HET GEGEVENSBESCHERMINGSRECHT OP DE SCHOP: NOODZAAK OF AFBRAAK?
Enkele kanttekeningen bij het pre-advies 'Homo Digitalis' van Lokke Moerel en Corien Prins

Bart van der Sloot ▪

Samenvatting | In hun pre-advies voor de Nederlandse Juristen Vereniging stellen Lokke Moerel en Corien Prins hetgeen al langer door met name marktpartijen te berde wordt gebracht: het huidige juridische systeem aangaande gegevensbescherming werkt niet meer en moet radicaal op de schop. De kern van hun voorstel is het loslaten van de diverse principes die in het huidige gegevensbeschermingsrecht zijn vervat en deze te vervangen door een uitgebreide belangenafwegingstoets. Alhoewel internetbedrijven en andere grote dataverwerkers dit voorstel ongetwijfeld zullen toejuichen is de vraag of de burger nog afdoende bescherming geniet onder een dergelijke benadering.

Trefwoorden | gegevensbescherming; big data; open normen; belangenafweging; utilisme.

Wolters Kluwer Navigator | NTM-NJCMBull. 2016/01

1 Inleiding

Er is het nodige te doen om het gegevensbeschermingsrecht, zoals dat thans in Nederland is geregeld in de Wet bescherming persoonsgegevens,[1] die een implementatie vormt van de in 1995 van kracht geworden Richtlijn bescherming persoonsgegevens[2] van de Europese Unie. Deze richtlijn zal in 2018 worden vervangen door de onlangs aangenomen Algemene Verordening Gegevensbescherming.[3] In deze verordening, die directe werking heeft in de gehele Europese Unie, zijn de meeste principes uit de richtlijn overeind gebleven. De verordening tracht met name het handhavingsprobleem aan te pakken, nu gebleken is dat de praktijk zich substantieel anders gedraagt dan de wet voorschrijft. Het feit dat de algemene principes dezelfde zijn gebleven is een doorn in het oog van veel internetbedrijven en andere grote gegevensverwerkers, die hun businessmodellen baseren op het verzamelen, analyseren en gebruiken van grote hoeveelheden data. Zij menen dat de regels die grenzen stellen aan deze verwerking de innovatie

▪ Mr. drs. B. van der Sloot is senior researcher aan het Tilburg Institute for Law, Technology, and Society, Universiteit van Tilburg.

1 Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens).

2 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

3 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 (hierna: Verordening (EU) 2016/679).

tegenhouden en winstmarges laten krimpen die anders met Big Data toepassingen zouden kunnen worden bereikt. De meest gangbare definitie van Big Data is die uit het Gartner rapport en stoelt op drie aspecten: het toenemende volume (hoeveelheid data), de toenemende snelheid (snelheid van de gegevensverwerking) en de toenemende variëteit (scala aan datatypes en -bronnen).[4] Er zijn globaal drie fases in ideaaltype Big Data processen te onderscheiden:[5]

Ten eerste het verzamelen van gegevens. Grote hoeveelheden gegevens kunnen worden verzameld en opgeslagen, bijvoorbeeld met behulp van *cloud computing*. Deze data kunnen afkomstig zijn uit verschillende bronnen, zoals interne bestanden, databases gekocht via derden en publieke gegevens die van het internet worden geschraapt. Daar de data-opslag zo goedkoop is en de technische middelen zo geavanceerd zijn, bestaat er vrijwel geen praktische drempel voor organisaties om op grote schaal gegevens te verzamelen. Daarom is de staande praktijk steeds meer om gegevens eerst te verzamelen, zonder een afgebakend doel, en pas naderhand te bekijken van welke waarde deze gegevens eventueel zouden kunnen zijn. Steeds meer is de standaard om de verzamelde gegevens te bewaren, omdat ze altijd op een later moment nog van pas zouden kunnen komen voor andere, nog onbekende doeleinden. Omdat Big Data technieken vooral goed draaien op grote datasets, is het doel doorgaans om zoveel mogelijk gegevens te verzamelen. De kwaliteit van de gegevens is steeds minder relevant; er kan worden gewerkt met zogenoemde 'dirty' of 'messy' data. 'Kwantiteit boven kwaliteit' is dan ook een vaak gehoorde slogan. Algoritmes kunnen relevante patronen en verbanden in grote datasets identificeren, zelfs als niet alle gegevens correct zijn.

De tweede fase betreft de analyse van gegevens, die bijvoorbeeld wordt uitgevoerd door algoritmen en zelflerende computerprogramma's. Deze middelen worden ingezet voor het modelleren van data en het blootleggen van patronen in deze data. De patronen worden gebruikt om profielen te maken. Profielen zijn gebaseerd op statistische correlaties, in plaats van causaliteit, en zijn geformuleerd op een algemeen of groepsniveau. Dergelijke profielen werken gewoonlijk met waarschijnlijkheidsberekeningen en worden met name toegepast voor predictive-analyses en toekomstvoorspellingen. Een typisch profiel is: '70% van de mensen die wonen in buurt Y kunnen worden verleid om product Z te kopen', 'van de groep met etnische achtergrond X en een inkomen lager dan W, is het waarschijnlijk dat 60% voor partij V stemt' of '0,1% van de mensen met een religieuze achtergrond U en familieleden in land T of S, maar niet land R, kan worden verleid een terroristische aanslag te plegen.'

Ten derde en tot slot is er het gebruik van de uit de gegevensanalyse verkregen patronen en profielen. Het toepassen van een profiel in de praktijk kan op een algemeen niveau blijven, bijvoorbeeld als de overheid besluit beweging onder de bevolking te promoten, omdat uit gegevensanalyse blijkt dat er een grote kans bestaat dat een fors deel van de populatie over 20 jaar aan overgewicht lijdt. Daarnaast kan het profiel worden toegepast op groepsniveau, bijvoorbeeld in het geval waarin de inwoners van een bepaalde wijk een ziektekostenverzekering wordt geweigerd of onder striktere voorwaarden wordt aangeboden, omdat de inwoners in een risicocategorie vallen. Ook kan het profiel worden toegepast op individueel niveau, zoals wanneer mensen niet wordt toegestaan ??om een ??land in te reizen of worden gearresteerd

4 https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

5 WRR, 'Big Data in een vrije en veilige samenleving', online te raadplegen via: www.wrr.nl/fileadmin/nl/publicaties/PDF-Rapporten/rapport_95_Big_Data_in_een_vrije_en_veilige_samenleving.pdf.

omdat ze aan het profiel van een potentiële terrorist voldoen. Hier geldt het tweeledig gevaar van valse negatieve en valse positieven.

Big Data, in zijn hier beschreven ideaalvorm, contrasteert met vrijwel ieder principe uit het gegevensbeschermingsrecht.[6]

- Ten eerste is het gegevensbeschermingskader gebaseerd op het concept van 'persoonsgegeven'.[7] Ook alle gegevens die binnen afzienbare tijd mogelijk kunnen worden gebruikt om een persoon (het datasubject) te identificeren of te personaliseren worden geacht een persoonsgegeven te zijn.[8] Omdat in Big Data-initiatieven, waarin databases eenvoudig kunnen worden samengevoegd en geïntegreerd, zelfs twee onbeduidende informatiepunten tot een gevoelig profiel kunnen worden samengevoegd, kunnen vrijwel alle gegevens worden beschouwd als persoonsgegeven, waardoor de wettelijke regels van toepassing zijn.
- Ten tweede geldt onder het gegevensbeschermingsrecht het dataminimalisatieprincipe dat kortgezegd inhoudt dat de gegevensverzameling moet worden beperkt tot het minimum en dat de gegevens moeten worden verwijderd zodra ze niet meer nodig zijn.[9] Dit principe contrasteert met de trend om juist zoveel mogelijk gegevens te verzamelen en voor langere tijd te bewaren.
- Ten derde mogen persoonsgegevens alleen worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De gerechtvaardigde doeleinden zijn limitatief opgesomd in het gegevensbeschermingsrecht, zoals de toestemming van het datasubject of een wettelijke plicht om gegevens te verwerken. Voor gevoelige persoonsgegevens, zoals aangaande ras, geloof of geaardheid, gelden striktere voorwaarden.[10] In Big Data processen is het mogelijk om gegevens juist te verzamelen zonder helder en vooraf bepaald doel; veeleer wordt naderhand gekeken welk doel deze gegevens kunnen dienen.
- Ten vierde volgt uit het doelbindingsprincipe dat persoonsgegevens niet verder mogen worden verwerkt op een met het oorspronkelijke doel onverenigbare wijze.[11] Dit principe wordt in de praktijk ondermijnd aangezien hergebruik van gegevens voor andere, nieuwe doeleinden nu juist het adagium is.
- Ten vijfde heeft de verantwoordelijke voor de gegevensverwerking de plicht om er voor zorg te dragen dat de persoonsgegevens die hij verwerkt juist zijn en up to date worden gehouden.[12] Dit principe staat steeds meer onder druk doordat wordt gewerkt met vervuilde data, vanuit het geloof dat kwantiteit boven kwaliteit gaat.
- Ten zesde is er de plicht tot het nemen van passende technische en organisatorische maatregelen om te voorkomen dat er datalekken ontstaan of dat onbevoegde personen binnen een organisatie bij de data kunnen.[13] Als databases openbaar worden gemaakt, aan elkaar

6 B. van der Sloot & S. van Schendel, 'International and comparative legal study on Big Data', online te raadplegen via:www.wrr.nl/fileadmin/en/publicaties/PDF-Working_Papers/WP_20_International_and_Comparative_Legal_Study_on_Big_Data.pdf.
7 Artikel 4(1) Verordening (EU) 2016/679.
8 Werkgroep 29, 'Advies 4/2007 over het begrip persoonsgegeven', 01248/07/NL, WP 136, 20 juni 2007.
9 Artikel 5.1(c) en 5.1(e) Verordening (EU) 2016/679.
10 Artikel 5.1(b), 6 en 9 Verordening (EU) 2016/679.
11 Werkgroep 29, 'Opinion 03/2013 on purpose limitation', 00569/13/EN, WP 203, 2 April 2013.
12 Artikel 5.1(d) Verordening (EU) 2016/679.
13 Artikel 5.1(f) en artikel 32-36 Verordening (EU) 2016/679.

worden gekoppeld en worden gedeeld tussen partijen komt dit principe onder druk te staan, nu steeds meer mensen toegang hebben tot de gegevens en het steeds moeilijker wordt datalekken te voorkomen.
- Ten zevende hebben verantwoordelijken voor de gegevensverwerking de plicht om voor zo ver mogelijk de datasubjecten ervan op de hoogte te stellen dat er gegevens over hen worden verwerkt, hoe dit geschiedt en voor welke doeleinden. Gespiegeld aan deze plicht geldt het recht van het datasubject om dergelijke informatie te vragen.[14] Het probleem is dat in de praktijk dataverwerkers vaak niet weten van wie zij gegevens verwerken noch hoe de personen in kwestie te bereiken; ook het datasubject tast vaak in het duister over welke partijen er data over hem hebben.
- Tot slot kent het gegevensbeschermingsrecht een aantal rechten toe aan het individu.[15] Er zijn echter simpelweg zoveel partijen die gegevens verwerken dat het praktisch bijna ondoenlijk is voor het datasubject om ieder individu, bedrijf en overheidsorganisatie te vragen welke gegevens er worden verwerkt, te evalueren of dit rechtmatig geschiedt en zo niet, een rechtszaak te starten.

