicherheitsmaßnahmen im öffentlichen Verkehr*. Wiesbaden: Springer.

Gibbs, S. 2015. “Musk, Wozniak and Hawking Urge Ban on Warfare AI and Autonomous Weapons”. *The Guardian*, 27 juli.

Gier, N.F. 1981. *Wittgenstein and Phenomenology; a Comparative Study of the Later Wittgenstein, Husserl, Heidegger, and Merleau-Ponty.* Albany, NY: State University of New York Press.

Gigerenzer, G. en C. Engel (red.) 2006. *Heuristics and the Law*. Cambridge, MA: MIT.

Gleick, J. 2010. *The Information: A History, a Theory, a Flood.* New York: Pantheon.

Gless, S. en T. Weigend. 2014. “Intelligente Agenten und das Strafrecht”. *ZStW* 126: 561–91.

González Fuster, G. 2014. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Cham: Springer.

De Graaff, B. 2015. “Pas of voor hersenvredebreuk”. *De Groene Amsterdammer* 139 (37), 9 september.

Halderen, R.C. en K.M. Lasthuizen. 2013. “Creatief gebruik van bevoegdheden. Een explorerend onderzoek binnen de Nederlandse politie”. *Tijdschrift voor veiligheid* 12 (1): 16–36.

Harcourt, B.E. 2007. *Against prediction: profiling, policing, and punishing in an actuarial age*. Chicago: University of Chicago Press.

Hayles, N. K. 1999. *How we became posthuman. Virtual bodies in cybernetics, literature, and informatics*. Chicago: University of Chicago Press.

Hegel, G.W.F. 1970. *Grundlinien der Philosophie des Rechts*. Frankfurt: Suhrkamp.

Helbing, D. 2012. *Social Self-Organization: Agent-Based Simulations and Experiments to Study Emergent Social Behavior*. Berlin: Springer.

Hern, A. 2015. "Yes, androids do dream of electric sheep". *The Guardian*, June 18.

de Hert, P. en S. Gutwirth. 2009. "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action". In S. Gutwirth, Y. Poullet, P. de Hert, C. Terwangne en S. Nouwt (red.) *Reinventing Data Protection?* Dordrecht: Springer, 3–44.

Hijink, M. 2012. "Flame: dit cyberwapen is 'erger dan Stuxnet'". NRC Handelsblad, 29 mei.

Hildebrandt, M. 2002. *Straf(begrip) en procesbeginsel. Een onderzoek naar de betekenis van straf en strafbegrip en naar de waarde van het procesbeginsel*. Deventer: Kluwer.

———. 2004. "Wetenschap in rechte". *TREMA*, nr. april: 187–96.

———. 2005. "Profiling and the identity of European citizens". In M. Hildebrandt en S. Gurtwirth, Profiling the European Citizen. Cross-Disciplinary Perspectives. Dordrecht: Springer.

———. 2008. "A Vision of Ambient Law". In R. Brownsword en K. Yeung (red.) *Regulating Technologies*. Oxford: Hart.

———. 2008a. "Ambient Intelligence, Criminal Liability and Democracy". *Criminal Law and Philosphy* 2 (2), 163-180

———. 2008b. "Defining Profiling: A New Type of Knowledge". In M. Hildebrandt en S. Gurtwirth, *Profiling the European Citizen. Cross-Disciplinary Perspectives*. Dordrecht: Springer, 17-45.

———. 2010. "Juridische bescherming 'by design'?" *Rechtsfilosofie & Rechtstheorie* (2): 101–6.

———. 2011a. "Criminal liability and 'smart' environments". In A. Duff en S. Green (red.) *Philosophical Foundations of Criminal Law*. Oxford: Oxford University Press, 507–32

———. 2011b. *De rechtsstaat in cyberspace?* Oratie Radboud Universiteit. Uitgegeven in eigen beheer.

———. 2011c. "Technologische en juridische normativiteit: het tekort van het reguleringsparadigma. Een respons op Leenes' 'Technoregulering'". *Recht der werkelijkheid* (1), 53–59.

———. 2012. "Oordeelsvorming door mens en machine: heuristieken, algoritmes en legitimatie". In E.T. Feteris, H. Kloosterhuis, H.J. Plug, J.A. Pontier en C.E. Smith (red.) *Gewogen oordelen. Essays over argumentatie en recht*. Den Haag: Boom Juridische Uitgevers, 243-257.

