Privacy voor de homo digitalis

Moerel, Lokke; Prins, Corien

Published in:
Homo Digitalis. Preadviezen 2016 Nederlandse Juristen-Vereniging 2016

Publication date:
2016

Handelingen Nederlandse Juristen-Vereniging

146e jaargang/2016-I

Homo Digitalis

Preadviezen van

E.M.L. Moerel en
J.E.J. Prins
M. Hildebrandt
T.F.E Tjong Tjin Tai
G-J. Zwenne en
A.H.J. Schmidt

Wolters Kluwer - 2016

Ontwerp omslag: Corps Ontwerpers, Den Haag

ISBN 978-90-13-13743-9
NUR 820-102

Mevr. prof. mr. E.M.L. (Lokke) Moerel is hoogleraar Global ICT Law aan de Universiteit van Tilburg en Senior Of Counsel bij het Amerikaanse advocatenkantoor Morrison & Foerster. Zij geeft strategisch advies aan multinationals over hun wereldwijde ICT en privacy & security compliance. Lokke is lid van de Nederlandse Cyber Security Raad en arbiter en mediator bij WIPO en de Stichting Geschillenoplossing Automatisering. Zij is auteur van 'Binding Corporate Rules' (Oxford University Press, 2012) en diverse internationale publicaties over big data, e-commerce, online reclame, privacy en outsourcing. Lokke heeft gestudeerd in Leiden en Cambridge en heeft toezichthoudende functies bij WWF International, WNF, het Mauritshuis en de Vereniging Rembrandt. Lokke heeft een tier 1 ranking in Chambers Global: 'She has a formidable reputation in the field of data protection, advising numerous blue-chip clients. She is doing market-leading work' (Chambers Global 2015).

Mevr. prof. mr. J.E.J. (Corien) Prins studeerde Slavische Taal- en Letterkunde en Rechtsgeleerdheid in Leiden en is sedert 1994 hoogleraar Recht en Informatisering aan de Universiteit van Tilburg. Momenteel is ze daar tevens decaan van de juridische faculteit. Corien was van 2008 tot 2013 raadslid bij de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en in die hoedanigheid onder meer verantwoordelijk voor het rapport *iOverheid*, over digitalisering binnen de publieke sector. Zij is lid van de Koninklijke Akademie voor Wetenschappen (KNAW), lid van Koninklijke Hollandsche Maatschappij der Wetenschappen (KHMW), vice-voorzitter van de Sociaal Wetenschappelijke Raad (SWR) en bestuurslid bij het Rathenau Instituut. Zij maakt deel uit van de redactie van het *Nederlands Juristenblad* en had van 2005-2009 zitting in het bestuur van de Nederlandse Juristenvereniging (NJV). Corien publiceert en doceert al jaren over onder meer privacy en gegevensbescherming. In 1995 werd onder haar leiding de Wet persoonsregistraties geëvalueerd.

Mevr. prof. mr. M. (Mireille) Hildebrandt is onderzoekshoogleraar bij de Faculteit Rechten & Criminologie, Vrije Universiteit Brussel en in deeltijd gewoon hoogleraar bij de Faculteit Natuurwetenschappen, Wiskunde en Informatica, Radboud Universiteit Nijmegen. Zij richt zich in Brussel, bij de onderzoeksgroep Law Science Technology & Society (LSTS) op kwesties rond 'Interfacing law and technology', en in Nijmegen, bij het institute for Computing and Information Sciences (iCIS) op 'Smart Environments, Data Protection and the Rule of Law'. Hildebrandt publiceert op het grensvlak van recht, kunstmatige intelligentie en techniekfilosofie, in 2015 gaf zij de Chorley Lecture bij de London School of Economics over 'Law *as* Information in the Era of Data-Driven Agency'. Haar laatste boek betreft 'Smart Technologies and the End(s) of Law'.

Dhr. prof. mr. T.F.E. (Eric) Tjong Tjin Tai heeft informatica gestudeerd aan de TU Delft en wijsbegeerte en rechten aan de Universiteit van Amsterdam. Na zes jaar werkzaam te zijn geweest als systeem-analist is hij overgestapt naar de advocatuur. Hij heeft gewerkt als cassatieadvocaat en in de ICT-IE praktijk bij Pels Rijcken & Droogleever Fortuijn. In 2007 promoveerde hij aan de Universiteit van Amsterdam op het proefschrift 'Zorgplichten en zorgethiek'. Sinds 2007 is hij werkzaam aan Tilburg University, vanaf 2010 als hoogleraar privaatrecht. Zijn onderzoek richt zich op service contracts, netwerken, ontwikkelingen rond data en Internet, burgerlijk procesrecht, en methodologie van (rechtsvergelijkend) doctrinair onderzoek.

Dhr. prof. mr. G-J. (Gerrit-Jan) Zwenne werd op 1 oktober 2011 benoemd tot hoogleraar recht en de informatiemaatschappij bij de afdeling eLaw@Leiden van de Universiteit Leiden en houdt zich vooral bezig met de toepassing en werking van de privacywet- en regelgeving, en met telecom- en internetrechtelijke vraagstukken. Gerrit-Jan is daarnaast advocaat bij het Amsterdamse kantoor Brinkhof. Verder is hij onder meer voorzitter van de Nederlandse Vereniging voor IT en Recht (NVvIR), bestuurslid van de Vereniging Privacy Recht (VPR), docent in de VIRA-Grotius opleiding voor ICT-recht advocaten; redacteur en auteur van Tekst & Commentaar Telecom- en privacyrecht en redacteur Sdu Monografieën ICT-recht. Hij maakte onder meer deel uit van de externe klankboordgroep van de Tijdelijke Commissie ICT-projecten ('Cie Elias'), die onderzoek deed naar mislukte overheids-ICTprojecten (kamerstukken II 2014/15, 33 326, nr. 5)

Dhr. prof. mr. A.H.J. (Aernout) Schmidt werkt sinds 1975 bij de Leidse Faculteit der Rechtsgeleerdheid, eerst als computerprogrammeur en sinds 1985 in wetenschappelijke functies. In zijn promotie-onderzoek (1987, "Pallas ex Machina") liet hij zien waarom een dynamisch kennissysteem beter dan stati(sti)sche modellen een ministerieel beleid kan beschrijven. In september 2003 benoemd als hoogleraar Recht en Informatica, is hij dat sinds maart 2010 onbezoldigd (emeritus). Zijn huidige aandacht gaat uit naar complexe, dynamische vraagstukken die in sociale systemen turbulentie veroorzaken, en naar de bijdragen die de rechtswetenschap (tezamen met andere disciplines) kan leveren om die turbulenties te domesticeren.

Inhoud

Privacy voor de homo digitalis[1]

Proeve van een nieuw toetsingskader voor gegevensbescherming in het licht van *big data* en *Internet of Things*

Lokke Moerel, Corien Prins

1. De auteurs bedanken Colette Cuijpers, Paul De Hert, Hielke Hijmans, Ronald Leenes en Nadya Purtova voor hun waardevolle commentaar op een eerdere versie.

"We cannot simply start by asking ourselves whether privacy violations are intuitively horrible or nightmarish. The job is harder than that. We have to identify the fundamental values that are at stake in the "privacy" question as it is understood in a given society. The task is not to realize the true universal values of "privacy" in every society. The law puts more limits on us than that: The law will not work *as law* unless it seems to people to embody the basic commitments of their society."

James Q. Whitman, The Two Western Cultures of Privacy: Dignity versus Liberty", *The Yale Law School Journal*, 2004, p. 1220.

1. Data-gedreven met de toekomst leven: inleiding en samenvatting

Stel dat een kennis u tijdens een gezellig avondje uit wijst op een App waarmee u aan de hand van uw verplaatsingen en belpatronen met een grote mate van zekerheid te weten kunt komen of u griep krijgt. Bovendien informeert de App u over – eveneens nog niet door griep getroffen – vrienden die u vooral moet ontwijken om te voorkomen dat u ziek wordt.[2] Gaat u deze applicatie zo snel mogelijk op uw smartphone installeren? Of wilt u toch maar liever niet data-gedreven uw kennelijke toekomst herschrijven?

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. Het doet bij sommigen waarschijnlijk de wenkbrauwen fronsen. Tegelijkertijd biedt een soortgelijke toepassing door bijvoorbeeld de Wereld Gezondheid Organisatie (**WHO**) belangrijke kansen om in specifieke gevallen burgers te behoeden voor gevaarlijke infectieziekten en pandemieën. Twee toepassingen van een applicatie waarmee persoonsgegevens voor hetzelfde doel worden verzameld, namelijk het in kaart brengen en persoonsgericht voorspellen van gezondheid en ziekte. Maar het oordeel dan wel gevoel bij de twee toepassingen pakt voor velen waarschijnlijk verschillend uit. Waar de commerciële toepassing niet, althans niet door iedereen, enthousiast zal worden verwelkomd, is de kans op een warm onthaal aanzienlijk groter wanneer de applicatie dienstbaar is aan het verbeteren van de wereldgezondheidszorg. Zelfs wanneer de WHO een commerciële partij zou inschakelen om deze service te verlenen.

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

2. Vgl. het onderzoek van MIT-hoogleraar Pentland en zijn groep, die door het analyseren van belgedrag en locatiegegevens met succes individuen wisten aan te wijzen die de griep hadden voordat zij zelf wisten dat ze ziek waren. Pentland, 2014, p. 173-176.

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. Toch redeneert de huidige privacywetgeving (de Wet bescherming persoonsgegevens, **Wbp**), primair vanuit het **doel** waarvoor de gegevens worden verzameld en verwerkt en veel minder vanuit het **belang** dat daarmee is gediend. Dat roept de vraag op of het huidig wettelijk regime nog wel effectief kan zijn en op legitimiteit kan rekenen. Het is deze vraag die leidend is voor de inzet van ons preadvies. Belangrijk daarbij is dat dit preadvies zich richt op de private sector en het door ons te ontwikkelen voorstel zich daarmee tot deze sector beperkt.[3]

Onze inzet komt er kort samengevat op neer dat een toets aan de hand van een gerechtvaardigd belang bij de verzameling en (verdere) verwerking van gegevens een effectievere privacybescherming oplevert die meer legitimiteit geniet dan een beoordeling zoals verlangd door het huidig wettelijk regime. Momenteel vindt de beoordeling primair plaats op basis van het doel waarvoor persoonsgegevens zijn verzameld, hetgeen concreet betekent: **a.** gegevens mogen alleen voor welbepaalde en rechtmatige doeleinden worden verzameld en verwerkt (*doelspecificatie*), en **b.** de gegevens mogen niet verder worden verwerkt indien dit onverenigbaar is met deze doeleinden (*verenigbaar gebruik*).[4] Ook het vereiste van *data minimalisatie* is verbonden aan het doel: niet meer gegevens mogen worden verwerkt dan noodzakelijk voor dit doel. In dit preadvies zullen wij betogen dat onder invloed van maatschappelijke ontwikkelingen en technologische mogelijkheden (zoals *big data* en het *Internet of Things*), doelbinding als separaat criterium zal moeten worden losgelaten. De tijd is gekomen om de gerechtvaardigd belang-grondslag aan te wijzen als de centrale (en enige) toets voor de verschillende fasen van de levenscyclus van persoonsgegevens: verzamelen, verwerken, verder verwerken en vernietigen van gegevens.[5] Dit voorstel houdt derhalve tevens in dat de andere wettelijke grondslagen voor de verwerking van persoonsgegevens (zoals

3. Zie over deze inperking nader: paragraaf 1.3.
4. Een eerste verkenning van dit voorstel is door ons gepubliceerd in IAPP Privacy Perspectives, "On the death of Purpose Limitation", te vinden op https://iapp.org/news/a/on-the-death-of-purpose-limitation/, en een uitgebreidere White Paper 'Further processing of data based on the legitimate interest ground: the end of purpose limitation?, te vinden op: https://www.tilburguniversity.edu/upload/bcbd911e-9902-485a-9de9-da88eae5042c_Prins_Moerel_Collection%20and%20further%20processing%20of%20data%20%28with%20foornotes%29%20doc.pdf. Dit preadvies betreft verder een uitwerking van eerdere kritiek op de huidige EU privacy wetgeving en voorstellen gedaan tot verbetering in: Moerel, 2014. Ten slotte is het preadvies mede geïnspireerd vanuit de in het WRR-rapport *iOverheid* ontwikkelde visie op de systeemverantwoordelijkheid van de overheid tegen de achtergrond van de ontwikkelingen in de informatiesamenleving. Zie: Wetenschappelijke Raad voor het Regeringsbeleid, 2011 en Broeders, Griffioen, Prins, 2012, p. 273-282.
5. Zie in deze zin eerder: Moerel, 2014, p. 51-54.

toestemming en uitvoering van overeenkomst – zie kader 1) als eigenstandige grondslagen komen te vervallen.

Achtergrond – huidig wettelijk kader

Op dit moment dient de verantwoordelijke niet alleen het doel van de gegevensverwerking vast te stellen en te specificeren, maar ook een rechtmatige grondslag voor de gegevensverwerking te hebben. De wet kent een limitatief aantal grondslagen. Eén daarvan is de grondslag van gerechtvaardigd belang. Omdat het systeem gecompliceerd is hebben we hierna de afzonderlijke toetsen op een rij gezet die dienen plaats te vinden om de rechtmatigheid van een gegevensverwerking te beoordelen:

(i) er dient sprake te zijn van een uitdrukkelijk omschreven en rechtmatig doel (*doelspecificatie*)[6]
(ii) er mogen niet meer gegevens worden verzameld (en langer worden bewaard) dan nodig voor dat doel (*data minimalisatie*);[7]
(iii) er dient sprake te zijn van een *grondslag voor de verwerking* (zie hierna)
(iv) voor *bijzondere persoonsgegevens*: dient een specifieke grondslag voor verwerking te bestaan;[8] en
(v) de verdere verwerking van de gegevens mag niet onverenigbaar zijn met het oorspronkelijke doel van verzameling (*verenigbaar gebruik)*.[9]

(iii) – *grondslag* voor de verwerking.[10]
De wet kent momenteel – limitatief – de volgende grondslagen (waarvan de **vetgedrukte** primair relevant zijn voor de private sector):

a. toestemming betrokkene
b. uitvoering van de overeenkomst
c. nakomen wettelijke verplichting
d. vitaal belang betrokkene
e. goede vervulling publiekrechtelijke taak
f. behartigen *gerechtvaardigd belang*

Zie kader 2 voor een uitwerking van de gerechtvaardigd belang-grondslag.

Kader 1

6. Artikel 6(1)(b) Privacy Richtlijn en artikel 7 Wbp; vergelijk art. 5(1)(b) Verordening Gegevensbescherming.
7. Artikel 6(1)(c) en (e) Privacy Richtlijn en artikel 11(1) Wbp; vergelijk art. 5(1)(c) en (e) Verordening Gegevensbescherming.
8. Artikel 8 Privacy Richtlijn en artikelen 16 – 23 Wbp; vergelijk artikel 9 Verordening Gegevensbescherming.
9. Artikel 6(1)(b) Privacy Richtlijn en artikel 9 Wbp; vergelijk artikelen 5(b) en 6(4) Verordening Gegevensbescherming.
10. Artikel 7 Privacy Richtlijn en artikel 8 Wbp; vergelijk artikel 6 Verordening Gegevensbescherming.

Overigens blijven de overige bestaande beginselen en grondslagen in ons voorstel wel relevant, maar dan als onderdeel van de gerechtvaardigd belang-toets. Zo behoudt het beginsel van databeperking (of *data minimalisatie*) zijn rol. Immers, ook nu al is dit beginsel onderdeel van de gerechtvaardigd belang-toets, namelijk via het proportionaliteitsbeginsel.[11] Data minimalisatie brengt mee dat niet meer gegevens mogen worden verzameld en verwerkt dan noodzakelijk voor het betreffende gerechtvaardigde belang. Hetzelfde geldt voor de grondslagen toestemming en uitvoering overeenkomst. Deze zullen niet langer als zelfstandige grondslagen voor de verwerking van gegevens gelden, maar zullen in ons voorstel een factor zijn bij de beoordeling van de vraag of sprake is van een gerechtvaardigd belang. Het enkel vragen van toestemming is onvoldoende, maar toestemming (*opt-in* of *opt-out*) kan wel een sluitstuk zijn bij de afweging of er aan de gerechtvaardigd belang-grondslag is voldaan. Ook het bestaan van een contractuele relatie is één van de factoren die een rol speelt bij de afweging. Relevant kunnen hierbij zijn: de status van het individu (betreft het een werknemer of een consument), de status van de verantwoordelijke (bijv. is dit een bedrijf met een machtspositie of betreft het een werkgever in diens relatie met een werknemer), en de implicaties voor het individu (die mogelijk groter kunnen zijn bij contractuele afhankelijkheid). Daarbij zou kunnen gelden dat hoe specifieker de contractuele relatie is, hoe meer beperkingen er zullen zijn voor het gebruik van de gegevens. We zullen hierna zien dat dit afwijkt van de huidige situatie waarbij de contractuele grondslag vaak ten onrechte worden gebruikt voor verwerkingen die niet aan de gerechtvaardigd belang-grondslag voldoen.

Kortom, anders dan door sommigen mogelijk wordt gedacht, betekent ons voorstel niet dat per definitie meer gegevens dan momenteel het geval is mogen worden verwerkt en dat aan het huidige beschermingsniveau afbreuk wordt gedaan.[12] Het kan namelijk zomaar zijn dat wanneer het data minimalisatie-beginsel wordt gerelateerd aan het belang bij het verzamelen en verwerken (denk aan het belang in het gegeven voorbeeld van de commerciële gezondheids-App), dit ertoe leidt dat juist minder gegevens mogen worden verzameld en verwerkt of dat in voorkomend geval in het geheel geen gegevens mogen worden verwerkt. In het onderstaande betoog werken we dit voorstel nader uit. Als onderdeel daarvan presenteren we eveneens voorstellen hoe om te gaan met **a.** de wettelijke vereisten voor

11. WP Opinie 06/2014, p. 33.
12. Zie onder meer de brief van de voorzitter van de privacytoezichthouder van 3 september 2015. Zie echter de (ontkennende) reactie van de minister van Veiligheid & Justitie bij brief van 7 oktober 2015 (Kamerstukken II, 2015/16, nr. 31761, nr. 88).

transparantie (informatieplichten en inzagerechten), **b.** de overige voor de private sector relevante grondslagen voor verwerking (zoals toestemming en uitvoering overeenkomst), **c.** het speciale regime voor de verwerking van bijzondere gegevens, en **d.** de kwaliteit van gegevens.

Ook hechten wij eraan hier in deze Inleiding al uitdrukkelijk te vermelden dat wij geen voorstander zijn van een zogenaamd *use based* system. In een dergelijk systeem wordt het verzamelen van gegevens vrij gelaten, en uitsluitend het gebruik daarvan gereguleerd.[13] Vooral in de Amerikaanse jurisdictie wordt dit systeem als de aangewezen aanpak voor regulering gezien, nu het in onze datagedreven samenleving niet langer mogelijk lijkt alle vormen van gegevensverwerking te reguleren. De gedachte is dat de wetgever geen rol heeft bij het stellen van voorwaarden aan het verzamelen en combineren van data, maar pas normstellend optreedt in de gevallen dat gegevens worden gebruikt op een wijze die als misbruik moet worden gekwalificeerd. Deze benadering sluit aan bij de regulering van reclame-uitingen: het maken van reclame in principe is toegestaan, maar misleidende reclame wordt gesanctioneerd. Hoewel er veel voor een dergelijk systeem is te zeggen,[14] dient in onze visie ook het verzamelen van gegevens als zodanig te blijven gereguleerd. Zonder nadere normering van ook het verzamelen van gegevens, zouden we al snel terechtkomen in een situatie waar overheden en bedrijven ongebreideld gegevens verzamelen, bijvoorbeeld door het plaatsen van *sniffers* op telecomnetwerken met als rechtvaardiging dat de gegevens wellicht in de toekomst nog van nut kunnen zijn. Ook het verzamelen van gegevens zal kortom aan de door ons nader uit te werken gerechtvaardigd belang-toets dienen te voldoen.

Met de geformuleerde ambitie kent dit preadvies een tweeledige doelstelling. Ten eerste verkennen en duiden we innovatie in gegevensgebruik, meer in het bijzonder in de private sector en de wisselwerking tussen de geschetste ontwikkelingen en privacy. We beogen de NVJ-leden die meer algemeen in de privacy-thematiek zijn geïnteresseerd een beeld van de huidige ontwikkelingen te bieden. Ten tweede ambiëren we een meer specifieke bijdrage te leveren aan het debat over effectiviteit en legitimiteit van gegevensbescherming. Aldus willen we ook de privacy-specialisten onder de NJV het nodige bieden. We doen dit door te bepleiten dat de zgn. gerechtvaardigd belang-grondslag (zie kader 2) centraal dient te staan bij het oordeel over de rechtmatigheid van een gegevensverwerking.

13. Zoals lijkt te worden voorgesteld in het World Economic Forum Report, 2013 en verder door de Senior Advisor van de CEO van Microsoft, Mundie (Mundie, 2014).
14. Zie over de verschillen en de voor- en nadelen van de Europese ‘rights-based’ en Amerikaanse ‘harm-based’ benadering in de privacycontext: Moerel 2014, p. 25-36.

Achtergrond – de gerechtvaardigd belang-grondslag

Conform het huidig wettelijk kader[15] mogen persoonsgegevens worden verwerkt indien de verwerking "noodzakelijk is voor de behartiging van een gerechtvaardigd belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert."
De toets om te kijken of een gegevensverwerking kan worden gestoeld op deze grondslag bestaat dus uit drie stappen:

– Heeft de verantwoordelijke (of een derde) een gerechtvaardigd belang?
– Is de gegevensverwerking noodzakelijk voor dat gerechtvaardigde belang? Anders geformuleerd: kan het betreffende belang anderszins of met minder ingrijpende middelen worden gediend? Zo ja, dan dient deze minder ingrijpende weg te worden gevolgd?
– Weegt het belang van de betrokkene bij bescherming van diens privacy zwaarder dan het belang van de verwerker?

De toets komt daarmee in essentie neer op een belangenafweging, welke – aldus de Europese Artikel 29 Werkgroep (**WP 29**)[16] – geen 'recht door zee'-belangenafweging is, maar een contextuele analyse waarbij diverse factoren dienen te worden afgewogen, waaronder de aard van de verwerkte gegevens (gevoelig of niet), de wijze waarop de gegevens worden verwerkt (betreft het grote hoeveelheden, worden gegevens gecombineerd met andere gegevens), de redelijke verwachtingen van degene van wie gegevens worden verwerkt, de positie van verantwoordelijke en het individu en hun onderlinge machtsverhouding, en verder de maatregelen die de verantwoordelijke heeft getroffen om de impact op de privacy van de betrokken individuen te beperken, zoals data minimalisatie en technische maatregelen zoals encryptie en pseudonimisatie.[17]

Kader 2

15. Zie artikel 7(f) Privacy Richtlijn en artikel 8(f) Wbp; vgl artikel 6(f) Verordening Gegevensbescherming. Het nieuw voorgestelde artikel 6(f) wijkt op een aantal punten af van artikel 7(f) Privacy Richtlijn, deze afwijkingen zijn echter niet zodanig dat onze verwachting is dat toepassing van de test anders uit zal vallen. Zie over de verschillen: Cuijpers, Purtova, Kosta, 2014, p. 4.
16. Deze werkgroep (hierna **WP 29**) bestaat uit vertegenwoordigers van de nationale toezichthouders en de European Data Protection Supervisor en heeft conform de Privacy Richtlijn onder meer de taak de bepalingen van de Richtlijn nader te duiden. Onder de Verordening verandert de aanduiding in European Data Protection Board (**EDPB**).
17. De WP29 geeft de volgende samenvatting van de gerechtvaardigd belang-toets:
"Applying the balancing test
When interpreting the scope of Article 7(f), the Working Party aims at a balanced approach, which ensures the necessary flexibility to data controllers for situations where there is no undue impact on data subjects, while at the same time providing sufficient legal certainty and guarantees to data subjects that this open-ended provision will not be misused. →

→ To carry out this balancing test, it is first important to consider the nature and source of the legitimate interests, and whether the processing is necessary to pursue those interests, on the one hand, and the impact on the data subjects on the other hand. This initial assessment should take into account the measures, such as transparency or limited collection of data that the controller plans to adopt to comply with the Directive.
After analysing and weighing the two sides against each other, a provisional 'balance' may be established: a preliminary conclusion may be drawn as to whether the legitimate interests of the controller prevail over the rights and interests of the data subjects. There may however be cases where the outcome of the balancing test is unclear, and there is doubt on whether the legitimate interest of the controller (or third party) prevails and whether the processing can be based on Article 7(f).
For this reason, it is important to carry out a further assessment in the balancing exercise. In this phase, the controller may consider whether it is able to introduce additional measures, going beyond compliance with other horizontal provisions of the Directive, to help protect data subjects. Additional measures may include, for example, providing an easily workable and accessible mechanism to ensure an unconditional possibility for data subjects to opt-out of the processing.
Key factors to be considered when applying the balancing test
- the nature and source of the legitimate interest, including:
  - whether the data processing is necessary for the exercise of a fundamental right, or
  - is otherwise in the public interest or benefits from social, cultural or legal/regulatory recognition in the community concerned;
- the impact on the data subjects, including:
  - the nature of the data, such as whether the processing involves data that may be considered sensitive or has been obtained from publicly available sources;
  - the way data are being processed, including whether the data are publicly disclosed or otherwise made accessible to a large number of persons, or whether large amounts of personal data are processed or combined with other data (e.g. in case of profiling, for commercial, law enforcement or other purposes);
  - the reasonable expectations of the data subject, especially with regard to the use and disclosure of the data in the relevant context;
  - the status of the data controller and data subject, including the balance of power between the data subject and the data controller, or whether the data subject is a child or otherwise belongs to a more vulnerable segment of the population.
- additional safeguards to prevent undue impact on the data subjects, including:
  - data minimisation (e.g. strict limitations on the collection of data, or immediate deletion of data after use);
  - technical and organisational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation');
  - extensive use of anonymisation techniques, aggregation of data, privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments; increased transparency, general and unconditional right to opt-out, data portability & related measures to empower data subjects.

