Opinie
arsaequi.nl/maandblad AA20160097

WAT WEET MIJN AUTO NOG MEER?

Juridische bescherming *by design* in tijden van het Internet van de Dingen

Mireille Hildebrandt*

Deze bijdrage gaat in op de datastromen die vrijkomen bij de introductie van 'connected and autonomous driving' en onderzoekt de mogelijke implicaties van technieken als machinaal leren voor fundamentele rechten zoals privacy en gegevensbescherming, alsmede een aantal grondbeginselen van het recht, met name proportionaliteit, transparantie, en de mogelijkheid zich te verzetten tegen geautomatiseerde beslissingen.

* Prof.mr.dr. M. Hildebrandt is onderzoekshoogleraar Interfacing Law and Technology aan de Vrije Universiteit Brussel en in deeltijd gewoon hoogleraar Smart Environments, Data Protection and the Rule of Law aan de Radboud Universiteit Nijmegen.

Begin augustus 2016 berichtte *NRC Handelsblad* dat 'de politie bij ernstige verkeersongelukken voortaan computergegevens uit auto's [gaat] gebruiken om te achterhalen wat er voor de crash gebeurde'.[1] Eind 2014 tekenden, volgens het *Algemeen Dagblad*, meer dan 25.000 mensen een petitie om een zwarte doos (*event data recorder*) verplicht te stellen,[2] in de hoop dat daders hun gerechte straf niet ontlopen. Op verschillende plekken in Nederland heeft de politie inmiddels experimenten gedaan met het uitlezen van de zwarte doos, die gegevens van de laatste 5 seconden voor een crash opslaat. In sommige gevallen biedt dit de mogelijkheid om ondanks het ontbreken van fysieke sporen meer duidelijkheid te verkrijgen over de toedracht van het ongeval. Het ontbreken van fysieke sporen wordt overigens deels veroorzaakt door veiligheidssystemen zoals het *Anti-lock Brake System* (ABS) en het *Electronic Stability Program* (ESP), waardoor het lastiger wordt de toedracht van een ongeluk achteraf vast te stellen.[3] Zo roept het gebruik van de ene technologie de inzet van de andere op.

> Om een zinvolle afweging te kunnen maken tussen de privacy van de automobilist en het maatschappelijk belang om 'te weten wat er gebeurd is', is het zaak om wat verder kijken dan onze speurneus lang is

In deze Opinie ga ik mij niet beperken tot het uitlezen van gegevens uit een zwarte doos door justitie na een ernstig ongeval, waar – op zichzelf genomen – veel voor te zeggen valt. Zeker wanneer de gegevens elke 5 seconden worden overschreven en een beperkt aantal waarnemingen bevatten. Om een zinvolle afweging te kunnen maken tussen de privacy van de automobilist en het maatschappelijk belang om 'te weten wat er gebeurd is', is het echter zaak om wat verder kijken dan onze speurneus lang is. Daartoe ga ik in paragraaf 1 kort in op de data die verwerkt wordt door de elektronica waarmee huidige en toekomstige auto's worden aangestuurd, en de mate waarin toegang tot die data tot een aantasting van het recht op privacy kan leiden (paragraaf 2). Daarna onderzoek ik in paragraaf 3 de inbreuken op het fundamentele recht op gegevensbescherming. Ik richt mij daarbij – tenzij anders vermeld – op de Algemene verordening gegevensbescherming (Avg)[4] en de Richtlijn gegevensbescherming opsporing en vervolging,[5] die vanaf mei 2018 van toepassing zijn. Daarbij zal ik, in paragraaf 4, in het bijzonder aandacht vragen voor de manier waarop het constitutioneel beginsel van doelbinding bescherming kan bieden tegen onrechtmatige verwerking van persoonsgegevens, die gemakkelijk tot uitholling van de onschuldpresumptie kan leiden. Dat laatste niet zozeer door specifieke bewijsvergaring naar aanleiding van een ernstig ongeval, maar door het afleiden van risicoprofielen die toekomstig rijgedrag in kaart brengen. Zoals bepleit in mijn NJV Preadvies 2016 wordt in een datagestuurde omgeving het belang van de onschuldpresumptie juist in het voorveld van de strafrechtelijke vervolging steeds groter.[6] De introductie van *connected and autonomous driving* (CAD) bevestigt de noodzaak

1 G. Ritzen, 'Politie gaat datarecorder gebruiken bij autocrashes', *NRC Handelsblad* 6 augustus 2016.
2 R. Boere, 'Massale steun voor zwarte doos in auto', *Algemeen Dagblad* 30 december 2014. In feite ging het om een petitie tegen taakstraffen in geval van een ernstig ongeluk. Dat laatste staat echter niet gelijk aan schuld of ernstige schuld, zie M. Remie, 'Petitie tegen taakstraffen voor veroorzakers dodelijke ongevallen', *NRC Handelsblad* 29 december 2014.
3 Zie bijvoorbeeld de website van een van de aanbieders van *post crash*-voertuigdiagnosetechnologie: *www.p-crashvd.nl*, het bedrijf is licentiehouder van een aantal merkspecifieke diagnosesystemen, zoals die van ODIS (Volkswagen, Audi, Skoda en Seat), VCDS (VAG-COM), BMW ISTA (BMW en Mini) en BMW Keyreader, Mercedes Xentry (Mercedes personenauto's en lichte bedrijfswagens) en Volvo VIDA (Volvo personenauto's).