Kortom, er is een behoorlijk spanningsveld tussen de wet en deze big data toepassingen. Al langer wordt door bedrijven gelobbyd om de gegevensverwerkingsregels te versoepelen of overboord te zetten, omdat de regels ouderwets zouden zijn en zij de bedrijfsmodellen en winstmarges onder druk zouden zetten. Het juridische regime kost banen en ontmoedigt datagedreven innovatie.[16] Lokke Moerel en Corien Prins, beide professor aan de Universiteit van Tilburg, gooien met hun pre-advies een steen in de vijver door deze opvatting naar een academisch niveau te tillen, nadat de eerste auteur iets dergelijks al had gedaan in haar oratie.[17] Daarbij pleiten zij voor een systeem dat niet is gebaseerd op rechten, plichten en principes, maar op een afweging van belangen. Een dergelijke belangenafweging kan van geval tot geval worden toegepast en geïnterpreteerd en is dus flexibeler en granulairder. Een dergelijke steen verdient aandacht en een kritische beschouwing, die dit artikel hoopt te bieden.[18] In paragraaf 2 wordt het voorstel van Moerel en Prins samengevat en in paragraaf 3 kritisch beschouwd. Dat gebeurt met name op het punt van methodologie en argumentatie, omdat deze op verscheidene punten vragen oproepen. In paragraaf 4 wordt het voorstel geduid en wordt in het bijzonder ingegaan op de focus die de auteurs willen verleggen van rechten en plichten, naar belangen en schade.

14 Artikel 12-15 Verordening (EU) 2016/679.
15 Artikel 16-22 Verordening (EU) 2016/679.
16 Dit wordt ook onderschreven door Moerel en Prins. Zie bijvoorbeeld: E.M.L. Moerel & J.E.J. Prins, 'Privacy voor de homo digitalis', http://njv.nl/wp-content/uploads/2011/04/Preadviezen-NJV-2016.pdf, p. 77-78.
17 L. Moerel, 'Big Data Protection How to Make the Draft EU Regulation on Data Protection Future Proof', www.debrauw.com/wp-content/uploads/NEWS%20-%20PUBLICATIONS/Moerel_oratie.pdf.
18 Dit artikel is mede geschreven vanuit het geloof dat er überhaupt, maar zeker in de privacywetenschap, te veel wordt gepubliceerd en te weinig kritisch op elkaar wordt gereageerd. Daarbij komt dat waar voorheen uitgebreide boekrecensies werden geschreven door professoren, deze nu doorgaans verworden zijn tot een korte samenvatting door Phd-studenten. Op conferenties worden te vaak powerpoint presentaties afgedraaid en vervolgens langs elkaar heen gesproken, ieder met zijn eigen theorie. Etc. Het pre-advies is duidelijk geschreven om debat op te roepen; dit artikel hoopt daaraan bij te dragen.

2 Het voorstel van Moerel en Prins

Het is lastig om een eloquent voorstel als dat van Lokke Moerel en Corien Prins, dat meer dan 100 pagina's beslaat, samen te vatten in enkele woorden. Toch lijkt de kern van het voorstel uit drie concrete stappen te bestaan. Ten eerste stellen Moerel en Prins voor om niet langer te kijken naar het doel van de gegevensverwerking en de daaraan gekoppelde doelbinding, maar enkel naar het belang van de dataverwerker aan de ene kant en het belang van het datasubject aan de andere kant. Ten tweede worden de legitieme verwerkingsgronden, zoals die vervat zijn in het gegevensbeschermingsrecht, teruggebracht tot één test, waarin het doel van de verwerking wordt afgewogen tegen de rechten van het datasubject. Ten derde en tot slot worden de andere principes uit het gegevensbeschermingsrecht niet langer gezien als zelfstandige criteria, maar vormen zij onderdeel van deze balanceerexercitie.

De eerste stap in het voorstel is dat de nadruk op het doel van de verwerking wordt verlaten en vervangen door een focus op de belangen van de diverse partijen. Het huidige wettelijke kader vereist dat wanneer de gegevens worden verzameld, de verantwoordelijke hiervoor een duidelijk omschreven en gerechtvaardigde doel moet hebben en dat deze gegevens niet verder mogen worden verwerkt voor een ander, onverenigbaar doel. Naast het doel en het doelbindingsprincipe, wordt ook in de balanceergrond, die door Moerel en Prins als enige verwerkingsgrond wordt gezien, gerept van het gerechtvaardigde doel, althans in de authoratieve Engelse tekst. Er wordt verwezen naar de situatie waarin de verwerking van persoonsgegevens noodzakelijk is 'for the purposes of the legitimate interests pursued by the controller or by a third party'.[19]

Moerel en Prins stellen voor om de balanceer-bepaling te herformuleren, zodat die zich uitsluitend richt op de belangen van de diverse partijen. Zij geloven dat het doel als zodanig niet ter zake doet.[20] Een gewichtig doel dat wordt nagestreefd, kan in de praktijk slechts minieme belangen dienen, en vice versa.[21] Zij verwijzen naar een commerciële dienst die onopgemerkt onze gezondheidstoestand vrijwel real-time in kaart brengt en zelfs kan voorspellen hoe wij ons de volgende dag zullen voelen en een soortgelijke toepassing die door de Wereld Gezondheid Organisatie (WHO) wordt voorgestaan om in specifieke gevallen burgers te behoeden voor gevaarlijke infectieziekten en pandemieën. Zij suggereren dat de eerste toepassing door velen met scepsis zal worden ontvangen, terwijl de tweede enthousiast zou worden onthaald, zelf als de WHO daarvoor een commerciële partij zou inschakelen.

> 'Wie nader bij het voorgaande stilstaat, stelt vast dat het voor velen onder ons bij de afweging of onze persoonsgegevens wel of niet voor een dergelijke toepassing mogen worden gebruikt, waarschijnlijk niet zozeer gaat om sec het doel waarvoor de gegevens worden gebruikt. Veeleer gaat het ons om het belang dat met de gegevensverwerking is gediend.'[22]

Daarom stellen de auteurs voor om de nadruk op het doel en de successievelijke doelbinding te verlaten en te vervangen door een focus op de belangen van de diverse met de dataverwerking gemoeide partijen en instanties.

19 Artikel 6.1(f) Verordening (EU) 2016/679.
20 Moerel & Prins 2016 (*supra* noot 16), p. 12.
21 Moerel & Prins 2016 (*supra* noot 16), p. 68.
22 Moerel & Prins 2016 (*supra* noot 16), p. 68.

Ten tweede schetsen de auteurs een aanpassing ten aanzien van de legitieme verwerkingsgronden. Het gegevensbeschermingsregime vereist dat persoonsgegevens worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden, waarbij er zes legitieme gronden limitatief zijn opgesomd. Dit zijn (1) de toestemming van het datasubject, (2) een contractuele relatie waaruit dataverwerking volgt, (3) een wettelijke plicht, (4) dataverwerking ter behartiging van de vitale belangen van een datasubject, (5) dataverwerking ter behartiging van een publiek belang en (6) het geval waarin de verwerking noodzakelijk is

> '(…) voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. De [laatste grond] geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken.'[23]

Dan geldt er nog een bijzonder regime voor de verwerking van gevoelige persoonsgegevens.

> 'Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.'[24]

Dit verbod lijdt slechts uitzondering in een aantal limitatief opgesomde gevallen. In ieder geval is belangrijk dat de laatstgenoemde grond ten aanzien van de verwerking van gewone persoonsgegevens, waarin, kortgezegd, de belangen van de verantwoordelijke voor de gegevensbescherming worden afgewogen tegen die van het datasubject, geen legitieme uitzondering is voor het verwerken van bijzondere persoonsgegevens.

Moerel en Prins signaleren dat een aantal van de opgesomde legitieme verwerkingsgronden moeilijk toe te passen is op Big Data processen.[25] Zij refereren aan de contractuele relatie en wijzen op de veelgehoorde kritiek dat toestemming bij internetdiensten en -applicaties vaak geen betekenisvolle toestemming is. Er wordt slechts op 'agree' geklikt, zonder dat de terms and conditions daadwerkelijk worden gelezen, laat staan begrepen. Hierdoor is aan één van de vereisten van legitieme toestemming zoals beschreven in het gegevensbeschermingsrecht niet voldaan, namelijk dat de toestemming geïnformeerd moet zijn. Ook aan het vereiste dat de toestemming specifiek dient te zijn en vrij moet worden gegeven wordt vaak niet voldaan.

> 'Een kernbeginsel van de privacywetgeving is dat toestemming 'vrij' wordt gegeven. Dat impliceert dat er een valide alternatief is. Met andere woorden, dat het weigeren van toestemming niet zo nadelig is dat de toestemming wel gegeven moet worden. Maar welke groepen binnen onze samenleving zullen naar verwachting toestemming geven? Dat zullen de minder kapitaalkrachtigen zijn, maar ook degenen die de gevolgen van het geven van dergelijke toestemming niet goed overzien, als dat sowieso al mogelijk zou zijn.'[26]

23 Artikel 6.1(f) Verordening (EU) 2016/679.
24 Artikel 9 Verordening (EU) 2016/679.
25 Moerel & Prins (*supra* noot 16), p. 12-13.
26 Moerel & Prins (*supra* noot 16), p. 45.

Als oplossing wordt geboden om, althans in de private sector, slechts te werken met de zesde van de genoemde legitieme verwerkingsgronden, waarin de belangen tegen elkaar worden afgewogen.[27] Daarbij kiezen Moerel en Prins er voor om het aparte regime ten aanzien van bijzondere persoonsgegevens te verlaten. Het verbod om gevoelige gegevens te verwerken, dat slechts in een aantal uitzonderlijke gevallen kan worden verlaten, geldt niet langer. Ook de verwerking van bijzondere persoonsgegevens wordt onderdeel van de balanceerexercitie.[28] De vraag dient zich aan of er geen enkel principieel verbod meer geldt ten aanzien van de verwerking van de bijzondere persoonsgegevens. Dit wordt inderdaad bevestigend beantwoord door de auteurs van het pre-advies. 'De meest gevoelige categorie gegevens is waarschijnlijk genetische data. Ons standpunt is dat hoe gevoelig ook, er toch altijd weer situaties denkbaar zijn waar er potentieel een gerechtvaardigd belang is om deze data te verwerken.'[29]

Ten derde en tot slot worden de andere principes in het huidige gegevensbeschermingsrecht onderdeel gemaakt van de belangenafwegingstest. Naast het vereiste van een legitieme verwerkingsgrondslag zijn er in het huidige gegevensbeschermingsregime tal van andere principes waaraan de verantwoordelijke voor de gegevensverwerking moet voldoen. Voorbeelden zijn het eerdergenoemde doelbindingsprincipe, het data minimalisatieprincipe, het vereiste van transparantie, veilige en vertrouwelijke opslag en datakwaliteit. De verantwoordelijke voor de gegevensverwerking moet aan ieder van deze principes voldoen, naast het vereiste van de legitieme verwerkingsgrondslag. Het is dus niet zo dat als er aan dataminimalisatie wordt gedaan, er geen legitieme grondslag meer hoeft te worden gevonden. Vice versa is het niet zo dat de toestemming van een datasubject voor een grootschalige gegevensverwerking betekent dat de verantwoordelijke inderdaad een dergelijke grootschalige gegevensverwerking op poten mag zetten: het dataminimalisatieprincipe is nog altijd van kracht.