Accountability, transparency, the right to object and beyond
- In connection with these safeguards – and the overall assessment of the balance – three issues often play a crucial role in the context of Article 7(f) and therefore require special attention:
- the existence of some and possible need for additional measures to increase transparency and accountability;
- the right of the data subject to object to the processing, and beyond objection, the availability of opt-out without the need for any justification; →

1.1 Gebrek aan effectiviteit en legitimiteit

Een vijftal pijlers draagt ons betoog en de daarin gepresenteerde voorstellen. Voor een belangrijk deel hebben deze te maken met de overtuiging dat de huidige benadering bij de bescherming van persoonsgegevens het draagvlak voor deze wettelijke regels ondermijnt. Enerzijds worden veel gegevens verwerkt in strijd met toepasselijke wetgeving waarbij niet handhavend wordt opgetreden terwijl burgers wel bezwaar tegen deze vormen van verwerking blijken te hebben.[18] Anderzijds verbiedt het huidige wettelijk kader het gebruik van persoonsgegevens voor bepaalde doeleinden, terwijl dit gebruik een duidelijke maatschappelijke waarde heeft[19] en de risico's zodanig beperkt zijn, dat dit gebruik toelaatbaar zou moeten zijn. Het huidig wettelijk systeem sluit met andere woorden onvoldoende aan bij de realiteit van alledag om nog effectief te kunnen zijn en daarmee op legitimiteit te kunnen rekenen.

De **eerste pijler** van onze benadering vormt de constatering dat persoonsgegevens in het verleden een bijproduct waren van het doel waarvoor zij werden verzameld, maar dat dit door de technologische ontwikkelingen lang niet meer altijd het geval is. Om dit punt te verduidelijken geven we allereerst een voorbeeld waarbij gegevens een bijproduct zijn. Wanneer we bij een reisbureau een vlucht boeken, worden we gevraagd naar naam, adres, geboortedatum en rekeningnummer. Met behulp van deze gegevens kan het reisbureau de geboekte vlucht naar wens laten uitvoeren. Daarmee vormen de persoonsgegevens primair een bijproduct van het doel waarvoor ze worden verzameld (de dienst van het boeken van de vlucht). In deze situatie vormt het wettelijk vereiste van doelbinding een op voorhand beperkende test om te bepalen welke gegevens dan voor de uitvoering van deze dienst mogen worden verzameld. Het vragen naar de geloofsovertuiging van de reiziger is niet nodig voor het boeken van de vlucht en dus niet toegestaan. Kenmerkend voor ontwikkelingen als big data en het Internet of Things is echter dat gegevens lang niet meer altijd worden verzameld als bijproduct van een doel.[20] In tegendeel, ze worden juist verzameld om vervolgens daarmee de dienst te leveren. Illustratief is de verzekeringsbranche waar via kastjes in auto's gegevens worden

→ • empowering data subjects: data portability and the availability of workable mechanisms for the data subject to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data."

18. Zie over het (relatief lage) vertrouwen van burgers in commerciële bedrijven voor wat betreft de omgang met hun persoonsgegevens, de TNO-survey uit 2015: TNO 2015.
19. Zie voor tien, specifiek voor Nederland, in kaart gebrachte big data-oplossingen met maatschappelijke impact: De Nationale Denktank Eind Rapport, 2014. Zie voor bredere voorbeelden: World Economic Forum Report, 2013; OESO, 2014.
20. Wij gaan in paragraaf 1.2 nader op beide ontwikkelingen in.

verzameld. Deze gegevens worden geanalyseerd om op basis daarvan nieuwe verzekeringsproducten te ontwikkelen.[21] In tegenstelling tot het bovenstaande voorbeeld van het reisbureau, brengen verzekeraars als eerste stap vele gegevens bijeen, om eerst op basis van de gevonden correlaties nieuwe producten te ontwikkelen en aan te bieden. Het gestelde doel is daarmee niet langer op voorhand beperkend voor zowel aard als omvang van de gegevens die worden verwerkt. In dit geval is het doel van de gegevensverzameling het benutten van de gegevens zelf en niet een afgeleide van een dienst (boeken van reizen) die met het gegevensgebruik als zodanig niets van doen heeft. Zolang het doel niet samenvalt met het verwerken van gegevens kan het doelbindingsbeginsel een beperkende test zijn. Zo mogen gegevens verstrekt voor het boeken van een reis niet voor een ander doel worden gebruikt. Maar als gegevensverzameling en analyse zelf het doel zijn, is doelbinding niet langer betekenisvol. Zeker nu de verantwoordelijke zelf het doel mag bepalen en een commercieel belang bij dat doel heeft. In onze ogen zou de toets moeten zijn of er een 'gerechtvaardigd belang' is bij de gegevensverwerking. Niet alleen zullen verantwoordelijken het **belang** bij de verwerking moeten expliciteren. Ook moeten zij aantonen dat het – gegeven de context – om een **gerechtvaardigd** belang gaat. Daarbij komt het aan op een weging tussen de verschillende belangen die aan de orde zijn, waaronder niet alleen de commerciële belangen van de verantwoordelijke maar ook de belangen voor en van de samenleving. Een blik op baanbrekende recente jurisprudentie van het EU Hof van Justitie, in het bijzonder de zaak *Google Spain*, toont dat bedrijven inmiddels wordt opgedragen een brede afweging van belangen te maken.[22]

De **tweede pijler** is de overtuiging dat we af moeten van de gedachte dat verwerkers van gegevens (in de terminologie van de wet: *verantwoordelijken*) rechtmatig handelen door individuen te informeren en hen te laten klikken op "OK", terwijl we tegelijkertijd vaststellen dat voor de betreffende gegevensverwerking geen zorgvuldige weging van de verschillende belangen heeft plaatsgevonden. De privacywetgeving dient zijn grensstellend karakter te hervinden nu het is verworden tot wat we hierna zullen aanduiden als 'mechanisch proceduralisme', waarbij verantwoordelijken mechanisch individuen informeren en hun toestemming verzamelen, zonder daadwerkelijke privacybescherming te bieden.

De **derde pijler** is de constatering dat het individu steeds zichtbaarder wordt, behalve voor zichzelf.[23] De realiteit van onze huidige datagedreven samenleving is dat individuen veelal niet weten welke gegevens er over hen

21. Zie hierover uitgebreid paragraaf 2.3.1. Tevens: Verbond van Verzekeraars, 2014.
22. Zaak C-131/12 Google Spain and Google Inc, 13 mei 2014, EU:C:2014:317. Zie: Hijmans, 2014.
23. Zie WRR, 2011.

worden verwerkt, op welke wijze ze door verwerkers worden beoordeeld en getypeerd en wat daarvan voor hen de gevolgen zijn.[24] Dit ondanks de wettelijke informatieverplichtingen die er op de verantwoordelijke rusten[25] en de rechten van individuen op inzage, correctie, etc.[26] In het huidige regime worden de informatierechten als hoeksteen van de privacywetgeving beschouwd, waarbij de aanname is dat een individu zijn rechten pas kan uitoefenen als hij/zij ook weet dat er gegevens over hem/haar worden verwerkt en door wie.[27] De Europese Verordening Gegevensbescherming[28] gaat voort op deze weg: "Individuals should have control over their own personal data"[29] en versterkt daartoe de informatie- en de toestemmingsvereisten.[30] Onze constatering is dat de informatieverplichtingen zoals die nu gelden niet werken. Hoewel de aankomende Verordening vele verbeteringen kent waarbij verantwoordelijken meer verplichtingen krijgen om de privacy-implicaties vooral bij aanvang van de verwerkingen te beperken,[31] zal de daarin opgenomen verzwaring van de informatie- en de toestemmingsvereisten individuen geen betere positie geven, laat staan een gevoel van controle over hun gegevensverwerkingen.[32] De onderliggende

24. Zie TNO, 2015, p. 35. Dit probleem wordt overigens ook onderkend door de Europese Commissie, 2012, p. 4, als wordt geconstateerd dat Europese burgers "feel they are not in control of their data. They are not properly informed of what happens to their personal information to whom it is transmitted and for what purposes. Often, they do not know how to exercise their rights online."
25. Zie voor de informatieverplichtingen van de verantwoordelijke, de artikelen 33-34 Wbp.
26. Zie artikelen 35-41 Wbp.
27. Zie Considerans 38 Privacy Richtlijn en de toelichting op de Privacy Richtlijn van Dammann, Simitis, 1997, p. 179.
28. Op het moment van de afronding van dit preadvies (31 december 2015) bevond het wetgevingsproces zich in de laatste fase. Begin december 2015 werd tijdens de trialoog tussen de Raad, het Europees Parlement en de Commissie overeenstemming over de tekst bereikt. Twee jaar na de datum waarop de Verordening wordt vastgesteld verkrijgt deze rechtstreekse werking (naar verwacht zullen de nieuwe bepalingen daarmee begin 2018 van kracht worden). Wij baseren ons in dit preadvies op de tekst waarover tijdens de trialoog overeenstemming werd bereikt. Deze versie volgt nog de nummering van het oorspronkelijke voorstel van de Commissie, waarbij later toegevoegde artikelen geen nieuw nummer hebben gekregen en geschrapte artikelen nog een nummer hebben. In de definitieve versie van de Verordening zullen de artikelen opnieuw doorgenummerd worden. Deze nummering was bij de afsluiting van het preadvies nog niet beschikbaar.
29. Zie Considerans 6 Verordening Gegevensbescherming; zie verder Commission Communication on the Proposed Regulation, 2012, p. 2: "In this new digital environment, individuals have the right to enjoy effective control over their personal information".
30. Commission Communication on the Proposed Regulation, 2012, p. 6; Considerans 6 Verordening Gegevensbescherming.
31. Zie bijvoorbeeld artikel 12(1) Verordening Gegevensbescherming dat verantwoordelijken specifiek verplicht de aldaar genoemde informatie te communiceren "in a concise, transparent, intelligible and easily accessible form, using clear and plain language" en in artikel 12(4b) het gebruik van standaard icons aanmoedigt.
32. Zie eerder : Moerel, 2014, p. 47-50 en verwijzingen naar relevante literatuur aldaar. Daaraan kan inmiddels worden toegevoegd: Solove, 2013, p. 1880-1888; Koops, 2014; Van Alesenoy, Kosta, Dumortier, 2014, paragraaf 3; Milne, Culnan, 2004.

logica van de gegevensverwerking en de doeleinden waarvoor deze worden toegepast, zijn inmiddels dusdanig gecompliceerd dat het beschrijven daarvan ingewikkelde *privacy policies* oplevert die voor de gemiddelde burger wat betreft zowel inhoud als lengte gewoonweg niet behapbaar zijn. En dus worden ze ook niet gelezen.[33] Deze complexiteit maakt individuen machteloos en murw, met als resultaat dat velen bij online diensten klakkeloos op "OK" klikken. Ieder van ons zal het herkennen. Verzwaren van de informatie- en toestemmingseisen zal daarom niet helpen. Integendeel, het levert nog meer ondoorgrondelijke informatie op, die nog minder zal worden gelezen.[34] Het is een illusie te denken dat door individuen beter te informeren over welke gegevens voor wat voor doeleinden worden verwerkt, we ze in staat stellen rationele keuzes te maken en hun rechten uit te oefenen.[35] De realiteit is verder dat verantwoordelijken soms welbewust de regels ondermijnen, door op een ondoorgrondelijke manier aan de informatievereisten te voldoen, of het verkrijgen van benodigde toestemmingen zo in te richten dat individuen worden ontmoedigd om hun echte voorkeuren te bepalen en veelal zijn genoodzaakt op 'OK' te klikken.[36] We moeten daarom af van het huidige systeem waarbij de veronderstelling is

33. Het World Economic Forum Report, 2013, p. 11 rapporteert dat: "The torrent of data being generated from and about data subjects imposes an undue cognitive burden on individual data subjects. Overwhelming them with notices is ultimately disempowering and ineffective in terms of protection – it would take the average person about 250 working hours every year, or about 30 full working days – to actually read the privacy policies of the websites they visit in a year." Uit de TNO-survey komt naar voren dat de helft van de respondenten de privacyvoorwaarden niet leest. Van hen vindt 53,5% ze 'te lang', 24,5% 'te moeilijk' en 16,6% meent dat ze beter anders weergegeven kunnen worden. Zie ook de overeenkomstige uitkomsten van een onderzoek onder EU burgers naar vertrouwen in big data-toepassingen: Vodafone Institute, 2016.
34. Zie over het dilemma dat als je de informatie korter maakt, burgers niet goed zijn geïnformeerd en als je de informatie langer maakt deze niet meer wordt gelezen, Koops 2014, p. 4: "Consent supporters focus on finding ways to make consent both more practical, e.g., using short texts and icons, and more meaningful, e.g., using plain language and technically enforcing that people actually see the text before ticking a box. However, they ignore the trade-off between practical consent and meaningful consent: the simpler you make the consent procedure, the less will users understand what they actually consent to; and the more meaningful you make the consent procedure (providing sufficient information about what will happen with the data), the less convenient the consent will become".
35. Zo de minister van Economische Zaken in de brief over Big Data en Profilering: "*Irrationeel gedrag* tenslotte, zorgt ervoor dat de burger zelf niet altijd een rationele afweging maakt, onder andere als gevolg van haast, een korte-termijn horizon of onvoldoende kennis. De lange en veelal complexe privacy-overeenkomsten waarmee gebruikers van diensten vaak instemmen zonder ze te lezen vormen een voorbeeld." Kamerstukken II, 2014/15, 32761, nr. 78, p. 4.
36. Een typerend voorbeeld hiervan is de huidige wijze waarop verantwoordelijken invulling geven aan hun verplichting om toestemming te verkrijgen voor het plaatsen van cookies. Leenes, Kosta (2015). We gaan hier in paragraaf 3.2 en 4.3 uitgebreider op in.

dat handhaving toch primair door individuen zelf zal moeten plaatsvinden (vanuit het uitgangspunt dat ze zijn geïnformeerd en rechten hebben).[37,38] Natuurlijk hebben individuen de mogelijkheid zelf voor hun privacybelangen op te komen en dient het transparantiebeginsel hen daartoe te faciliteren. Maar zoals wij in het navolgende zullen betogen: ten onrechte ligt de handhavingsopdracht momenteel primair bij individuen. De realiteit van onze datagedreven samenleving is dat zij hier, ondanks de hen toegekende rechten, nauwelijks toe in staat zijn. We zullen de verantwoordelijkheid voor handhaving daarom op andere manieren moeten beleggen en andere instrumenten moeten implementeren. Zo moeten verantwoordelijken worden verplicht hun verwerkingen *privacy-by-design*[39] in te richten waardoor de privacy-implicaties van de verwerking al bij aanvang worden gemitigeerd en het niet primair de burger is op wiens bord de handhavingsopdracht – via het uitoefenen van zijn rechten – ligt.[40] Waar opportuun zal de wetgever de verplichtingen om de technische infrastructuur privacy-by-design in te richten overigens niet uitsluitend moeten beleggen bij de verantwoordelijken voor de gegevensverwerking (die een eigen commercieel belang hebben bij de verzameling en verwerking van gegevens). Deze verantwoordelijkheid zal tevens moeten gelden voor bijvoorbeeld de leveranciers van de infrastructuur of onderdelen daarvan, die geen eigen belang hebben bij het omzeilen van de regels.

Een relevante mitigerende factor bij de beoordeling van de gerechtvaardigd belang-grondslag zal verder zijn in hoeverre de verantwoordelijke het individu daadwerkelijk *controle* over zijn of haar gegevens biedt. Ook zul-

37. World Economic Forum Report, 2013, p. 17, acht het beginsel van 'notice and consent' kandidaat voor hervorming: "In particular, reliance on mechanisms of "notice and consent" to ensure individual participation is seen as increasingly anachronistic. The current manifestation of the principles through notice and consent as a binary, one-time only involvement of the individual at the point of data collection was identified in the dialogue as an area ripe for reconsideration to better empower individuals, build trust in the system, and encourage the reliable, predictable and more valuable flow of data into and within the system."
38. Met Koops, 2014, p. 3, verbazen wij ons erover dat de meeste auteurs die constateren dat burgers de informatie niet begrijpen en klakkeloos toestemming geven, vervolgens niet de voor de hand liggende conclusie trekken dat de grondslag van toestemming dus moet worden afgeschaft. In tegendeel. Veelal worden juist voorstellen gepresenteerd om de informatievereisten te verbeteren en ook de toestemmingsvereisten te versterken of zelfs uit te breiden.
39. Privacy-by-design impliceert dat de naleving en handhaving van wettelijke normen onderdeel is van het technisch ontwerp. We komen hier later in dit preadvies op terug.
40. Zie in vergelijkbare zin: Nissenbaum, 2011, p. 32-48; Tene, Polonetsky, 2012, paragraaf 1: "In the context of online privacy, this implies emphasis should be placed less on notice and choice and more on implementing policy decisions with respect to the utility of given business practices and on organizational compliance with fair information principles (FIPs). In other words, the focal point for privacy should shift from users to (a) policymakers or self-regulatory leaders to determine the contours of accepted practices; and (b) businesses to handle information fairly and responsibly."

len verantwoordelijken over de door hen gemaakte afwegingen en keuzes transparant moeten zijn en hier verantwoording over af moeten leggen.[41] Een belangrijk rol zien wij hier weggelegd voor de in paragraaf 5.2 nader te bespreken Data Protection Impact Assessment (**DPIA**). De Verordening zal op deze punten substantiële verbeteringen brengen,[42] maar gaat, zoals wij nader toelichten, op onderdelen niet ver genoeg.[43]

De **vierde pijler** onder ons voorstel is de constatering dat het regime voor bijzondere persoonsgegevens (medische gegevens, geloof, ras, etc.) niet meer zinvol is. Steeds minder is op voorhand duidelijk of gegevens (als zodanig) gevoelig zijn. Veeleer gaat het om gebruik dat gevoelig is. Bedrijven en overheid benutten in aanleg 'onschuldige' gegevens (die deels beschikbaar zijn in het publieke domein) om tot onderscheidingen (discriminatie) tussen individuen te komen die bijzonder gevoelig kunnen zijn. Een bekend voorbeeld is de Target-kwestie, waarbij de Amerikaanse supermarktketen Target op basis van big data-analyse reclameaanbiedingen stuurde voor babyproducten aan vrouwen die ineens geurloze cosmeticaproducten gingen kopen. De data-analyses toonden namelijk een verband tussen het kopen van die producten en zwangerschap. In feite ging het hier om het gebruik van in aanleg onschuldige gegevens, maar vertelde het resultaat van dat gebruik iets over de gezondheid van een individu, namelijk zwangerschap. Dat dit gevoelig kan liggen, blijkt uit het feit dat door de vader van een tienerdochter een klacht tegen Target werd ingediend over de reclame-uitingen. Later bleek overigens het meisje inderdaad zwanger.[44]

Andersom zijn er genoeg voorbeelden van bijzondere persoonsgegevens die voor het doel waarvoor ze worden verwerkt niet gevoelig zijn, waarmee 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

41. Zie WRR, 2011; Moerel 2014, p. 60.
42. Zo verplicht de Verordening verantwoordelijken om verwerkingen *privacy-by-design* in te richten (artikel 23); geeft deze een algemene *accountability* verplichting om de noodzakelijke technische en organisatorische maatregelen te treffen om nakoming van wettelijke verplichtingen te verzekeren, deze periodiek te herzien en de getroffen maatregelen op verzoek aantoonbaar te maken (artikel 22) en bij verwerkingen die mogelijk een hoog risico voor privacy hebben een Data Protection Impact Assessment (**DPIA**) te verrichten (artikel 33).
43. Artikel 33 Verordening ziet alleen op verwerkingen die een hoog risico voor privacy hebben en verplicht verantwoordelijken niet de DPIA (of in ieder geval de gemaakte keuzes en afwegingen daaromtrent) openbaar te maken. De Verordening bevat verder geen verplichting voor leveranciers van software en infrastructuur waarmee gegevens worden verwerkt om hun producten privacy-by-design in te richten. Overweging 61 bevat wel een aanbeveling aan de lidstaten om deze producenten "hiertoe aan te moedigen".
44. Duhigg, 2012.

geaardheid van de betreffende persoon blijkt. Voor verantwoordelijken is het toepassen van het speciale regime voor alleen die gegevens niet intuïtief. Met de toepassing van de door ons voorgestelde gerechtvaardigd belang-toets is het speciale regime voor bijzondere persoonsgegevens (medische gegevens, geloof, ras, etc.) niet langer nodig. De aard van de gegevens en het potentiële gebruik daarvan zullen factoren zijn bij de beoordeling of sprake is van een gerechtvaardigd belang voor de verzameling en het gebruik, als ook welke mitigerende maatregelen door de verantwoordelijke in dat verband dienen te worden getroffen om het effect op de privacy te beperken.

De **vijfde pijler** onder ons voorstel is ten slotte de constatering dat het huidige systeem voor de beoordeling van gegevensverwerkingen te gecompliceerd is voor verantwoordelijken om toe te passen. 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.[45] 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 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. Ten opzichte van de diverse toetsen die momenteel doorlopen moeten worden (zie hiervoor, kader 1), betekent dit een aanzienlijke vereenvoudiging van het wettelijk toetsingskader voor de rechtmatigheid van de verwerking.

45. Koops, 2012, p. 5.

Achtergrond – ons voorstel.

Zeer verkort weergegevens bepleiten wij dat komen te vervallen:
- het vereiste van doelbinding zoals dat nu geldt;
- de andere wettelijke grondslagen voor de verwerking van persoonsgegevens (zoals toestemming en uitvoering van overeenkomst). Toestemming en het bestaan van een contractuele relatie zullen een factor zijn bij de beoordeling van de vraag of sprake is van een gerechtvaardigd belang;
- de aparte grondslagen voor bijzondere gegevens; de gevoeligheid van zowel de gegevens als het gebruik daarvan zal een factor zijn bij de beoordeling of sprake is van een gerechtvaardigd belang bij de verwerking;
- de toets van verenigbaar gebruik voor de verdere verwerking van gegevens.

Kader 3

Is ons voorstel achterhaald met de Verordening Gegevensbescherming?

Wij realiseren ons dat over de uiteindelijke tekst van de Verordening Gegevensbescherming inmiddels overeenstemming is bereikt en onze voorstellen daarop geen invloed meer kunnen uitoefenen. Bovendien strookt ons voorstel om het criterium van doelbinding te verlaten niet met het EU Handvest, nu het criterium daarin is vastgelegd en loslaten een verdragswijziging vereist. Toch denken we dat de uitgewerkte gedachten en het concrete voorstel dat wij aan het slot van het preadvies presenteren relevant zijn. Allereerst verwachten wij, zoals we in paragraaf 5 en 6 nader zullen betogen, dat op de langere termijn het normerend kader zich langs de door ons geschetste lijnen zal gaan ontwikkelen. Maar ook op de kortere termijn is de door ons uitgewerkte toets relevant. We zullen zien dat juist de toets voor de rechtmatigheid van de **verdere** verwerking van gegevens (kortom, het bij big data en Internet of Things zo cruciale **hergebruik** van gegevens) steeds crucialer wordt. In de Verordening zijn de criteria die bij deze toets moeten worden gehanteerd vastgelegd.[46] Het betreft, zoals we in paragraaf 4.1. aantonen, nagenoeg dezelfde criteria die de WP29 al eerder had geformuleerd. En deze criteria overlappen op hun beurt weer nagenoeg met de criteria die de WP29 opstelde voor de beoordeling van de gerechtvaardigd belang-grondslag. Het betreft telkens een beoordeling van de verwerking in de betreffende context (gegeven de betrokken belangen die aan de orde zijn), de proportionaliteit van de verwerking en de getroffen maatregelen om de privacyimplicaties voor betrokkenen te mitigeren. De verwachting is dan ook (zoals nu ook al het geval) dat in de praktijk de

46. Artikel 6(4) Verordening Gegevensbescherming.

twee toetsen veelal hetzelfde zullen uitvallen.[47] Gezien de additionele eisen die de WP29 inmiddels aan de overige grondslagen zoals toestemming, uitvoering overeenkomst en de verwerking van gevoelige gegevens stelt (zie paragraaf 4), lijkt het voor verwerkers in de dagelijkse praktijk de meest rechtszekere weg om door middel van een eenvormig protocol (in de praktijk een *Privacy Impact Assessment* genoemd)[48] een contextuele beoordeling uit te voeren van de implicaties van het gebruik en hergebruik van gegevens. Via deze beoordeling wordt de verwerking langs de lat van alle criteria van de gerechtvaardigd belang-toets gelegd (en de verenigbaarheidstoets) en worden de uitkomsten van de beoordeling alsmede de gemaakte afwegingen gedocumenteerd. Op deze manier kunnen verwerkingen binnen bedrijven via één inhoudelijke toets op hun rechtmatigheid worden beoordeeld (in plaats van aan de hand van de diverse wettelijke criteria) en wordt tegelijkertijd aan de nieuwe vereisten onder de aankomende Verordening voldaan.[49]

Behalve de genoemde vijf pijlers bepaalt nog een tweetal keuzes de insteek en contouren van dit preadvies. Allereerst is dat de focus op twee innovaties in gegevensgebruik: big data en Internet of Things (paragraaf 1.2). Daarnaast is dat de beperking tot gegevensgebruik in private verhoudingen (paragraaf 1.3).