om de reikwijdte van de onschuldpresumptie te herijken en het beginsel van juridische bescherming *by design* handen en voeten te geven in de opsporing in brede zin. Kort gezegd vraagt de *institutionele architectuur* van de rechtsstaat om verankering in de *datagestuurde architectuur* van de informatiesamenleving. Daarmee sluit ik dan ook af in paragraaf 5.

1 De auto als datafabriek in een datagestuurde economie

Niet alleen de *event data recorder*, maar ook de boordcomputer (het besturingssysteem van de auto, waaronder de hierboven al genoemde rem- en stabilisatiesystemen), het navigatiesysteem, eventuele rijstijldetectoren (sensoren) en zelfs de meegebrachte mobiele telefoon vormen een schier onuitputtelijke bron van data. Sommige daarvan betreffen de toestand van de auto (de tank is bijna leeg, oliepeil te laag, banden te glad). Andere data hebben meer direct te maken met het gedrag van de inzittenden en/of de bestuurder: de riemen zijn al dan niet aangegespt, de auto is niet afgesloten, de verlichting is uit. Nog weer andere hebben direct betrekking op het gedrag van personen: de snelheid, het remgedrag, vermoeidheidssymptomen, eten of bellen tijdens het rijden, of zelfs gesprekken met medepassagiers die uit de hand lopen. Locatiegegevens betreffen intussen de mobiliteit van zowel de auto als die van de bestuurder en andere inzittenden.[7]

Het samenstel van gegevens laat toe om zeer specifieke profielen te ontwerpen van individuele personen, van reisgedrag en rijstijl tot en met een inschatting van persoonlijkheidskenmerken

Het samenstel van gegevens waar het hier om gaat, laat toe om zeer specifieke profielen te ontwerpen van individuele personen, van reisgedrag en rijstijl tot en met een inschatting van persoonlijkheidskenmerken. Daarenboven kunnen uit geaggregeerde rijgedraggegevens allerlei predicties worden afgeleid omtrent individueel rijgedrag, over drukte en rijstijl op bepaalde tijden en locaties, en over het rijgedrag van bepaalde type weggebruikers (denk aan oudere vrouwen, rokers, jonge mannen, allochtonen, vegetariërs, werklozen, bildragers, etc.). Het is van belang om beide typen profielen te onderscheiden: (1) een individueel profiel bestaande uit historische persoonsgegevens en (2) een individueel of groepsprofiel dat bestaat uit predicties van toekomstig gedrag, gebaseerd op geaggregeerde datasets van een veelheid van voertuigen, bestuurders, inzittenden en de slimme omgeving van de weggebruikers. Predicties kunnen bijvoorbeeld betrekking hebben op verkeerssituaties, de toestand van het wegdek, weersomstandigheden, en rijgedrag van personen. Juist deze predicties zijn aanleiding tot risicoanalyses en tot al dan niet geautomatiseerde beslissingen. Denk aan verzekeringspremies die fluctueren op basis van al dan niet gevaarlijk rijgedrag, navigatiesystemen of verkeersborden die alternatieve routes aangeven of opleggen naar aanleiding van verwachte stremmingen, intelligente verkeerskaarten die het mogelijk maken om controle op verkeersovertredingen af te stemmen op locaties waar overtredingen worden voorzien, of het remgedrag van een autonoom voertuig dat 'in gesprek is' met andere voertuigen en aldus een botsing voorkomt. Dit is allemaal geen *science fiction*, ook al staan we nog maar aan het begin van deze en soortgelijke ontwikkelingen.[8]

Het geloof dat *big data* innovatieve, efficiënte en effectieve oplossingen mogelijk maakt op schier alle terreinen van het maatschappelijk leven lijkt inmiddels pseudoreligieuze dimensies aan te nemen