Volgens de auteurs zijn deze regels en principes te ingewikkeld voor dataverwerkers. Bovendien zijn ze veelal achterhaald. Het doelbindingsprincipe is niet meer te handhaven, omdat gegevens niet voor een specifiek doel worden verzameld en omdat hergebruik van data nu juist de kern vormt van veel van de nieuwe data-toepassingen. Dit geldt bijvoorbeeld ook voor het vereiste van datakwaliteit. Volgens de auteurs is dit principe niet langer als zodanig noodzakelijk; zoals besproken kan er immers ook waardevolle informatie worden verkregen door het doen van complexe analyses op vervuilde data.[30] Als laatste voorbeeld menen Moerel en Prins ook dat het dataminimalisatieprincipe niet meer houdbaar is als voorwaarde voor een legitieme verwerking van persoonsgegevens, gezien het feit dat er juist zo veel mogelijke gegevens worden verzameld.[31] Moerel en Prins stellen voor om deze punten niet als onafhankelijke principes te zien, maar onderdeel te maken van de belangenafwegingstoets.[32] Dit betekent dat wanneer verantwoordelijken hun gegevensverzameling beperken tot een minimale hoeveelheid, dit kan helpen de balans in hun voordeel te kantelen. Dit geldt ook als de verantwoordelijke ervoor zorgdraagt dat de gegevens die worden verwerkt juist en up-to-date zijn. Echter, als de verant-

27 Werkgroep 29, 'Opinion 03/2013 on purpose limitation', 00569/13/EN, WP 203, 2 April 2013.
28 Moerel & Prins (*supra* noot 16), p. 24.
29 Moerel & Prins (*supra* noot 16), p. 89.
30 Moerel & Prins (*supra* noot 16), p. 99 e.v.
31 Moerel & Prins (*supra* noot 16), p. 13-14.
32 Moerel & Prins (*supra* noot 16), p. 14.

woordelijke het minimaliseringsprincipe of het vereiste van datakwaliteit niet respecteert betekent dit niet langer dat de gegevensverwerking per se als onrechtmatig moet worden beschouwd.[33]

De reden waarom de auteurs van het pre-advies geloven dat hun voorstel beter is dan het huidige recht is met name gestoeld op het feit dat het recht, en dus ook het gegevensbeschermingsrecht, doorgaans is gebaseerd op principes en normen. Deze normen zijn altijd onderen over inclusief. Omdat principes algemeen zijn geformuleerd zijn er altijd situaties denkbaar die niet onder de norm vallen, maar dat wel zouden moeten doen, en situaties denkbaar die wel onder de norm vallen, terwijl het misschien wenselijker zou zijn om daar een uitzondering voor te maken.[34] Door het verlaten van standaarden en normen en te kiezen voor een model waarin van geval tot geval wordt bekeken wat de meest wenselijke uitkomst is, kan volgens de auteurs een granulairder systeem ontstaan.[35] Alhoewel het duidelijk is dat het gedane voorstel er met name op is gericht de wet meer aansluiting te laten vinden bij de huidige praktijk, waarin op grote schaal persoonsgegevens worden verzameld, opgeslagen en verwerkt, geven de auteurs terecht aan dat er ook situaties zijn waarin hun systeem tot striktere uitkomsten leidt dan onder het huidige regime.[36] Daarbij is het van belang dat in de door Moerel en Prins voorgestane toets niet alleen de belangen van de verantwoordelijke voor de gegevensverwerking en het datasubject worden meegenomen, maar ook de algemene belangen en voor- en nadelen voor de maatschappij als geheel.[37] Factoren die in de belangenafwegingstest van Moerel en Prins worden meegewogen zijn het al dan niet gerechtvaardigde belang dat met de dataverwerking is gemoeid,[38] of er sprake is van *privacy by design*,[39] het type gegevens dat wordt verwerkt,[40] hoe deze gegevens zijn verkregen, wat de relatie is tussen de verantwoordelijke en het datasubject, wat voor type datasubject het betreft, wat voor type verwerker het betreft en in hoeverre betekenisvolle controle en informatie aan het individu wordt geboden.[41]

3 Kritische beschouwing

Het voorstel van Moerel en Prins komt er dus kortgezegd op neer dat alle principes in het gegevensbeschermingsrecht worden losgelaten en onderdeel worden gemaakt van een algemene belangenafwegingstest, waarin vragen naar dataminimalisatie, datakwaliteit en doelbinding

33 Moerel & Prins (*supra* noot 16), p. 24.
34 Uiteraard bevat het gegevensbeschermingsrecht reeds tal van uitzonderingen, ook op een aantal van de eerdergenoemde principes en uitgangspunten. Zowel de principes als de uitzonderingen daarop zijn het resultaat van de keuze in de priorisering van verschillende uitgangspunten en belangen door de (Europese) wetgever.
35 Moerel & Prins (*supra* noot 16), p. 26. In die zin zijn de uitzonderingen die in het huidige gegevensbeschermingsrecht zijn vervat voor de auteurs onvoldoende. Op de uitzonderingen zouden ook weer uitzonderingen moeten zijn, daarop ook weer, ad infinitum. Daarom kan er beter helemaal niet met uitgangspunten en uitzonderingen worden gewerkt, zo menen de auteurs.
36 Moerel & Prins (*supra* noot 16), p. 81-82.
37 Moerel & Prins (*supra* noot 16), p. 45.
38 Moerel & Prins (*supra* noot 16), p. 19, p. 34.
39 Moerel & Prins (*supra* noot 16), p. 22. Dit is opmerkelijk omdat er in hun voorstel geen principes meer zijn om by design te kunnen implementeren. Hun voorstel ziet er nu juist op om altijd rekening te kunnen houden met de context en de omstandigheden van het geval, terwijl data protection by design juist draait om gekozen standaarden technisch te implementeren.
40 Moerel & Prins (*supra* noot 16), p. 51.
41 Moerel & Prins (*supra* noot 16), p. 94-99 en 103-110.

worden meegenomen. Omdat het hier om een gezaghebbend pre-advies voor de NJV gaat, geschreven door twee gerenommeerde professoren, en omdat het een controversieel voorstel betreft, is het belangrijk het pre-advies kritisch te beschouwen. Daarbij zijn het met name de methodologie en argumentatie van het stuk die vragen oproepen. Een aantal van de punten zal hier kort worden aangestipt. Allereerst wordt besproken de gedachte van de auteurs dat er een spanningsveld bestaat tussen de wet en de praktijk, dat zou moeten worden opgelost door het loslaten van de gegevensbeschermingsprincipes (sub-paragraaf 3.1). Dan worden de verschillende argumenten besproken die door de auteurs worden aangedragen: de huidige regels zijn op zich goed, maar worden verkeerd uitgelegd (sub-paragraaf 3.2), de huidige gegevensbeschermingsregels zijn verouderd (sub-paragraaf 3.3), de regels staan te ver af van de praktijk en missen derhalve legitimiteit en effectiviteit (sub-paragraf 3.4), de gegevensbeschermingsprincipes zijn te complex voor de dataverwerker om te begrijpen (sub-paragraaf 3.5), de regels zijn te complex voor het datasubject om te begrijpen (sub-paragraaf 3.5) en de regels zijn te veel op het verzamelen van gegevens gericht en te weinig op het gebruik daarvan (sub-paragraaf 3.6). Elk van deze punten zal hieronder kort worden besproken. Los van de inhoudelijke kritiek moet worden opgemerkt dat deze argumenten in het stuk vaak door elkaar lopen, net zoals de probleemanalyse van de auteurs en de geopperde oplossingen, waardoor het stuk argumentatief moeilijk leest en op punten tegenstrijdigheden lijkt te vertonen.

Voor toe te komen aan de inhoudelijke kritiek is het van belang dat de auteurs hun voorstel beperken tot de private sector. Dit is opmerkelijk omdat, zoals de auteurs zelf ook aangeven, het onderscheid tussen de private en de publieke sector in dataverwerkingsverband steeds minder relevant lijkt. Moerel en Prins citeren de Guardian waarin wordt geconstateerd: 'Were Big Brother to come back in the 21st century, he would return as a public-private partnership.'[42] Toch kiezen de auteurs er voor om zich uitsluitend op de private sector te richten, onder meer gezien het feit dat de overheid een geweldsmonopolie heeft.

> 'Daarbij zijn de belangen van burgers bij de inzet van big data in hun relatie met de overheid meestal fundamenteler van aard dan wanneer het de relatie met een bedrijf of ander individu betreft. Een bekend voorbeeld is de *no-fly list* die de Amerikaanse overheid op basis van profilering samenstelt van potentiële terroristen en die door de vliegmaatschappijen moeten worden gecontroleerd voordat ze passagiers kunnen toelaten. Een ander voorbeeld is de *Crime Prediction Tool* die de Amerikaanse staat Oregon heeft ontwikkeld en geïmplementeerd. Hiermee kunnen rechters een inschatting maken van het risico van recidive en dit meenemen in hun beslissingen over bijvoorbeeld vervroegde vrijlating van gevangenen.'[43]

Het is opmerkelijk dat de auteurs in hun argumentatie twee keer naar de Amerikaanse situatie verwijzen.[44] Dergelijke praktijken zijn in Europa aan banden gelegd en lijken dan ook niet een rigide onderscheid tussen de private en de publieke sector te legitimeren. Ook moet worden opgemerkt dat bepaalde bedrijven als Facebook en Google op andere terreinen ook een monopoliepositie hebben en dat de impact van beslissingen door private partijen als banken, hypo-

42 Moerel & Prins (*supra* noot 16), p. 30.
43 Moerel & Prins (*supra* noot 16), p. 31.
44 Alleen terloops vermelden de auteurs dat iets soortgelijks plaats zou vinden in Nederland binnen de jeugdzorg. Hoe dat wordt toepast blijft onduidelijk; belangrijker is dat toepassing van profilering in het strafrecht iets anders is en veel minder ingrijpend lijkt dan het hulpaanbod aanpassen aan mogelijke profielen van kinderen.

theekverstrekkers en zorgverzekeraars wel degelijk verstrekkende consequenties kunnen hebben.[45] De afbakening van de auteurs zou dan ook gebaat zijn bij een verdere onderbouwing.