1.2 Keuze voor invalshoek big data en het Internet of Things

Wie het discours over privacy en het gebruik van persoonsgegevens anno 2016 overziet, stelt vast dat de meeste bijdragen de ontwikkelingen de maat nemen vanuit één specifieke invalshoek. Zo figureren in beleidsdocumenten van de overheid dan wel plannen en ambities van bedrijven veelal de nieuwe mogelijkheden en kansen die grootschalig en innovatief gegevensgebruik bieden. Het gaat dan om ambities als een veilige samenleving waarin maatschappelijke risico's tijdig in beeld komen; innovatie en efficiëntie in (commerciële) dienstverlening dan wel gemak en plezier voor burgers en consumenten. In de wetenschappelijke en maatschappelijke fora is de invalshoek veelal die van onzekere risico's, onvoldoende oog voor nieuwe kwetsbaarheden van de burger en aantasting van fundamentele waarden. Opvallend is ook dat veel discussies van de vaak onuit-

47. Zie in die zin ook Opinie WP29 06/2014.
48. En in de Verordening Gegevensbescherming aangeduid met Data Protection Impact Assessment (DPIA).
49. Zoals de *accountability* verplichting waarbij dient te kunnen worden aangetoond dat verwerkingen overeenkomst de wet worden verwerkt (artikel 22); de verplichting verwerkingen te documenteren (artikel 28), en de verplichting om voor specifieke verwerkingen die mogelijk een hoog risico voor privacy vormen een 'Data Protection Impact Assessment' (DPIA) uit te voeren en indien inderdaad blijkt dat er een hoog risico bestaat over deze verwerking vooraf de toezichthouder te consulteren (artikel 33 en 34).

gesproken veronderstelling uit lijken te gaan dat initiatieven tot ontwikkeling komen vanuit één concrete ambitie (het realiseren van commerciële dienst X of beleidsplan Y) en dat die ambitie kan worden geformuleerd en nagestreefd door één helder aan te wijzen actor (overheidsinstantie A, bedrijf B). In werkelijkheid is dat niet het geval.

In de huidige samenleving waar het delen van gegevens eerder regel dan uitzondering is, komt de reikwijdte en aard van het gegevensgebruik niet voort uit een *grand design*. Vrijwel per definitie wordt het speelveld namelijk bepaald door een complex geheel van samenwerkende en van elkaar afhankelijke (publieke en private) partijen. Bovendien zijn het al lang niet meer uitsluitend bedrijven en overheidsinstellingen die gegevens over ons verzamelen en delen. Voor vele burgers is het online uitwisselen van nieuwtjes, foto's en allerhande wetenswaardigheden inmiddels een vast patroon in het leven van alledag. Al die gegevens vormen vervolgens een schat aan informatie voor bedrijven en overheden. Ieder van ons draagt zo bij aan de uiterst complexe dynamiek van verzamelen, delen en hergebruiken van gegevens. En uiteindelijk oefenen we daarmee ook allemaal invloed uit op het niveau en de ontwikkeling van privacybescherming.

Om te voorkomen dat dit preadvies vanuit deze inherente complexiteit van de thematiek te abstract in zijn bespiegelingen en redenering blijft, presenteren we ons betoog aan de hand van twee concrete ontwikkelingen, te weten big data en het Internet of Things (**IoT**). 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.

Zijn big data en IoT meer dan een hype?

Zeker, big data en IoT zijn deels massaal omarmde hypes.[50] Eerder waren velen in de ban van de ongekende mogelijkheden van internet, virtuele dienstverlening en online winkelen, waarna de nieuwe economische bedrijvigheid een forse tik kreeg om vervolgens gestaag uit te groeien tot een vanzelfsprekend onderdeel van onze moderne samenleving. Zo zal dat ook het geval zijn met de nieuwe inzichten, sturingsmogelijkheden en economische waardecreatie die big data en allerhande met het internet verbonden voorwerpen (IoT) ons bieden. De kracht en daarmee het 'hype-overstijgende' van het fenomeen schuilt echter in de combinatie van een aantal ontwikkelingen. Allereerst is dat de exponentiële groei in beschik-

50. Volgens de 2014 Gartner Hype Cycle Special Report was Big Data in 2014 op zijn top qua hype, waarna ontnuchtering plaatsvond. Burton, Willis, 2014.

bare gegevens, onder meer omdat onze omgeving meer en meer data genereert met behulp van sensoren in auto's, het wegdek, apparaten in huis, sieraden, etc.[51] Ten tweede is dat de steeds grotere rekencapaciteit, die ons – daarbij gebruik makend van analyse-algoritmen – in staat stelt patronen en verbanden te ontwaren waarvan we het bestaan niet konden vermoeden. Het gaat hier om correlaties (het vaststellen van een significant statistisch verband tussen factoren) en daarmee waarschijnlijkheden zonder dat we weten waarom dit verband bestaat. "It is looking for the what without knowing the why".[52] Bovendien zijn de systemen intelligent in de zin dat ze zijn ontworpen om niet alleen de patronen bij te houden en deze te herkennen, maar ook om op basis van aanvullende gegevens (bijvoorbeeld doordat een consument wel of juist niet ingaat op het gedane aanbod) deze patronen bij te stellen en nieuwe verbanden te genereren. Hergebruik van gegevens vormt een wezenlijk onderdeel van deze nieuwe manier van gegevensverwerking. Het is juist de optelsom van deze en andere kenmerken die ons voor lastige uitdagingen en afwegingen stelt (zie kader 4 en paragraaf 2.2).

Achtergrond – implicaties van big data

Voor big data geldt dat we een omgang hebben te vinden met:

1. de black-box van:
– op algoritmen gebaseerde systemen,
– die, gebruik makend van geprogrammeerde analyse-criteria,
– enorme hoeveelheden gegevens, bijeengebracht uit talloze bronnen (waaronder ook apparaten, de omgeving en ons lichaam) combineren en analyseren,
– om zo patronen en verbanden te kunnen ontwaren,
– en deze patronen en verbanden automatisch bij te stellen als nieuwe informatie (bijvoorbeeld doordat een consument wel of juist niet ingaat op het gedane aanbod) daartoe aanleiding geeft.

2. de realiteit dat bedrijven en organisaties m.b.v. deze black box in staat zijn om:
– zonder zelf het waarom van gesignaleerde correlaties te kennen,
– daarbij wetende dat deze correlaties iets over een kans, maar niet een vaststaand feit zeggen,

51. Zie voor de veelheid aan toepassingen: http://uk.businessinsider.com/internet-of-everything-2015-bi-2014-12?r=US&IR=T. Gegeven de potentieel ontelbare toepassingen spreken sommigen over *Internet of Everything.*
52. Zie: Mayer-Schönberger, Cukier, 2013; Centre for Information Policy leadership, 2013, p. 1; Hildebrandt, 2013, p. 6-7.

– het gedrag van individuen te duiden (descriptive), te voorspellen (predictive) en te sturen (prescriptive)
– en zo invloed hebben op zowel de autonomie en positie van individuen als de inrichting van onze samenleving,
– terwijl zij daar naar deze individuen en de bredere samenleving toe onvoldoende transparant over zijn en rekenschap over afleggen.

Kortom, big data betekent dat we potentieel in staat zijn 16 miljoen Nederlanders uniek tot een product te 'verpakken' en daarop te sturen, zonder in staat te zijn dat product uit te leggen en daar verantwoording over af te leggen. Deze nieuwe producten bieden de samenleving ongetwijfeld kansen. Maar risico's zijn er zoals we in onder meer paragraaf 2 laten zien, evenzeer.

Kader 4

En hype of meer dan een hype, het is de geschetste data-gedreven ontwikkeling die de komende jaren onlosmakelijk met talloze maatschappelijke en economische processen zal zijn verbonden. Ons preadvies is ingegeven vanuit de overtuiging dat juist deze ontwikkeling en daarmee samenhangende dilemma's (zie ook paragraaf 2.3.1), in combinatie met het ogenschijnlijk ongebreideld verlangen bij bedrijven, overheden maar ook burgers om gegevens te verzamelen en te delen, het draagvlak voor het huidige wettelijke regime ondermijnt.

1.3 Horizontale verhoudingen centraal

Privacy, oftewel de bescherming van de persoonlijke levenssfeer, is als fundamenteel recht verankerd in art. 10 van onze Grondwet. Ook het Handvest van de Grondrechten van de Europese Unie kent bescherming toe en wel gesplitst naar eerbiediging van het privéleven (art. 7) en bescherming van persoonsgegevens (art. 8).[53] Met een specifiek op de EU toegesneden rechtsregime heeft het Hof van Justitie in Luxemburg (**HvJ**) de bevoegdheid te oordelen over de bescherming van persoonsgegevens en het privéleven. Mensenrechten gelden traditioneel in de eerste plaats in verticale verhoudingen tussen burgers en overheid.[54] Maar voor de bescher-

53 Dit 'Handvest van de Grondrechten van de Europese Unie' heeft sedert december 2009 de status van een Verdrag (art. 6 Verdrag betreffende de Europese Unie).

54. Het is vaste rechtspraak onder het EVRM dat indien een bepaling positieve verplichtingen aan de verdragsstaten oplegt, dit een verplichting inhoudt om de betreffende rechten ook te waarborgen tussen burgers en niet-statelijke actoren onderling, zie EHRM 24 juni 2004, 59320/00 (Von Hannover v Germany); zie over de horizontale werking van grondrechten Verhey, 1992; De Vos, 2010.

ming van persoonsgegevens geldt dat burgers deze ook in horizontale relaties jegens bedrijven en derden geldend kunnen maken. Illustratief is dat het HvJ geen onderscheid maakt tussen publiek en privaat bij de interpretatie van de Privacy Richtlijn in licht van art. 7 en art. 8 EU Handvest.[55] Hoewel de Privacy Richtlijn uit 1995 zowel op de private als publieke sector van toepassing is, zijn belangrijke terreinen van overheidsbeleid uitgesloten van de werkingssfeer, zoals verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de staat en gegevensgebruik op strafrechtelijk gebied.[56] Inmiddels heeft het Verdrag van Lissabon via artikel 16 de data protectiebepalingen in het Handvest van algemene toepassing verklaard. Met de herziening van het wettelijk kader van de Privacy Richtlijn, neergelegd in de Verordening Gegevensbescherming, verandert niets wat betreft de werkingssfeer.[57] Echter, het gegevensgebruik door de overheid op voornoemde gebieden zal door een aparte richtlijn worden bestreken.[58]

In dit preadvies staat de horizontale relatie tussen burgers en bedrijven centraal. Verticale relaties zijn onderwerp van de andere bijdragen: Hildebrandt wat betreft het strafrecht en Schmidt en Zwenne wat betreft het publiekrecht. We beseffen dat deze afbakening soms zal wringen. Allereerst omdat het voor burgers lang niet altijd lijkt uit te maken of hun gegevens door de overheid of private sector worden verwerkt.[59] Bovendien, digitalisering trekt zich natuurlijk niets aan van de op grondwettelijk niveau afgebakende grenzen tussen de publieke en private sector.[60] Een strakke cesuur tussen de horizontale en verticale relaties zal daarom niet altijd zijn te realiseren. Illustratief is de ruime toegang die overheden hebben tot door bedrijven verwerkte data. Als de Snowden-affaire iets heeft laten zien, is dat overheden ruim gebruik maken van de bij internetbedrijven aanwezige data, door daar stelselmatig toegang toe te zoeken veelal met medewerking van de betreffende bedrijven. Een veel geciteerde quote in dit verband is van historicus Timothy Garton-Ash in een ingezonden stuk in The Guardian: ‘Were Big Brother to come back in the 21st century, he would return as a public-private partnership’.[61] Waar relevant, zullen we deze wisselwerking tussen private en publieke sector zijdelings in onze beschouwing meenemen.

55. Bijvoorbeeld: Zaak C-131/12 Google Spain and Google Inc, 13 mei 2014, EU:C:2014:317.
56. Artikel 3 Privacy Richtlijn.
57. Artikel 2(2) Verordening Gegevensbescherming.
58. Zie nader het preadvies van Mireille Hildebrandt.
59. Alhoewel privacysurveys ook laten zien dat burgers meer vertrouwen in de overheid hebben dan in het bedrijfsleven als het op het gebruik van hun persoonsgegevens aankomt. Attema, De Nood, 2010, p. 2.
60. Zie hierover uitgebreid: WRR, 2011.
61. WRR, 2015, p. 28 en p. 82.

Vanuit de focus op de horizontale relatie tussen burgers en bedrijven stellen we tegelijkertijd vast dat het voorstel dat wij presenteren mogelijk onvoldoende kaderstellend en daarmee beschermend is in de verhouding tussen overheid en burgers. In de relatie met de overheid hebben burgers te maken met een monopolist. Daarmee 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.[62] Een ander voorbeeld is de *Crime Prediction Tool* die de Amerikaanse staat Oregon heeft ontwikkeld en geïmplementeerd.[63] Hiermee kunnen rechters een inschatting maken van het risico van recidive en dit meenemen in hun beslissingen over bijvoorbeeld vervroegde vrijlating van gevangenen. Min of meer soortgelijke toepassingen worden ook in ons land ingezet, onder meer binnen de jeugdzorg.[64] Tegelijkertijd kunnen dergelijke analyses ook een waardevolle bijdrage voor de samenleving hebben ("dit is een probleembuurt, laten we daar extra aandacht aan geven"). We merken op deze plaats op dat in de verticale relaties de door ons voorgestane aanpak voor het rechtmatig verwerken van gegevens niet tot afdoende voorspelbaarheid en daarmee bescherming zal kunnen leiden. Hier zullen de toegestane verwerkingen telkens nader wettelijk moeten worden verankerd.[65] In de Verordening Gegevensbescherming is de grondslag van gerechtvaardigd belang niet beschikbaar voor overheidsinstanties.[66] Voor een aanzet hiertoe verwijzen wij naar zowel de andere preadviezen als het door de Wetenschappelijk Raad voor het Regeringsbeleid (**WRR**) in het voorjaar 2016 te presenteren rapport over Big Data.

1.4 Door welke lens kijken we?

In aanvulling op de eerdergenoemde vijf pijlers, is ons betoog op een aantal opvattingen en rechtstheoretische idealen gestoeld. Allereerst is dat onze visie op de begrippen privacy en persoonsgegevensbescherming. In situaties waarin bedrijven, organisaties of andere personen onze gegevens gebruiken hebben we het veelal over 'inbreuk op onze privacy'. Toch

62. Kerr, Earle, 2013, p. 66; Provost, Fawcett, 2013.
63. Dit instrument en de ethische dilemma's zijn uitvoering beschreven door Siegel, 2013, p. 59-62.; zie ook de eerdere bespreking in: Moerel, 2014, p. 10-11.
64. Keymolen, Prins, 2011.
65. Te denken valt hier aan privacyinbreuken voor staatsveiligheidsdoeleinden. Zie daarover: Adviesraad Internationale Vraagstukken, 2014; WRR 2015. Evelien Brouwer wijst in dit verband op de paralel tussen het doelbindingsvereiste in private verhoudingen en het legaliteitsbeginsel dat de bevoegdheden van overheden begrenst. Brouwer, 2010.
66. Zie Overweging 38 en artikel 6.1(f) Verordening Gegevensbescherming.

maakt de wetgever een onderscheid tussen privacy enerzijds en persoonsgegevensbescherming anderzijds (zie nader paragraaf 3). Belangrijkste reden voor de loskoppeling is geweest het verschil in functie tussen enerzijds het klassieke recht op privacy (een subjectief recht verbonden aan de exclusieve zeggenschap om bepaalde privéaangelegenheden buiten het bereik van derden te houden) en anderzijds het gegevensbeschermingsrecht (diverse beginselen van behoorlijk gegevensgebruik die moeten garanderen dat gegevens zorgvuldig worden verwerkt en recht wordt gedaan aan de belangen van alle betrokken partijen).[67] Innovatieve vormen van gegevensgebruik laten echter zien dat de scheidslijn tussen de twee steeds minder duidelijk is te trekken.[68] Daarbij komt dat de loskoppeling geen antwoord geeft op het probleem dat ook bij gegevensverwerkingen uiteindelijk ergens een vastomlijnde en heldere grens moet worden getrokken wat wel of niet een gerechtvaardigde inbreuk is.[69] Onze conclusie zal zijn dat voor gegevensverwerking niet kan worden volstaan met een systeem van primair zorgvuldigheidsnormen in een bilaterale relatie, maar de wetgever vanuit de collectieve belangen die toenemend aan de orde zijn, grenzen heeft te trekken. Alleen dan kan recht worden gedaan aan de grondwettelijke verankering op EU-niveau (artikel 8 EU Handvest) van persoonsgegevensbescherming.

In ons betoog laten wij ons verder 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".[70] Dat doen wij vanuit een denkkader dat wordt gevormd door de overtuiging dat de noodzakelijke theorievorming recht moet doen aan de complexiteit van zowel gegevensgebruik als de juridische 'privacywerkelijkheid'. Kortom, we ambiëren een betoog neer te zetten dat niet alleen 'theory-based' maar ook 'reality-based' is. Een eerste element van ons theoretisch denkkader is daarom het ideaal van *responsieve regulering*, waarin de rechtsstaat wordt opgevat als grensbewaking en het concrete programma van wetgeving en beleid mede vanuit de samenleving dient op te rijzen en daarin moet zijn verankerd. Uitgangspunt dient te zijn dat empirisch waarneembare praktijken en instituties van gegevensbescherming de regulering en handhaving mede voeden en effectiviteit en legitimiteit geven.[71] We gaan daarbij tevens in op wat Witteveen eerder de werkelijkheidszin en

67. Het is dit verschil in functie dat voor de EU onder meer aanleiding was om in het EU Handvest de bescherming van het privéleven (art. 7) los te koppelen van de bescherming van persoonsgegevens (art. 8). Zo ook de aanbeveling van de Staatscommissie Grondwet om privacy en persoonsgegevensbescherming op grondwettelijk niveau los te koppelen. www. rijksoverheid.nl/documenten/rapporten/2010/11/11/rapport-staatscommissie-grondwet.
68. WRR, 2011.
69. Floridi, 2005, p. 185-200.
70. Witteveen, 2014, p. 456.
71. Zie ook: Dorbeck-Jung, 2015, p. 24.

mogelijkheidszin van regulering noemt.[72] We combineren het ideaal van responsive regulering met de overtuiging dat een samenleving haar burgers ook in de huidige tijd nog steeds zal moeten garanderen dat privacy en persoonsgegevensbescherming daadwerkelijk iets voorstelt. En als blijkt dat de overheid daartoe een veel actievere rol heeft te vervullen dan in het verleden, dan dient ze zich daarvoor sterk te maken. In de uitwerking van deze overtuiging baseren we ons mede op de *capability approach* van Nobelprijswinnaar Amartya Sen. Vanuit zijn gedachtegoed werken we uit dat gegevensbescherming in een nauwe relatie heeft te staan tot de kansen en **mogelijkheden** die mensen hebben om ook daadwerkelijk een bepaalde ruimte voor zichzelf te verwezenlijken (zie paragraaf 3).[73] Toegepast op privacy en persoonsgegevensbescherming impliceert dit dat de huidige procedurele benadering van gegevensbescherming onvoldoende garanties biedt. Om individuen werkelijk in de gelegenheid te stellen gebruik te maken van hun recht een uniek mens te kunnen zijn en de daarvoor (in fysieke en informationele zin) noodzakelijke ruimte te hebben, moeten ze daartoe ook feitelijk in staat worden gesteld. Bij een toetsingskader voor gegevensgebruik zal daarom de vraag **naar de principiële (on)toelaatbaarheid van bepaalde vormen van gebruik** ook aan de orde moeten komen.[74] Daarbij dienen niet alleen het individuele maar zeker ook het collectieve belang dat bij privacy in het geding is, op het netvlies te staan.[75] Het recht op privacy is immers een voorportaal voor andere fundamentele rechten en vrijheden van het individu die gezamenlijk weer instrumenteel zijn voor het goed functioneren van onze democratische rechtsstaat (zie ter illustratie ons betoog in paragraaf 2.3.1 over "*pay-how-you-drive"*). Concreet betekent dit dat het huidige uitgangspunt – waarbij de beoordeling van de rechtmatigheid van een gegevensverwerking en het nemen van de voor die rechtmatigheid noodzakelijke maatregelen primair in handen liggen van gegevensverwerkers en voornamelijk worden beoordeeld

72. Witteveen, 2014.
73. Amartya Sen, 2009.
74. Borgesius concludeerde eerder dat in de wetgeving een aantal concrete verboden (ontoelaatbaar gebruik) opgenomen moet worden in de context van behavioural targeting, zie Borgesius, 2014, paragraaf 9.7. Het verbieden van specifieke verwerkingshandelingen heeft overigens niet onze voorkeur, al was het maar omdat in het snel veranderende tijdsgewricht de genoemde handelingen snel achterhaald zijn, en het ook telkens weer van de getroffen mitigerende maatregelen en de betrokken belangen zal afhangen of iets al dan niet toelaatbaar is. Sprekend voorbeeld is het in eerste instantie in artikel 20(1) en (3) van de concept-Verordening opgenomen verbod om besluiten te nemen die uitsluitend zijn gebaseerd op profilering op basis van speciale categorieën gegevens. Deze bepaling is waarschijnlijk om de voornoemde reden uiteindelijk geschrapt.
75. Waarmee ook is gezegd, dat de met een zekere regelmaat verkondigde opvatting dat privacy minder, zo niet geen betekenis meer zou hebben, nu burgers zich hier toch niet langer druk om lijken te maken, te kortzichtig en onjuist is. Zie ter bevestiging ook: TNO 2015.

vanuit de bilaterale verhouding tussen verantwoordelijke en betrokkenen – niet meer voldoet. Onze analyse laat zien dat dit in de praktijk resulteert in 'meebewegen' in plaats van 'grenzen stellen'. Wat ons betreft zal de rechtmatigheid van gegevensgebruik vanuit meer overwegingen moeten worden beoordeeld dan slechts de zorgvuldigheid die wordt verlangd in een bilaterale verhouding tussen verantwoordelijke en betrokkenen. De toets zal moeten zijn of vanuit een bredere beoordeling dan uitsluitend het belang van de verwerker een **gerechtvaardigd belang** met de gegevensverwerking is gediend. Ook zullen in onze benadering toestemming van individuen en het bestaan van een contractuele relatie niet langer zelfstandige grondslagen kunnen zijn voor de rechtmatigheid van een gegevensverwerking. Concreet kan dit betekenen dat een aantal vormen van gegevensverwerking niet langer zal zijn toegestaan, terwijl voor de verwerking momenteel wel een rechtmatigheidsgrondslag is te vinden.

1.5 Opzet

We starten in de navolgende paragraaf 2 met een nadere toelichting op de belangrijkste ontwikkelingen in het verwerken en analyseren van persoonsgegevens en de risico's die deze voor fundamentele rechten, waaronder privacy, met zich meebrengen. Het theoretisch kader dat de basis vormt voor ons pleidooi voor een nieuw juridisch kader, ontwikkelen we in paragraaf 3. Vervolgens stappen we in paragraaf 4 over naar een analyse van huidige leidende beginselen bij het verwerken van persoonsgegevens (doelbinding, gegevenskwaliteit en informationele zelfbeschikking). Gegeven onze conclusie dat de effectiviteit en legitimiteit van deze beginselen steeds meer onder druk komen te staan, presenteren we in deze paragraaf ook een eerste proeve van de door ons gesuggereerde alternatieve benadering. Daarbij introduceren we de belangrijkste bouwstenen en normstellende voorwaarden en gaan we in op de vraag of en op welke wijze ons voorstel concreet vorm kan krijgen. In paragraaf 5 bespreken we een mogelijk verbod op bepaalde toepassingen van big data en IoT alsmede scenario's voor handhaving van de door ons voorgestelde aanpak. In paragraaf 6, ten slotte, wordt het betoog kort afgerond.

2. De hedendaagse context van gegevensbescherming

2.1 Wel of niet iets nieuws onder de zon?

In een tijd waarin niet langer alleen internet en apps op *smartphones* instrumenteel zijn bij het verzamelen en verspreiden van persoonsgegevens maar ook onze omgeving met behulp van vrijwel onzichtbare senso-

ren steeds vaker over ons doen en laten 'communiceert',[76] staat het buiten kijf dat privacy een terugkerend onderwerp van discussie is. Deels is er in die discussie niets nieuws onder de zon: ons begrip van privacy heeft zich altijd al gevormd en aangepast in reactie op maatschappelijke ontwikkelingen en nieuwe technologieën. Privacy is een sociaal construct en als zodanig onderwerp van voortdurende verandering.[77] De hedendaagse aandacht voor bijvoorbeeld veiligheid en de allesomvattendheid van digitalisering vormen daarop geen uitzondering. Wie het beroemde artikel van Warren en Brandeis (1890)[78] in herinnering roept, weet dat het Amerikaanse privacyrecht zich ontwikkelde in reactie op de uitvinding van de draagbare fotocamera. In ons land vormde in de jaren zeventig de volkstelling – gefaciliteerd door computersystemen – aanleiding om wettelijke verankerde grenzen te trekken voor privacy en het grootschalig verzamelen van gegevens. En alhoewel het concept zich onder invloed van digitalisering heeft ontwikkeld vanuit een fysiek (het huisrecht) naar een meer immaterieel georiënteerd aanknopingspunt, blijft een centrale pijler van privacybescherming het reële recht op een bepaalde mate van afzondering.

> "In very early times, the law gave a remedy only for physical interference with life and property. […] Gradually the scope of these rights broadened; and now the right to life has come to mean the right to enjoy life – the right to be let alone."
>
> S.D. Warren, L.D. Brandeis, "The Right to Privacy", *Harvard Law Review, Boston* 1890-5, p.193.