2 CAD, *big data* en privacy

Het geloof dat *big data* innovatieve, efficiënte en effectieve oplossingen mogelijk maakt op schier alle terreinen van het maatschappelijk leven lijkt inmiddels pseudoreligieuze dimensies aan te nemen. *Big data* vereist echter lerende zoeksystemen om informatie van ruis te scheiden en/of nieuwe kennis te 'mijnen'. *Data mining* verwijst naar analysetechnieken die geen informatie uit een databestand halen dat er als zodanig in is gezet (dat heet een *query*), maar *nieuwe* informatie afleiden uit de data op basis van statistische verbanden.[9] Intussen gaat het daarbij meestal om 'machinaal leren' (ML), een sub-discipline van de computerwetenschappen en kunstmatige intelligentie.[10] Zonder ML levert *big data* geen nieuwe inzichten. In plaats van er bij voorbaat van uit te gaan dat meer data noodzakelijkerwijs betere oplossingen levert, is het zaak het hoofd koel te houden en tijdens het ontwikkelen van datagestuurde toepassingen steeds ook gedegen onderzoek te doen naar de *trade-offs* die inherent zijn aan ML. Die *trade-offs* bepalen de betrouwbaarheid van de resultaten van ML en dat is bij *predictive policing* om twee redenen cruciaal. Ten eerste is het verleggen van de aandacht van de werkelijkheid *naar de data over die werkelijkheid* alleen zinvol als de investeringen in datagestuurde politie leiden tot betere preventie en opsporing, anders gaan we er *de facto* op achteruit. Ook de politie kan immers een dubbeltje maar één keer uitgeven en datagestuurde systemen vragen grote investeringen in aanschaf en onderhoud, inclusief de herinrichting van gegevensstromen, taakverdeling en controle. Ten tweede kunnen de inbreuken op fundamentele rechten die inherent zijn aan *predictive policing* niet worden gerechtvaardigd als sprake is van allerhande irrelevante bias waardoor, bijvoorbeeld, de rechten van bepaalde groepen disproportioneel worden geschonden.[11] Afhankelijk van de omvang, kwaliteit en relevantie van de data waarmee ML-algoritmes worden getraind en getest, en afhankelijk van het type algoritme, van de gewenste snelheid van resultaten (bijv. *real time*), en van de mogelijkheid om de output te verklaren of begrijpen, zullen die resultaten al dan niet robuust, duurzaam, onzinnig, *self-*

4 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming). De Avg zal de huidige Wet Bescherming Persoonsgegevens vervangen. Zie verder het voorstel Uitvoeringswet Avg, dat tot 20 januari 2017 in internetconsultatie is: *www.internetconsultatie.nl/uitvoeringswetavg*.

5 Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad. De toepasselijkheid van de nieuwe richtlijn zal leiden tot aanpassing van de Wet Politiegegevens en andere relevante wetgeving.

6 M. Hildebrandt, 'Datagestuurde intelligentie in het strafrecht', in: E.M.L. Moerel e.a., *Homo Digitalis* (Handelingen Nederlandse Juristen-Vereniging 2016-I), Den Haag: Wolters Kluwer 2016, p. 137-240, zie ook *http://njv.nl/preadviezen/preadviezen-2016/*.

7 Over de implicaties van het verzamelen van locatiegegevens: M. Herrmann e.a., 'Privacy in Location-Based Services: An Interdisciplinary Approach', *SCRIPTed* (13) 2016, afl. 2, p. 144-170, *https://script-ed.org/wp-content/uploads/2016/08/13-2-Herrmann_et_al.pdf*.

8 Richard Viereckl e.a., 'Connected Car Report 2016: Opportunities, Risk, and Turmoil on the Road to Autonomous Vehicles' (PWC), 28 september 2016, zie *www.strategyand.pwc.com/reports/connected-car-2016-study*.

Foto © Vladimiroquai / 123RF.com | Bewerking: Manon Heinsman

fulfilling of zelfs gevaarlijk (want onbetrouwbaar) zijn. Computerwetenschappers die machinaal-lerende systemen ontwikkelen zijn zich ervan bewust dat het ontwerp van zulke systemen allerlei aannames bevat die mogelijk onjuist of anderszins problematisch zijn; zij zien de methodologische valkuilen onder ogen die nu eenmaal horen bij het doen van wetenschappelijk onderzoek.[12] Dat geldt niet noodzakelijkerwijs voor degenen die afhankelijk zijn van de verkoop van slimme auto's, navigatiesystemen, besturingssystemen en allerhande applicaties. Op de korte termijn hebben deze marktpartijen er nu eenmaal belang bij om hun koopwaar aan te prijzen, risico's voor de klant te bagatelliseren en aansprakelijkheid contractueel uit te sluiten of beheersbaar te houden. Zolang de meeste klanten (waaronder ook overheden) geen zicht hebben op de achterkant van de slimme systemen die CAD op het goede spoor houden is het lastig om bezwaar te maken tegen de utopische verwachtingen waarmee technologieontwikkelaars en beleidmakers de komst van een datagestuurde omgeving aanprijzen. Goed doordachte vormen van onafhankelijk geïmplementeerde softwareverificatie staan nog in de kinderschoenen, maar zouden eigenlijk een standaardvoorwaarde moeten zijn voordat miljoenen worden geïnvesteerd in systemen waarvan onduidelijk is of ze daadwerkelijk voordeel opleveren. Daar komt bij dat die voordelen eigenlijk pas in kaart kunnen worden gebracht als CAD op grote schaal vaart gaat maken. Om die reden is het zaak om te onderzoeken of, en zo ja hoe CAD een aantal fundamentele rechten op het spel zet.