———. 2013a. "From Galatea 2.2 to Watson – And Back?" In M. Hildebrandt en J. Gaakeer (red.) *Human Law and Computer Law: Comparative Perspectives*. Ius Gentium: Comparative Perspectives on Law and Justice 25. Dordrecht: Springer, 23-45.

———. 2013b. "Legal Protection by Design in the Smart Grid". In opdracht van het Smart Energy Collective. Nijmegen: Radboud University Nijmegen.

———. 2013c. "Extraterritorial Jurisdiction to Enforce in Cyberspace". *Toronto Law Journal* 63 (2), 196-224.

———. 2013d. "Balance or Trade-off? Online Security Technologies and Fundamental Rights". *Philosophy & Technology* 26 (4): 357–79.

———. 2014. "ICT en Rechtsstaat". In *Recht en computer*, bewerkt door S. Van der Hof, A.R. Lodder en G.J. Zwenne. Deventer: Kluwer, 25–45.

———. 2015a. *Smart Technologies and the End(s) of Law. Novel Entanglements of Law and Technology*. Cheltenham: Edward Elgar.

———. 2015b. "Radbruch's Rechtsstaat and Schmitt's Legal Order: Legalism, Legality, and the Institution of Law". *Critical Analysis of Law* 2 (1). <http://cal.library.utoronto.ca/index.php/cal/article/view/22514>.

———. 2016a te verschijnen. "Law as information in the era of data-driven agency (Chorley Lecture)". *The Modern Law Review*, januari.

———. 2016b te verschijnen. "New animism in global policing Re-animating the Rule of Law?" In *Handbook of Global Policing*. London: SAGE.

Hildebrandt, M. en L. Tielemans. 2013. "Data Protection by Design and Technology Neutral Law". *Computer Law & Security Review* 29 (5), 509-521.

Hildebrandt, M. en M. Koning. 2012. “Universele handhavingsjurisdictie in cyberspace?” *Strafblad*, nr. 3: 195-203.

Hildebrandt, M. en B.-J. Koops. 2010. “The challenges of Ambient Law and legal protection in the profiling era”. *The Modern Law Review* 73 (3): 428–60.

Holmes, O.W. 1996. “The Path of the Law”. *Harvard Law Review* 110: 991-1009.

Hoogenboom, B. 2010. *The Governance of Policing and Security*. Hampshire: Palgrave Macmillan.

———. 2009. *Bringing the police back in. Notes on the lost & found character of the police in police Studies*. Oratie VU, Stichting Maatschappij, Veiligheid en Politie (SMVP). <http://www.maatschappijenveiligheid.nl/kennisbank/hoogenboom_english/>.

Huizinga, J. 2010. *Homo Ludens. Proeve eener bepaling van het spel-element der cultuur*. Amsterdam: Amsterdam University Press.

IBM. 2011. “Watson - A System Designed for Answers. The future of workload optimization”. White Paper,

Jacobs, B. 2015. “NJB: blog - interceptie door AIVD en MIVD”. *Nederlands Juristenblad*, 5 februari. <http://njb.nl/blog/vluchtig-en-stelselmatig-een-bespreking-van.13474.lynkx>.

Jensma, F. 2013. “Oom agent surft volautomatisch met u mee”. *NRC Weekend*, maart 23.

———. 2015. “Misstap VW is voorbeeld van ‘gaming the system’”. *NRC Handelsblad*, oktober 3. <http://www.nrc.nl/handelsblad/2015/10/03/misstap-vw-is-voorbeeld-van-gaming-the-system-1540071>.

Jensma, F., T. Barkhuysen en J. Hulskamp. 2013. “De Uitspraak: Mag Justitie een vordering van 6 euro automatisch verhogen tot 711 euro?” *NRC Handelsblad*, 14 juni.

Jensma, F., Y. Buruma en A. de Swart. 2010. “Uitspraak 64: Mag de politie rijbewijzen controleren om zo drugskoeriers te vangen?” *NRC Handelsblad*, 19 oktober.