Die afzondering hebben we als mens nodig om onze persoonlijkheid en identiteit te vormen en invulling te geven. In de woorden van Hannah Arendt: "A life spent entirely in public, in the presence of others, becomes […] shallow. [I]t loses the quality of rising into sight from some darker ground which must remain hidden if it not to lose its depth in a very real, non-subjective sense".[79]

Waar met de ontwikkeling en vorming van het begrip privacy als zodanig weinig nieuws aan de hand is, is dat wel het geval met het instrumentarium dat de noodzakelijke grenzen moet trekken. Zowel technologische

76. Prins, 2015a. Medio augustus 2015 lanceerde Microsoft een speciale versie van Windows 10 waarmee apparaten zoals tv's en ijskasten via een kabel of via bluetooth een wifi verbinding met andere apparaten in een netwerk kunnen maken. De verwachting is dat het Internet of Things zal uitgroeien tot een markt waarin wereldwijd meerdere miljarden euro's in omgaan (NRC Handelsblad 12 augustus 2015, p. 18).
77. European Commission, 2011, p. 102.
78. Warren, Brandeis, 1890, p. 193.
79. Geciteerd in: Solove, 2008, p. 164.

als maatschappelijke ontwikkelingen (fraudebestrijding, terrorismebestrijding, noodzaak tot meer efficiëntie, diensteninnovatie, gemak, etc.) zetten de ruimte om onbespied door het leven te gaan onder druk. Tegelijk met de stortvloed van nieuwe vormen van inmenging in onze persoonlijke levenssfeer neutraliseren allerhande sentimenten de inbreuken op het wettelijk verankerde privacykader. Eerdere onverschilligheid 'ik heb toch niets te verbergen' lijkt inmiddels te hebben plaatsgemaakt voor gelatenheid: 'ik moet mijn gegevens wel invullen, wil ik ....'. Meer en meer wordt het als normaal dan wel onontkoombaar beschouwd dat we zowel in kwantitatief als in kwalitatief opzicht transparanter worden voor niet alleen bedrijven en overheid, maar ook onze vrienden en medeburgers. Hoewel privacy – geformuleerd als het recht op bescherming van de persoonlijke levenssfeer – als nationaal en internationaal verankerd grondrecht naar zijn aard een grensstellend karakter heeft, blijken we dus toch steeds zichtbaarder te worden. Daarbij gaat het al lang niet meer alleen om het voortdurend in de gaten houden van mensen. Belangrijker is dat we steeds meer in staat zijn om maatschappelijke en economische processen te sturen met behulp van gegevens. Wie staat er bijvoorbeeld bij stil dat de Belastingdienst ervan uitgaat dat mensen die in een scheiding liggen, sneller fouten maken bij het invullen van hun belastingaangifte dan mensen die niet in deze omstandigheden verkeren? 'Logisch,' aldus algemeen directeur van de Belastingdienst Blokpoel: "Scheiden is complex. Vroeger zou de instinctieve reactie bij de dienst zijn: we moeten die aangiftes beter gaan controleren. Nu benaderen we die groep *vooraf*. We schrijven ze een brief waarin we zeggen: mensen in uw situatie maken vaak fouten. Wat blijkt? Afhankelijk van de groep, worden er 30 tot 70 procent *minder* fouten gemaakt. Een doorslaggevend succes." [80]

Zeker, dit is een relatief onschuldig voorbeeld. Maar we kunnen allemaal situaties bedenken waarin we er een (groot) belang bij hebben te weten hoe en waarom organisaties ons in een bepaalde categorie belastingbetalers, burgers, patiënten en consumenten plaatsen. En soms zullen we die typering willen laten corrigeren of zelfs verbieden. Maar waar het voor burgers steeds belangrijker wordt een bepaalde zeggenschap over en controle op het gebruik van hun persoonsgegevens en daarmee privacy te hebben,[81] is de realiteit een geheel andere. Eenvoudig gesteld: we worden als individu steeds zichtbaarder, behalve voor onszelf.[82] En hoewel uitspraken van het

80. https://decorrespondent.nl/2720/Baas-Belastingdienst-over-Big-Data-Mijn-missie-is-gedragsverandering/83656320-f6e78aaf
81. Zie TNO 2015.
82. De Jong, 2014, typeert dit probleem als dat het "individu steeds transparanter [lijkt] te worden", maar "dat de 'vraag is of de betrokkene ook voldoende terug kan kijken, of dat hij geconfronteerd wordt met een situatie van een eenrichtingsspiegel waarbij transparantie maar eenzijdig is". Eerder sprak Keymolen in dit verband over 'onzichtbare zichtbaarheid': Keymolen, 2007. Zie ook Prins, 2007, p. 111-134.

Europees Hof voor de Rechten van de Mens over de inzet van technologie ten behoeve van opsporings- en veiligheidsdoeleinden laten zien dat het Hof met art. 8 EVRM in de hand duidelijke eisen stelt aan onder meer de legaliteit van privacyinbreuken,[83] blijkt het realiseren van betekenisvolle privacybescherming ook in het *post-Snowden tijdperk* een complexe aangelegenheid.

Diverse factoren zijn hier debet aan. Bekend is het probleem dat de natiestaat weinig soevereine macht heeft als het gaat om het sturen van het gedrag van organisaties en mensen op internet en daarmee ook het gegevensgebruik. In een vernetwerkte grenzeloze wereld werken traditionele governance structuren lang niet altijd meer, met als gevolg dat nieuwe arrangementen voor controle en handhaving ontstaan. Wij verwijzen voor een analyse van deze en andere factoren naar de vele literatuur die hierover is verschenen.[84] Dat het realiseren van betekenisvolle privacybescherming een complexe aangelegenheid is, heeft zeker ook te maken met de vraag die wij in dit preadvies centraal stellen, namelijk of bepaalde wettelijke criteria (met name het beginsel van doelbinding en de transparantieverplichtingen) hun regulerende werk nog wel voldoende kunnen verrichten. Voor een goed begrip van deze discussie, gaan we in deze paragraaf allereerst in op het kenmerkende van nieuwe vormen van gegevensverwerking (2.2), om aansluitend de risico's voor fundamentele rechten en waarden in beeld te brengen (2.3).

2.2 Nieuwe vormen van gegevensverwerking

Een aanzienlijk deel van het gegevensgebruik kenmerkt zich nog steeds door een vrij klassiek verzamelen, gebruiken en opslaan van gegevens binnen een bedrijf of organisatie. Een verzekeraar verlangt gegevens om tot uitkering van een schadeclaim over te kunnen gaan, een reisbureau wil de noodzakelijke gegevens hebben om de gekozen vakantiereis te kunnen boeken en bol.com verzoekt u gegevens aan te leveren om de bestelling af te leveren en te factureren. Maar wie kijkt naar innovatie in gegevensgebruik, ziet dat het steeds meer gaat om het op slimme wijze verzamelen, hergebruiken, combineren en analyseren van grote hoeveelheden gegevens.[85] Daarmee worden correlaties en patronen inzichtelijk (*descriptive*), om op basis daarvan het waarschijnlijke gedrag en handelen van actoren te voorspellen (*predictive*) en vervolgens via diensten en beleid deze actoren

83. De Hert, 2009, p. 37.
84. Van Klink, Prins, Witteveen, 2001, p. 85-201. Zie ook de diverse hoofdstukken in: Koops, Lips, Prins, Schellekens (red.), 2006.
85. Wie in meer detail over de ontwikkelingen wil lezen: Provost, Fawcett 2013; Baesens 2014; Leskovec, Rajaraman, Ullmann 2014.

in hun gedrag en handelen te sturen (*prescriptive*).[86] Zo biedt LinkedIn niet alleen een platform waar mensen zich werkgerelateerd kunnen profileren, maar brengt het ook tendensen op de arbeidsmarkt in kaart. Door zorgvuldig bij te houden hoe mensen hun profiel aanpassen, ziet het bedrijf patronen in de keuzes die worden gemaakt bij het accepteren van een nieuwe functie. Daarmee genereert LinkedIn kennis over bijvoorbeeld banengroei in een bepaalde branche, arbeidsmigratie over de grenzen heen en mogelijkheden die werknemers hebben om wel of niet in ons land aan de slag te komen en in welke branche.[87] Ook Twitter is inmiddels veel meer dan een platform voor het delen van wetenswaardigheden in een beperkt aantal tekens. Het bedrijf zet eveneens in op het te gelde maken van de correlaties en waarschijnlijkheden die uit de miljarden berichten zijn te genereren. Weer andere bedrijven benutten deze inzichten om het gedrag van hun klanten te beïnvloeden.

Een tweede kenmerk van de huidige innovatie is het groeiend aantal toepassingen dat gegevens volledig geautomatiseerd en real-time verwerkt. Een voorbeeld: om het dagelijkse fileleed aan te pakken is het wegdek van snelwegen voorzien van sensoren die voertuigen waarnemen en relevante informatie draadloos doorgeven aan kastjes langs de weg. Daar vertalen slimme algoritmen de data naar inzichten in verkeersstromen, verwachte toe- of afname van auto's, potentiële effecten van gerichte verkeersmaatregelen, etc. Deze *real-time* en zeer nauwkeurige informatie stelt wegbeheerders vervolgens in staat om snel en gericht de meest wenselijke maatregel te nemen.[88]

Nu steeds meer persoonsgegevens beschikbaar komen, de opslag- en verwerkingscapaciteit geen probleem meer is en vrijwel volautomatisch met behulp van slimme analysesoftware bepaalde patronen in gecombineerde sets van gegevens vallen te ontwaren, is gedrag te voorspellen en kan men daarnaar handelen. Citron en Pasquale spreken in dit verband over de *Scored Society*.[89] Met de term verwijzen ze naar een samenleving waarin scoringscriteria leidend zijn bij het oordeel over kwesties als kredietwaardigheid voor leningen, verzekerbaarheid voor arbeidsongeschiktheid, risico op frauduleus handelen, succesvol functioneren onder bepaalde werkomstandigheden[90] of aanleg voor risicogedrag of ziekten. De scoringscriteria worden geformuleerd op basis van correlaties in eerdere situaties tussen uitkomst X (al dan niet gewenst) en kenmerk Y (van personen, producten, omstandigheden, etc.). Concreet: consumenten wonend

86. Zie voor een oriëntatie op deze driedeling: http://www.informationweek.com/big-data/big-data-analytics/
big-data-analytics-descriptive-vs-predictive-vs-prescriptive/d/d-id/1113279.
87. NRC Handelsblad, 12 augustus 2015, p. 18.
88. Zie ook het rapport van Deloitte, 2012.
89. Keats Citron, Pasquale, 2014.
90. Zie voor voorbeelden en een analyse: Sprague, 2015.

in postcodegebied A met etnische afkomst B hebben een sterke voorkeur voor product C. Kinderen die scoren op criteria E, F & G lopen meer risico in de criminaliteit te belanden dan kinderen die hier niet op scoren. Individuen met leefpatroon X, leeftijdscategorie Y en sociale achtergrond Z lopen meer risico op arbeidsongeschiktheid ten gevolge van ziekte N.[91]

Illustratief is de groeiende populariteit van online profileringsdiensten zoals TalentBin[92], Gild[93] maar ook van Facebook bij de werving en selectie van personeel.[94] Ophef veroorzaakte vorig jaar in de VS het bericht dat bij een van 's werelds grootste *data brokers*, Acxiom Corp., informatie te koop was over individuen met (kennelijke) aanleg voor diabetes. "The lists typically sell for about 15 cents per name and can be broken down into sub-categories, like ethnicity, income level and geography for a few pennies more."[95] Bedrijven als Acxiom, KBM[96] en Epsilon verkrijgen gegevens onder meer via enquetes onder consumenten: "Epsilon, which has data on 54 million households based on information gathered from its Shopper's Voice survey, has lists containing information on 447,000 households in which someone has Alzheimer's, 146,000 with Parkinson's disease, and 41,000 with Lou Gehrig's disease. The Irving, Texas-based company provides survey respondents with coupons and a chance to win $10,000 in exchange for information on their household's spending habits and health." [97] In ons land experimenteren bedrijven inmiddels met premiekorting op verzekeringen in ruil voor persoonsgegevens.[98]

In de zoektocht en zucht naar meer en meer informatie, neemt ook de reikwijdte van het type gegevens dat wordt benut toe. Zo sorteren vele commerciële bedrijven als Google, Amazon en Apple naar verluid voor om de rijkdom aan informatie die met genetische gegevens straks voorhanden is, te kunnen benutten.[99]

Kwetsbaar aan scoringspraktijken en profileringsdiensten is dat de gehanteerde criteria en toegepaste foutmarges veelal uitsluitend bekend

91. Zie voor een 'ludieke' illustratie de website "Heel Holland Transparant" – www.heelhollandtransparant.nl (een initiatief van *De Correspondent*, *Bits of Freedom* en Atelier Yuri Veerman). Zie daarover ook: Goslinga, 2015.
92. https://www.talentbin.com/
93. http://www.gild.com/
94. Richtel, 2013, p. BU1. Uit onderzoek blijkt dat iemand's profiel op Facebook meer voorspellende waarde heeft over zijn functioneren in een baan dan IQ testen. Zie: Kluemper, Rosen, Mossholder, 2012, p. 1143-1172.
95. http://www.bloomberg.com/news/articles/2014-09-11/how-big-data-peers-inside-your-medicine-chest
96. http://kbmghealth.com/AnalyticsData.aspx
97. http://www.bloomberg.com/news/articles/2014-09-11/how-big-data-peers-inside-your-medicine-chest
98. http://nos.nl/artikel/2060561-achmea-biedt-premiekorting-bij-delen-privedata.html. Zie ook: Prins, 2015b, p. 2269
99. Zie: NRC Handelsblad 4 juli 2015, p. 6-7. Zie ook: Prins, 2008, p. 555.

zijn bij degenen die ze toepassen.[100] Transparantie over de gehanteerde criteria en marges, parameters en analytische inzichten alsmede de methodologische verantwoording daarvan, wordt zelden geboden. Bovendien blijken de voor de scoring gebruikte persoonsgegevens niet altijd accuraat. Bijvoorbeeld omdat de gegevens zijn verouderd dan wel onbetrouwbaar blijken buiten de context waarin ze oorspronkelijk werden verzameld. Problematisch is bovendien dat binnen maatschappelijke en sociale verhoudingen universele correlaties[101] niet dan wel nauwelijks te leggen zijn (in tegenstelling tot correlaties binnen de fysica). Dit betekent dat een voorspelling die op basis van een bepaalde correlatie is gedaan, onherroepelijk een bepaalde foutmarge kent. Zelden echter worden resultaten van geautomatiseerde scoring via menselijke interventie op hun betrouwbaarheid gecontroleerd. Al met al ligt het risico van ondoorzichtig, willekeurig en onjuist oordelen over anderen dus op de loer. Belangrijk is het besef dat een correlatie nog niet betekent dat er ook daadwerkelijk een causale relatie te leggen valt.[102] Met andere woorden, patronen en verbanden die aan de hand van data-analyse zichtbaar worden, bieden geen zekerheid wat betreft de voorspelde ontwikkeling of het te verwachten gedrag. Bovendien gaat het slechts om patronen en verbanden op een geaggregeerd niveau. Wederom: daarmee wordt geen zekerheid verkregen of het patroon ook geldt op het specifieke niveau, bijvoorbeeld dat van een individu.

2.3 Spanning met fundamentele rechten

Voor de Amerikaanse overheid vormden deze en andere risico's aanleiding om in de zomer van 2014 een publieksconsultatie te initiëren.[103,104] In de consultatie kwamen ook risico's voor fundamentele rechten aan de orde. Immers, waar (potentieel) gedrag en handelen inzichtelijk wordt, valt te sturen op niet alleen type weggebruikers, consumenten, patiënten en belastingbetalers maar ook op bepaalde bevolkingsgroepen. Daarmee komen de grenzen met in- en uitsluiting, zo men wil 'discriminatie' in beeld. Niet verrassend is dan ook dat een belangrijk thema dat veelvuldig wordt geagendeerd in relatie tot big data zich richt op de zorgen over een toenemende ongelijkheid, het risico van stigmatisering en mogelijk discriminatie (vanuit een bewuste discriminatoire intentie dan wel als effect).[105]

100. Van der Hof, Prins, 2008, p. 111-127. Zie recent: http://www.theguardian.com/commentisfree/2015/dec/06/algorithm-writers-should-have-code-of-conduct?CMP=share_btn_tw
101. Altijd, overal en onder alle omstandigheden geldende correlaties.
102. Hildebrandt, 2013, p. 6-7; CIPL, 2013, p. 1.
103. *Big Data and Consumer Privacy in the Internet Economy*, 79 Federal Register 32714 (June 6, 2014). Zie ook: Executive Office of the President, 2014. Vgl over het debat in de VS ook de opinies vanuit wetenschap en beleid in: Peña Gangadharan et al., 2014.
104. http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/
105. Zie over Big Data en discriminatie: Barocas, Selbst, 2016; Zarsky, 2014, p. 1375.

In ieder geval komen potentieel in het gedrang de bescherming van persoonlijke autonomie, keuzevrijheid, identiteit, en een ongehinderde stroom van informatie en denkbeelden als basis voor zelfontwikkeling.[106] Al deze rechten en vrijheden zijn op hun beurt weer instrumenteel voor het goed functioneren van onze democratische samenleving. Zo is de vrijheid om informatie te vergaren en te ontvangen[107] niet alleen een belangrijke voorwaarde voor de zelfontplooiing van het individu, maar ook voor een pluriforme democratische samenleving.[108] En wat blijft er over van de vrijheid om informatie te ontvangen en de vrije vorming van gedachten, als er door profilering op het internet een "filter bubble" ontstaat waardoor we in feite maar in steeds beperktere mate in staat zijn vrij onze eigen mening te vormen?[109] Illustratief is ook dat profileren wordt gebruikt voor het selecteren van potentiële kiezers die mogelijk van partijvoorkeur kunnen veranderen.[110]

Zeker, deze voorbeelden zijn niet nieuw. Eerder al selecteerden presidentskandidaten buurten met zogenaamde *swing-votes* om daar vervolgens langs de deur te gaan. Het verschil is dat dit nu veel preciezer en systematischer gebeurt, op een veel grotere schaal en volautomatisch. Ook het beïnvloeden van koopgedrag van consumenten is van alle tijden.[111] Een relevant verschil met de oude situatie is dat door big data-analyse veel eenvoudiger en meer van deze gedragscorrelaties kunnen worden geïdentificeerd. Marketingverleiding – *influential marketing* of *persuasion profiling* – kan kortom op veel grotere en vaak indringender schaal plaatsvinden.[112]

106. De Jong, 2014, p. 7, onder verwijzing naar de considerans van de Privacy Richtlijn en een uitspraak van het (al wat oudere, maar niet minder relevante) Duitse Bundesvervassungsgericht in 1083, BVerfG 15 december 1983, 65. Zie verder AIV, 2014, p. 21.
107. Besloten in artikel 7 Gw. en expliciet gewaarborgd in artikel 10 EVRM en artikel 11 EU Handvest. Zie het wetenschappelijk commentaar bij Artikel 7 Grondwet door B.P. Vermeulen op de website Nederland Rechtsstaat (http://www.nederlandrechtsstaat.nl/grondwet/artikel.html?artikel=7&categorie=&auteur=&trefwoord=&1=1##artikel7).
108. De Jong, 2014, p. 8.
109. Pariser, 2012. De zoektechnologie werkt op basis van het principe dat eerdere zoekpreferenties mede bepalend zijn voor volgende zoekresultaten. Als gevolg daarvan wordt het eenvoudiger om gelijkgestemden te vinden, waardoor mensen in hun bestaande meningen worden bevestigd en overtuigd raken dat deze juist zijn, terwijl ze worden afgeschermd van andere meningen. Zie: Smidt, Cohen, 2013, p. 35; Herz, 2013, p 267-269; Sunstein, 2001, p. 192; Carr, 2013, p. 165-167.
110. Issenberg, 2012.
111. Zie voor een reeks voorbeelden: Ariely, 2010.
112. Zie voor een Nederlandse start-up Sagent die met software zorgt dat een webwinkel 20% meer verkoopt, bijvoorbeeld door te differentiëren al naar gelang bezoekers op de site komen via de prijsvergelijkingssite kieskeurig.nl (koopjesjagers) of via Facebook, Het bedrijf maakt naar eigen zeggen gebruik van tien beinvloedingstechnieken op het snijvlak van marketing en psychologie. Zie: *Financieele Dagblad*, zaterdag 1 augustus 2015, "Sagent, Onze onze software zorgt ervoor dat een webwinkel 20% meer verkoopt". Zie ook: Kapitein, 2012.

Beïnvloeding op koopgedrag is één ding (het gevoel van veel mensen is dat ze toch uiteindelijk zelf de beslissing nemen om tot aankoop over te gaan), maar zodra profilering wordt ingezet voor prijsdifferentiatie (de een krijgt op basis van zijn profiel een lagere verzekeringspremie dan een ander) of voor het uitsluiten van een bepaald type individu van een verzekering of lening, zijn de reacties vaak diametraal anders. En dan worden we geconfronteerd met diverse vragen. Bijvoorbeeld: welke effecten heeft dit gebruik op de – toch al zwakkere – positie van consumenten ten opzichte van bedrijven? Of: wat is de betekenis voor de verhoudingen tussen (groepen) consumenten onderling ('iedereen is gelijk, maar sommigen zijn meer gelijk dan anderen')? Maar ook: hebben zorgverzekeraars een (zorg)plicht om consumenten te waarschuwen mocht aan de hand van de analyse blijken dat ze met het continueren van een bepaald gedrag een sterk verhoogd risico lopen op ziekte X of ongeluk Y?[113]

Als we stilstaan bij specifiek de verzekeringsbranche en de ontwikkelingen verbinden met de thematiek van dit preadvies wordt ook duidelijk met welke vragen we worden geconfronteerd. Zo is bij gegevensverwerking ten behoeve van premiedifferentiatie bij verzekeringen een cruciale vraag of we het belang dat de verzekeraar bij deze vormen van differentiatie heeft wel of niet als gerechtvaardigd aanmerken. En welke omstandigheden zijn van invloed op dit oordeel? Relevant is ook de vraag of toestemming van de betrokkenen voor dergelijke toepassingen een geldige grondslag voor het verwerken van de gegevens kan zijn. Is toestemming wel in vrijheid gegeven als degene die toestemming geeft daarvoor een lagere verzekeringspremie in retour krijgt? Om duidelijk te maken dat de discussie over deze en andere vragen aan fundamentelere kwesties raakt dan slechts het 'afvinken' van een aantal voorwaarden van de privacywet, staan we hierna stil bij een recente ontwikkeling in de verzekeringsbranche.

2.3.1 "Pay-how-you-drive" en de noodzaak van een debat

De aankondiging, zomer 2015, door Achmea om een pilot te starten waarbij klanten premiekorting krijgen als ze gegevens over hun rijgedrag leveren heeft veel stof doen opwaaien.[114] Nieuw is het initiatief overigens niet. Eerder al kwam Fairzekering met een soortgelijk verzekeringsmodel.[115] Bij verzekering op basis van *pay-how-you-drive* betalen burgers die beter

113. Over zorgplichten en digitalisering: Prins, 2007, 321.
114. "Verzekeraars onderzoeken tot hoever ze gedrag kunnen sturen", *Financieele Dagblad*, 6 oktober 2015; "Ook verzekeraar bekeert zich. Verzekeraar Achmea biedt premieverlaging voor schadeverzekeringen als de klant intelligente apparaten installeert en de gegevens met het bedrijf wil delen", *Financieele Dagblad*, 1 oktober 2015; "Achmea biedt korting in ruil voor privédata. Verzekeraar wil via kastje in huis of auto gegevens verzamelen , Volkskrant 1 oktover 2015. Zie hierover eerder Moerel, 2015a.
115. Zie bijv. Fairzekering, te vinden op: https://fairzekering.nl/.

rijgedrag vertonen minder voor hun verzekering dan degenen die minder goed rijgedrag vertonen. Deze nieuwe technologie biedt voordelen. Zo krijgen klanten meer inzicht in hun eigen risico-gedrag. Via de kastjes in auto's krijgen ze *real-time* feedback op hun rijgedag, wat (gecombineerd met de bonus van een lagere verzekeringspremie) bestuurders stimuleert veiliger te rijden. Naar verluid heeft deze aanpak inmiddels tot een sterke reductie in schadeclaims geleid.[116] Deze vorm van premiedifferentiatie biedt ook de mogelijkheid om jongeren – die als collectieve groep een hogere verzekeringspremie betalen (omdat bestuurders in deze categorie in de regel meer schade rijden) – gepersonaliseerd korting te bieden indien ze beter rijgedrag (dan gemiddeld) vertonen.

Een belangrijk punt van kritiek op dit nieuwe verzekeringsmodel is dat het de solidariteit onder ons verzekeringsstelsel ondermijnt.[117] In reactie hierop wordt opgemerkt dat differentiatie tussen groepen verzekerden niet nieuw is. Zo betalen jongeren (maar ook ouderen) een hogere premie voor autoverzekeringen omdat zij in de regel meer schade rijden.[118] Tegen *pay-how-you-drive* en soortgelijke verzekeringsconcepten zou om die reden geen bezwaar moeten bestaan. De aanbieders van deze verzekeringen vragen bovendien voor het gebruik van de gegevens vooraf toestemming van hun klanten.