3.1 Spanningsveld tussen wet en praktijk

Moerel en Prins gaan uit van een spanning tussen de wet en de praktijk, ongeveer zoals in de inleiding van dit artikel is aangegeven. In de inleiding werd echter wel benadrukt dat het een beschrijving van het ideaaltype van Big Data betrof. Er zijn namelijk veel experts die ofwel niet geloven dat Big Data iets werkelijk nieuws is, geloven dat het een hype is of menen dat Big Data veel minder vermag dan soms wordt geloofd. Zo wordt er benadrukt dat er thans zoveel data worden geproduceerd dat het opslaan, laat staan het analyseren daarvan, in toenemende mate ondoenlijk wordt, dat de kwaliteit van de gegevens en de deugdelijkheid van de onderzoeksmethode nog altijd van groot belang zijn, dat er veel onbetrouwbare uitkomsten uit Big Data analyses volgen en dat grootschalige gegevensverwerking voor veel doeleinden niet het juiste middel is.[46] Omdat de auteurs van het pre-advies nauwelijks inhoudelijk ingaan op deze kritiek en de tegenargumenten[47] blijft onduidelijk of de noodzaak tot een radicaal voorstel als het hunne op de realiteit is gebaseerd of op een idée fixe.

Zelfs als er inderdaad een dergelijke spanning is of zal ontstaan tussen de wet en de praktijk, moet worden opgemerkt dat er verschillende oplossingen zouden kunnen worden aangedragen. Ook aan de verschillende mogelijkheden wordt echter weinig aandacht besteed. Zo hebben de Europese regelgever en de diverse handhavingsinstanties het spanningsveld tussen de wet en de praktijk in het gegevensbeschermingsrecht uiteraard ook geconstateerd.[48] Ze maken echter een andere keuze. Waar de auteurs menen dat de wet aan de praktijk moet worden aangepast, meent de Europese regelgever dat de praktijk aan de wet moet worden aangepast. De Verordening houdt de principes en standaarden uit het gegevensbeschermingsrecht in grote lijnen in stand, maar zet tegelijkertijd fors in op diverse handhavingsinstrumenten, onder meer door het

45 Daarbij is ook opmerkelijk dat de aanleiding voor het schrijven van het stuk juist is een toepassing van Big Data technologie in de verzekeringswereld. Moerel & Prins (*supra* noot 16), p. 42-47.

46 De literatuur op dit punt is te uitgebreid om te citeren. Een startpunt kan gevonden worden in het eerder geciteerde WRR rapport, p. 81 e.v., en de daarin vermelde literatuur. D. Lazer, R. Kennedy, G. King & A. Vespignani, 'The parable of Google Flu: Traps in big data analysis', *Science* 2014/343. J. Lerman, 'Big Data and its exclusions', *Stanford Law Review Online* 2013. S. D. Levitt & S. J. Dubner, *Freakonomics. A rogue economist explores the hidden side of everything*, New York: Harper Collins 2005. L. Kool, J. Timmer & R. van Est, *De datagedreven samenleving*, Den Haag: Rathenau Instituut 2015 (online publiek). T. Harford, 'Big data: are we making a big mistake?', *Financial Times* 28 maart 2014. T. Gillespie, 'The relevance of algorithms', in: T. Gillespie, P. Boczkowski en K. Foot (red.), *Media technologies: Essays on communication, materiality, and society*, Cambridge: MIT Press 2014. N.N. Taleb, 'Beware the big errors of 'Big Data'', *Wired* 2013. Z. Tufekci, 'Big questions for social media Big Data: Representativeness, validity and other methodological pitfalls' in *Proceedings of the 8th International AAAI Conference on Weblogs and Social Media*, The AAAI Press 2014.

47 In de twee stukken waar de auteurs dit aankondigen benadrukken zij vooral hun eigen visie. Moerel & Prins (*supra* noot 16), p. 27-29 en p. 34-37.

48 Zie de vele documenten en onderzoeken van en voor de Europese Commissie ter voorbereiding van de Verordening. Zie ook: International Working Group on Data Protection in Telecommunications: 'Working Paper on Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics', https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group.

belang van technische middelen als *privacy by design* en *privacy by default* te vergroten,[49] door grote dataverwerkers een interne privacy controleur aan te laten stellen,[50] door de regels en de handhaving daarvan naar een EU-wijd niveau te trekken,[51] zodat bedrijven zich niet aan de regels kunnen onttrekken door zich in een EU-land te vestigen dat slechts een zwak raamwerk of tamme privacy-waakhond kent,[52] en vooral door het introduceren van boetes die kunnen oplopen tot 20 miljoen euro of 4% van de wereldwijde jaarlijkse omzet van een bedrijf per schending van een gegevensverwerkingsregel.[53] De auteurs geven zich geen rekenschap van deze keuze van de Europese regelgever en maken niet duidelijk waarom zij menen dat deze oplossingsrichting niet zal werken. Daarmee wordt de lezer wederom niet duidelijk waarom de auteurs menen dat hun radicale oplossing noodzakelijk of althans de beste is.

Daarnaast moet worden opgemerkt dat zelfs als er voor wordt gekozen om niet de praktijk aan de wet, maar de wet aan de praktijk aan te passen, er meer opties voorhanden zijn dan de gegevensbeschermingsregels simpelweg niet langer als zelfstandige principes te zien. Als wordt geconstateerd dat de huidige principes niet langer voldoen, dan had het voor de hand gelegen dat de auteurs zich de moeite hadden getroost om naar nieuwe en betere dataverwerkingsprincipes te zoeken. In ieder geval had een poging daartoe en een eventuele verklaring waarom ook dergelijke nieuwe principes niet volstaan om het bestaande probleem te verhelpen niet hebben misstaan. Wederom verklaren de auteurs niet waarom zij een dergelijke oplossingsrichting ontoereikend vinden en blijft derhalve ook hier in het midden of het bestaande probleem niet had kunnen worden opgelost met minder radicale middelen.

3.2 Regels worden verkeerd uitgelegd

Er bestaat enige onduidelijkheid omtrent de benadering en probleemanalyse van de auteurs van het pre-advies. Enerzijds benadrukken zij meermaals dat de huidige gegevensbeschermingsprincipes simpelweg achterhaald zijn. Anderzijds wordt ook gesuggereerd dat het probleem niet zozeer is dat de principes achterhaald zijn, maar dat de interpretatie van deze principes onnodig strikt is. Als voorbeeld kan dienen het vereiste van datakwaliteit, waarbij Moerel en Prins expliciet aangeven dat deze plicht beperkt en relatief is: 'De wetgever legt de verantwoordelijke dus geen verplichting op tot een 100%-controle op juistheid en nauwkeurigheid. Het gaat om maatregelen die in redelijkheid mogen worden verlangd, waarbij de context waarin de gegevens worden gebruikt bepalend is voor het oordeel over de toereikendheid van de genomen maatregelen.'[54] Eenzelfde argument geldt ten aanzien van het vereiste van veilige gegevensopslag; ook daar gaat het om de redelijke inspanningen die de verantwoordelijke dient te hebben getroffen, onder meer rekening houdend met de stand van de techniek. Als laatste voorbeeld

49 Artikel 25 Verordening (EU) 2016/679.
50 Artikel 37-39 Verordening (EU) 2016/679.
51 Een Verordening heeft in tegenstelling tot een Richtlijn direct effect. Ook de handhaving wordt in grotere mate gelijkgetrokken, onder andere door samenwerking tussen de nationale organisaties. Artikel 60-76 Verordening (EU) 2016/679.
52 Door velen wordt bijvoorbeeld aangenomen dat één van de redenen voor tech-bedrijven om zich te vestigen in Ierland niet alleen is het gunstige belastingklimaat, maar ook de milde privacyregels en handhaving daarvan.
53 Artikel 83 Verordening (EU) 2016/679.
54 Moerel & Prins (*supra* noot 16), p. 99

kan worden gegeven het doelbindingsprincipe, dat volgens Moerel en Prins hergebruik van data reeds toestaat. Daarbij verwijzen de auteurs naar de Britse toezichthouder. 'The DPA does not say that processing for a new purpose is not permissible, nor does it say that the new purpose must be the same as the original purpose, nor even that it must be compatible with the original purpose: it says that it must not be incompatible with it.'[55] Als dergelijke argumenten doel treffen dan lijkt er geen directe aanleiding om het huidige juridische systeem radicaal te wijzigen, zoals de auteurs voorstaan, maar moet veeleer worden ingezet op een juiste uitleg van de thans geldende regels.

3.3 Regels zijn verouderd

Vaker lijken de auteurs zich echter op het standpunt te stellen dat de regels verouderd zijn en achterhaald door de technische ontwikkelingen. Toch is ook deze analyse niet op alle punten overtuigend. Een voorbeeld is hun constatering dat persoonsgegevens in het verleden een bijproduct waren van het doel waarvoor zij werden verzameld, maar dat dit door de technologische ontwikkelingen niet altijd meer het geval is. Als voorbeeld geven zij dat verzekeraars als eerste stap vele gegevens bijeenrapen, om op basis van de gevonden correlaties nieuwe producten te ontwikkelen en aan te bieden. Hier is de 'gegevensverzameling en analyse zelf het doel', zo wordt gesteld.[56] Er is dus geen doel *waarvoor* de gegevens worden verzameld, zo menen de auteurs, en het vereiste van een legitiem doel en van de successievelijke doelbinding zijn daarmee ook niet langer betekenisvol.[57]

Toch zal dataverzameling als zodanig nimmer een doel op zich zijn. Het zal immers altijd gaan om wat er vervolgens met de data wordt gedaan, zoals het doorverkopen van data aan derden, het gebruik daarvan voor advertenties, om onderzoek te verrichten of voor welk ander doel dan ook. Het hebben van data als zodanig, zonder daar volgens iets mee te toen, is nimmer interessant. Wat de auteurs veeleer lijken te bedoelen is niet dat het verzamelen van data zelf een doel is, maar dat het doel niet altijd op voorhand duidelijk is en dat er later altijd nieuwe doeleinden voor de gegevensverwerking kunnen worden gevonden. Data zijn echter nog altijd een middel voor het bereiken van een bepaald doel, niet een doel als zodanig. Dit betekent dat het door Moerel en Prins gestelde geen argument kan zijn voor het verlaten van het vereiste van een legitiem doel en het doelbindingsprincipe.[58]