Kahneman, D. en A. Tversky. 1979. “Prospect Theory: An Analysis of Decision under Risk”. *Econometria* 47 (2): 263–92.

Karnow, C.E.A. 1997. *Future Codes: Essays in Advanced Computer Technology and the Law*. Boston London: Artech House.

Keulen, B.F. 2014. “Wetboek op stelten - Over de modernisering van het Wetboek van Strafvordering”. *Rechtsgeleerd Magazijn Themis* (5): 211–22.

Klip, A.H. en A.-S. Massa. 2010. “Communicerende grondslagen van extraterritoriale rechtsmacht”. Den Haag: Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC).

Knigge, G. 1994. “De strafvordering in het geding”. In *Handelingen Nederlandse Juristen-Vereniging 1994-I: Herbezinning op (de grondslagen van) het Wetboek van Strafvordering*, Zwolle: W.E.J. Tjeenk Willink: 37–117.

Koning, M. 2012. “Van teugelloos ‘terughacken’ naar ‘digitale toegang op afstand’”. *Privacy & Informatie* (2): 46–52.

———. 2015. “Het recht op bescherming van persoonsgegevens in de Europese en nationale rechtsorde na Lissabon”. In J.H. Gerards, H. de Waele, K. Zwaan (red.) *Vijf jaar bindend EU-Handvest van de Grondrechten*, 351-385.

Kooijmans, T. 2002. *Op maat geregeld? Een onderzoek naar de grondslag en de normering van de strafrechtelijke maatregel*. Deventer: Kluwer.

Kool, L. en R. van Est. 2015. “Laat iedereen zij aan zij werken met robots”. *De Volkskrant*, Opinie, 5 september.

Koops, B.- J. 2010. “The Internet and its Opportunities for Cybercrime”. In M. Herzog-Evans (red.) *Transnational criminology manual*. Nijmegen: Wolf Legal Publishers, 735–54.

———. 2011. “Digitale Grondrechten en de Staatscommissie: Op Zoek Naar de Kern”. *Tijdschrift voor Constitutioneel Recht*, 168-185.

———. 2013 “The (In)flexibility of Techno-Regulation and the Case of Purpose-Binding”, *Legisprudence* 5 (2), 171-194.

Koops, B.-J., G. Bodea, G. Broenink, C. Cuijpers, L. Kool, C. Prins en M. Schellekens. 2012. “Juridische scan openbrononderzoek. Een analyse op hoofdlijnen van de juridische aspecten van iRN/iColumbo-infrastructuur en HDIeF-tools”. Tilburg: TILT - TNO.

Koops, B.-J. en M. Goodwin. 2014. “Cyberspace, the cloud, and cross-border criminal investigation”. Den Haag: Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC).

Kuitenbrouwer, F. 2007. “Pas op voor bedoelingen”. *NRC.nl,* 2 oktober. <http://weblogs.nrc.nl/kuitenbrouwer/2007/10/02/pas-op-voor-bedoelingen/>.

van de Laar, T. en S. Voerman. 2011. *Vrije wil*. Rotterdam: Lemniscaat.

Lakoff, G. en M. Johnson. 2003. *Metaphors We Live By*. Chicago: University Of Chicago Press.

Lamme, V. 2011. *De vrije wil bestaat niet*. Bert Bakker.

Latour, B. 1998. “For Bloor and Beyond - a Reply to David Bloor’s Anti-Latour”. *Studies in History and Philosophy of Science* 30 (1): 113–29.

———. 2005. *Reassembling the social: an introduction to actor-network-theory*. New York: Oxford University Press.

Leenes, R. 1998. *Hercules of Karneades. Hard cases in recht en rechtsinformatica*. Enschede: Twente University Press.

———. 2010. *Harde lessen. Apologie van Technologie als Reguleringsinstrument*. Tilburg: Universiteit van Tilburg.

———. 2011. “Technoregulering: regulering of ‘slechts’ disciplinering”. *Recht der Werkelijkheid*, nr. 1.

Leezenberg, M. en G. De Vries. 2012. *Wetenschapsfilosofie voor geesteswetenschappen*. 2de ed. Amsterdam: Amsterdam University Press.

Leydesdorff, L. 2010. “The Communication of Meaning and the Structuration of Expectations: Giddens’ ‘structuration Theory’ and Luhmann’s ‘self-Organization’”. *Journal of the American Society for Information Science and Technology* 61 (10): 2138–50.