Goed doordachte vormen van onafhankelijk geïmplementeerde softwareverificatie zouden eigenlijk een standaardvoorwaarde moeten zijn voordat miljoenen worden geïnvesteerd in systemen waarvan onduidelijk is of ze daadwerkelijk voordeel opleveren

Het meest voor de hand liggende recht is de privacy van de bestuurder en/of inzittenden. CAD bestaat bij de gratie van een constante stroom van gedragsgegevens, deels van het voertuig en deels van de bestuurder en/of inzittende. Beide typen gegevens kunnen zonder veel moeite gerelateerd worden aan een identificeerbaar persoon (de eigenaar of gebruiker van het voertuig), tenzij daar technisch en/of organisatorisch een stokje voor wordt gestoken (denk aan effectieve pseudonimisering).[13] Daarnaast gaat het om gegevens die door de slimme omgeving worden gegenereerd, die echter – voor zover zij een identificeerbaar voertuig of persoon betreffen – eveneens informatie verschaffen over het gedrag of de toestand van die persoon. De aanhoudende stroom van gegevens maakt het mogelijk een rijkgeschakeerd beeld op te maken van individuele weggebruikers, hetgeen op zichzelf genomen al een inmenging vormt in het

9 Over *data mining* en de implicaties voor het recht, zie bijv. B. Custers, *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Nijmegen: Wolf Legal Publishers 2004.

10 Thomas Mitchell, *Machine Learning*, New York: McGraw-Hill Education 1997. Over machinaal leren en de implicaties voor het recht, zie bijv. M. Hildebrandt, *Smart Technologies and the End(s) of Law. Novel Entanglements of Law and Technology*, Cheltenham: Edward Elgar 2015.

11 Zie bijvoorbeeld J. Angwin e.a., 'Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks', *ProPublica* 23 May 2016, zie *www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing*.

12 T. Mitchell 1997, p. 6.

privéleven.[14] Degenen die deze gegevens verzamelen, degenen die er toegang toe hebben en degenen die ze gebruiken zullen juridisch gezien een rechtvaardiging nodig hebben voor de inmenging in het privéleven (art. 8 lid 1 EVRM, inclusief mogelijke horizontale werking). Voor zover het om overheidsmaatregelen gaat, zal de maatregel bij moeten dragen aan een legitiem doel, zal een wettelijke bevoegdheid nodig zijn en rijst de proportionaliteitsvraag (art. 8 lid 2 EVRM). Zelfs als we aannemen dat het bevorderen van de verkeersveiligheid en/of het economisch welzijn hier het doel is dat de middelen zou kunnen heiligen, is een duidelijke juridische bevoegdheid vereist die toegankelijk en voorzienbaar is en van afdoende waarborgen voorzien, en zal de ernst van de inmenging in redelijke verhouding moeten staan tot de verkeersveiligheid en/of het economisch welzijn. Mij dunkt dat alles hier zal afhangen van de mate waarin de CAD-architectuur mogelijke inmenging in de privacy tot een minimum beperkt en mogelijkheden biedt tot verzet. Daarbij zal van de overheid verwacht worden dat zij daartoe ook de nodige waarborgen inbouwt waaraan private partijen moeten voldoen (indirecte horizontale werking),[15] terwijl privaatrechtelijke aansprakelijkheid in geval van onrechtmatig gebruiken, verkopen of doorspelen van data gebaseerd kan worden op de onrechtmatige daad (directe horizontale werking).[16]

De aanhoudende stroom van gegevens maakt het mogelijk een rijkgeschakeerd beeld op te maken van individuele weggebruikers, hetgeen op zichzelf genomen al een inmenging vormt in het privéleven

3 Gegevensbescherming

De vloed aan gegevensstromen biedt echter nog heel andere mogelijkheden om fundamentele rechten aan te tasten. Zoals hierboven aangegeven, kan ML worden toegepast op geaggregeerde rijgedragsgegevens, waardoor allerhande statistische correlaties worden ontgonnen die een stroom van voorspellingen op gang brengen waarmee individuele personen kunnen worden getarget. Het gaat daarbij in juridische zin om profilering.[17] Hoewel deze voorspellingen of afgeleide profielen zelf *niet* gerelateerd zijn aan een bepaalde persoon en dus zelf *geen* persoonsgegeven zijn, vormt de toepassing op een persoon die binnen de 'gelding' van het profiel past wel degelijk de verwerking van een persoonsgegeven. Daarmee is het fundamentele recht op gegevensbescherming aan de orde, zoals neergelegd in artikel 8 Handvest van de grondrechten van de EU en uitgewerkt in de Avg en de Richtlijn gegevensbescherming opsporing en vervolging (en de huidige Wbp, Wpg). Het recht op gegevensbescherming valt niet samen met het recht op privacy.[18] Het bevat een bundel rechten en plichten die beogen de privacy te beschermen – voor zover de verwerking van persoonsgegevens een inmenging vormt in de privacy – maar ook andere fundamentele rechten zoals non-discriminatie en juridische beginselen zoals verzetsrechten, transparantie en proportionaliteit. In beginsel ziet het fundamentele recht op gegevensverwerking op de voorwaarden waaronder het verwerken van persoonsgegevens rechtmatig is. De bepalingen inzake profilering hebben echter een groter bereik omdat zij eisen stellen aan geautomatiseerde beslissingen die worden genomen op basis van profilering.