De privacytoezichthouder (Autoriteit persoonsgegevens – voorheen College bescherming persoonsgegevens) acht dit type verzekeringen dan ook niet in strijd met de privacywet, mits de verzekeraar open is over het doel van de gegevensverzameling.[119] Wel voegt de privacytoezichthouder er aan toe dat intern discussie wordt gevoerd over de "wenselijkheid van deze ontwikkeling". De minister van Economische Zaken maakt zich ogenschijnlijk ook weinig zorgen:

> "Het nastreven van winstmaximalisatie en andere commerciële doelen door het bedrijfsleven is op zichzelf legitiem, en het inzetten van big data-processen ten behoeve van die winstmaximalisatie eveneens. Als het middel om het nagestreefde doel (winstmaximalisatie) te bereiken passend en noodzakelijk is, kan indirect onderscheid, mits deugdelijk gemotiveerd, met objectiveerbare feiten worden gerechtvaardigd. Zo kunnen verzekeraars niemand uitsluiten op grond van geslacht of godsdienst, ook al lijkt de uitkomst van een bigdata-analyse daartoe aanleiding te geven. Wel kunnen zij als gevolg van besluit-

116. Zie Tucker, 2014; Timmer, Elias, Kool, Van Est, 2015, p. 39.
117. Zie Moerel, 2015a.
118. Zie over leeftijdsdiscriminatie de webiste van de Consumentenbond met een oproep om op dit punt de wet te wijzigen, zie http://www.consumentenbond.nl/autoverzekeringen/premie/autoverzekering-leeftijd/. Inmiddels zijn er ook talloze nieuwe verzekeringen speciaal voor hogeropgeleiden, of voor ambtenaren. Zie bijvoorbeeld voor hoger opgeleiden: https://www.promovendum.nl/ en voor ambtenaren: http://www.vngv.nl/producten/verzeker-uw-ambtenaren/14-voordelige-autoverzekering-voor-bestuurders-en-ambtenaren
119. Volkskrant, 1 oktober 2015.

> vorming op grond van big data-uitkomsten premies differentiëren aan de hand van bepaalde gedragskenmerken die iets zeggen over het risico van een verzekerde. Als dat besluit vervolgens in de uitwerking leidt tot indirect onderscheid op grond van één van de in de wet genoemde kenmerken, moeten de verzekeraars daarvoor een objectiveerbare rechtvaardiging aanvoeren. Het proces van profilering kan ook zorgen voor onterechte conclusies." [120]

Wanneer we iets langer stilstaan bij deze ontwikkelingen, valt toch wel een aantal dilemma's en punten van zorg in relatie tot privacy en andere fundamentele waarden en rechten te signaleren. Om twee redenen staan we hier nader bij stil. Ten eerste omdat we deze ontwikkelingen niet mogen negeren gegeven de fundamentele vragen waar we voor komen te staan, zoals de rol van solidariteit binnen onze samenleving. Daarmee is deze ontwikkeling illustratief voor onze eerdere observatie dat het recht op privacy een voorportaal is voor de bescherming van andere fundamentele rechten en vrijheden van het individu. Ten tweede illustreren we aldus dat bij gebrek aan een politieke en maatschappelijke discussie over deze ontwikkelingen ook een zorgvuldige beoordeling van de rechtmatigheid van de daarbij verwerkte persoonsgegevens problematisch is. Concreet agendeert de ontwikkeling immers de vraag: hebben verzekeraars nu wel of niet een gerechtvaardigd belang bij het gegevensgebruik voor deze productinnovatie? We mogen ons willen afwenden van het fundamentele debat over deze bovenstaande ontwikkeling, het is wel deze concrete vraag die in de praktijk van alledag bij bedrijven en organisaties op tafel ligt. Immers, de vraag behoeft vanuit de grondslag van art. 8f Wbp in bepaalde gevallen beantwoording. Als voorzet voor dit debat, brengen we daarom de volgende observaties in.

Om te beginnen: dat nu al premiedifferentiatie plaatsvindt kan geen rechtvaardiging zijn dat **dus** het monitoren van rijgedrag door middel van digitale kastjes in auto's is gerechtvaardigd om deze differentiatie nog **preciezer** te kunnen maken. Tot nu toe vond premiedifferentiatie plaats op basis van analyse van gegevens uit het **verleden,** met andere woorden door de achteruitkijkspiegel (op basis van beperkte gegevens van de bestuurders, zoals leeftijd, geslacht en gemaakte ongelukken). Bovendien werden de resultaten **generiek** op een bepaalde categorie bestuurders toegepast (bijv. jongeren betaalden een hogere verzekeringspremie dan gemiddeld). Door middel van de sensoren in de kastjes wordt nu rijgedrag (met een groot aantal niet eerder verzamelde variabelen, zoals acceleratie, snelheid, nemen van bochten), **real-time** op individueel niveau in kaart gebracht en wordt premiedifferentiatie op basis van de **voorspelling** op basis van het vertoonde rijgedrag (dus in de vooruitkijkspiegel) op **persoonlijke**

120. Kamerstukken II, 2014/15, 32761, nr. 78, p.7.

basis vastgesteld.[121] Hoe precies verzekeraars tot deze voorspelling over ons gedrag komen, blijft echter onduidelijk.[122] De privacywet vereist dat individuen inzicht wordt gegeven in de logica die ten grondslag ligt aan de profilering waarop een beslissing is gebaseerd. In de dagelijkse praktijk blijkt echter op geen enkele wijze te zijn geborgd dat dit inzicht ook daadwerkelijk kan worden gegeven. Bovendien komen diverse vragen op. Wat, als blijkt dat sommige bestuurders wel prima rijgedrag vertonen, maar (in afwijking van de reguliere voorspelling) toch relatief veel ongelukken overkomen terwijl anderen gevaarzettend rijgedrag vertonen, maar (in afwijking van de gevonden correlaties) weinig brokken maken, zonder dat vaststaat waar dit precies door komt? Wordt degene die op die basis meer premie betaalt (slecht rijgedrag vertoont maar geen ongelukken maakt), nu wel of niet gediscrimineerd?

Als onderdeel van de toets of verzekeraars een gerechtvaardigd belang bij deze vorm van gegevensverwerking hebben, zal de vraag moeten worden beantwoord of de positieve resultaten van deze vorm van premiedifferentiatie (verbeterd rijgedrag) niet ook op een minder ingrijpende wijze dan voortdurende monitoring kunnen worden bereikt.[123] Relevant voor het oordeel over een al dan niet gerechtvaardigd belang is de weging van de positieve effecten (reductie van ongelukken) en de negatieve effecten. Over die negatieve effecten – die zowel individuen als de samenleving raken – merken we het volgende op.

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. Met dit soort *pay-how-you-drive* (en op termijn *pay-how-you-live* verzekeringen, waarbij individuen premiekorting kunnen krijgen als uit onder meer Facebook-data blijkt dat ze een gezonde life style hebben) krijgen we straks groepen binnen onze samenleving waarvan het gedrag continue wordt gemonitord om nog (betaalbaar) verzekerd

121. Prins, 2015b, p. 2269.
122. Timmer, Elias, Kool, Van Est, 2015, paragraaf 7.5 en aanbeveling 5 op p. 63.
123. Denkbaar is bijvoorbeeld (en met de privacywet te verenigen) dat een verzekeraar kastjes in auto's plaatst en de daarmee gegenereerde data vervolgens analyseert. De resultaten kunnen vervolgens worden gebruikt om via een *driver dashboard* de bestuurder feedback te geven op zijn of haar rijstijl en om, als de scores niet goed zijn, trainingen in rijstijl aan te bieden en zelfs om bij verbetering in rijgedrag beloningen te geven (zoals gratis autowasbeurten). Onderzoek toont aan dat voor het beïnvloeden van gedrag het geven van beloningen meestal beter werkt dan straffen (in dit geval met hogere premies): WRR 2014; Tiemeijer, 2012.

te kunnen blijven.[124] Dit is geen speculatie. De Amerikaanse verzekeraar Oscar biedt nu al fitnessbandjes aan en geeft klanten kortingen op het moment dat ze meer dan een bepaald aantal stappen per dag zetten.[125] Wat blijft er over van individuele autonomie als keuzes in ons dagelijks levenspatroon een groeiende invloed hebben op niet alleen onze positie in de samenleving maar ook de mogelijkheid om ons daarin financieel en sociaal staande te houden? Wie aan het einde van de maand naar de maatstaf van de verzekeraar onvoldoende stappen op z'n teller heeft staan, kiest niet voor een avondje bioscoop met vrienden maar loopt nog een paar blokken om. En met deze ontwikkeling zijn het meer en meer grote commerciële partijen die over de noodzakelijke (hoeveelheden) gegevens beschikken om aan de hand van data-analyse te bepalen welk type risicogedrag wel of niet acceptabel is en waar kennelijk de grenzen van solidariteit liggen. De suggestie dat we met de komst van big data een beter beeld van risico's krijgen en deze daarmee beter vooraf te beïnvloeden zijn, kan er toe leiden dat individuen in een toenemende mate een eigen verantwoordelijkheid krijgen voor het voorkomen van deze risico's. Auto-ongelukken die eerst domme pech leken, kunnen nu meer en meer worden geduid als een risico (dat een bepaald type mensen loopt). Dat risico hadden de betrokkenen deels actief kunnen inperken. Waar risico's te beïnvloeden zijn (wat met het verkrijgen van inzichten door het monitoren van gedrag steeds meer mogelijk wordt) zal de solidariteit van degenen met een (vermeend) laag risico afnemen ten opzichte van degenen met een hoog risico die daar kennelijk hun gedrag niet op wensten aan te passen ('dan had je maar gezonder moeten leven', etc).[126]

Relevant is dat op grond van het EVRM de uitoefening van wettelijk verankerde rechten verzekerd dient te zijn "zonder enige discriminatie op welke grond dan ook, zoals geslacht, ras, kleur, taal, godsdienst, politieke of andere mening, nationale of maatschappelijke afkomst, het behoren tot een nationale minderheid, vermogen, geboorte of andere status."[127]

124. Morozov, 2013, waarschuwt dat de keuze voor bepaalde mensen niet een volledig vrije zal zijn, nu degenen met een klein budget het zich lang niet altijd kunnen permiteren te kiezen voor een privacyvriendelijke verzekering. Deze zal immers duurder zijn.
125. Zie voor de app https://play.google.com/store/apps/details?id=com.hioscar.member&hl=nl; Voor een bespreking: Khouri, 2015.
126. Timmer, Elias, Kool, Van Est, p. 47-48.
127. Zie artikel 14 EVRM. De reikwijdte van de non-discriminatie bepaling is met het twaalfde protocol van het EVRM uitgebreid en ziet nu op alle wettelijke rechten in plaats van de rechten en vrijheden onder het EVRM. Voor Nederland is dit protocol in 2005 in werking getreden. Zie ook artikel 21 EU Handvest dat een algeheel verbod op discriminatie bevat, met name op grond van geslacht, ras, kleur, etnische of sociale afkomst, genetische kenmerken, taal, godsdienst, of vertuigingen, politieke of andere denkbeelden, het behoren tot een nationale minderheid, vermogen, geboorte, een handicap, leeftijd of seksuele geaardheid. Ingevolge artikel 6 lid 1 van het Verdrag van Lissabon heeft dit Handvest bindende rechtskracht verkregen voor de EU.

Het EU Hof van Justitie heeft in dit verband onder meer geoordeeld dat verzekeraars geen onderscheid mogen maken op grond van geslacht.[128] Verzekeringen waarbij vrouwen minder verzekeringspremie hoefden te betalen, omdat ze in de regel minder schade rijden, zijn niet geoorloofd. Het behoeft weinig toelichting dat met het systeem van '*pay-how-you-drive*' het onderscheid op basis van geslacht via de achterdeur wordt ingevoerd. Uit de met de autokastjes verzamelde data zal immers ongetwijfeld blijken dat vrouwen in de regel voorzichtiger rijden dan mannen. En wat als duidelijk wordt dat er in een buurt waar voornamelijk Antillianen wonen veel ongelukken worden gemaakt? Indien de verzekeringspremie voor Antillianen wordt verhoogd wordt dit gekwalificeerd als discriminatie. Maar is dat ook het geval wanneer voor de buurt als zodanig de verzekeringspremie wordt verhoogd?[129] Gedrag valt bovendien maar tot een bepaald niveau te beïnvloeden. De rechtvaardiging voor premiedifferentiatie – namelijk dat iedereen uiteindelijk zijn of haar eigen rijgedrag (en straks: leefpatroon) kan bepalen, waarmee premiedifferentiatie zou zijn gelegitimeerd – gaat met andere woorden slechts gedeeltelijk op.

Ten slotte: risico's nemen en daarmee leren om te gaan, vormt een wezenlijk onderdeel van de groei (naar volwassenheid) van individuen en een samenleving. In die zin heeft de aanwezigheid van risico's ook positieve effecten. Vanuit deze vaststelling sluiten we deze paragraaf daarom af met een mooie quote van Wijnberg in de Correspondent: 'had Columbus een app in zijn broekzak gehad die zijn verzekeringspremie zou hebben aangepast aan zijn "risicoprofiel", dan was hij nooit uitgevaren om De Nieuwe Wereld te ontdekken.'[130]

2.4 Variaties in identificeren, voorspellen en beïnvloeden

Bij het duiden en beoordelen van de hiervoor geschetste dilemma's is het belangrijk voor ogen te houden dat bedrijven en organisaties nogal wat keuzes hebben in de wijze waarop ze omgaan met de via data-analyse verworven kennis. Zo kunnen de gevonden correlaties en voorspellingen op verschillende manieren worden ingezet (kader 5), is er variatie in de manier waarop mensen identificeerbaar worden (kader 6) en kennis over hen wordt verkregen (kader 7). Bij het toepassen van de verderop uit te werken gerechtvaardigd belang-toets zijn deze onderscheidingen relevant, nu ze op verschillende wijze inwerken op de positie en privacy van personen.

128. Zaak C-236/09, Association Belge des Consommateurs Test-Achats, 1 maart 2014, EU:C:2011:100. Het betreft een baanbrekend arrest, waarin het Hof zich baseerde op art. 21 en art. 23 EU Handvest.
129. Schrage, 2014.
130. Wijnberg, 2015.

Als we starten met gevonden correlaties en voorspellingen alsmede de wijze waarop deze zijn te gebruiken, dan onderscheiden we:[131]
– *preferential predictions* - voorpellingen over voorkeuren;
– *consequential predictions* - voorspellingen over gevolgen van bepaald gedrag;
– *preemptive predictions* - voorspellingen op basis waarvan expliciet de toekomstige handelingsopties van een individu worden beïnvloed.

Preferential prediction*:* voorpellingen over voorkeuren, zoals de Google zoekmachine en de gepersonaliseerde aanbiedingen van Amazon. Deze voorspelling redeneert in beginsel vanuit het perspectief van het individu.
Consequential predictions*:* voorspellingen over gevolgen van bepaald gedrag (al dan niet in combinatie met andere factoren, zoals gezondheid), bijvoorbeeld door zorgverzekeraars of financiële instellingen. Ook deze voorspelling hanteert in beginsel het perspectief van het individu.
Preemptive predictions*:* voorspellingen op basis waarvan expliciet de toekomstige opties van een individu worden beïnvloed. Bekend voorbeeld is de zgn. no-fly lijst van de Amerikaanse overheid om terroristische activiteiten aan boord van vliegtuigen te voorkomen. Anders dan de twee voorgaande is het perspectief hier dat van degene die bepaald gedrag van een personen of groepen van personen beoogt te beïnvloeden.

Kader 5

De meeste effecten op privacy heeft duidelijk de laatste vorm van voorspellen. Immers in dit geval worden de handelingsopties van een individu beïnvloed (veelal worden ze ontnomen) en vaak gebeurt dit zonder dat de betreffende persoon daar weet van heeft. Het zijn de *preemptive* voorspellingen die vaak een schending van meer fundamentele rechten en waarden met zich meebrengen. Het ontnemen van opties (uitsluiting van een verzekering, het afwijzen van een lening) heeft over het algemeen meer implicaties voor de positie van een individu dan wanneer iemand op basis van eerdere voorkeuren een volgende aanbieding krijgt. In dat geval heeft het individu toch (althans als er daadwerkelijke keuzevrijheid bestaat) nog altijd zelf de optie om daar al dan niet op in te gaan.

De scheidslijn tussen preferential predictions en preemptive predictions is soms lastig te trekken, vooral wanneer de voorspellingen worden ingezet bij marketing (*influential marketing* of *persuasion profiling*). Hoewel hier strikt genomen geen opties worden ontnomen, worden individuen wel zodanig beïnvloed in hun keuzes (bijvoorbeeld op grond van hun inhe-

131. Kerr, Earle, 2013, p. 67.

rente gevoeligheid voor aanbiedingen), dat lastig nog te spreken valt van preferenties en het maken van keuzes. Deze vorm van voorspelling is ook niet vanuit het perspectief van het individu ingezet (wil hij/zij die aanbieding namelijk daadwerkelijk?), maar vanuit degene die de aanbieding doet. Deze laatste maakt daarbij gebruik van persoonlijkheidskenmerken van het individu (bijv. gevoeligheid voor koopjes) en veelal niet diens eerdere voorkeuren. Hoewel hier geen toekomstige opties worden uitgesloten, betreft het wel beslissingen die negatieve implicaties voor iemand kunnen hebben. Wat ons betreft dient deze categorie voorspellingen op basis van profilering onder de *preemptive predictions* te worden geschaard. Het zou derhalve niet alleen moeten gaan om uitsluiting maar ook om andere negatieve effecten.

De tweede relevante onderscheiding is die naar soorten identificeerbaarheid.[132] Voor het 'privacygevoel' van velen zal het nogal wat uitmaken of een online dienstenaanbieder ons identificeert aan de hand van het IP-adres van de computer die we gebruiken dan wel ons paspoortnummer. Voor diverse online diensten is het namelijk helemaal niet nodig dat we als bezoekers uniek, bijvoorbeeld via een paspoortnummer, worden geïdentificeerd. Heel goed kan een website ons door middel van cookies automatisch herkennen om vervolgens het aanbod aan te passen aan eerder gebleken voorkeuren (bijv. de taal-instelling). Wat de aanbieder wil weten is of u *dezelfde* persoon bent als degene die bij eerdere bezoeken een voorkeur had voor onder meer een aanbod in de Nederlandse taal en diensten binnen een bepaalde prijscategorie. Wie u exact bent, in de zin van een mevrouw A, met bankrekeningnummer B, mobiele nummer C of zelfs paspoortnummer D dan wel DNA-profiel E,[133] is voor vele diensten niet relevant. Het proces waarbij met een grote mate van zekerheid wordt vastgesteld welke unieke persoon het betreft, wordt in het reguliere spraakgebruik *identificatie* genoemd (we zullen dit hier "opzoek-identificeerbaarheid" noemen). Dit ter onderscheid van de situatie waarbij het gaat om het vaststellen of het om dezelfde persoon gaat, zonder te weten wie exact het betreft (we zullen dit "herken-identificeerbaarheid" noemen).[134] Er is nog een derde identiteit, waarbij individuen aan een groepsprofiel worden herkend (we

132. Zie over identificeerbaarheid ook Opinie 4/2007 van WP29 over het begrip persoonsgegeven. Deze opinie stelt (wat voor het bredere publiek nog niet zo evident is) dat identificeerbaar (*identifiable*) voldoende is: "Accordingly, the natural person is "identifiable" when, although the person has not been identified yet, it is possible to do it (that is the meaning of the suffix "-able")."
133. Ook commerciële bedrijven, waaronder Google, Amazon en Apple, verzamelen naar verluid steeds meer genetische gegevens van individuen. Zie NRC Handelsblad 4 juli 2015, p. 6-7.
134. Over deze onderscheidingen: Grijpink, Prins, 2001a, p. 379-389; Grijpink, Prins, 2001b, p. 116-127.

zullen dit "categorische-identitificeerbaarheid" noemen). Bij big data-toepassingen spelen alle drie de varianten van identificeerbaarheid een rol.[135]

Herken-identificeerbaarheid: waarbij iemand is te onderscheiden van anderen, maar geen link is te leggen naar de burgerlijke dan wel unieke identiteit van een persoon. Het illustratieve voorbeeld is een cookie, waarbij de website-eigenaar de bezoeker wel kan herkennen, maar deze persoon niet kan relateren aan NAW of andere identificerende gegevens.
Opzoek-identificeerbaarheid: waarbij iemand is te herleiden naar zijn/haar burgerlijke of unieke identiteit. Dit herleiden kan ook indirect, bijvoorbeeld als een gegeven wordt gebruik waarmee uiteindelijk ook de opzoek-identiteit kan worden gevonden, zoals (in veel gevallen bij) een IP-adres of een paspoortnummer (zogenaamde indirect identificerende gegevens).
Categorische-identificeerbaarheid*:* waarbij het niet gaat om het herkennen of identificeren van een persoon als concreet individu, maar een individu in dit geval aan de hand van een groepsprofiel wordt herkend als passend binnen dit groepsprofiel. Vaak worden op basis van de groepsindeling vervolgens nog additionele kenmerken toegedicht, die overigens niet werkelijk op de betrokkene van toepassing behoeven te zijn.

Kader 6

Voor toepasselijkheid van het wettelijk privacykader is niet vereist dat de gegevens die worden verwerkt zijn te herleiden naar iemands opzoek-identiteit. Voldoende is dat iemand kan worden herkend ('*can be distinguished from all other members of the group*').[136] Het onderscheid tussen de opzoek-identificeerbaarheid en herken-identificeerbaarheid lijkt daarmee minder relevant, maar speelt wel een rol bij vereisten van de inrichting van verwerkingen volgens beginselen van *privacy-by-design*. Om de effecten van verlies of diefstal van gegevens te verminderen, zullen bijvoorbeeld de gegevens voor de opzoek-identificeerbaarheid (bijv. NAW-gegevens) gescheiden dienen te worden opgeslagen en verwerkt van andere gegevens die deze persoon betreffen.[137]

Kijkend naar de drie vormen van identificeerbaarheid lijkt de conclusie dat ze in aflopende volgorde effect hebben op de mate waarin onze privacy wordt geraakt. Echter, bij big data-toepassingen kan juist de laatste categorie (waarbij iemand aan een groepsprofiel wordt herkend) grote implicaties hebben, omdat in dat geval vaak ook attributen worden toegevoegd (zogenaamde *geïnduceerde gegevens*, zie hierna). Deze kunnen onjuist

135. Zie voor deze aanduidingen: Leenes, 2007, p. 148-153.
136. Zie WP Opinion 04/2007, p. 12.
137. Wij gaan in paragraaf 5.2 nader op privacy-by-design in.

zijn (of griezelig juist, zoals het in de Inleiding genoemde voorbeeld van de supermarktketen Target, die reclameaanbiedingen voor babyproducten stuurde aan vrouwen die plotseling geurloze cosmeticaproducten gingen kopen). Dergelijke attributen kunnen ook stigmatiserend werken en zijn veelal niet inzichtelijk voor het individu.

De laatste voor ons betoog relevante onderscheiding betreft het type gegeven dat wordt gebruikt. In navolging van de OECD maken we onderscheid tussen gegevens die:[138]

- hun oorsprong vinden in directe handelingen van het individu, en waarbij de betrokkene zich ervan bewust is dat de betreffende handeling leidt tot de verwerking van gegevens (*verstrekte gegevens*);
- buiten het individu om worden verzameld. Al veel langer zijn camera's hier een illustratief voorbeeld, meer recent verzamelen niet alleen bedrijven maar ook onze vrienden gegevens over ons om deze vervolgens te delen via sociale media (*geobserveerde gegevens*);
- logisch kunnen worden afgeleid uit de combinatie van bestaande gegevens (*gededuceerde gegevens*);
- niet logisch kunnen worden afgeleid uit de beschikbare combinatie van gegevens over het individu, maar wel te verkrijgen zijn via de inzet van intelligente systemen en analyse-algoritmes (*geïnduceerde gegevens*).

Voor de drie laatstgenoemde type gegevens geldt dat individuen veelal niet van het bestaan en het gebruik daarvan op de hoogte zullen zijn. Kortom, transparantie is lang niet altijd gegarandeerd. Tegelijkertijd zien we ook dat dit probleem het sterkst is bij geïnduceerde gegevens, nu het gebrek aan transparantie niet alleen de gegevens als zodanig en de uitkomst van de data-analyse betreft, maar ook de logica op basis waarvan deze uitkomst wordt gegenereerd.[139] Bovendien worden in het geval van geïnduceerde gegevens attributen toegevoegd die, zoals al opgemerkt, onjuist maar ook griezelig juist kunnen zijn.

Verstrekte gegevens*:* gegevens die hun oorsprong vinden in directe handelingen van het individu, en waarbij de betrokkene zich ervan bewust is dat de betreffende handeling leidt tot de verwerking van gegevens. Illustratieve voorbeelden zijn gegevens die worden verstrekt bij aanvraag van een lening (geïnitieerde gegevens), gegevens die worden gecreëerd bij de aankoop van een product (transactiegegevens) of gegevens die door betrokkene zelf actief via social media worden gedeeld. De OECD noemt dergelijke gegevens 'posted data', waarbij men er kennelijk vanuit gaat dat het publieke informatie

138. OECD, 2014, p. 5, onderscheidt: provided data, observed data, derived data en inferred data.
139. Zie eerder in dit preadvies de 'black box' in Kader 4.

betreft. Dit behoeft natuurlijk lang niet altijd het geval te zijn. Denk bijvoorbeeld aan gegevens die op Facebook zijn gezet, maar alleen toegankelijk zijn gemaakt voor een beperkt aantal vrienden.[140] We zullen gegevens die door betrokkenen daadwerkelijk voor het brede publiek toegankelijk zijn gemaakt, in het vervolg publieke gegevens noemen,[141] maar deze wel onder de categorie verstrekte gegevens plaatsen.