Leyten, J.C.M. 1997. “Afweging en de mythe van de weegschaal”. *Nederlands Juristen Blad*, 636–37.

Loof, J.P., J. Uzman, T. Barkhuysen, A.C. Buyse, J.H. Gerards en R.A. Lawson. 2015. “Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten”. Den Haag: CTIVD. <http://www.ctivd.nl/documenten/publicaties/2015/08/26/rapport-universiteit-leiden>.

Loth, M.A. en J. Gaakeer. 2005. *Meesterlijk Recht, M.A. Loth & A.M.P. Gaakeer* 3de ed. Den Haag: Boom Juridische Uitgevers.

Mackor, A.R. en V. Geeraets. 2013. “Special Issue. Antony Duff: The Presumption of Innocence”. *Netherlands Journal of Legal Philosophy* 42 (3)

Markoff, J. 2015a. “Relax, the Terminator Is Far Away”. *The New York Times*, 25 mei. <http://www.nytimes.com/2015/05/26/science/darpa-robotics-challenge-terminator.html>.

———. 2015b. *Machines of Loving Grace: The Quest for Common Ground Between Humans and Robots*. New York: Ecco.

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

Mead, G.H. en Ch.W. Morris. 1962. *Mind, self, and society from the standpoint of a social behaviorist*. Chicago, Ill: University of Chicago Press.

Van der Meij, P.P.J. 2015. “Opsporingsonderzoek bij: Wetboek van Strafvordering, Artikel 132a [Opsporingsonderzoek]”. In *Tekst & Commentaar Strafvordering*. Online versie (bijgewerkt tot 1 juli 2015).

Mitchell, T. 1997. *Machine Learning*. New York: McGraw-Hill Education.

Mooij, A. 2004. *Toerekeningsvatbaarheid: over handelingsvrijheid*. Boom.

Morozov, E. 2011. *The Net Delusion: The Dark Side of Internet Freedom*. PublicAffairs.

Morse, S.J. 2008. “Determinism and the Death of Folk Psychology: Two Challenges To Responsibility from Neuroscience”. *Minnesota Journal of Law Science & Technology* 9 (1): 1–35.

Muller, E.R., M.J. Dubelaar en C.P.M. Cleiren. 2007. “Algemene beginselen van behoorlijke politiezorg”. In *Politie: studies over haar werking en organisatie*, Deventer: Kluwer, 559–600.

Nationaal Coordinator Terrorismebestrijding en Veiligheid. 2015. “Themanummer ‘Herijking vitale infrastructuur’”. *Magazine Nationale Veiligheid en Crisisbeheersing*, 7 juli.

Neumann, S. en M. Volkamer. 2014. “A Holistic Framework for the Evalutation of Internet Voting Systems”. In *Design, Development, and Use of Secure Electronic Voting Systems*. Hershey, PA: IGI Global, 76–91.

Nietzsche, F. 1969. *On the Genealogy of Morals*. New York: Random House.

Van Noort, W. en R. Kist. 2015. “Het misdrijf is al ontdekt voor het gepleegd is”. *NRC Handelsblad*, 23 augustus.

Novotny, A. en S. Spiekermann. 2013. “Personal Information Markets AND Privacy: A New Model to Solve the Controversy”. In M. Hildebrandt, K. O’Hara en M. Waidner (red.) *Digital Enlightenment Yearbook 2013: The Value of Personal Data*, Amsterdam: IOS Press.

Oerlemans, J. J. 2011. “Hacken als opsporingsbevoegdheid”. *Delikt en Delinkwent* 41 (8): 888–908.

Oerlemans, J.J. en B.-J. Koops. 2012. “Surveilleren en opsporen in een internetomgeving”. *Justitiële verkenningen* 38 (5): 35–49.

Open Science Collaboration. 2015. “Estimating the reproducibility of psychological science”. *Science* 349 (6251).

Packer, H.L. 1968. “Two Models in the Criminal Process”. In *The Limits of the Criminal Sanction*. Standford: Standford University Press, 149–74

Pagallo, U. 2013. *The Laws of Robots*. Dordrecht: Springer Netherlands.