Eenzelfde argumentatief probleem komt naar voren bij de analyse van Moerel en Prins met betrekking tot de andere gegevensbeschermingsprincipes.[59] Als voorbeeld kan worden gegeven hun analyse ten aanzien van het regime voor bijzondere persoonsgegevens, zoals aangaande medische gegevens, geloof en ras, dat in hun ogen niet meer zinvol is. Enerzijds is dit regime volgens de auteurs achterhaald omdat ook uit het gebruik van ongevoelige gegevens, gevoelige patronen of informatie kan worden afgeleid. 'Andersom zijn er genoeg voorbeelden van bijzondere persoonsgegevens die voor het doel waarvoor ze worden verwerkt niet gevoelig zijn, waarmee

55 Moerel & Prins (*supra* noot 16), p. 66.
56 Moerel & Prins (*supra* noot 16), p. 19.
57 Zie over hergebruik ook Moerel & Prins (*supra* noot 16), p. 25 en p. 68.
58 Moerel & Prins (*supra* noot 16), p. 17-18.
59 Zie ten aanzien van de kwaliteit van gegevens bijvoorbeeld: Moerel & Prins (*supra* noot 16), p. 99-103.

het onnodig is dat het gebruik aan een zwaarder regime wordt onderworpen. Te denken valt aan het geval dat in de pensioenadministratie iemands partner en geslacht wordt geregistreerd, en daarmee de seksuele geaardheid van de betreffende persoon blijkt.'[60] Hiermee keren de auteurs zich direct tegen de argumentatie die destijds leidde tot de introductie van de categorie van bijzondere persoonsgegevens in het gegevensbeschermingsrecht,[61] namelijk dat de verwerking van sommige type gegevens vrijwel altijd aan een aanmerkelijk belang van het datasubject raakt. Er zijn uiteraard altijd voorbeelden te noemen waarin de ratio achter een algemene norm niet opgaat; een gratuite verwijzing naar de pensioenadministratie voldoet dan ook niet. Het gaat er om duidelijk te maken dat het in het algemeen het zo is dat de ratio voor een speciaal beschermingsregime voor bijzondere persoonsgegevens niet meer opgaat. Daarin slagen de auteurs niet.

Daarbij moet worden opgemerkt dat de twee door de auteurs opgeworpen argumenten ook gelden voor de definitie van en het beschermingsregime voor gewone 'persoonsgegevens'. Ook daarbij geldt dat op basis van niet identificeerbare gegevens beslissingen kunnen worden genomen die een persoon treffen en ook daarbij geldt dat identificeerbare gegevens kunnen worden verkregen of afgeleid uit de combinatie van twee of meer niet identificeerbare gegevens. Ook hoeft de verwerking van persoonsgegevens helemaal niet in alle gevallen aan een persoonlijk belang van het datasubject te raken. Het feit dat iemand de naam van de auteurs van het preadvies heeft opgeslagen (een naam is een persoonsgegeven), lijkt bijvoorbeeld niet werkelijk aan een belang van de auteurs als datasubjecten te raken. Het is niet duidelijk waarom de auteurs hun argumenten niet doortrekken naar persoonsgegevens als zodanig. Ook blijft onduidelijk waarom het volgens de auteurs niet gevoelig is dat een pensioenorganisatie of -ambtenaar weet dat een bepaald persoon een relatie heeft met iemand van hetzelfde geslacht. Een maatstaf of criterium voor een dergelijke beslissing wordt niet gegeven; deze gedachte lijkt dan ook met name een weerspiegeling van het subjectieve oordeel van de auteurs.

De analyse van de auteurs waaruit zou moeten blijken dat de huidige gegevensbeschermingsregels achterhaald zijn overtuigt dan ook niet op alle punten.[62] Daarbij moet nog het volgende worden opgemerkt: zelfs al zouden de huidige regels achterhaald zijn in het licht van de nieuwe technologische ontwikkelingen, dan nog volgt daar niet uit dat het gehele gegevensbeschermingsrecht op de schop moet. De auteurs kiezen in hun voorstel voor een focus op de fenomenen Big Data en het internet der dingen.

60 Moerel & Prins (*supra* noot 16), p. 23-24.

61 In de Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, van de Raad van Europa uit 1981, waarop de EU richtlijn uit 1995 is gebaseerd, werd deze doctrine geïntroduceerd. De reden daarvoor: 'While the risk that data processing is harmful to persons generally depends not on the contents of the data but on the context in which they are used, there are exceptional cases where the processing of certain categories of data is as such likely to lead to encroachments on individual rights and interests.' Explanatory memorandum Convention 1981, p. 43, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434.

62 Belangrijk is om te merken dat ten aanzien van het gegevensbeschermingsrecht, met de nieuwe Algemene Verordening Gegevensbescherming, de algemene gedachte dat de wet altijd achter de werkelijkheid aanhobbelt en derhalve reeds verouderd is op het moment dat ze wordt aangenomen niet opgaat. Het gaat hier om een doelbewuste keuze van de Europese regelgever om de reeds geldende principes te laten voortbestaan, ook al ziet zij dat de praktijk zich tot nu toe anders heeft ontwikkeld.

> 'Beide zijn niet in zichzelf van belang voor onze redenering, maar zijn in hoge mate illustratief voor de veranderingen in aard, reikwijdte en effect van het persoonsgegevensgebruik die we centraal stellen. Het zijn deze veranderingen die maken dat enkele kerncriteria in het huidige wettelijk kader onder druk zijn komen te staan. En daarmee zijn het deze criteria die we nader analyseren en waar we een alternatief voor aanreiken.'[63]

De voorstellen die de auteurs doen met betrekking tot de herziening van het gegevensverwerkingsrecht zijn dus niet beperkt tot deze twee fenomenen; deze worden slechts gebruikt als aanleiding en illustratie. De auteurs hebben niet voor ogen dat het huidige gegevensbeschermingsrecht van toepassing blijft op 'small data' en dat de door de auteurs voorgestelde variant van het gegevensbeschermingsrecht van toepassing wordt op 'Big Data'. In tegendeel, het gehele gegevensbeschermingsrecht dient volgens de auteurs te worden herzien. Dit is pijnlijk omdat zowel de aanleiding als de argumentatie van de auteurs beperkt blijft tot deze twee voorbeelden. Vaak lijkt dan ook het kind met het badwater te worden weggegooid. De analyse ten aanzien van de ongeschiktheid van de huidige principes voor de nieuwe technologische omgeving, zo die al deugdelijk is, wordt zonder uitleg of argumentatie geëxtrapoleerd naar alle gegevensverwerkingsprocessen.

3.4 Regels staan te ver van de feitelijke praktijk

Dan valt er nog een ander argument in het pre-advies te ontwaren. Deze bestaat er uit dat niet zozeer de regels verouderd zijn, maar dat ze simpelweg zo ver van de feitelijke realiteit staan dat ze legitimiteit en effectiviteit ontberen. De filosofische basis voor hun voorstel zoeken de auteurs in Lon Fuller, Phillip Selznick en Amataya Sen. Zij laten zich inspireren door het door Fuller en Selznick ontwikkelde ideaal dat 'wetgevers het perspectief moeten innemen van degenen die met de regels moeten werken en leven'. Moerel en Prins refereren aan Witteveen, die voortbouwend op het werk van Fuller en Selznick wijst op het gevaar van het ontbreken van zowel werkelijkheidszin als mogelijkheidszin bij de regelgever. Bij werkelijkheidszin gaat het om kennis omtrent hoe de regels uitwerken in de praktijk, bij mogelijkheidszin gaat het om een goede inschatting van wat de begrenzingen zijn van het werken met wetten en regels. Moerel en Prins menen dat aan beide principes een gebrek is in het gegevensbeschermingsrecht. Er is volgens de auteurs geen werkelijkheidszin nu de kans van slagen van de regels doorgaans nihil is. 'Zo beogen de informatieplichten die aan gegevensverwerkers worden opgelegd individuen meer inzicht te bieden in wat er met hun gegevens gebeurt. Maar realiseren deze plichten inderdaad in de huidige tijd dit oogmerk nog wel?'[64] Ook mogelijkheidszin is bij privacybescherming problematisch menen Moerel en Prins, waarbij ze refereren aan de Algemene Verordening Gegevensbescherming:

> 'zoals we eerder al constateerden, zijn burgers nauwelijks nog in staat met de toegekende rechten in de hand controle uit te oefenen en wordt hen in feite geen daadwerkelijk praktische rechtszekerheid geboden. Waar de begrensde rationaliteit van actoren in de fysieke wereld al van betekenis is, geldt dat in nog veel

63 Moerel & Prins (*supra* noot 16), p. 27.
64 Moerel & Prins (*supra* noot 16), p. 63.

> sterkere mate voor de digitale wereld. Consumenten die een online dienst, een App of sociaal netwerk gebruiken zijn niet in staat om de privacygevolgen van hun keuze te overzien.'[65]

Naast het feit dat de auteurs wederom negeren dat de Europese regelgever nieuwe regels heeft gegeven om de praktijk meer op de wet te laten aansluiten, moet worden opgemerkt dat noch Fuller noch Selznik bedoeld heeft dat de wetgever een bestaande situatie niet mag wijzigen of tegen een gaande trend mag ingaan. Uiteraard mag en moet een wetgever dat soms doen, zelfs als partijen daar hinder van ondervinden of als datgene dat verboden wordt reeds een staande praktijk is. Bij de grenzen aan wetgeving in het kader van bijvoorbeeld de mogelijkheidszin moet veeleer worden gedacht aan zeer verregaande beperkingen op het privéleven van het individu. Zo meende Fuller dat een wetgever zich beter niet kan mengen in het seksuele leven van burgers, bijvoorbeeld door het verbieden van homoseksuele handelingen in de privésfeer, omdat het voor personen niet of nauwelijks te doen is om hun seksuele verlangens te onderdrukken.[66] Een dergelijke praktijk verbieden zou volgens Fuller een schending van het 'mogelijkheidsprincipe'[67] zijn; het gaat daarbij dus om wezenlijk andere belangen dan bedrijven die minder winst maken als ze minder gegevens mogen verwerken.[68] Ook bij milieuvervuiling gaat het bijvoorbeeld om een grote en reeds bestaande industrietak; natuurlijk hebben striktere milieuregels tot gevolg dat organisaties meer kosten moeten maken en er minder bedrijfsmodellen zijn toegestaan. Dat betekent echter niet dat er geen milieuregels moeten worden aangenomen.

3.5 Regels zijn te complex voor de verantwoordelijke

Ook opperen de auteurs dat het probleem niet zozeer is dat de huidige regels verkeerd worden uitgelegd, dat ze zijn achterhaald of dat ze te ver van de feitelijke realiteit afstaan, maar dat ze an sich te complex zijn voor bedrijven om te begrijpen en te volgen.