De vloed aan gegevensstromen biedt echter nog heel andere mogelijkheden om fundamentele rechten aan te tasten

Bij CAD gaat het om voorspellende profielen, die op basis van voortdurende datastromen steeds worden aangepast en aldus een nieuw type doorzichtigheid scheppen. Personen worden doorzichtig in de zin dat het profiel toestaat om dwars door de persoon heen te kijken naar – statistisch – vergelijkbare personen en op basis daarvan een aantal geautomatiseerde beslissingen te nemen.[19] Denk aan het verhogen of verlagen van de verzekeringspremie, het ontzeggen of opschorten van de rijbevoegdheid, interventies in snelheid of remgedrag, maar denk ook aan het monitoren van individuele personen op grond van voorspelde gevaarzetting. Het feit dat dit wellicht (nog) niet allemaal aan de orde is mag de aandacht niet afleiden; de ervaring leert dat 'functiekruip' voor de hand ligt als het om de inzet gaat van *big data*. Het monitoren van individuele personen op grond van voorspelde gevaarzetting tast intussen niet alleen de rechtens veronderstelde autonomie van individuele personen aan, maar creëert een heel nieuwe 'keuze-architectuur', waardoor het gedrag van burgers en consumenten in toenemende mate bewust wordt aangestuurd, ingeperkt en bijgestuurd. Burgers en consumenten zijn zich daar intussen juist niet van bewust, zij hebben weinig zicht op deze sturing.

Anders dan bij het uitvaardigen en toepassen van geschreven rechtsnormen gaat het hier om *nudge*-technieken, bedoeld om de burger onmerkbaar te verleiden tot het 'optimaliseren' van haar gedrag

Anders dan bij het uitvaardigen en toepassen van geschreven rechtsnormen gaat het hier om *nudge*-technieken,[20] bedoeld om de burger onmerkbaar te verleiden tot het 'optimaliseren' van haar gedrag (waarbij het dan weer niet de burger is die bepaalt wat optimaal is, maar de door beleidmakers en computerwetenschappers ontworpen keuze-architectuur). Hier komen andere fundamentele rechten in zicht, in het bijzonder directe of indirecte discriminatie en de onschuldpresumptie in brede zin. Het gaat bij dat laatste eerder om een recht om *niet zonder reden* stelselmatig te worden gevolgd met het oog op mogelijk strafbaar gedrag, dan om het klassieke recht om gevrijwaard te blijven van punitief ingrijpen totdat de schuld in rechte vaststaat. Daarbij is dan weer van belang dat risicoscores geen 'reden' zijn in juridische zin, ook al kunnen ze

13 Art. 4(5) Avg definieert pseudonimisering als: 'het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld'. Zogenaamde anonimisering is in juridische zin dan ook meestal pseudonimisering, zie ook art. 29 Werkgroep, Advies 5/2014 over anonimiseringstechnieken, WP 216 en HvJ EU 19 oktober 2016, C-582/14, ECLI:EU:C:2016:779 (*Breyer tegen Duitsland*).

14 Vgl. bijvoorbeeld r.o. 27-30 inzake de schending van art. 7 Handvest EU in HvJ EU 8 april 2014, ECLI:EU:C:2014:238, *NJ* 2016/446, m.nt. E.J. Dommering (*Digital Rights Ireland tegen Ierland*) en r.o. 68 inzake de schending art. 8 EVRM in EHRM 4 december 2008, ECLI:NL:XX:2008:BH1813, *NJ* 2009/410, m.nt. E.A. Alkema (*S. en Marper tegen het Verenigd Koninkrijk*).

15 EHRM 12 januari 2016, ECLI:CE:ECHR:2016:0112JUD006149608, *EHRC* 2016/91, m.nt. B.P. ter Haar (*Barbulescu tegen Romania*), r.o. 23.