Pedreshi, D., S. Ruggieri en Franco Turini. 2008. “Discrimination-aware data mining”. In *KDD ’08 Proceeding of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM Press, 560-568.

Pentland, A. 2014. *Social Physics: How Good Ideas Spread—The Lessons from a New Science*. New York: Penguin.

Pfeifer, R. en J. Bongard. 2007. *How the Body Shapes the Way We Think. A New View of Intelligence*. Cambridge, MA - London, England: MIT Press.

Pitlo, A., P.H.M. Gerver, H. Sorgdrager en R.H. Stutterheim. 1995. *Het systeem van het Nederlandse privaatrecht*. Deventer: Gouda Quint.

de Poot, C.J., R.J. Bokhorst, W.H. Smeenk en R.F. Kouwenberg. 2008. “De opsporing verruimd? De Wet opsporing terroristische misdrijven een jaar in werking.” Den Haag: Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC).

Prigogine, I. en I. Stengers. 1984. *Order out of Chaos.* New York: Bantam Books.

Fokkens, J.W. 2014. “Beschikt en gewogen. Over de naleving van de wet door het openbaar ministerie bij het uitvaardigen van strafbeschikkingen (Een rapport van de procureur-generaal bij de Hoge Raad in het kader van het in art. 122 lid 1 Wet RO bedoelde toezicht)”. Den Haag.

Purtova, N. 2012. *Property Rights in Personal Data: A European Perspective*. Alphen aan den Rijn: Kluwer Law International.

Putnam, H. 1995. *Pragmatism: An Open Question*. Oxford, UK; Cambridge, MA: Wiley-Blackwell.

Radbruch, G. 1945. “Fünf Minuten Rechtsphilosophie”. *Rhein Neckar Zeitung*, 12 september.

———. 1950. *Rechtsphilosophie. Herausgegeven von Erik Wolf*. Stuttgart: Koehler.

Redactie AD. 2014. “Rechters laken gijzeling wanbetaler door justitie”. *Algemeen Dagblad,* 24 februari, <http://www.ad.nl/ad/nl/1012/Nederland/article/detail/3602492/2014/02/24/Rechters-laken-gijzeling-wanbetaler-door-justitie.dhtml>.

Ricoeur, P. 1975. *La Métaphore vive*. Parijs: Seuil.

———. 1986. *Du Texte a l’action. Essais d’herméneutique II*. Parijs: Seuil.

Roby-Brami, A., J. Hermsdorfer, A. C. Roy en S. Jacobs. 2012. “A Neuropsychological Perspective on the Link between Language and Praxis in Modern Humans”. *Philosophical Transactions of the Royal Society B: Biological Sciences* 367 (1585): 144–60.

Roessingh, M. 2013. “iColumbo kan meer dan hij mag”. *Trouw*, 2 november.

Russell, S. en P. Norvig. 2009. *Artificial Intelligence: A Modern Approach*. 3de ed. Upper Saddle River, NJ: Prentice Hall.

Schermer, Bart. 2007. *Software Agents, Surveillance, and the Right to Privacy. A Legislative Framework for Agent-Enabled Surveillance*. Proefschrift Universiteit van Leiden. Leiden: Leiden University Press.

Schmitt, C. 1993. *Über die drei Arten des rechtswissenschaftlichen Denkens.* Berlin: Duncker & Humblot.

Schuyt, C.J.M. 1986. *Filosofie van de sociale wetenschappen*. Leiden: Martinus Nijhoff.

Schuyt, K. 2009. *Recht, orde en burgerlijke ongehoorzaamheid.* Amsterdam: Amsterdam University Press.

Sieburgh, C.H. 2015. “Waarom het Unierecht de invloed van grondrechten op het privaatrecht aanjaagt en versterkt”. *Rechtsgeleerd Magazijn Themis*, (1): 3–13.

Slors, M. 2015. *Dat had je gedacht*. Amsterdam: Boom.

Solum, L.B. 1992. “Legal Personhood for Artificial Intelligences”. *North Carolina Law Review* 70 (2): 1231–87.

Stengers, I. 2010. *Cosmopolitics I*. Vertaald door Robert Bononno. Minneapolis: University Of Minnesota Press.