Door observatie verkregen gegevens*:* gegevens die buiten het individu om over hem/haar worden verzameld. Al veel langer worden bijvoorbeeld camera's hiervoor ingezet. Meer recent verkrijgen bedrijven en overheidsorganisaties dergelijke gegevens ook met behulp van cookies of sensoren. De via het IoT gegenereerde gegevens vallen bijvoorbeeld onder deze categorie.

Door deductie verkregen gegevens*:* gegevens die logisch kunnen worden afgeleid uit de combinatie van bestaande gegevens over het individu. We noemen hier het gegeven dat een klant van een bedrijf tot de categorie meest bestedende klanten behoort.

Geïnduceerde gegevens*:* gegevens die niet logisch kunnen worden afgeleid uit de beschikbare combinatie van gegevens over het individu, maar wel te verkrijgen zijn via de analyse van gegevens van anderen door middel van inzet van intelligente systemen (analyse-algoritmes). Het meest bekende voorbeeld hier is de genoemde 'Target' kwestie.

Kader 7

De verschillende hiervoor besproken onderscheidingen overziend,[142] moet de conclusie zijn dat onze privacy het meest in het geding is wanneer over ons zgn. *preemptive* voorspellingen worden gedaan aan de hand van groepsprofielen die gebruik maken van *geïnduceerde* gegevens. Kortom, wanneer we worden onderworpen (zonder dat we dit veelal weten) aan voorspellingen die onze toekomstige handelingsopties beperken en dit wordt gedaan met behulp van gegevens die niet logisch kunnen worden afgeleid uit de beschikbare combinatie van gegevens. Het is ook deze vorm van voorspellen en profileren die in het huidig wettelijk kader aan voorwaarden is gebonden (artikel 42 Wbp over geautomatiseerde besluitvorming). Artikel 20(1) van de Verordening Gegevensbescherming bevat een

140. Het betreft dan geen openbaar toegankelijke gegevens, zie ook WP 29 Opinion 03/2014.
141. Anders dan vaak gedacht is de Wbp gewoon van toepassing op de verwerking van openbare gegevens, hoewel de noodzakelijke grondslag voor de verwerking eerder gevonden kan worden. Zie: WP29 Opinion 06/2014.
142. Zonder overigens te willen aangeven dat dit dè relevante en juiste onderscheidingen zijn. Op dit punt is nader onderzoek gewenst.

regeling die vergelijkbaar is met het huidige artikel 42 Wbp: het individu heeft het recht om niet onderwerp te zijn van een besluit dat uitsluitend is gebaseerd op geautomatiseerde verwerking, daaronder begrepen profilering, indien aan dit besluit voor hem/haar rechtsgevolgen zijn verbonden of dit hem/haar in aanmerkelijke mate treft.[143]

2.5 Conclusie

In deze paragraaf hebben we getracht in kort bestek meer duidelijkheid en duiding te geven aan zowel nieuwe vormen van gegevensgebruik als de vragen en dilemma's die deze oproepen. De geschetste achtergronden zijn namelijk ook relevant bij een zorgvuldige toepassing van het beoordelingskader dat we verderop in dit preadvies uitwerken, namelijk of al dan niet sprake is van een gerechtvaardigd belang bij gegevensgebruik. 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. Haken we aan bij de data-analyse als zodanig of gaat het veeleer om de toepassing van de resultaten van deze analyse? 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.[144] 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 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

143. Uitzonderingen zijn geformuleerd in artikel 20(2), waaronder de situatie waarin de verwerking is gebaseerd op toestemming van het individu.
144. Zie eerder ook Moerel, 2015b. En voor kritiek hierop: Lodder, 2015; Kohnstamm, 2015.

regels indien nodig op aan moeten passen.[145] Een oproep tot een dergelijk fundamenteel debat klinkt inmiddels vanuit meer kanten.[146]

3. Responsieve privacyregulering die individuen in staat stelt hun positie vorm te geven

In paragraaf 4 zullen we betogen dat – gegeven de hiervoor geschetste ontwikkelingen – het huidige wettelijk kader op een aantal essentiële onderdelen steeds meer gaat wringen. Alvorens die stap te zetten werken we in deze derde paragraaf eerst het perspectief uit dat wij ten grondslag leggen aan de te presenteren benadering.

3.1 Privacy en persoonsgegevensbescherming

We starten met de begrippen privacy en persoonsgegevensbescherming. Hoewel beide in het dagelijks gebruik vaak in één adem worden genoemd, is het goed ze van elkaar te onderscheiden.[147] Privacy is sinds 1983 als algemeen recht op bescherming van de persoonlijke levenssfeer verankerd in onze Grondwet (art. 10, eerste lid, Gw) en garandeert principieel dat bepaalde persoonlijke of intieme aspecten van ons leven moeten blijven gevrijwaard van inmenging. De bescherming van persoonsgegevens (voortvloeiend uit de instructienormen in art. 10, lid 2 en 3, Gw) bestaat uit een set normen voor behoorlijk gegevensgebruik, in ons land neergelegd in de Wet bescherming persoonsgegevens (**Wbp**). In internationaal verband zijn de normen onder meer te vinden in art. 8 EVRM en het Handvest van de Grondrechten van de Europese Unie, waarbij het Handvest de eerbiediging van het privéleven (art. 7) en de bescherming van persoonsgegevens (art. 8) afzonderlijk benoemd. Met deze expliciete verzelfstandiging van het recht op bescherming van persoonsgegevens gaf de Europese wetgever uitdrukking aan de toegenomen betekenis van een grondwettelijk verankerde bescherming voor persoonsgegevens. In lijn met deze regeling bepleitte in ons land ook de Staatscommissie Grondwet een verzelfstandiging van persoonsgegevensbescherming.[148]

Het recht op bescherming van persoonsgegevens is in gedetailleerde normen uitgewerkt in de Privacy Richtlijn uit 1995, waarvoor enkele jaren

145. Moerel, 2015b.
146. Waaronder vanuit het Verbond van Verzekeraars: De Boer, 2015. Zie ook het redactioneel commentaar Financiële Dagblad, 1 oktober 2015.
147. Zie voor een verhelderende bespreking van het onderscheid tussen de begrippen: Hustinx, 2013. Voor een historisch overzicht van de ontwikkeling van het begrip privacy en privacyregulering, zie: Kranenborg, Verhey, 2011, p.2; Nissenbaum, 2004; Post, 2000.
148. Staatscommissie Grondwet, 2010, p. 81-82.

geleden een herziening in gang werd gezet. Behalve een stevige revisie van het wettelijk kader kiest de Europese wetgever ditmaal voor het instrument van de Verordening.[149] De Europese wetgever erkent daarbij weliswaar dat het kader moet worden versterkt, maar stelt zich op het standpunt dat de inhoudelijke beginselen nog steeds actueel zijn en geen aanpassing behoeven. Wij trekken deze conclusie in dit preadvies in twijfel. Vanuit de diverse ontwikkelingen die wij schetsen is onze stellige overtuiging dat niet alleen bij de eerbiediging van het privéleven, maar evenzeer bij de bescherming van persoonsgegevens vanuit collectieve belangen een beschermwaardige kern dient te worden gegarandeerd. Anders geformuleerd: ook gegevensbescherming zal vanuit het oogpunt van collectieve belangen grensstellend moeten werken. Hoewel het huidige normenkader van de Privacy Richtlijn een toetsing aan collectieve belangen niet in de weg staat, en aldus grensstellend zou kunnen werken, is de wijze waarop de richtlijn in de praktijk wordt toegepast en ook door de toezichthouders wordt gehandhaafd (zie de hierna in paragraaf 3.2 te noemen voorbeelden) beperkt tot een toetsing aan de belangen in voorliggende bilaterale verhoudingen. Bovendien blijkt de toepassing van de normen in de praktijk verworden tot 'mechanisch proceduralisme', waarbij verantwoordelijken mechanisch individuen informeren en hun toestemming verzamelen, zonder daadwerkelijke privacybescherming te bieden. Nu de Verordening op dezelfde weg voortgaat is hier geen verbetering te verwachten.

Belangrijk voor onze overtuiging dat veel explicieter dan momenteel het geval is dient te worden getoetst aan collectieve belangen, zijn de volgende overwegingen.

Startpunt voor de erkenning van het grondrecht op privacy is de overtuiging dat een fatsoenlijke maatschappij het "mensenrecht op ruimte" erkent.[150] Om een uniek mens te kunnen zijn heeft een ieder ruimte nodig; zowel om zich terug te trekken als te ontplooien. En om die ruimte te kunnen garanderen, heeft de overheid zich bovenal te onthouden van *willekeurige* inmenging in de persoonlijke levenssfeer van individuen. Met andere woorden, telkens weer zullen de belangen die een inmenging rechtvaardigen moeten worden afgewogen tegen het legitieme belang van burgers op hun ruimte. Maar behalve dat de overheid zich heeft te onthouden van inmenging, dient ze ook actief de privésfeer *veilig te stellen*. Anders gezegd, onder omstandigheden is de overheid gehouden tot optreden om die ruimte te garanderen. Die opdracht geldt zowel richting overheidsinstellingen, als – en dit is juist voor ons betoog relevant – de private sector en burgers. Een beschermingsverplichting kan kortom aan

149. Voor een verdere bespreking van de voorstellen verwijzen wij onder meer naar: Kuner, 2012; Hijmans, 2014; Cuijpers, Purtova, Kosta, 2014; Burton, De Boel, Kuner, Pateraki, 2015.
150. Mertens, 2012, p. 213.

de orde zijn wanneer het recht op persoonlijke ruimte onder druk staat in relaties tussen burgers en private partijen

Wat dan concreet moet worden veiliggesteld, kortom wat privacy precies inhoudt, is voor velen moeilijk te omschrijven. Van het begrip wordt vaak gezegd dat het diffuus is. Dit komt allereerst omdat privacy een sociaal construct is en als zodanig voortdurend aan verandering onderhevig is. Ter illustratie: vroeger werd door werknemers het lidmaatschap van een vakbond als een privacygevoelig gegeven aangemerkt. Hun salaris, daarentegen, was voor velen min of meer hetzelfde en bekend. Nu is het lidmaatschap van een vakbond bekend, maar beschouwen werknemers veeleer hun financiële situatie als privé. Dit is niet problematisch, het concept van privacy evolueert met de tijd.[151] Een tweede reden waarom privacy als diffuus wordt aangemerkt, is omdat het in de meeste situaties een afwegingskarakter heeft. Voor de reikwijdte van zowel privacy als gegevensbescherming geldt dat de context grote relevantie heeft. Deze reikwijdte wordt namelijk in sterke mate bepaald door de weging die verwerkers, politici, toezichthouders en rechters telkens weer hebben te maken tussen enerzijds bescherming en anderzijds belangen die een inmenging in de privésfeer dan wel het gebruik van gegevens rechtvaardigen. Ook een fundamenteel recht als privacy, zelfs al is het reëel in het geding, kan niet op voorhand in absolute zin de doorslag geven. Zo bepaalt art. 8, lid 2 EVRM dat inmenging op het in lid 1 gegarandeerde recht op respect voor privéleven is gerechtvaardigd indien de inmenging: een legitiem doel dient (te denken valt aan nationale veiligheid), noodzakelijk is in een democratische samenleving en is voorzien bij wet.[152] Behalve dat voor privacy (zoals ook voor andere grondrechten) beperkingen kunnen gelden waar het recht botst met andere grondrechten, wordt de ruimte ook bepaald door kwesties en belangen die in een specifieke context de rechtvaardiging voor een inperking vormen. Overigens heeft Blok er terecht op gewezen dat de context niet de betekenis van privacy vormgeeft. “De vaak verkondigde visie dat de betekenis van het recht op privacy contextueel bepaald zou zijn en per relatie verschilt, berust dus op een misverstand. Niet het recht op privacy als zodanig, maar de rechtvaardigingsgronden voor een inbreuk op privacy, verschillen per context en relatie.”[153] Wat er ook zij van deze discussie, *bottom line* is dat de reikwijdte van privacy weliswaar kan verschillen, maar dat er ook een kern is waarmee exclusieve ruimte blijft voor de privésfeer.

Voor ons staat vast dat een dergelijke kern niet alleen moet zijn gegarandeerd voor de eerbiediging van het privéleven, maar ook voor de bescher-

151. Zie voor deze voorbeelden eerder Moerel, 2014, p. 36, verwijzend naar: European Commission 2011.
152. Voor een recente bespreking van relevante EHRM-jurisprudentie inzake art. 8 EVRM: Galetta, De Hert, 2014, p. 55-75.
153. Blok, 2002, p. 25.

ming van persoonsgegevens. Allereerst geldt dat onze eerdere analyse van de innovatieve vormen van gegevensgebruik toont dat de scheidslijn tussen de privacy- en gegevensbeschermingsfunctie steeds minder duidelijk is te trekken en er een steeds groter schemergebied ontstaat waar privacy en gegevensbescherming in elkaar overlopen. Een simpel voorbeeld is de eerdergenoemde Target-zaak, waarbij een simpele commerciële communicatie onacceptabel indringt in de privésfeer van een tienermeisje en de relatie met haar vader. Voor de toekomst geldt dat het schemergebied alleen maar groter zal worden. Te denken valt aan allerhande Internet of Things-toepassingen die de beslotenheid van ons huis dan wel de integriteit van ons lichaam raken. Van diverse kanten is inmiddels opgemerkt dat het onderscheid steeds problematischer wordt.[154] Een diepgaande discussie over het al dan niet verlaten van het 'digitale' onderscheid tussen privacy en gegevensbescherming valt buiten de reikwijdte van dit preadvies. Voor ons staat echter wel vast dat het onderscheid steeds meer aan relevantie inboet.

Steun voor onze opvatting dat ook voor persoonsgegevensbescherming heeft te gelden dat individuen meer wordt geboden dan primair de garantie op een zorgvuldige verwerking van gegevens, vinden wij in het eerdergenoemde op EU-niveau grondwettelijk verankerde opdracht voor niet alleen de eerbiediging van het privéleven (art. 7), maar juist ook de bescherming van persoonsgegevens (art. 8). De Europese wetgever beoogde daarmee de bescherming van persoonsgegevens aanzienlijk te versterken, en gewicht te geven dat uitgaat boven wat in de betreffende bilaterale verhouding als behoorlijk gegevensgebruik dient te worden aangemerkt. Met de grondwettelijke erkenning van gegevensbescherming heeft de Europese wetgever overduidelijk het signaal afgegeven dat ook het collectieve belang dat bij gegevensgebruik in het geding is, op het netvlies dient te staan.

Niet langer alleen het recht op privacy, maar ook dat van gegevensbescherming is – zoals we bijvoorbeeld zagen bij de bespreking van 'pay-how-you-drive' – een voorportaal voor de bescherming van andere fundamentele rechten en vrijheden van het individu. Al deze rechten gezamenlijk zijn weer instrumenteel voor het goed functioneren van onze democratische samenleving. Ook de rechtmatigheid van gegevensgebruik zal daarom vanuit collectieve belangen moeten worden beoordeeld. Een individu kan bijvoorbeeld belang hebben bij een pay-how-you-drive verzekering (omdat hij/zij dan voor een lagere premie in aanmerking komt). Indien het collectief belang in de afweging wordt betrokken zal de afweging echter zomaar anders kunnen uitvallen. Juist bij big data-toepassingen zal het type informatie dat beschikbaar komt vaak (ook) het collectieve belang dienen. Zo zal data-analyse van *life style* gegevens gecombineerd met ziektekosteninformatie ons inzichten verschaffen in verleden, heden

154. Clarke, 2000; Finn, Wright, Friedewald, 2013, p. 3-32; Wright, Raab, 2014, p. 277-298.

en toekomst van een bepaald type individu en daarmee wetenschappelijke en maatschappelijke waarde verschaffen. Maar de uitkomst van die analyse vertelt evenzeer een onvolledig verhaal dat potentieel instrumenteel kan worden in het ten onterechte profileren van individuen als specifiek type mensen of bevolkingsgroepen. Een goede belangenafweging hier vereist dat aan beide zijden het collectief belang wordt betrokken. Dit zien we bevestigd in de recente rechtspraak van het EU HvJ en de Opinies van de WP29. Ook collectieve belangen moeten worden betrokken in de afwegingen, zo is hier het overduidelijke signaal.[155] Pas dan wordt recht gedaan aan de grondwettelijke verankering op EU-niveau van persoonsgegevensbescherming. Het is deze overtuiging die ten grondslag ligt aan ons voorstel en de in paragraaf 5.1 geformuleerde aanbeveling aan de WP29 om in zijn opinies ook aan te geven welke verwerkingen niet aan de vereiste maatstaven voldoen.

3.2 Responsieve regulering voor privacy capabilities

In aanvulling op het voorgaande, laten wij ons bij de zoektocht naar een alternatieve aanpak in belangrijke mate inspireren door de overtuiging dat de normsteller zich bij het formuleren van concrete regulering mede dient te verplaatsen in de diverse bij gegevensgebruik betrokken actoren (primair verwerkers en individuen), hun belangen en de reële mogelijkheden om deze belangen vorm en inhoud te geven. Onze voorgestelde benadering is daarom gestoeld op twee uitgangspunten.

Ten eerste is dat het concept van *responsieve regulering*, dat voorschrijft dat empirisch waarneembare praktijken en instituties regulering en handhaving mede dienen te voeden en effectiviteit en legitimiteit dienen te geven. Kernelementen van responsieve regulering zien we ook terug in de recente ambities van de Europese Commissie wat betreft *Better Regulation* of *Smart Regulation*.

> "'Better Regulation' means designing EU policies and laws so that they achieve their objectives at minimum cost. Better Regulation is not about regulating or deregulating. It is a way of working to ensure that political decisions are prepared in an open, transparent manner, informed by the best available evidence and backed by the comprehensive involvement of stakeholders."
>
> http://ec.europa.eu/smart-regulation/guidelines/index_en.htm

155. Zie Zaak C-131/12 Google Spain and Google Inc, 13 mei 2014, EU:C:2014:317 en Zaak C-362/14, Schrems, 6 oktober 2014, EU:C:2015:650. Zie ook Opinie WP29 06/2014. In meer detail over de uitspraken van het HvJ: Kranenborg, 2014; Hijmans 2016.

Het tweede uitgangspunt is de overtuiging dat ook in de huidige tijd een samenleving haar burgers moet garanderen dat privacy daadwerkelijk iets voorstelt. Dat is de kern van de opdracht die in artikel 16 EU Verdrag is neergelegd en vormt ook de grondslag van de jurisprudentie EU HvJ.[156] En als blijkt dat de overheid daartoe een veel actievere rol heeft te vervullen dan in het verleden, dan dient ze zich aldus sterk te maken. Juist nu privacy, zoals hiervoor al besproken, weliswaar een kern kent maar buiten deze kern contextuele inkleuring krijgt (en daarmee als zodanig geen gefixeerd begrip is), wordt de inhoud van dit recht ook bepaald door de mogelijkheden die iemand heeft om van dit recht gebruik te maken. Gebruikmakend van een kernelement uit het werk van Nobelprijswinnaar Amartya Sen, menen we dat privacy als fundamentele vrijheid in een nauwe relatie staat tot de kansen en **reële mogelijkheden** die mensen hebben om een bepaalde ruimte voor zichzelf te verwezenlijken.[157] Voor een volwaardig menselijk bestaan moet, aldus Sen, ieder individu in een samenleving kunnen beschikken over de reële vrijheid en mogelijkheden om te kiezen en te handelen. Een goede samenleving is een samenleving die ieder van haar leden in de gelegenheid stelt om boven een bepaald drempelniveau van 'capabilities' uit te kunnen komen.

Als we dit concreet maken voor bescherming van persoonsgegevens betekent het dat de overheid er voor dient te zorgen dat ieder individu werkelijk in staat is eigen levenskeuzen en levensstijlen vorm te geven. Kortom, dat mensen het vermogen hebben (*capability* hebben) om mee te kunnen beslissen over de inrichting van de eigen sociale en informationele leefomgeving, relaties aan te gaan en vorm te geven, een veilig leven te leiden, zich intellectueel in vrijheid te kunnen ontwikkelen en eigen afwegingen te maken over wat goed en niet goed is.[158] Daartoe biedt de huidige procedurele benadering van gegevensbescherming absoluut onvoldoende garanties. Eerder hebben we immers gezien dat de huidige wettelijk gegarandeerde informatierechten en andere transparantievoorwaarden burgers geen betekenisvol inzicht in hun gegevensgebruik bieden, laat staan dat zij over dat gebruik controle hebben en aldus de reële mogelijkheid wordt geboden in vrijheid hun (informationele) levenskeuzen vorm te geven en te garanderen. Daarvoor is meer nodig dan formele regelgeving die in procedurele zin het recht op transparantie of een vereiste van toestemming biedt, maar in materiële zin dat niet (langer) bewerkstelligt. Wie rechtvaardigheid ziet als "het verschaffen van voldoende mogelijkheden aan individuen

156. Zie: Hijmans, 2014, p. 556 , signaleert dat de jurisprudentie van het Europese Hof is gebaseerd op het "principle of effectiveness (*effet utile*): "EU law is not just law on paper, but should be relied on in practice", onder verwijzing naar de zaak C-131/12 Google Spain and Google Inc, 13 mei 2014, EU:C:2014:317.]. Zie tevens: Hijmans 2016.
157. Amartya Sen, 2009.
158. Zo ook: Nussbaum, 2007.

om hun leven vorm te geven en hun rechten überhaupt op te eisen",[159] stelt bijvoorbeeld vast dat het enkele bestaan van een toezichthouder (Autoriteit persoonsgegevens, voorheen College Bescherming Persoonsgegevens) nog geen privacyrechtvaardigheid oplevert, zeker nu ook blijkt dat al jaren sprake is van een handhavingstekort[160] en individuele klachten van burgers niet of slechts in uitzonderlijke situaties worden opgepakt.[161] Belangrijkste is echter dat waar de toezichthouder wel handhavend optreedt, vaak ook een procedurele benadering van privacy is te bespeuren, in plaats van dat (in navolging van het Europese Hof van Justitie)[162] daadwerkelijk wordt getoetst of de kernwaarden van privacy in materiële zin worden aangetast (zie kader).

Hèt voorbeeld hiervan is het standpunt van de toezichthouders (zowel CBP als ACM)[163] inzake het toestemmingsvereiste voor het plaatsen van cookies en met name wat betreft de rechtmatigheid van zogenaamde *cookie walls*. Websitehouders voldoen aan de toestemmingsvereisten door de bezoeker weliswaar toestemming te vragen, maar tegelijkertijd toegang tot hun site en diensten te blokkeren als de bezoeker toestemming weigert. Volgens OPTA zijn cookie walls toegestaan, maar onwenselijk.[164] Het CBP staat cookie walls eveneens toe, met uitzondering van websites die een publieke functie hebben, zoals bijvoorbeeld de 'uitzending gemist'-website van de publieke omroep.[165]

159. Bodelier, 2012, p. 254.
160. http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2007/05/15/onderzoeksrapport-eerste-fase-evaluatie-wbp-literatuuronderzoek-en-knelpuntenanalyse.html
161. Hier liggen capaciteitsgebrek en beleidsmatige overwegingen aan ten grondslag (https://cbpweb.nl/nl/over-het-cbp/taken-en-bevoegdheden/onderzoek-en-handhaving).
162. Zie onder meer: Zaak C-131/12 Google Spain and Google Inc, 13 mei 2014, EU:C:2014:317. Zie: Hijmans 2016 in meer detail over relevante uitspraken en de beoordeling door het HvJ.
163. ACM (voorheen OPTA) is in eerste instantie belast met de handhaving van de cookiebepalingen in de Telecommunicatiewet. Omdat door middel van cookies vaak persoonsgegevens worden verwerkt is ook het CBP bevoegd. In een samenwerkingsprotocol daterend uit 2005 hebben ACM en CBP afspraken gemaakt terzake van handhaving waarbij het CBP de cookieregels "meeneemt" bij meer omvattender onderzoeken naar inbreuken op privacy.
164. Zie Tweakers.net "OPTA: cookiemuur is ongewenst", Joost Schellevis, woensdag 30 januari 2013, te vinden op http://tweakers.net/nieuws/86973/opta-cookiemuur-is-ongewenst.html. Op de website van ACM zijn "Veelgestelde vragen over de cookie regels (2013)" te vinden, waarin (toen nog) OPTA cryptisch is over de vraag of en zo ja wanneer "cookie walls" zijn toegetstaan: zie p. 7: "**Mag ik de toegang tot mijn website ontzeggen aan mensen die geen toestemming geven?** Als een gebruiker geen toestemming geeft voor het plaatsen van een cookie is het mogelijk dat een website niet goed werkt. Het is voor een website niet verplicht een gebruiker toegang te geven en die toegang kan afhankelijk worden gemaakt van het accepteren van een cookie. Echter de cookiebepaling beoogt de gebruiker een keuze te geven ten aanzien van zijn privacy. Als websites gebruikers alleen toegang geven indien alle cookies worden geaccepteerd, wordt de gebruiker juist beperkt in zijn keuze."
165. CBP, 2014.

Het behoeft weinig toelichting dat het toestemmingsvereiste een lege huls wordt als bezoekers bij weigering van toestemming de toegang tot de site en diensten wordt ontzegd. Op grond van de richtlijnen van de WP29[166] en ook de e-Privacy Richtlijn[167] hadden de toezichthouders hier heel wel tot een ander oordeel kunnen (en wat ons betreft: moeten) komen. Ook onder de Verordening zou toestemming hier namelijk niet geldig zijn.[168]

Een vergelijkbare procedurele houding neemt het CBP in ten aanzien van de nieuwe *pay-how-you-drive* verzekeringen. Mits de betrokkenen goed door de verzekeraar worden geïnformeerd en toestemming is verkregen acht de toezichthouder de Wbp uitgespeeld. Zoals besproken, had de toezichthouder ook in dit geval met de huidige wet in de hand tot een ander oordeel kunnen (en wat ons betreft moeten) komen. Nog afgezien van deze beoordeling, de voorbeelden illustreren in ieder geval dat onder het huidige systeem individuen vaak geen daadwerkelijke controle over hun gegevensverwerkingen wordt geboden.