16 Zie bijv. Rechtbank Groningen 31 mei 2012, ECLI:NL:RBGRO:2012:BW7184, r.o. 4.6: 'De voorzieningenrechter volgt [eisers] in de stelling dat aan het grondrecht tot manifestatie een zekere horizontale werking toekomt, maar niet dat een eigenaar of rechthebbende daarmee ook onverkort gebonden is aan de beperkingen die de Grondwet stelt aan het ingrijpen in de manifestatievrijheid.'

wellicht een rol spelen bij beslissingen om burgers stelselmatig te volgen in een slimme omgeving (interceptie, hacken, opvragen van gedragsdata of metadata). Zo'n beslissing moet echter altijd zijn uit te leggen, hoe complex het algoritme ook zou zijn.[21] Het is juist op dat punt dat het fundamentele recht op gegevensbescherming (art. 8 Handvest EU) kansen biedt om de achterkant van CAD-infrastructuur doorzichtig te maken, en dat is zonder meer de mogelijkheidsvoorwaarde voor een effectief recht om zich te verzetten tegen onrechtmatige discriminatie of *redenloos* 'stelselmatig volgen'.

Het meest centrale beginsel van het gegevensbeschermingsrecht in de EU is de eis dat elke verwerking noodzakelijk is voor het legitieme, specifieke doel dat door de verantwoordelijke is bepaald en aan betrokkenen moet worden gecommuniceerd

4 Doelbinding, onschuldpresumptie en profieltransparantie

Kern van het gegevensbeschermingsrecht in de EU is niet dat gegevens alleen met toestemming van de betrokkene verwerkt mogen worden (er zijn vijf andere rechtsgronden voor legitieme verwerking, waaronder contract en een wettelijke plicht). Kern is ook niet het gerechtvaardigde belang van de verantwoordelijke (dat sowieso een lastige afweging vraagt tegen de belangen, rechten en vrijheden van de betrokkene). Het meest centrale beginsel is de eis dat elke verwerking noodzakelijk is voor het legitieme, specifieke doel dat door de verantwoordelijke is bepaald en aan betrokkenen moet worden gecommuniceerd. Bij hergebruik moet het dan in ieder geval gaan om een doel dat verenigbaar is met het oorspronkelijke doel, zodat de burger in kan schatten waarvoor haar gegevens worden ingezet. De voorzienbaarheidseis is cruciaal als het gaat om het vertrouwen van betrokkenen, en hangt direct samen met de redelijke of legitieme verwachting die bepalend is voor de omvang van het fundamentele recht op privacy. De eis van doelbinding geldt zowel voor private partijen (de autofabrikant, de software-leverancier, de app-aanbieder) als voor politie en justitie (die in beginsel altijd handelen op basis van wettelijk omschreven bevoegdheden).

Door sommigen wordt gesuggereerd dat doelbinding in geval van *big data* een onzinnige of achterhaalde eis zou zijn. De gedachte is dat juist ongericht zoeken in *big data* toegevoegde waarde zou opleveren. Dit is zeker niet het geval

Door sommigen wordt gesuggereerd dat doelbinding in geval van *big data* een onzinnige of achterhaalde eis zou zijn.[22] De gedachte is dat juist ongericht zoeken in *big data* toegevoegde waarde zou opleveren. Dit is zeker niet het geval. Machinaal leren vraagt om hechte samenwerking tussen domeinexpert, verantwoordelijke en datawetenschapper om te bezien wat er mogelijk is, welke data beschikbaar zijn, hoe groot de risico's zijn voor betrokkenen, welk type algoritmes betrouwbare nieuwe inzichten op kunnen leveren, in hoeverre beschikbare data relevant, voldoende compleet en accuraat is en hoe dit zich verhoudt tot de taken, bevoegdheden en/of verdienmodellen van de opdrachtgever (de verantwoordelijke). In het iteratieve proces van ontwerp, testen, inrichten en instellen van te ontwerpen systemen zal die samenwerking leiden tot een steeds verfijnder afstemming tussen mogelijke doelen en betrouwbare software, totdat helder kan worden vastgesteld waar de meerwaarde gesitueerd kan worden. Dit hele proces past in de juridisch verplichte *data protection impact assessment* (art. 35 Avg), dat dan ook goed aansluit bij wat intussen *agile computing* wordt genoemd.[23] *Agile computing* betekent dat het ontwerp en de inrichting van software en/of cyberfysieke infrastructuur in een iteratief proces tussen klant en ontwikkelaar wordt afgestemd, getest en bijgesteld. Dit in plaats van de tot mislukking gedoemde *waterfall*-aanpak, waarbij het hele systeem in een keer wordt afgeleverd. *Agile computing* gaat prima samen met de zorgvuldigheidseisen die inherent zijn aan de verplichte *data protection impact assessment* en past ook goed bij de juridische eis dat applicaties voldoen aan *data protection by default and design* (art. 25 Avg). Dit betekent bijvoorbeeld dat het doel van de testfase ook als zodanig benoemd en gecommuniceerd moet worden.