Strikwerda, L. 2014. “Virtual acts, real crimes? A legal-philosophical analysis of virtual cybercrime”, Enschede: Universiteit Twente.

Struijk, S. 2015. *De ISD in perspectief*. Proefschrift Erasmus Universiteit Rotterdam. Nijmegen: Wolf Legal Publishers.

Suh, S.C., U.J. Tanik, J.N. Carbone en A. Eroglu (red.) 2014. *Applied Cyber-Physical Systems*. New York, NY: Springer.

Sunstein, C. 2001. *Republic.com*. Princeton, Oxford: Princeton University Press.

Swaab, D. 2010. *Wij zijn ons brein*. Amsterdam: Atlas-Contact.

Teubner, G. 2007. “Rights of Non-humans? Electronic Agents and Animals as New Actors in Politics and Law”. European University Institute.

Thaler, R.H. en C.R. Sunstein. 2008. *Nudge : improving decisions about health, wealth, and happiness*. New Haven: Yale University Press.

NJB. 2013. “Themanummer Neurolaw in Nederland”. *Nederlands Juristen Blad*, 2611–3161.

Timan, T. en E.J. Koops. 2014. “Sociale media en surveillance: over verschuivende rollen en vervagende grenzen”. *Strafblad*, oktober, 284–90.

TNO. 2010. “Herkenning van digitale informatie”. Delft.

Tokmetzis, D. 2015. “Kun je mensen straffen op basis van statistiek?” *De Correspondent*. 8 augustus. <https://decorrespondent.nl/3174/Kun-je-mensen-straffen-op-basis-van-statistiek-/33597393060-c0a8e51c>.

van Delft, D. 2003. “‘Geléérd zijn jullie wel’”. *NRC Handelsblad*, 12 april.

van Hamel, G.A. 1907. *Inleiding tot de studie van het Nederlandsche Strafrecht*. Haarlem: De Erven K. Bohn.

Varela, F.J., E. Thompson en E. Rosch. 1991. *The Embodied Mind. Cognitive Science and Human Experience*. Cambridge, MA: MIT.

Vedder, A. 1999. “KDD: The challenge to individualism”. *Ethics and Information Technology* 1 (4): 275–81.

Verbeek, P.-P. 2011. *Moralizing Technology: Understanding and Designing the Morality of Things*. Chicago; London: The University of Chicago Press.

Vervaele, J. 2005. “Gegevensuitwisseling En Terrorismebestrijding: Emergency Criminal Law?” *Panopticon: Tijdschrift Voor Strafrecht, Criminologie En Forensisch Welzijnswerk* 26 (2): 27–52.

Vincent, N.A. 2013. *Neuroscience and Legal Responsibility*. New York, NY: Oxford University Press.

de Visser, E. 2015. “Gevangenissen bestrijden agressie met supplementen”. *De Volkskrant*, 5 september.

de Vries, K., R. Bellanova, P. De Hert en S. Gutwirth. 2011. “The German Constitutional Court Judgement on data retention: proportionality overrides unlimited surveillance (doesn’t it ?)”. In S. Gutwirth, Y. Poullet, P. De Hert en R. Leenes (red.) *Privacy and data protection: an element of choice*, Dordrecht: Springer, 3–24.

Vitkauskas, Dovydas. 2012. *Protecting the right to a fair trial under the European Convention on Human Rights*. (Council of Europe human rights handbooks). Strasbourg: Council of Europe.

Waldron, J. 2003. “Security and Liberty: The Image of Balance”. *Journal of Political Philosophy* 11 (2): 191–210.

Weigend, T. 2013. “There is Only One Presumption of Innocence”. In: *Netherlands Journal of Legal Philosophy* 42 (3), 193-204.

Wendt, J.A.I. 2015. *De methode der rechtswetenschap vanuit kritisch-rationeel perspectief*. Deventer: Paris.

Wiener, N. 1988. *The Human Use Of Human Beings: Cybernetics And Society*. Cambridge, MA: Da Capo Press.

Wittgenstein, L. 1992. *Filosofische onderzoekingen*. Meppel en Amsterdam: Boom.

Zedner, L. 2008. “Review of Against Prediction by Bernerd E Harcourt, UCP 2007”. *New Criminal Law Review: In International and Interdisciplinary Journal* 11 (2): 359–62.