De twee uitgangspunten voor het perspectief dat wij hanteren, impliceren een ambitie om in praktische termen op zoek te gaan naar een normenkader dat realistische mogelijkheden biedt om in de huidige tijd een persoonlijke levenssfeer daadwerkelijk vorm te geven en daarmee wint aan effectiviteit en (inhoudelijke en procedurele) legitimiteit ten opzichte van de huidige aanpak. Voor de liefhebbers lichten we de twee uitgangspunten meer specifiek toe voor de context van privacybescherming en haken daarbij aan bij wat Witteveen de werkelijkheidszin en mogelijkheidszin van regulering heeft genoemd.[169]

Responsieve regulering: werkelijkheidszin en mogelijkheidszin van privacyregulering

In zijn klassieke werk *The Morality of Law* betoogt Lon Fuller vanuit een rechtstheoretische benadering dat uitgangspunt voor goede regulering niet

166. WP 29 Opinion 15/2011.
167. Zie Overweging 25 van Directive 2002/58/EC: "Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose." Dit laatste laat een uitleg toe waarbij het plaatsen van een cookie wall niet is toegestaan voor bijvoorbeeld tracking cookies voor behavioural targeting doeldeinden, omdat hiervoor geen gerechtvaardigd belang kan worden gevonden. Deze bepaling wordt echter vaak geciteerd als onderbouwing voor het standpunt dat cookie walls zijn toegestaan. Zie bijvoorbeeld: Cofone, 2015, p. 208.
168. Artikel 7(4): "When assessing whether consent is freely given, account shall be taken of the fact whether, amongst others, the performance of a contract, including the provision of a service is made conditional on the consent to the processing of data that is not necessary for the performance of this contract".
169. Witteveen, 2010, p. 91.

mag zijn gehoorzaamheid als zodanig.[170] Pas wanneer de norm is gebaseerd op een wederkerige relatie tussen normstellers en zij die deze norm hebben te volgen en bovendien voortkomt uit door actoren gerespecteerde reciprociteit, leggen de normen verplichtingen op. Bedrijven, organisaties en burgers die zich naar de wet hebben te voegen, verwachten daarvan niet alleen een kader voor het handelen dat men als het ware klakkeloos serieus heeft te nemen. Er bestaat bij hen ook een inhoudelijke verwachting over de kwaliteiten die wetten en regels moeten bezitten om aanspraak te kunnen maken op het predicaat wet of regel. Een van de eisen voor die kwaliteit is dat de opstellers van wetten de ervaringen en bevindingen van degenen die ermee moeten werken of ernaar moeten leven ook serieus nemen.[171]

> "If a legal system is inefficient, or indifferent to social needs, it will deliver a cramped, selective and impoverished justice. Legal ideas and institutions must be open to social knowledge and attentive to all legitimate interests. In short, justice requires a responsive social order. (…) Mere openness is not enough, however. A spirit of consultation must prevail and authority be subject to criticism and reconstruction, while the institution's basic commitments, and its capacity to function, are preserved and protected."
>
> Selznick, 1992, p. 463.

Binnen het door Selznick uitgewerkte ideaal van een integratie van recht en samenleving speelt responsiviteit een belangrijke rol. Deze begint wat Sleznick betreft met het creëren en versterken van rechten en rechtsbescherming. In ons land is het pleidooi voor een responsief bestuur door Hirsch Ballin uitgewerkt, waarbij hij overigens de eigen verantwoordelijkheid van burgers sterk benadrukt. Behalve deze eigen verantwoordelijkheid zijn belangrijke elementen van responsief bestuur binnen zijn betoog het vergroten van de overtuigingskracht van het overheidsbeleid en het versterken van het handhavingsvermogen.[172]

Verwijzend naar het werk van Fuller en Selznick wijst Witteveen op het ontbreken van zowel werkelijkheidszin als mogelijkheidszin in de huidige regelcultuur. Er is onvoldoende werkelijkheidszin, dat wil zeggen kennis hoe de regels uitwerken in de praktijk, wat de bedoelde en onbedoelde effecten zijn, op wat voor manier en moment een interventie kans van slagen heeft dan wel succesvol is en hoe organisaties, bedrijven en individuen die met de regels moeten omgaan, het functioneren makkelijker kan

170. Fuller, 1969, p. 23.
171. Zie voor een meer uitgebreide bespreking: Witteveen, 2010.
172. Hirsch Ballin, 1993, p. 16.

worden gemaakt. Bovendien is er te weinig mogelijkheidszin. "De makers van regels denken onvoldoende na over de mogelijkheden en beperkingen van het werken met wetten en regels."[173]

Zonder twijfel tonen onvoldoende werkelijkheidszin en mogelijkheidszin zich ook in de privacyregelcultuur. Er is onvoldoende **werkelijkheidszin** nu de kans van slagen van de regels vaak vooral retorisch wordt omarmd, als ware het een vanzelfsprekend en vaststaand kenmerk van privacywetgeving. Veelal ontbreekt een concrete uitwerking en echte verantwoording van de meer algemene claims en doelen die in het kader van de reguleringsambitie worden geformuleerd. 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? Heeft de wetgever wel voldoende oog voor de risicofactoren en omstandigheden die kunnen verklaren waarom het bestaande wettelijk kader individuen kennelijk zo weinig daadwerkelijke privacybescherming kan bieden? Wat zijn hier de determinanten en spelen hier nog verschillen tussen individuen?

Ook **mogelijkheidszin** is bij privacybescherming problematisch. Illustratief is hier de aankomende Verordening Gegevensbescherming, waarin op een meer algemeen niveau de wetgevingsambitie vanuit een tweevoudig doel is geformuleerd: **a**. het versterken van de rechten van personen inzake bescherming van gegevens en **b**. het verbeteren van kansen voor het bedrijfsleven door het vrij verkeer van persoonsgegevens in de digitale interne markt te faciliteren. Naar goed gebruik benut de Europese wetgever het instrument van de considerans voor de nadere inkleuring van deze doelen. Zo gaat het onder meer om: een krachtiger en coherenter kader voor gegevensbescherming in de EU, dat wordt gesteund door strenge handhaving, omdat dit van belang is voor het vertrouwen dat nodig is om de digitale economie zich op de hele interne markt te laten ontwikkelen. Natuurlijke personen dienen *controle* over hun eigen persoonsgegevens te hebben en er dient meer *praktische rechtszekerheid* te worden geboden aan personen, bedrijven en overheden.[174]

Deze doelstellingen beoordelend vanuit mogelijkheidszin: 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

173. Witteveen, 2010, p. 21.

174. Considerans 6 luidt letterlijk: "In verband met deze ontwikkelingen moet een krachtiger en coherenter kader voor gegevensbescherming in de EU tot stand worden gebracht en bovendien scherp worden toegezien op de handhaving daarvan, omdat zulks van belang is voor het vertrouwen dat nodig is om de digitale economie zich op de hele interne markt te laten ontwikkelen. Natuurlijke personen dienen controle over hun eigen persoonsgegevens te hebben en er dient meer praktische en rechtszekerheid te worden geboden aan personen, bedrijven en overheden."

rationaliteit van actoren in de fysieke wereld al van betekenis is, geldt dat in nog veel 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. "What happens to your family's photo collection if it's held in the cloud and your password goes to the grave with you? And what about your documents and emails – all likewise stored in the cloud on someone else's server".[175] Wie in de huidige tijd nog pretendeert de consequenties in kaart te kunnen brengen van de keuze tot het verstrekken van bepaalde gegevens, zal voor verrassingen komen te staan. Sprekend illustratief is de column van de Nijmeegse hoogleraar Bart Jacobs over de zeer gevoelige gegevens die via allerhande onschuldige websites en Apps worden verzameld.[176] Dit is niet alleen het gevolg van de verspreiding van gegevens over alle hoeken en gaten van de digitale wereld en de diffuse grenzen tussen de organisaties en bedrijven die de gegevens met elkaar (zullen) delen. De consequenties zijn ook onmogelijk helder te krijgen vanwege de sterke dynamiek en verandering. Daarbij komt dat veel online diensten niet tot de grenzen van ons land beperkt blijven en individuen hun keuzes (als ze al een keuze hebben) slechts op basis van een beperkte (tijds)horizon kunnen maken. Echter, een eenmaal gegeven akkoord voor het gebruik van gegevens is niet (of alleen met heel veel moeite) omkeerbaar.

Eén ding is duidelijk: digitalisering is tot in de haarvaten van onze samenleving doorgedrongen, maar niemand is nog in staat deze wereld te overzien. Redenerend vanuit de *capability* benadering (waarbij burgers de reële mogelijkheid moeten hebben om het recht op gegevensbescherming te verwezenlijken) kan de conclusie geen andere zijn dan dat we vraagtekens moeten plaatsen bij een reguleringssysteem dat onder meer sterk leunt op het informeren van burgers en de veronderstelling dat burgers kennelijk zo digitaal vaardig zijn dat ze zelfstandig het gewenste niveau van gegevensbescherming kunnen realiseren.

Onze conclusie is dat gegevensbescherming dient te staan voor niet alleen het bieden van een materieel en procedureel kader voor gegevensbescherming op het niveau van het individuele belang. Het normenkader moet ook de collectieve belangen die bij gegevensverwerking in het geding zijn veilig kunnen stellen. Het gaat dan om zowel het bredere maatschappelijke belang dat is gediend met privacy, als andere waarden die door de ontwikkelingen van big data en het Internet of Things in het geding zijn – autonomie, vrijheid, solidariteit, pluriformiteit en goede gezondheid. Gegevensverwerking is niet langer een aangelegenheid die primair vanuit individuele belangen vorm krijgt, maar beïnvloedt en bepaalt meer en meer

175. Naughton, 2010.
176. Jacobs, 2015, http://pilab.nl/index.php/2015/12/13/nederlands-klantverraders/?lang=nl#more-1543

het klimaat van onze samenleving. We hebben het dan niet alleen over het klimaat voor innovatie, maar juist ook over het sociale, maatschappelijke en morele klimaat in onze samenleving. Wat ons betreft noopt dit tot een zoektocht naar een reguleringskader dat behalve het individuele belang ook het collectieve – publieke – belang vertegenwoordigt. Resultaten en implicaties van grootschalige data-analyse betreffen immers niet slechts grote aantallen individuen, maar zeker ook bestaande en nieuw op grond van deze analyse te onderscheiden collectiviteiten.[177] En daarmee zijn we ook weer terug bij onze eerdere stelling dat het onderscheid tussen privacy en persoonsgegevensbescherming dient te worden heroverwogen.

4. Proeve van een alternatief kader

Voorzien van de bagage gepresenteerd in de voorgaande paragrafen, keren we terug naar het wetgevend kader. We beargumenteren in het onderstaande dat leidende uitgangspunten in het huidige wettelijke kader door nieuwe fenomenen als big data en het Internet of Things onder druk komen te staan. We bespreken achtereenvolgens het vereiste van doelbinding, het regime voor bijzondere persoonsgegevens, het recht van individuen op informationele zelfbeschikking en de eisen aan kwaliteit van gegevens. We zullen vervolgens de door ons voorgestelde alternatieve aanpak in het licht van deze criteria bespreken en telkens aangeven hoe ons voorstel de gesignaleerde knelpunten adresseert. Afsluitend rapen we de verschillende onderdelen bijeen en presenteren we de door ons voorgestelde toets in z'n volledige vorm. Zoals we zullen zien sluit onze benadering in veel opzichten aan bij de wijze waarop WP29 de gerechtvaardigd belang-toets nu al heeft uitgewerkt.[178] Onze inschatting is dat ook deze werkgroep de knelpunten in de huidige wetgeving inmiddels heeft gesignaleerd en voorsorteert op een regime waarin de gerechtvaardigd belang-toets, inclusief de als onderdeel daarvan uit te voeren belangenafweging en te treffen mitigerende maatregelen, leidend wordt.

4.1 Doelbinding is onvoldoende beperkend

De toets die momenteel vanuit het beginsel van doelbinding aan gebruikers van persoonsgegevens wordt opgelegd, bestaat uit twee elementen:[179]

– gegevens mogen alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verkregen en verwerkt (*doelspecificatie*); en

177 Zie eerder hierover in verband met biobanken: Somsen, 2009, p. 54.

178. Zie Kader 2 en bijbehorende voetnoot voor meer details.

179. Artikel 6(1)(b) Privacy Richtlijn en artikel 7 en 9 Wbp; vergelijk art. 5(b) en 6(4) Verordening Gegevensbescherming. Zie ook WP29 Opinion 03/2013, p. 20.

– deze gegevens mogen vervolgens niet verder worden verwerkt op een wijze die onverenigbaar is met die doeleinden (*verenigbaar gebruik*).

Onderdeel van de eerste beoordeling is dat het doel waarvoor de gegevens worden verwerkt *gerechtvaardigd* dient te zijn. De wetsgeschiedenis van de Privacy Richtlijn geeft aan dat daartoe moet worden getoetst of de verzameling van gegevens *rechtmatig* is, waarmee wordt gedoeld op een toetsing aan zowel de Richtlijn als het recht van de Lidstaten.[180]
Ook het vereiste van *data minimalisatie* is verbonden aan het doel: niet meer gegevens mogen worden verwerkt dan noodzakelijk voor dit doel.[181]
Wat betreft de toets van *verenigbaar gebruik* valt op dat deze als een dubbele negatie is geformuleerd (gegevens mogen **niet** verder worden verwerkt als verwerking **on**verenigbaar is). De toets van verenigbaar gebuik is in feite een uitzondering op het beginsel van doelbinding, waarbij de wetgever flexibiliteit heeft gebracht voor verwerkingen voor andere doeleinden dan het oorspronkelijke doel waarvoor de gegevens werden verzameld. Deze secundaire doeleinden behoeven daarbij niet verenigbaar te zijn met dit oorspronkelijke doel, maar mogen niet **on**verenigbaar zijn. Juister zou dus zijn te spreken van een verbod op onverenigbaarheid. Dit is mooi verwoord door de Engelse 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."[182]

Het doelbindingsbeginsel is vastgelegd in het EU Handvest[183] en vormt een van de grondbeginselen voor gegevensbescherming van de Privacy

180. Zie Dammann, Simitis, 1979 commentaar bij artikel 6 (1) sub b op p. 137 en p. 140. Zie verder WP29 Opinion 03/2013, p. 20, waar WP29 stelt dat 'in accordance with the law' betekent de 'law in the broadest sense'. "This includes all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and taken into account by the competent courts".
181. Art. 6(1)(c) Privacy Richtlijn en artikel 11 Wbp; vergelijk art. 5(1)(c) en (e) Verordening Gegevensbescherming.
182. United Kingdom's Information Commissioner's Office, 2014, p. 21.
183. Het EU Handvest heeft sinds december 2009 de status van een Verdrag, zie artikel 8(2): "Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet." Indien ons voorstel zou worden doorgevoerd betekent dit dus dat het EU Handvest zal moeten worden gewijzigd.

Richtlijn en vindt zijn oorsprong in internationale normen die de OESO[184] en de Raad van Europa al eerder ontwikkelden.[185] Bij de vaststelling van de Privacy Richtlijn in 1995, toonde het beginsel zich nog een werkbare norm voor het beoordelen van de rechtmatigheid van een gegevensverwerking.[186]

In de huidige datagedreven maatschappij lijkt dat echter steeds minder het geval te zijn. We merkten al eerder op: daar waar persoonsgegevens in het verleden primair een bijproduct waren van het doel waarvoor zij werden verzameld, zijn ze dat met de nieuwe mogelijkheden tot het combineren, analyseren en verrijken van data lang niet meer altijd.[187] In tegendeel, gegevens worden juist verzameld om vast te stellen welke diensten interessant en waardevol zijn om te gaan leveren. In de inleiding gaven we al het voorbeeld van verzekeraars die data-analyse juist inzetten voor hun zoektocht naar nieuwe producten en diensten. Een voorbeeld waar we vrijwel nu al allemaal mee in aanraking komen zijn de online dienstenaanbieders die websitebezoekersgegevens verzamelen (het surfgedrag van de bezoekers van de site: welke producten heeft de bezoeker aangeklikt maar niet gekocht?, waar verbleef hij/zij het langst op de site?, hoe is de bezoeker door de site genavigeerd en welke informatie en aanbiedingen heeft hij/zij bekeken?). Bijna allemaal verzamelen ze dergelijke gegevens. Toch is het verzamelen daarvan niet strikt noodzakelijk voor het verlenen van toegang tot de website. Uiteraard zijn ze wel nuttig voor analysedoeleinden om zo de website en diensten te kunnen verbeteren. Hier geldt dat het gestelde doel (analyse ter verbetering en het ontwikkelen van dienstverlening) niet langer op voorhand beperkend is voor zowel aard als omvang van de gegevens die worden verwerkt omdat het samenvalt met het belang van de aanbieder om de gegevens te verzamelen. Met deze ontwikkeling boet het beperkend oogmerk van doelbinding aan relevantie in.

Illustratief is ook het Internet of Things (IoT), waarbij meer en meer objecten in zowel de publieke ruimte (lantaarnpalen, wegdek van de snelweg) als (meer of minder) besloten omgevingen (koelkast, huis, auto) worden voorzien van sensoren die metingen verrichten en data verzamelen. Deze gegevens worden vervolgens gedeeld dan wel gekoppeld aan andere data (zoals in het geval van auto's gegevens van de RDW, TomTom, Facebook, Q-Park, etc.),[188] onder meer om via analyse van de gecombi-

184. Zie paragraaf 9 van OECD, 1980: 'The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose'.
185. Zie artikel 5(b) van Raad van Europa, 1981.
186. Dammann, Simitis, 1997, p. 139, sub 5 noemen het doelbindingsvereiste een centraal concept voor de Europese Richtlijn. Zie verder Opinie 03/2013, p. 4.
187. Zie eerder: Moerel, 2014, p. 5.
188. Voor nieuwe, op data gebaseerde, diensten in de automobielindustrie, zie: http://oem.myremoto.com/ en http://incadea.com/pages/en.php

neerde data op zoek te gaan naar nieuwe diensten. In dit geval is het doel van de gegevensverzameling het benutten van de gegevens zelf en niet een afgeleide van een dienst (boeken van reizen) die met het gegevensgebruik als zodanig niets van doen heeft. Zolang het doel niet samenvalt met het verwerken van gegevens kan het doelbindingsbeginsel een beperkende test zijn.[189] Maar als gegevensverzameling en analyse zelf het doel is, is doelbinding niet langer betekenisvol. En dat is problematisch nu de gegevensverwerker een belang bij het doel heeft en de wetgever het tegelijkertijd ook aan hem overlaat het doel van de gegevensverzameling vast te stellen. De enige beperking daarbij is dat het doel 'rechtmatig' dient te zijn, dat wil zeggen niet in strijd met de wet in ruime zin. Voor veel big data- en IoT-toepassingen zal gelden dat deze op zich rechtmatig zijn. Bij relatief onschuldige toepassingen kan men hierover nog de schouders ophalen. Maar om weer het voorbeeld van sensoren te nemen: deze bevinden zich nu nog in apparaten en objecten. Tegelijkertijd is het aantal toepassingen groeiende waar sensoren in het menselijk lichaam worden geplaatst.[190] Binnen de gezondheidszorg wordt hard gewerkt aan een breed scala aan wearables[191] en sensor-gebaseerde toepassingen en die gaan verder dan het welbekende voorbeeld van de defibrillator van de voormalige vicepresident van de VS, Cheney, die bevreesd was voor hackers die het apparaat op afstand zouden kunnen uitschakelen.[192]

Het **doel** van deze toepassingen (bevordering van de gezondheid) zal niet onrechtmatig zijn, waarmee de drempel van het doelbindingsbeginsel is genomen. Veel relevanter in de beoordeling is wat ons betreft echter het **belang** bij het gegevensgebruik en of dit belang – vanuit een bredere beoordeling dan uitsluitend het belang van de verwerker – als gerechtvaardigd valt aan te merken.

In de Inleiding van dit preadvies hebben we de inzet van ons preadvies al kort geformuleerd: doelbinding als separaat criterium zal moeten worden losgelaten en de gerechtvaardigd belang-grondslag zal de centrale (en enige) toets voor de verschillende fasen van de levenscyclus van persoonsgegevens moeten zijn. Wie nauwlettend de beleidsdocumenten van de EU Artikel 29 Werkgroep (**WP 29**) doorneemt, stelt vast dat daarin impliciet

189. Alhoewel ook los van de geschetste ontwikkelingen het doelbindingsbeginsel de afgelopen jaren meer en meer werd opgerekt en het beperkende karakter daarmee is uitgehold. Zie: Prins, 2011, p. 9-21. Zie tevens Brouwer, 2010, p. 273-274.
190. Zie voor voorbeelden van implanteerbare items en 'elektronische' medicijnen: Schmidt, Cohen, 2013, p. 25-26. Betoogd wordt dat uiteindelijk het internet zelfdenkend wordt en rechtstreeks met ons brein zal communiceren. Zie: Kurzweil, Director of Engineering of Google in een interview met Keith Kleiner, te vinden op http://www.youtube.co/watch?v=YABUffpQY9w.
191. https://www.computable.nl/artikel/achtergrond/zorg/5155745/1444691/wearables-zijn-toekomst-van-gezondheidszorg.html
192. http://www.independent.co.uk/news/world/americas/dick-cheney-altered-heart-defibrillator-over-terrorist-attack-fears-8891416.html.

al een verschuiving naar een meer leidende rol voor de gerechtvaardigd belang-toets doorklinkt. Op z'n minst is sprake van een worsteling van de WP 29 met de toetsende rol van doelbinding enerzijds en het gerechtvaardigd belang anderzijds. In de beleidsdocumenten hield de WP29 bij de beoordeling of een verwerking voldoet aan de Privacy Richtlijn steevast de volgorde aan van de betreffende bepalingen van deze richtlijn: eerst de beoordeling op grond van artikel 6 of is voldaan aan het doelbindingsvereiste (*mogen de gegevens worden verzameld voor het beoogde doel*) om vervolgens te beoordelen of er een grondslag was voor de verwerking van de gegevens op de voet van artikel 7 (of artikel 8 wat betreft bijzondere gegevens).[193] Maar opvallend genoeg is in de recente Opinie van de WP29 over het Internet of Things de volgorde ineens omgedraaid.[194] Eerst toetst de WP29 of er een grondslag is voor de verwerking (de gerechtvaardigd belang-grondslag) om vervolgens pas de toets van doelbinding ter hand te nemen: niet meer data mag worden verwerkt dan gerechtvaardigd voor het **doel zoals gespecificeerd** door de verantwoordelijke (hetgeen *de facto* samenvalt met het **gerechtvaardigd belang** van de verantwoordelijke). Redenerend vanuit de door ons geformuleerde uitgangspunten voor responsieve regulering is de stelling: als dit de wijze is waarop de toets kennelijk moet worden toegepast, getuigt het dan niet van een streven naar effectieve regulering door de normatieve beoordeling te vereenvoudigen en doeltreffender te maken namelijk via één en dezelfde toets: is er een gerechtvaardigd belang voor de verschillende verwerkingshandelingen: het verzamelen, verwerken, verder verwerken en vernietigen?

Een tweede aanwijzing voor de impliciete erkenning door de WP29 van een leidende rol voor de gerechtvaardigd belang-toets vinden we in het feit dat de werkgroep inmiddels heeft aangegeven dat de *contractuele relatie* een relevante factor is bij de belangenafweging die een verwerker heeft te maken. De WP29 wijst in dit verband op de volgende punten die bij de vaststelling of sprake is van een gerechtvaardigd belang meegenomen moeten worden: in welke hoedanigheid handelen het individu (werknemer, consument) en de verantwoordelijke (werkgever, bedrijf – al dan niet vanuit een machtspositie); onder welke omstandigheden vindt de gegevensverwerking plaats (is bijvoorbeeld sprake van een (contractuele) afhankelijkheid van de consument?), en wat zijn de gerechtvaardigde verwachtingen van het individu (die voor een groot deel worden bepaald door de aard van de relatie tussen het individu en de betrokkenen, w.o. of sprake is van een contractuele relatie, of toezeggingen gedaan ten tijde van de verzameling van de gegevens). Daarbij geldt dat hoe specifieker de relatie is, hoe meer beperkingen er waarschijnlijk voor het gebruik van

193. Zie bijvoorbeeld WP29 Recommendation 2/2001, p. 7.
194. WP29 Opinion 8/2014, para. 4.2: legal basis for the processing (article 7 of Directive 95/46) en para. 4.3: principles relating to data quality (waar het doelbindingsbeginsel wordt besproken).

de data zullen zijn.[195] Kort samengevat concluderen we dat de lijn van de WP29 een verschuiving impliceert. Het zwaartepunt in de beoordeling ligt niet langer bij de vraag of de verwerking is toegestaan op grond van een overeenkomst, maar of sprake is van een gerechtvaardigd belang, mede **in het licht** van een contractuele relatie tussen partijen.

Kritiek op loslaten doelbindingsvereiste

In de literatuur en door de toezichthouders is betoogd dat met het loslaten van het doelbindingsvereiste de privacybescherming op de tocht komt te staan.[196] Dit, omdat de toets van doelbinding in twee opzichten verder zou gaan dan de gerechtvaardigd belang-toets:

(i) doelbinding omvat mede de toets dat de verwerking rechtmatig is, d.w.z. in overeenstemming is met de wet (in de ruimste zin van het woord). Met andere woorden, de eis is wel degelijk normstellend;
(ii) doelbinding noodzaakt tot het expliciet specificeren van het doel vóórdat de verzameling en verwerking van de gegevens plaatsvindt. Anders gesteld:doelbinding speelt als criterium al een rol **voordat** de gegevens mogen worden verzameld en verwerkt, terwijl bij de grondslag van gerechtvaardigd belang pas achteraf verantwoording dient te worden afgelegd.