Met name wanneer data wordt hergebruikt is het zaak om goed na te denken over de juridische grond

Met name wanneer data wordt hergebruikt is het zaak om goed na te denken over de juridische grond (die vaak af zal wijken van de oorspronkelijke grond) en indien nodig duidelijk te maken dat gegevens worden verwerkt met het oog op nieuw te ontdekken inzichten in het kader van de bedrijfsvoering (legitiem belang van de verantwoordelijke) of in het kader van een publieke taak (een van de andere zes rechtsgronden voor verwerking). Door helder te communiceren worden betrokkenen in staat gesteld zich eventueel te verzetten tegen de verwerking, hetzij op basis van hun persoonlijke omstandigheden, hetzij omdat zij menen dat de verwerking niet noodzakelijk is voor de gestelde grond. Dat brengt het hele proces terug onder rechtsstatelijke toetsing en zal bovendien tot een veel efficiënter, effectiever en robuuster toepassing van ML leiden. Betrokkenen worden daadwerkelijk 'betrokkenen', wier waardigheid en autonomie wordt gerespecteerd. Kants oproep om een mens nooit uitsluitend te gebruiken als een instrument voor het bereiken van eigen doelen kan dan weer handen en voeten krijgen. De automobilist of inzittende is niet meer alleen een generator van rijgedragsdata maar de persoon waar het om gaat. De auto mag weer een vervoermiddel

17 De Avg, art. 4(4) en Richtlijn (EU) 2016/680, art. 3(4) definiëren profilering als: 'elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling aspecten betreffende zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen'.

18 P. De Hert & S. Gutwirth, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power', in E. Claes, A. Duff & S. Gutwirth (red.), *Privacy and the Criminal Law*, Antwerpen/Oxford: Intersentia 2006.

19 M. Hildebrandt, 'Profile Transparency by Design: Re-Enabling Double Contingency', in: M. Hildebrandt & K. de Vries (red.), *Privacy, Due Process and the Computational Turn*, Abingdon: Routledge 2013.

20 R.H. Thaler & C.R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness*, New Haven: Yale University Press 2008. Zie ook K. Yeung, '"Hypernudge": Big Data as a Mode of Regulation by Design', *Information, Communication & Society* (20) 2017, afl. 1, p. 118-136.

21 Over diverse vormen van 'opaciteit' in geval van machinaal leren J. Burrell, 'How the Machine "thinks": Understanding Opacity in Machine Learning Algorithms', *Big Data & Society* (3) 2016, afl. 1.

22 E.M.L. Moerel & J.E.J. Prins, 'Privacy voor de Homo Digitalis', in: E.M.L. Moerel e.a., *Homo Digitalis* (Handelingen Nederlandse Juristen-Vereniging 2016-I), Den Haag: Wolters Kluwer 2016, p. 1-136, zie ook *http://njv.nl/preadviezen/preadviezen-2016/*.

23 S. Gurses & J. van Hoboken, 'Privacy after the Agile Turn', *Open Science Framework* 2016, zie *https://osf.io/27x3q/*.

zijn; de auto als datafabriek blijft ondergeschikt aan het specifieke doel van 'het vervoeren van personen of zaken'.

We kunnen er niet van uitgaan dat deze voorspellingen kloppen en zullen waarborgen moeten inbouwen om te zorgen dat deze systemen *getest* en *weersproken* kunnen worden zodat de geautomatiseerde beslissingen die ze oproepen betrouwbaar en in rechte aanvechtbaar zijn