> 'Zo dient de verantwoordelijke momenteel aan te tonen dat a. er een uitdrukkelijk omschreven en legitiem doel is; b. er bovendien een grondslag is voor de gegevensverwerking; c. er voor bijzondere persoonsgegevens een specifieke grondslag is voor verwerking (en als deze toets minder stringent uitvalt dan de toets voor reguliere gegevens onder b. dan dient ook aan b. te worden voldaan); en d. een eventuele verdere verwerking van de persoonsgegevens 'niet onverenigbaar' is met het oorspronkelijke doel waarvoor de gegevens werden verzameld. Onze ervaring is dat de meeste verwerkers de finesse van het onderscheid tussen de verschillende toetsen (en de verschillende grondslagen) ontgaat. Het systeem is gewoonweg te complex, hetgeen resulteert in het ridiculiseren van de regels in plaats van een serieuze poging deze na te leven. Nu het systeem van de Verordening Gegevensbescherming op dit punt hetzelfde blijft, blijft deze

65 Moerel & Prins (*supra* noot 16), p. 63-64.

66 L.L. Fuller, 'Freedom as Allocating choice', *Proceedings of the American Philosophical Society Vol. 112 No. 2*, L*aw and Liberty* 1968, p. 103.

67 Een term die hij overigens niet bezigt.

68 Door de auteurs wordt vaak verwezen naar de falende cookie-regels. Dit is opmerkelijk omdat dit een typisch voorbeeld is van onwil van advertentiebedrijven om zich te matigen in het aantal cookies dat op apparaten wordt geplaatst. In plaats daarvan is er voor gekozen om de consument te overladen met zinloze 'I agree' statements, op basis waarvan soms meer dan 100 cookies van derde partijen worden geplaats per websitebezoek, zodat de bezoeker van meerdere kanten in de gate kan worden gehouden. Dit is uiteraard noch een legitieme vorm van toestemming, noch in overeenstemming met de bedoeling van de Europese regelgever, die juist de integriteit van consumentenapparaten wilde beschermen.

> kritiek onverminderd van kracht. We zullen naar één toets moeten voor de verschillende fasen van de levenscyclus van data: het verzamelen, verwerken, verder verwerken en de vernietiging van gegevens'.[69]

Dit beeld lijkt nogal eenzijdig. Ten eerste wordt door velen juist aangenomen dat er bij grote dataverwerkingsbedrijven vaak eerder sprake is van onwil dan van onbegrip. Als de auteurs dit anders zien zullen zij met meer dan anekdotisch bewijs moeten komen. Ten tweede wordt iedereen in een rechtstaat geacht de wet te kennen, ook bedrijven die persoonsgegevens verwerken. Ten derde is niet direct duidelijk wat er nu zo ingewikkeld is aan het gegevensbeschermingsrecht. Het lijkt juist gebaseerd op tamelijk voor de hand liggende principes: 'als u gegevens verwerkt, verzamel dan niet meer dan nodig is', 'als u gegevens niet langer nodig heeft, verwijder ze dan', 'als u gegevens opslaat, zorg dan dat dit veilig geschiedt', etc. Ten vierde kunnen bedrijven een privacy specialist vragen om hen te helpen aan de regels te voldoen. De Verordening verplicht grotere data verwerkers reeds een interne privacy controleur aan te stellen. Voor grote dataverwerkingsbedrijven die het geld hebben om met geavanceerde Big Data technieken en het internet der dingen te werken, lijkt het geen onredelijke eis om een klein bedrag op zij te zetten voor een privacy specialist, net zoals bedrijven een mededingingsexpert kunnen inhuren of iemand die verstand heeft van auteursrecht. Tot slot, wat het huidige gegevensbeschermingsrecht enigszins ingewikkeld maakt is het feit dat sommige normen interpretatie vergen: wat moet worden gezien als een 'onverenigbaar doel', welke technische en organisatorische maatregelen moeten er in een specifiek geval worden getroffen als er rekening moet worden gehouden met onder meer 'de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel', wanneer zijn data aan te merken als 'up to date', wanneer zijn de uitzonderingen van toepassing, etc. Dit is op zich een terecht punt, alleen deze complexiteit zal alleen maar toenemen in de door Moerel en Prins voorgestelde situatie, omdat alles wordt teruggebracht tot een open norm die van geval tot geval moet worden ingevuld, geïnterpreteerd en beoordeeld. In deze zin zal het voorstel dan ook een averechts effect hebben.

3.6 De regels zijn te complex voor het individu

Daarnaast voeren Moerel en Prins aan dat de huidige gegevensbeschermingsregels te complex zouden zijn voor het individu. Dit lijkt op punten een zijpad in het voorstel waarbij niet op voorhand duidelijk is hoe deze gedachte zich verhoudt tot de andere punten. Een voorbeeld hiervan is de aanbeveling om niet het individu primair verantwoordelijk te maken voor de naleving van zijn rechten, maar dat veeleer moet worden ingezet op collectieve belangen acties[70] en public interest litigation.[71] Dit is een mooi punt, maar lijkt los te staan van en niet te volgen uit de andere punten die in het pre-advies worden gemaakt. Het is één vraag welke principes er van toepassing moeten zijn op gegevensverwerkingsprocessen (ten aanzien hiervan stellen Moerel en Prins voor de huidige principes te vervangen door een belangenafwegingstoets), het

69 Moerel & Prins (*supra* noot 16), p. 24. Eenzelfde beeld doemde ook al op bij de vierde pijler, waarbij de auteurs ten aanzien van het verbod op de verwerking van bijzondere persoonsgegevens opmerkten: 'Voor verantwoordelijken is het toepassen van het speciale regime voor alleen die gegevens niet intuïtief.' Omdat de regel niet intuïtief aanvoelt voor bedrijven kan die klaarblijkelijk beter worden geschrapt.

70 Moerel & Prins (*supra* noot 16), p. 104.

71 Moerel & Prins (*supra* noot 16), p. 113-114.

is een andere vraag hoe deze principes (de huidige of de door Moerel en Prins voorgestelde) moeten worden gehandhaafd. Ook schenken de auteurs weinig aandacht aan het feit dat in de Algemene Verordening Gegevensbescherming reeds een mogelijkheid tot algemene belangenacties wordt geboden.[72] Klaarblijkelijk kunnen de huidige gegevensbeschermingsprincipes prima samengaan met een collectieve vorm van rechtshandhaving.

Ook inhoudelijk lijkt dit punt niet geheel te overtuigen. Moerel en Prins stellen dat individuen steeds minder weten welke gegevens er over hen worden verwerkt, door wie en hoe.[73] 'We moeten daarom af van het huidige systeem waarbij de veronderstelling is dat handhaving toch primair door individuen zelf zal moeten plaatsvinden (vanuit het uitgangspunt dat ze zijn geïnformeerd en rechten hebben).'[74] Deze stelling is opmerkelijk omdat het uitgaat van een grove versimpeling van het huidige systeem. Niet het individu, maar de verantwoordelijke voor de gegevensverwerking (niet voor niets de verantwoordelijke genoemd) is belast met de plicht om aan de gegevensverwerkingsprincipes te voldoen. Daarnaast heeft elk land een genoemde Data Protection Authority, in Nederland de Autoriteit Persoonsgegevens geheten.[75] Deze kunnen, los van klachten van individuen, zelf onderzoek doen naar misstanden en zelfstandig boetes of lasten onder dwangsom opleggen.[76]

Wellicht belangrijker is de overtuiging van de auteurs dat de gedachte dat verwerkers van gegevens rechtmatig handelen door individuen te informeren en hen te laten klikken op 'OK' niet langer geldig is. Zij noemen dit 'mechanisch proceduralisme', waarbij verantwoordelijken mechanisch individuen informeren en hun toestemming verzamelen, zonder daadwerkelijke privacybescherming te bieden.[77] Het is de vraag tot wie de auteurs zich hier richten. Er zijn slechts weinigen die inderdaad geloven dat het drukken op 'OK' afdoende is voor legitieme gegevensverwerking. Belangrijker is dat dergelijke gegevensverwerking onder het huidige regime niet legitiem is, zowel daar deze vorm van toestemming niet vrij, specifiek en geïnformeerd is, en derhalve niet rechtmatig, alsook omdat er naast het vereiste van een legitiem doel tal van andere begrenzende principes zijn, zoals het dataminimalisatieprincipe en het doelbindingsprincipe. Als het al zo is dat er gegevensverwerkers zijn die denken dat door datasubjecten mechanisch te laten klikken op 'OK' zij rechtmatig handelen, dan lijkt het eerder voor de hand te liggen om een voorlichtingscampagne te starten dan het huidige gegevensbeschermingsrecht radicaal te wijzigen.[78]

72 Artikel 80 Verordening (EU) 2016/679.
73 Moerel & Prins (*supra* noot 16), p. 20-21.
74 Moerel & Prins (*supra* noot 16), p. 22.
75 Voorheen het College Bescherming Persoonsgegevens
76 Moerel en prins merken daarbij met name op dat de privacy policies zo ingewikkeld zijn dat het gemiddelde individu deze niet meer snapt. Moerel & Prins (*supra* noot 16), p. 20-21.
77 Moerel & Prins (*supra* noot 16), p. 19.
78 Daarnaast is het opmerkelijk dat de auteurs stellen dat 'informed consent' als zodanig niet afdoende is voor een adequate bescherming van datasubjecten en tegelijkertijd zelf alle principes die verdere bescherming bieden, zoals het dataminimialisatieprincipe en het doelbindingsprincipe, overboord zetten.

3.7 De huidige regels zijn te veel op het verzamelen gericht en te weinig op het gebruik

Tot slot vormt dit pre-advies onderdeel van het zogenoemde acces-use debat.[79] Kortgezegd komt dit debat er op neer dat het huidige gegevensbeschermingsregime voornamelijk regels stelt ten aanzien van het verzamelen en opslaan van de persoonsgegevens. Tegenstanders van een dergelijke benadering menen dat dit niet langer houdbaar is, nu het voor overheden, bedrijven en burgers zeer gemakkelijk en goedkoop is om grote hoeveelheden data te verzamelen en op te slaan via mass surveillance, cookies of camera's op smart phones. Zij menen dat deze principes beter kunnen worden losgelaten. In plaats daarvan zouden er regels moeten worden gesteld ten aanzien van het gebruik van gegevens, zoals een verbod op discriminatoire toepassingen of gebruik dat burgers in aanmerkelijke mate negatief treft. Moerel en Prins ontkennen expliciet dat zij zich met dit advies in het laatste kamp scharen.[80] Toch is gekozen voor een benadering waar niet alleen het verzamelen onder valt, maar juist ook het analyseren en het gebruik van data.[81] Daarnaast worden alle verboden en standaarden die nu een barrière vormen voor grootschalige gegevensverzameling niet langer als zelfstandige principes gezien, maar onderdeel gemaakt van een algemene belangenafwegingstest.