5 Conclusies: effectief toezicht op dwingende algoritmes

CAD is een testcase voor de juridische implicaties van de concrete inzet van kunstmatige intelligentie. Met name wanneer de fysieke omgeving online wordt verbonden via het zogenaamde Internet of Things (IoT), ofwel cyberfysieke infrastructuren.[24] Het uitlezen van de zwarte doos lijkt op zichzelf genomen geen schending van het recht op privacy of gegevensbescherming, wanneer het gaat om een rechtens toegekende bevoegdheid die zich beperkt tot de laatste 5 seconden voorafgaand aan een ernstig ongeval. Het zou echter naïef zijn de analyse te beperken tot dit soort geïsoleerde toegang tot persoonsgegevens. CAD leidt tot voortdurende uitwisseling van grote hoeveelheden persoonsgegevens die samen met andere gegevens een verrijkt profiel van individueel gedrag kunnen bieden. Daarnaast roept die gegevensstroom de inzet op van machinaal lerende systemen, die voertuigen, verzekeraars en politie in staat zouden stellen toekomstig rijgedrag te voorspellen en – wederom in samenhang met andere datasets – ook ander gedrag, waaronder strafrechtelijk relevant gedrag. Mijn punt is dat we er niet van uit kunnen gaan dat deze voorspellingen kloppen en waarborgen in moeten bouwen om te zorgen dat deze systemen *getest* en *weersproken* kunnen worden zodat de geautomatiseerde beslissingen die ze oproepen betrouwbaar en in rechte aanvechtbaar zijn. Het gaat dan met name om voorspellingen die tot 'stelselmatig volgen' leiden of tot andere gevolgen die een aanzienlijke invloed hebben op de betrokkene (weigeren verzekering, verhoging premie, of – wanneer de rijgedragsgegevens worden samengevoegd met data uit andere contexten – afwijzing bij een sollicitatie, weigeren krediet). De Avg eist dat volledig geautomatiseerde beslissingen, bijvoorbeeld gebaseerd op *profiling*, bekend worden gemaakt aan de persoon die het betreft en dat zowel de onderliggende logica als de voorziene gevolgen op een begrijpelijke manier worden uitgelegd (art. 13 lid 2 sub f en 14 lid 2 sub g). De Richtlijn gegevensbescherming opsporing en vervolging stelt naast de eisen van een *wettelijke* grondslag en doelbinding (die beide voortvloeien uit het constitutionele en strafvorderlijke legaliteitsbeginsel) ook de eis van een recht op menselijke interventie wanneer volledig geautomatiseerde beslissingen worden gebaseerd op *profiling* (art. 11). Hoe betrokkenen erachter zouden moeten komen dat zij op basis van geautomatiseerde beslissingen bijvoorbeeld stelselmatig worden gevolgd wordt echter niet duidelijk in de richtlijn, nu er geen verplichting is opgenomen om daarover te communiceren. Dat is begrijpelijk voor zover het gaat om heimelijke bevoegdheden die hun effectiviteit verliezen bij bekendmaking. Dan is het echter van groot belang dat op een meer abstract niveau voorzienbaar is wanneer en hoe burgers worden geprofileerd. Daarover zwijgt de richtlijn. Naast de voorzienbaarheid van *predictive policing* voor burgers, gaat het ook om adequaat onafhankelijk toezicht ten aanzien van zowel de effectiviteit en betrouwbaarheid van de gebruikte systemen (in het kader van de proportionaliteitstoets) als het voorkomen van niet gerechtvaardigde discriminatie op het niveau van de algoritmes of de uitkomsten daarvan (waarbij met name indirecte discriminatie lastig te achterhalen is).[25] In de richtlijn wordt gestipuleerd dat de inzet van *profiling* gedocumenteerd wordt (art. 24 lid 1 sub c) en wordt vereist dat de toezichthoudende instantie 'effectieve onderzoeksbevoegdheden' heeft en 'toegang tot alle persoonsgegevens die worden verwerkt en tot alle informatie die noodzakelijk is voor de uitvoering van haar taken' (art. 47). Dit gaat echter minder ver dan de Avg, die daarenboven eist dat de toezichthouders 'toegang […] verkrijgen tot alle bedrijfsruimten van de verwerkingsverantwoordelijke en de verwerker, daaronder begrepen tot alle uitrustingen en middelen voor gegevensverwerking' (art. 57 lid 2 sub f).

De inzet van CAD en andere vormen van datagestuurde infrastructuur vraagt om herankering van effectieve *checks and balances* in de cyber-fysieke architectuur van de datagestuurde samenleving

De *checks and balances* van de rechtsstaat zijn na eeuwen van strijd redelijkerwijs verankerd in de institutionele grondstructuur van onze samenleving. Die verankering vraagt permanent onderhoud en is geenszins vanzelfsprekend. De inzet van CAD en andere vormen van datagestuurde infrastructuur (denk aan *smart energy grids*),[26] vraagt om herankering van effectieve checks and balances in de cyber-fysieke architectuur van de datagestuurde samenleving. De systemen waarop wij ons in toenemende mate verlaten en waarvan wij in toenemende mate afhankelijk zijn moeten testbaar en weerspreekbaar worden *gemaakt*. Zowel *voor* de burger en de consument als *door* toezichthouders met adequate expertise en bevoegdheden. Ik verwijs graag naar de vraagpunten bij mijn Preadvies NJV 2016 die ook hier relevant en pertinent zijn. Ten eerste: in het nieuwe Wetboek van Strafvordering moet een bepaling worden opgenomen die het ontwerp en de inrichting van datagestuurde systemen normeert. Ten tweede: het is noodzakelijk een toezichthouder in te stellen die de werking controleert van datagestuurde systemen die bij heimelijk onderzoek worden ingezet.

24 Zie het uitgelekte concept van de Europese Commissie: *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, waarin CAD als testcase wordt opgevoerd: 'Building a European Data Economy', zie *www.euractiv.com/wp-content/uploads/sites/2/2016/12/data-communication.pdf*.

25 Een interne kritiek op de inzet van *predictive policing*: B.E. Harcourt, *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*, Chicago: University of Chicago Press 2007; toegespitst op het strafrecht M. Hildebrandt, 'Criminal Law and Technology in a Data-Driven Society', in *The Oxford Handbook of Criminal Law* (Oxford Handbooks in Law), Oxford: OUP 2014.

26 *Smart energy grids* verwijst naar slimme energiesystemen (waarvan de slimme meter een onderdeel vormt), zie bijv. M. Hildebrandt, *Legal Protection by Design in the Smart Grid*, Nijmegen: Radboud University Nijmegen, Smart Energy Collective, Privacy & Identity Lab 2013, *http://repository.ubn.ru.nl/bitstream/handle/2066/111368/111368.pdf?sequence=1*.