De auteurs richten zich in hun eigen voorstel ook meer op begrenzingen ten aanzien van het gebruik van gegevens, dan ten aanzien van het verzamelen daarvan.[82] Ze verwijzen naar aanvullende pakketten bij ziektekosten- of arbeidsongeschiktheidsverzekeringen waarbij de premie is gebaseerd op data-analyse met behulp van onder meer genetische informatie. Farmaceutische bedrijven zouden inmiddels intensief optrekken met bedrijven als Google en Apple in de zoektocht naar waardevolle genetische kennis om die commercieel te benutten. Zolang hun data-analyse zich beperkt tot het genereren van abstracte inzichten en modellen, zal er volgens de auteurs voor het doen van de analyses een gerechtvaardigd belang te vinden zijn. 'Zodra de uitkomsten van de analyses echter worden vertaald naar een dienst of product gericht op een concrete persoon, kan de belangenafweging anders uitpakken.'[83]

Nog duidelijker wordt het als de auteurs concluderend bespiegelen.

> 'Kijkend naar de geschetste ontwikkelingen en dilemma's blijkt een cruciale vraag te zijn die naar het vertrekpunt voor de beoordeling van de aanvaardbaarheid van gegevensgebruik. Anders geformuleerd: willen we het doen van data-analyses verbieden om de enkele reden dat we zorgen hebben over de uiteindelijke toepassing van de resultaten van die analyses? Als we teruggaan naar het voorbeeld waarmee we dit preadvies startten, dan zou een bevestigend antwoord op deze vraag betekenen dat alle mogelijke toepassingen voor het persoonsgericht voorspellen van gezondheid en ziekte niet zijn toegestaan. Maar dienen eventuele beperkingen niet veeleer gericht te zijn op de uiteindelijke toepassing van de analyseresultaten? Wij denken dat het laatste het geval is. Het blijkt allereerst steeds moeilijker bedrijven en organisaties weg te houden van bepaalde data. Bovendien richt het oordeel over de kansen van – maar ook de zorgen

79 Zie onder andere: J. van Hoboken, 'From Collection to Use in Privacy Regulation? A Forward-Looking Comparison of European and us Frameworks for Personal Data Processing', in: B. van der Sloot, D. Broeders & E. Schrijvers (eds.), *Exploring the Boundaries of Big Data*, te raadplegen via: www.wrr.nl/fileadmin/en/publicaties/PDFVerkenningen/Verkenning_32_Exploring_the_Boundaries_of_Big_Data.pdf.

80 Moerel & Prins (*supra* noot 16), p. 15.

81 Moerel & Prins (*supra* noot 16), p. 33.

82 'Steeds minder is op voorhand duidelijk of gegevens (als zodanig) gevoelig zijn. Veeleer gaat het om gebruik dat gevoelig is.' Moerel & Prins (*supra* noot 16), p. 23.

83 Moerel & Prins (*supra* noot 16), p. 110-111.

> over – gegevensgebruik zich steeds meer op de toepassing van gegevens (gegeven een specifieke context) dan de verzameling als zodanig. Data-analyse heeft zowel in negatieve als in positieve zin de nodige consequenties. Ons inziens is de samenleving gebaat bij inzichten op een – van het individu – geabstraheerd niveau, in bijvoorbeeld de correlaties tussen levensstijl en kosten van de zorg, om zo te kunnen bepalen of de zorgkosten op termijn beheersbaar blijven. Het heeft geen zin deze verwerkingen te verbieden om de enkele reden dat we zorgen hebben over de uiteindelijke toepassing van de resultaten van die analyses. We zullen een debat moeten voeren welke toepassingen (welke onderscheidingen) al dan niet toelaatbaar zijn, en hier de regels indien nodig op aan moeten passen. Een oproep tot een dergelijk fundamenteel debat klinkt inmiddels vanuit meer kanten.'[84]

Het gaat de auteurs dus wel degelijk om het verlaten van regels die zien op het verzamelen en analyseren van persoonsgegevens ten faveure van regels aangaande de toepassing en het gebruik van gegevens. Dit is belangrijk, omdat de use-based benadering vrijwel altijd is gebaseerd op een inschatting van schade en belangen en niet op regels en principes, waarover hieronder meer.

4 Analyse

Tot slot nog iets over de duiding van het voorstel. In wezen gaat het de auteurs om een andere benadering van het recht als zodanig. Hun kernkritiek, die keer op keer terugkomt, is dat het recht thans op principes, regels en standaarden is gebaseerd, maar dat deze zowel onder- als overinclusief zijn. De regels ten aanzien van gevoelige persoonsgegevens zijn in de ogen van de auteurs bijvoorbeeld te strikt als het gaat om informatie over een relatie met een persoon van het gelijke geslacht en zijn andersom juist niet van toepassing op gevallen waarin zonder gebruikmaking van gevoelige persoonsgegevens toch gevoelige profielen worden gemaakt of maatregelen worden getroffen die een grote impact hebben op het individu. Eenzelfde argument wordt door de auteurs op tal van punten gegeven. Zo merken zij op dat het huidige regime in het algemeen zaken verbiedt die niet verboden zouden moeten worden en zaken toestaat die als onrechtmatig zouden moeten worden bestempeld. Het voorstel van Moerel en Prins is dan ook om te werken met een open norm in de vorm van een algemene belangenafwegingtoets, in plaats van met vast principes en regels. Bij ieder concrete toepassing van deze norm kan de context worden meegenomen en rekening worden gehouden met de omstandigheden van het geval. Zo kan per gegevensverwerkingsproces de wenselijkheid daarvan puur en alleen op zijn eigen merites worden beoordeeld, los van vaststaande principes.

De auteurs geven aan te verwachten dat er kritiek op hun voorstel zal komen, zoals dat het werken met een open norm in de praktijk onvoldoende sturend zal zijn, vatbaar is voor verschillende interpretaties en aldus onvoldoende rechtszekerheid biedt aan verwerkers en dat de toets in eerste instantie door de verantwoordelijke zelf dient te worden uitgevoerd, wat een bepaald risico met zich brengt. Moerel en Prins stellen echter dat ook nu al de verantwoordelijke voor de gegevensverwerking de meeste beslissingen neemt, althans in eerste instantie. Dit is een opmerkelijk tegenargument omdat de auteurs eerder in hun advies nog expliciet benadrukten dat thans het datasubject primair verantwoordelijk is voor de naleving van de regels (en dat

84 Moerel & Prins (*supra* noot 16), p. 53-54.

ging nu juist niet meer).[85] Daarnaast viel elders in het stuk te lezen dat er nu, naar de smaak van de auteurs, al te veel verantwoordelijkheden liggen bij de gegevensverwerkers. Het is de vraag of dit voorstel daar verlichting in zal brengen. Weliswaar komt alles neer op een simpele balanceerexercitie, maar alle vaste principes en uitgangspunten zijn overboord gezet. Omdat de auteurs menen dat de balanceerexercitie van geval tot geval, met medeneming van de context, dient te geschieden en omdat ieder geval uniek is, zal de verantwoordelijke iedere keer opnieuw een zorgvuldige afweging moeten maken, zonder zich te kunnen verlaten op principes en standaarden. Tot slot lijkt het wel degelijk zo dat door het verlaten van alle principes, standaarden en verboden in het gegevensbeschermingsrecht, de burger is overgeleverd aan de keuzes die de verantwoordelijke maakt. Van rechtszekerheid voor het datasubject is dan ook nauwelijks sprake.[86]

De auteurs staan derhalve een algemene belangenafwegingstoets voor, waarin de kosten en baten, de negatieve en positieve gevolgen van een gegevensverwerking, van geval tot geval tegen elkaar worden afgewogen. Daarbij moeten twee kanttekeningen worden geplaatst. Ten eerste lijken Moerel en Prins soms te suggereren dat de open norm die de auteurs voorstaan in de praktijk moet worden ingevuld door bijvoorbeeld een rechter. Als dit inderdaad zo is dan blijft echter het gesignaleerde probleem met het gegevensbeschermingsrecht in stand: de rechter zal de norm immers invullen en handen en voeten geven door principes, standaarden en uitgangspunten te formuleren. (De open norm moet in zo'n situatie zus of zo worden ingevuld, daarvoor gelden deze en deze criteria, gevallen waarin de negatieve gevolgen in ieder geval te groot zullen zijn, zijn deze en die, etc.) Ook deze principes zullen weer over- en onderinclusief zijn en op termijn worden achterhaald door de nieuwe technologische ontwikkelingen, waarna hetzelfde probleem ontstaat. Een dergelijke aanpak kan dus zorgen voor een tijdelijke opfrisbeurt, en daarmee mogelijk aan de kritiek tegemoetkomen dat de wetgever te ver afstaat van de praktijk (alhoewel het de vraag is of de rechter in alle gevallen meer aansluiting heeft bij de praktijk dan de wetgever), het zal geen duurzame oplossing vormen voor het feit dat regels en standaarden (of die nu in de wet staan of in de jurisprudentie zijn ontwikkeld) altijd zowel onder- als overinclusief zijn. Om echt van geval tot geval een beslissing op maat te kunnen nemen moet de norm haar open karakter behouden.[87] Ten tweede, en daarop aansluitend, geven de auteurs, zoals vermeld, een aantal factoren die moeten worden meegewogen in de belangenafwegingstoets, zoals de aard van de gegevens, van de verwerker en van het datasubject, de doeleinden, de mate waarin het individu daadwerkelijke controle wordt geboden, etc. Dit zijn echter geen begrenzende principes voor de belangenafweging, maar factoren die in de weging tussen positieve en negatieve gevolgen moeten worden meegenomen.

Het voorstel komt er dus op neer een belangenafwegingstest die van geval tot geval moet worden toegepast. Daarbij kunnen veel kanttekeningen worden geplaatst, de vijf meest in het oog springende zullen hier kort worden aangestipt; hopelijk kunnen ze leiden tot een interessant wetenschappelijk debat.

85 Zie ook: Moerel & Prins (*supra* noot 16), p. 114.
86 Moerel & Prins (*supra* noot 16), p. 70-73.
87 Daarnaast zou het stuk wel erg lang zijn voor de simpele aanbeveling, laat niet de Europese regelgever, maar de rechters nieuwe normen ontwikkelen: welke weten we nog niet precies.

- Ten eerste richt zo'n belangenafwegingstest zich op de nadelige en voordelige consequenties van een gegevensverwerkingsproces. Het probleem met veel Big Data processen is echter precies dat zowel de voor- als de nadelen vaak vaag en onduidelijk zijn.[88] Juist als er, zoals de auteurs stellen, bij Big Data geen vooraf bepaald doel is en ook niet duidelijk is waarvoor de gegevens in de toekomst zullen worden gebruikt, dan kan alleen maar per geval dat de data worden gebruikt en daadwerkelijk worden toegepast worden getoetst welke voor- en nadelen dit heeft (dit leidt dan ook wel vrijwel automatisch tot een use-based benadering). Welke positieve effecten heeft de massale gegevensverwerking van de NSA gehad? Hoeveel aanslagen zijn daarmee voorkomen, hoeveel terroristen zijn op basis van deze gegevens berecht, etc.? Ook de mogelijke belangen aan de andere kant, dan wel individueel dan wel gemeenschappelijk, zijn in Big Data processen vaak moeilijk te duiden. Welk concreet negatief effect heeft de grootschalige gegevensverzameling door de NSA bijvoorbeeld gehad op de doorsnee Amerikaanse of Europese burger? Welke schade ondervindt een individu of de maatschappij nu echt van het feit dat er in sommige steden op vrijwel elke straathoek één of meerdere camera's hangen? Deze belangen zijn steeds moeilijker te specificeren. Het is dan ook de vraag of de door Moerel en Prins voorgestane methode niet precies de verkeerde is gegeven de technologische ontwikkelingen.
- Ten tweede is de algemene problematiek van een belangenafwegingstest dat het onduidelijk is hoe deze kan geschieden.[89] Morele concepten als privacy en veiligheid hebben namelijk helemaal geen gewicht. Hoe kan privacybescherming worden uitgedrukt in een eenheid, waarin ook veiligheid kan worden gemeten? Er zijn geen gewichten en er is geen uniforme eenheid waarin de gewichten zouden kunnen worden uitgedrukt. Daarnaast is er geen methode om belangen af te wegen op een objectieve manier en geen standaard meetapparaat of -instrument. De metafoor van balancing is dan ook misleidend; het suggereert de objectiviteit en exactheid van de fysieke wereld die meetbaar en weegbaar is, terwijl het hier juist gaat om een open metafoor die slechts kan worden ingevuld door het subjectieve oordeel van bijvoorbeeld een rechter of een gegevensverwerker, iets wat de auteurs van het pre-advies overigens ook voorstaan.
- Ten derde, en daarop voortbouwend, is het niet voor niets dat het recht in zijn algemeenheid met meer concrete normen en regels werkt, waarop evenwel vrijwel altijd uitzonderingen gelden, namelijk juist om aan subjectieve oordelen te ontsnappen en om rechtszekerheid te bieden. Neem het lekken van een seksfilm. Dit is onder het huidige recht in principe verboden. Onder de benadering van Moerel en Prins zal van geval tot geval moeten worden bekeken of de voordelen opwegen tegen de nadelen die met de verwerking zijn gemoeid. Als er maar genoeg mensen plezier beleven aan de gelekte sekstape, zullen hun belangen dan opwegen tegen de negatieve effecten op één persoon? Wat als het gezicht van de persoon onherkenbaar wordt gemaakt? De auteurs zullen ongetwijfeld stellen dat in het bovengenoemde voorbeeld de belangen van het datasubject zwaarder wegen dan die van de anderen, een dataverwerker kan daar echter een andere opvatting over hebben. Om dit soort discussies

88 B. van der Sloot, 'Privacy in het post NSA-tijdperk: tijd voor een fundamentele herziening?', *NJB* 2014/89.
89 B. van der Sloot, 'The Practical and Theoretical Problems with 'Balancing': Delfi, Coty and the Redundancy of the Human Rights Framework', *Maastricht Journal of European and Comparative Law* 2016/3.

te vermijden kan het handig zijn om met standaarden en uitgangspunten te werken, in plaats van met een open norm.[90]

- Ten vierde geldt de kritiek van de auteurs ten aanzien van de normen en standaarden in het gegevensbeschermingsrecht uiteraard veel breder. Vrijwel het hele juridische regime is gebaseerd op standaarden, principes en regels, die altijd in zekere mate algemeen en statisch zijn geformuleerd. Altijd is er dan ook sprake van onder- en overregulering; altijd vallen zaken buiten de definitie van een juridisch concept, die er beter wel onder hadden kunnen vallen, en altijd vallen er zaken binnen de definitie van een doctrine, waarvan achteraf kan worden betwijfeld of dat een goed idee is. De oplossing die nu bij de meeste juridische doctrines wordt gekozen is om de rechters enige mate van flexibiliteit toe te kennen om regels en standaarden te interpreteren en om eens in de zoveel tijd de wet te herzien als de doctrines te weinig specifiek en doeltreffend zijn geworden. De oplossing is echter doorgaans niet om de regels en standaarden in hun geheel op te heffen en te vervangen door een open norm in de vorm van een belangenafwegingstoets. Ook in het gegevensbeschermingsrecht hebben rechters de normen verder ingevuld en halverwege 2016 heeft de Europese regelgeving een algehele herziening van het gegevensbeschermingsrecht voltooid. Waarom de auteurs menen dat het gegevensbeschermingsrecht in deze zin uniek is en wel in zijn geheel moet worden vervangen door een open norm wordt niet duidelijk.[91]

90 Zo geldt er op de wegen in Nederland een maximumsnelheid, variërend per weg en omgeving. Dit is om te voorkomen dat de weggebruiker steeds op nieuw zelf moet inschatten wat de meest gewenste snelheid is en om ingewikkelde discussies, bijvoorbeeld na een ongeluk, over de omstandigheden van het geval, met medeneming van de context en wat de bestuurder daar in die specifieke situatie uit mocht afleiden, te voorkomen. Uiteraard is het zo dat er uitzonderingen op regels kunnen gelden. Op een weg waar er maximaal 120 kilometer per uur mag worden gereden kan het soms verwijtbaar zijn als een bestuurder deze snelheid inderdaad aanhoudt, bijvoorbeeld bij dichte mist en gladheid, en kan het soms rechtmatig zijn om harder te rijden, bijvoorbeeld als er een gewonde naar het ziekenhuis moet worden vervoerd. Het feit dat er uitzonderingen denkbaar zijn op de regel (en deze soms ook in de wet zijn vervat) en dat de regel altijd zowel onder- als overinclusief is, betekent echter niet dat het beter is om de regel maar niet te stellen. Het zou goed zijn als Moerel en Prins uitleggen waarom dat in het gegevensbeschermingsrecht anders is. Deze vergelijking kan wellicht ook iets zeggen over het regime voor bijzondere persoonsgegevens. De gedachte daarachter is dat met de verwerking van deze gegevens vaak een gewichtig persoonlijk belang van het datasubject is gemoeid. Daarom gelden er extra strikte voorwaarden. De auteurs werpen tegen dat niet bij *elke* verwerking van bijzondere persoonsgegevens inderdaad gewichtige persoonlijke belangen zijn gemoeid en dat er ook situaties denkbaar zijn waarin geen bijzondere persoonsgegevens worden verwerkt en er toch gewichtige persoonlijke belangen op het spel staan. Daarom kan dit extra beschermingsregime beter worden afgeschaft, zo menen Moerel en Prins. Net zoals bij het gegevensbeschermingsrecht zijn er ten aanzien van de maximumsnelheid speciale gebieden aangewezen, bijvoorbeeld woonwijken en gebieden rond scholen, waar extra zorgvuldigheid moet worden betracht, onder meer gegeven het gevaar van spelende kinderen. De maximumsnelheid is daar aanzienlijk lager. Hier zou hetzelfde argument kunnen worden geopperd als die door Moerel en Prins naar voren wordt gebracht. Niet *altijd* is het in woonwijken en rond scholen immers noodzakelijk om extra zacht te rijden en ook zijn er andere situaties, buiten woonwijken en gebieden rond scholen, denkbaar waar kinderen spelen of het anderszins noodzakelijk is om meer zorgvuldigheid te betrachten. Dit lijkt echter geen reden om de algemene regel, dat er in woonwijken en rond scholen extra zorgvuldigheid moet worden betracht en er zachter moet worden gereden, af te schaffen. Het zou goed zijn als de auteurs van het pre-advies ook op dit punt nader zouden toelichten waarin het verschil precies schuilgaat of waar deze vergelijking mank gaat.

91 Het feit dat er ten aanzien van het gegevensbeschermingsrecht veel technologische ontwikkelingen zijn, geldt wel voor meer doctrines. Ook is duidelijk dat de redenering die door de auteurs wordt geboden niet één op één van toepassing is op andere rechtsgebieden. Kort samengevat komt de argumentatie van Moerel en Prins er op dit punt op neer dat (1) er rechtsregels en normen gelden in het gegevensbeschermingsrecht, (2) dat enkele daarvan in de praktijk stelselmatig worden ondermijnd en dat dus (3) het rechtsgebied beter niet langer kan werken met

- Tot slot lijkt dit pre-advies te staan in de traditie die kijkt naar schade en belangen, in plaats van principes en geboden. Het recht is nu juist van oudsher deontologisch geïnspireerd, dat wil zeggen op de ethiek die nadruk legt op plichten en eventueel daaraan correlerende rechten.[92] Het biedt daarmee een tegenwicht aan het utilistisch denken, dat vaak in onder andere het politieke discours dominant is, waarin er geen principes en geboden gelden, maar slechts wordt gekeken naar de vraag of een handeling het algemeen welzijn bevordert of niet. Zelfs al zou het het algemene welzijn bevorderen, dan nog is martelen niet rechtmatig, zelfs al zou het het algemene welzijn bevorderen, dan nog mag er niet gediscrimineerd worden, etc. Eenzelfde uitgangspunt geldt in het gegevensbeschermingsrecht; het stelt principes, voorwaardes en verboden waaraan dataverwerkers zich moeten houden, zelfs al zou dit niet uit een belangenafweging volgen. Niet alleen maakt de wetgever door middel van wetten en regelgeving reeds in veel gevallen een keuze tussen de verschillende belangen, iets wat zeker ook voor het gegevensbeschermingsrecht geldt,[93] ook stelt het voorwaarden en beperkende principes ten aanzien van het nastreven van bepaalde belangen. Moerel en Prins gooien met hun voorstel dan ook niet alleen de meerwaarde van het huidige gegevensbeschermingsrecht, maar ook van het recht als zodanig, namelijk het tegenwicht bieden aan utilistische belangenafwegingen, overboord. Het is sterk de vraag of dat wenselijk is.

Let the games begin

deze rechtsregels en normen, maar liever met een belangenafwegingstoets. Toegepast op een ander rechtsgebied zou deze redenatie als volgt kunnen worden uitgedrukt: (1) er gelden rechtsregels en normen in het strafrecht, (2) een aantal daarvan wordt in de praktijk stelselmatig ondermijnd en (3) daarom kan het strafrecht beter worden vervangen door een open norm, waarbij van geval tot geval de voor- en nadelen van een bepaalde daad tegen elkaar worden afgewogen of (1) er gelden rechtsregels en normen in de Wegenverkeerswet, (2) een aantal daarvan wordt stelselmatig ondermijnd en (3) daarom kan dit rechtsgebied beter worden vervangen door een belangenafwegingstoest. Waarschijnlijk zullen de auteurs het er mee eens zijn dat de redenering toegepast op andere rechtsgebieden niet opgaat, maar waarin het verschil precies schuilt, wat het gegevensbeschermingsrecht precies uniek maakt, behoeft nadere uitleg.

92 J. Habermas, *Between facts and norms: contributions to a discourse theory of law and democracy*, Cambridge: The MIT Press cop 1996.

93 Dit lijken de auteurs overigens ook te erkennen, maar dit is klaarblijkelijk niet naar hun zin geschied.