Aanvullende kritiek is dat:

(iii) de gerechtvaardigd belang-toets met een open norm werkt en daarmee onvoldoende sturend kan zijn, vatbaar is voor verschillende interpretaties door de handhavende instanties en aldus onvoldoende rechtszekerheid biedt aan verwerkers;
(iv) de toets in eerste instantie door de verantwoordelijke zelf dient te worden uitgevoerd.

We zullen deze punten van kritiek hierna bespreken en met de laatste twee beginnen.

Re (iii) en (iv) toets is onvoldoende sturend en wordt door de verantwoordelijke zelf uitgevoerd

Hierover kunnen we kort zijn. Voorzover de kritiek al terecht zou zijn, is de situatie in ieder geval niet anders dan deze nu reeds het geval is. Ook

195. Opinie WP29 06/2014, p. 40
196. Rauhofer, 2014, p. 152-153; Cuijpers, Purtova, Kosta, 2014, p. 7-8; Zie voor fundamentele kritiek op de gerechtvaardigd belang-grondslag Ferretti, 2014, p. 858-862 en voor kritiek op ondermijning van het doelbindingsvereiste Brouwer, 2010, Chapter 14. Zie voor de positie van de privacytoezichthouders en privacy belangenorganisaties, de Opinie WP29 06/2014.

wat het doelbindingsvereiste geldt dat het de verantwoordelijke zelf is die het doel specificeert, en verder de grondslag kiest en doorvoert. In veel gevallen is die grondslag ook nu al de gerechtvaardigd belang-grondslag. Toetsing van zowel naleving van het doelbindingsvereiste als grondslagvereiste gebeurt ook nu achteraf (uitzonderingen waarbij specifieke verwerkingen vooraf door de toezichthouder moeten worden getoetst daargelaten).[197] Verder geldt dat, zoals bij zoveel andere open normen (denk aan het verbod op 'misleidende reclame'), deze uiteindelijk in de rechtspraak moet uitkristalliseren, waarmee duidelijk wordt hoe de afweging in nieuwe gevallen uit zou moeten pakken. Het EU HvJ heeft inmiddels geoordeeld dat de grondslag van artikel 8(f) Privacy Richtlijn 'rechtstreekse werking' heeft.[198] Nationale rechters zullen hun nationale regels derhalve moeten uitleggen conform EU-jurisprudentie en bij onduidelijkheid prejudiciële vragen moeten stellen. Een recent voorbeeld is de Google Spanje zaak, waar het Hof de toets van artikel 8(f) toepast op verwerkingen van persoonsgegevens door zoekmachines.[199] Aan de betreffende open norm wordt verder invulling gegeven door de WP29 via het uitvaardigen van opinies, zoals de Opinie inzake gerechtvaardigd belang.[200] Dit zal in het door ons voorgestelde systeem niet anders zijn.

Re (i) en (ii) doelbinding is strenger
Anders dan betoogd door de critici, vormen de bovengenoemde elementen wel degelijk onderdeel van de gerechtvaardigd belang-grondslag. De elementen die relevant zijn voor de beoordeling of sprake is van een rechtmatig doel zijn namelijk, *mutatis mutandis,* ook van toepassing op de gerechtvaardigd belang-toets. Met andere woorden, ook bij de beoordeling van gerechtvaardigd belang dient het belang (i) in overeenstemming te zijn met de wet (in de ruimste zin van het woord) en (ii) te zijn gespecificeerd **voordat** de gegevens worden verzameld en verwerkt. Verschil is slechts dat de specificatie niet het **doel** van de verwerking betreft maar het **belang** dat aan de verwerking ten grondslag ligt (alsmede de gemaakte afweging daaromtrent alsook de in dat kader door de verantwoordelijke getroffen mitigerende maatregelen om de implicaties voor de privacy van de betrokken individuen te beperken).

197. Artikel 31-32 Wbp.
198. Het ASNEF-FEMCED arrest van 24 november 2011 (zaken C-468/10 en C-469/10).
199. Zaak C-131/12 Google Spain and Google Inc, 13 mei 2014, EU:C:2014:317. Zie: Hijmans, 2014.
200. Opinie WP29 06/2014.

Zie in deze zin ook de WP29 (vetdruk toegevoegd):
"Accordingly, an interest can be considered as legitimate as long as the controller can pursue this interest in a way that is in accordance with data protection and other laws. In other words, a legitimate interest must be 'acceptable under the law'. In order to be relevant under Article 7(f), a 'legitimate interest' must therefore:
– **be lawful** (i.e. in accordance with applicable EU and national law);
– be **sufficiently clearly articulated** to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently specific);
represent a real and present interest (i.e. not be speculative)."

Opinie WP29 06/2014, p. 25.

Onderdeel van de toets is namelijk dat de door de verantwoordelijke gemaakte belangenafweging wordt gedocumenteerd en bij voorkeur ook wordt gepubliceerd, zodat hierover naar derden verantwoording kan worden afgelegd. Wij verwijzen in deze zin ook naar de Opinie over de gerechtvaardigd belang-grondslag.

"In that sense, Article 7(f) is based on the accountability principle. The controller must perform a careful and **effective test in advance**, based on the **specific facts of the case** rather than in an abstract manner, taking also into account the reasonable expectations of data subjects. As a matter of good practice, where appropriate, carrying out this test should be **documented in a sufficiently detailed and transparent way** so that the complete and correct application of the test could be verified – when necessary – by relevant stakeholders including the data subjects and data protection authorities, and ultimately, by the courts. (…)
The notion of accountability is closely linked to the **notion of transparency**. In order to enable data subjects to exercise their rights, and to allow public scrutiny by stakeholders more broadly, the Working Party recommends that controllers explain to data subjects in a clear and user-friendly manner, the reasons for believing that their interests are not overridden by the interests or fundamental rights and freedoms of the data subjects, and also explain to them the safeguards they have taken to protect personal data, including, where appropriate, the right to opt out of the processing."

Opinie WP29 06/2014, p. 43-44. Vetdruk preadviseurs.

Op basis hiervan kan de conclusie geen andere zijn dan dat de elementen van het doelbindingsbeginsel evenzeer onderdeel uitmaken van de gerecht-

vaardigd belang-toets. Anders geformuleerd, in dit opzicht heeft het doelbindingsbeginsel geen zelfstandige betekenis.

Relevantie doelbinding overige grondslagen

Het beginsel van doelbinding heeft wel een zelfstandige rol voor de overige grondslagen die een verwerking rechtvaardigen, waartoe de voor de private sector relevante grondslagen van toestemming en uitvoering van een overeenkomst. En met deze constatering komen we op een ander cruciaal punt, we zouden kunnen stellen: de e*lephant in the room,* wat betreft het huidige beschermingsregime.

Eerder zagen we al dat de grondslagen van toestemming en uitvoering van overeenkomst in de praktijk vaak worden uitgehold door het feit dat bedrijven weten dat burgers routinematig toestemming geven en voorwaarden accepteren door op de 'OK' button te klikken, terwijl we met een beoordeling via de toets van gerechtvaardigd belang zouden vaststellen dat ze deze toets niet kunnen doorstaan.[201] Problematisch is namelijk dat beide grondslagen geen belangenafweging vereisen, waarbij tevens een factor is welke mitigerende maatregelen door de verantwoordelijke zijn getroffen om de negatieve gevolgen voor de persoonlijke levenssfeer beperken. Anders dan vaak gedacht, kan in dit opzicht de gerechtvaardigd belang-grondslag (die in de noodzaak van deze afweging veel explicieter is) wel eens meer privacybescherming bieden. Treffend is hier de volgende observatie van de WP29:

> "(…) an appropriate assessment of the balance under Article 7(f), often with an opportunity to opt-out of the processing, may (…) be a valid alternative to inappropriate use of, for instance, the ground of 'consent' or 'necessity for the performance of a contract'. Considered in this way, Article 7(f) presents complementary safeguards – which require appropriate measures – compared to the other pre-determined grounds. It should thus not be considered as 'the weakest link' or an open door to legitimise all data processing activities which do not fall under any of the other legal grounds."
>
> Opinie WP29 06/2014, p. 9-10.

Mogelijk is dit de reden waarom de WP29 in de Opinie over doelbinding, voor de beoordeling of er sprake is van een rechtmatig **doel**, ook relevant acht "de algemene context en feiten van het geval", daaronder begrepen "de aard van de onderliggende relatie tussen de verantwoordelijke en de

201. Zie Moerel, 2014.

betrokkenen, of deze nu van commerciële of andere aard is".[202] Op die manier brengt de WP29 in de toets of sprake is van een rechtmatig **doel**, de contextuele belangenafweging in, die zo node wordt gemist bij de grondslagen van toestemming en uitvoering overeenkomst. Problematisch in deze interpretatie van de WP29 is echter dat deze contextuele beoordeling niet terug is te vinden in de wetsgeschiedenis van de Privacy Richtlijn. Daar staat slechts dat de rechtmatigheid van het doel wordt beoordeeld aan de hand van de vraag of het verzamelen van gegevens al dan niet strijdig is met het recht van de lidstaten. Met de aanvulling dat ook een contextuele analyse onderdeel uitmaakt van de toets van rechtmatig doel maakt de werkgroep het toetsingskader voor bedrijven nog weer complexer. Zoals eerder aangegeven moet een bedrijf onder het huidige wettelijke systeem namelijk vier toetsen langslopen:

(i) is er sprake van een rechtmatig doel (*doelspecificatie*);
(ii) worden niet meer gegevens verzameld dan nodig voor dat doel (*data-minimalisatie)*;
(iii) is er sprake van een grondslag voor de verwerking (zoals toestemming, uitvoering van een overeenkomst of gerechtvaardigd belang), en
(iv) is de verdere verwerking van de gegevens niet onverenigbaar met het oorspronkelijke doel van de verzameling (*verenigbaar gebruik).*

Indien de genoemde factoren die de WP29 relevant acht voor de verschillende toetsen[203] – (i) rechtmatig doel, (ii) gerechtvaardigd belang[204] en (iv) verenigbaar gebruik, naast elkaar worden gezet, dan is de conclusie dat **iedere toets** een beoordeling van het feitencomplex en de context van de gegevensverwerking vereist, daaronder begrepen de verhouding tussen verantwoordelijke en individu en de redelijke verwachtingen van het individu. De conclusie is bovendien dat de gerechtvaardigd belang-toets reeds alle gecombineerde factoren omvat van de toetsen (i) rechtmatig doel en (ii) verenigbaar gebruik. Voor de overzichtelijkheid zetten we de toetsen concreet naast elkaar.

202. Opinie WP29 06/2014, p. 12 en p. 20.
203. Zie Kader 1 in de Inleiding van dit preadvies.
204. Zie Kader 2 in de Inleiding van dit preadvies.

Legitimate purpose (WP29)	**Legitimate interest (WP29)**
- must be **specified**, that is, sufficiently defined to enable the implementation of any necessary data protection safeguards, and to delimit the scope of the processing operation	- be sufficiently **clearly articulated** to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently specific); represent a real and present interest (i.e. not be speculative)."
- be **explicit**, the purpose must be sufficiently unambiguous and clearly expressed. - be **legitimate**, this requires that the purposes must be in accordance with all provisions of applicable data protection law, as well as other applicable laws such as employment law, contract law, consumer protection law, and so on. - The notion of legitimacy must also be interpreted within the **context** of the processing, which determines the '**reasonable expectations**' of the data subject.	- be **lawful** (i.e. in accordance with applicable EU and national law);
Compatible use (WP29)	
the relationship between the purposes for which the personal data have been collected and the purposes of further processing;	
- the **context** in which the personal data have been collected and the **reasonable expectations of the data subjects** as to their further use;	the **reasonable expectations of the data subject**, especially with regard to the use and disclosure of the data in the **relevant context**
the **nature of the personal data** and the **impact of the further processing on the data subjects**;	the **impact on the data subjects**, including: - the **nature of the data**, - the way data are being processed; - the status of the data controller and data subject, including the balance of power between the ata subject and the data controller
- the **safeguards** adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.	- additional **safeguards** to prevent undue impact on the data subjects

De Verordening Gegevensbescherming

Voor de in de wetgevingshistorie geïnteresseerde leden van de NJV merken we op dat het er aan de vooravond van de totstandkoming zelfs op leek dat het systeem van de Verordening nog ingewikkelder zou worden. Door de Europese Commissie was in eerste instantie voorgesteld in de Verordening[205] de verdere verwerking van gegevens (dus hergebruik) ook toe te staan indien dit weliswaar onverenigbaar was met het oorspronkelijke doel, maar hiervoor wel een grondslag was, daaronder niet begrepen de gerechtvaardigd belang grondslag. De Raad nam dit voorstel over maar vulde de voor verder gebruik toegestane grondslagen aan met ook de gerechtvaardigd belang-grondslag. Met andere woorden, bovenop de eerder genoemde vier toetsen zou nog een vijfde gelden:

(v) indien niet aan het verenigbaarheidsvereiste van (iv) wordt voldaan, is er dan een grondslag voor de verdere verwerking (inclusief de gerechtvaardigd belang-grondslag).

Dit voorstel stuitte op heftige weerstand bij privacytoezichthouders, privacybelangengroepen en consumentenorganisaties. Zij meenden dat het doelbindingsbeginsel daarmee krachteloos werd.[206] Verdere verwerking was onder het voorstel ook rechtmatig in situaties waar het nieuwe doel geen enkele verbinding had met het oorspronkelijke doel van verzameling. Toch was er niet alleen kritiek. Het voorstel van Commissie en Raad werd in ons land instemmend onderschreven door de minister van Veiligheid & Justitie.

205. Artikel 6(4) van de Verordening Gegevensbescherming zoals aangenomen door de Europese Raad op 15 juni 2015, 9565/15.
206. Zie WP29 Press Release on Chapter II of the draft regulation for the March JHA Council, te vinden op http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20150317__wp29_press_release_on_on_chapter_ii_of_the_draft_regulation_for_the_march_jha_council.pdf. Ook een 65-tal non-gouvernementele organisaties betoogde in een brief aan de president van de Europese Commissie, Junker, dat met invoering van deze nieuwe grondslag de privacybescherming beneden het niveau van de huidige Privacy Richtlijn zou dalen, hetgeen in strijd zou zijn met de eerdere beloften van de Europese Commissie, te vinden op: https://edri.org/citizens-groups-from-around-the-world-call-on-ec-to-defend-privacy/. Zie voor de kernpunten: https://edri.org/files/GDPR-key-issues-explained.pdf and http://protectmydata.eu/topics/limitations/. Zie in deze zin ook: EDPS recommendations on the EU's options for data protection reform. Opinion 3/2015: Europe's big opportunity, 27 juli 2015, p. 7.

"In de praktijk van de verwerking van persoonsgegevens is het echter dringend noodzakelijk gegevens te kunnen verwerken voor andere doeleinden dan waarvoor ze oorspronkelijk werden verzameld. Zou dat niet zo zijn dan zouden de voordelen die ICT aan de samenleving biedt niet kunnen worden benut. (...) De Raad is van oordeel dat het gerechtvaardigd belang wel een rechtvaardigingsgrond is die het gebruik van gegevens voor een ander doel kan ondervangen. (...) geldt dat weliswaar moet worden gewaakt tegen het verlagen van het beschermingsniveau maar dat ook niet te snel moet worden geoordeeld dat elke verandering die de verordening ten opzichte van het bestaande recht brengt een verlaging van het beschermingsniveau betekent. De verordening moet ook met zijn tijd meegroeien en voldoen aan huidige en toekomstige ontwikkelingen."

Brief Minister van V&J van 7 oktober 2015 (Kamerstukken II, 2015/16, nr. 31761, nr. 88).

Ook het Centraal Planbureau (**CPB**) achtte het onder bepaalde voorwaarden mogelijk om doelbinding te verlaten, zo valt in de Policy Brief "Kiezen voor Privacy" te lezen.[207]

Het voorstel van de Commissie/Raad heeft de uiteindelijke versie van de Verordening niet gehaald. Maar wie nauwkeurig kijkt, stelt vast dat de voorgestelde aanvullende toets voor verder gebruik van gegevens (toets vi) duidelijk een poging was om binnen het bestaande kader toch ruimte te scheppen voor hergebruik van gegevens in situaties waar er geen nauwe relatie bestaat met het oorspronkelijk doel. Kortom, ook de Commissie en Raad zagen de noodzaak in om de deur op een kier te zetten voor hergebruik[208] dat is losgekoppeld van het oorspronkelijke doel waarvoor gegevens werden verzameld.[209] Positief geredeneerd kan de conclusie zijn dat de Commissie en Raad hiermee toonden oog te hebben voor de realiteit dat dergelijk hergebruik nu eenmaal inherent is aan digitale innovatie in

207. CPB 2014, p. 12: "Sta een standaardcontract toe waarin doelbinding wordt vervangen door meer algemene voorwaarden voor gebruik, zodat toestemming gegeven kan worden voor hergebruik van gegevens."
208. Het voorstel richtte zich slechts op het hergebruik door de verantwoordelijke zelf. Dit had ons overigens onnodig beperkend geleken. Met de juiste mitigerende maatregelen zou ook hergebruik door derden mogelijk moeten kunnen zijn. Zie ter illustratie van dit punt onder meer de later in dit preadvies genoemde applicatie voor diagnose van hersenbloedingen.
209. Dit met in het achterhoofd de Commissie recent 500 mln heeft geïnvesteerd in een fonds voor het ontwikkelen van publiek-private partnerships op het gebied van big data met als leidende motivatie dat big databedrijven nu veelal uit de VS komen en Europa hier achterblijft. Zie persbericht te vinden op: http://europa.eu/rapid/press-release_IP-14-1129_en.htm.

onze huidige samenleving.[210] En daarmee voor de eerdergenoemde, door Witteveen zo noodzakelijk geachte, werkelijkheidszin.

Tegelijkertijd moeten we constateren dat de wijze waarop de Commissie en Raad de verruiming van hergebruik beoogden te realiseren niet aan de eisen van goede wetgeving voldeed. De voor de hand liggende vraag die de extra toets opriep was allereerst of we dan niet überhaupt zonder het vereiste van 'verenigbaar gebruik' zouden kunnen (immers, er diende sprake te zijn van een grondslag, van verenigbaar gebruik, en als dat er niet was, van een grondslag). De finesse van het onderscheid tussen de vier (en in de voorstellen van de Commissie en de Raad zelfs: vijf) verschillende toetsen was hoogstens voor de juridische fijnproever duidelijk. Afgaande op onze ervaring als docent voor praktijkbeoefenaars en adviseur van bedrijven bij hun privacy-compliance, is onze constatering dat degenen die met de wetgeving in de praktijk moeten werken dit onderscheid volledig zou ontgaan.

Overigens lijkt het erop dat ook in de definitieve versie van de Verordening meer ruimte is geschapen voor de verdere verwerking van gegevens. Zo zijn in de Verordening nu de criteria voor verenigbaar gebruik van de WP29 vastgelegd.[211] Wie het wetgevingsproces nauwlettend heeft gevolgd, stelt vast dat in de definitieve versie van de Verordening plots het criterium "the reasonable expectations of the data subject", is komen te vervallen en is verplaatst naar de Overwegingen van de Verordening.[212] In de versie van het Europese Parlement maakte dit element nog onderdeel uit van de bepaling inzake gerechtvaardigd belang, maar in de definitieve versie is ook dit element overgeheveld naar de Overwegingen van de Verordening.[213] De consequentie van een en ander is dat het subjec-

210. WRR, 2011, p. 229; Prins, 2011, p. 10-21.
211. Art 6 (4) Verordening Gegevensbescherming luidt in de definitieve versie:
"Where the processing for another purpose than the one for which the data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in points (aa) to (g) of Article 21(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the data are initially collected, take into account, inter alia:
(a) any link between the purposes for which the data have been collected and the purposes of the intended further processing;
(b) the context in which the data have been collected, in particular regarding the relationship between data subjects and the controller;
(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9 or whether data related to criminal convictions and offences are processed, pursuant to Article 9a;
(d) the possible consequences of the intended further processing for data subjects;
(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.
212. Overweging 40 Verordening Gegevensbescherming.
213. Overweging 38 Verordening Gegevensbescherming.

tieve element uit zowel de verenigbaarheidstoets als de gerechtvaardigd belang-toets is gehaald. Daarmee is de verwachting dat objectiever zal worden getoetst of sprake is van een gerechtvaardigd belang en/of de verdere verwerking verenigbaar is met het oorspronkelijke doel waarvoor de gegevens werden verzameld. Om onze analyse inzichterlijker te maken zetten we in het navolgende kader de door WP29 relevant geachte factoren wederom op een rij met in de derde column de factoren die uiteindelijk in de Verordening zijn opgenomen.

Compatible use WP29 (Privacy Directive)	**Legitimate interest WP29 (Privacy Directive)**	**Compatible use (Data Protection Regulation)**
the **relationship** between the purposes for which the personal data have been collected and the purposes of further processing		any **link** between the purposes for which the data have been collected and the purposes of the intended further processing
- the **context** in which the personal data have been collected and the **reasonable expectations of the data subjects** as to their further use	the **reasonable expectations of the data subject**, especially with regard to the use and disclosure of the data in the **relevant context**	the **context** in which the data have been collected, in particular regarding the relationship between data subjects and the controller
the **nature of the personal data** and the **impact of the further processing on the data subjects**	the **impact on the data subjects**, including: - the **nature of the data**, - the way data are being processed - the status of the data controller and data subject, including the balance of power between the ata subject and the data controller	- the **nature** of the personal data, in particular whether special categories of personal data are processed, - the **possible consequences** of the intended further processing for data subjects

the **safeguards** adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects	additional **safeguards** to prevent undue impact on the data subjects	the existence of appropriate **safeguards**

Op basis van het voorgaande is onze conclusie dat de Verordening Gegevensbescherming op het punt van complexiteit geen verbetering gaat brengen en het systeem zelfs complexer maakt. Dit zal het toch al geringe draagvlak voor de privacyregelgeving geen goed doen met als concreet risico het ridiculiseren van de regels in plaats van een serieuze poging om deze na te leven. Het is meer dan alleen een publiek geheim dat de privacywetgeving bijzonder slecht wordt nageleefd.[214] De recente substantiële verhoging van de boetes op niet-naleving van de Wbp (die worden vervangen door de eveneens hogere boetes in de Verordening zodra deze van kracht wordt)[215] kan mogelijk een zet in de richting van betere naleving geven. De effectiviteit zal hiermee waarschijnlijk worden verbeterd, maar aan legitimiteit schort het nog steeds. Er is, kortom, dringend behoefte aan een eenvoudiger normenkader. Daarbij brengen we in herinnering dat al bij de eerste evaluatie van de Privacy Richtlijn[216] is geconstateerd dat de regels te strikt en gecompliceerd zijn. In de woorden van het evaluatierapport:[217]

> "An overly strict approach (…) would fail to respect the legitimate needs of international trade (…) and risks creating a gap between law and practice which is damaging for the credibility of the Directive and for Community law in general."

214. Zie destijds al de evaluatie van de voorganger van de Wbp: Prins, Van de Donk, Duivenboden, Nouwt, Ten Have, Vorselaars, Zouridis, 1995; zie meer recent Moerel, 2014, p. 17 en de lijst referenties aldaar in voetnoot 110. Zie ook recent internationaal: Bamberger, Mulligan, 2013, p. 1529.
215. De boete is per 1 januari 2016 verhoogd naar maximaal EUR 810.000 of 10% van de jaaromzet, zie Staatsblad 230, Wet van 4 juni 2015 tot wijziging van de Wet bescherming persoonsgegevens. Ingevolge artikel 79a Verordening Gegevensbescherming kan maximaal een boete voor bedrijven van 4% van de jaaromzet worden opgelegd.
216. Europese Commissie, 2003. Een vergelijkbare observatie is gemaakt door Kuner, 2010, p. 13: "when the jurisdictional scope of the law is much broader than the chance that the law will be enforced, there is a risk that respect for the law will be diminished", en p. 15: "a low chance of enforcement may cause controllers to regard data protection rules as a kind of bureaucratic nuisance rather than as 'law' in the same category as tax laws, employment laws, etc."
217. Europese Commissie, 2003, p. 19.

Wat ons betreft worden zowel effectiviteit als legitimiteit gediend door de gerechtvaardigd belang-grondslag aan te wijzen als de enige toets voor de verschillende fasen van de levenscyclus van gegevens: van het verzamelen, via het verwerken en verder verwerken tot het vernietigen daarvan. Nogmaals, dit betekent niet dat deze toets automatisch meer ruimte biedt dan het doelbindingsvereiste. In sommige gevallen zal de toets juist stringenter uitpakken en meer grensstellend zijn dan nu het geval is. We geven twee voorbeelden ter illustratie.

Een stringentere uitkomst

Illustratief voor een situatie waarin de gerechtvaardigd belang-toets stringenter uitvalt, is de App waarmee we ons pre-advies startten en waarmee gezondheid en ziekte van individuen in kaart kunnen worden gebracht en voorspeld. De gegevens die worden verzameld (waaronder het opgeven van een overzicht van alle mensen waarmee iemand regelmatig in contact komt) zijn waarschijnlijk allemaal dienstig aan het doel van de app. Met andere woorden, het klassieke doelbindingsvereiste legitimeert deze gegevensverwerking. Toetsend aan de door ons voorgestelde gerechtvaardigd belang-toets zal de uitkomst heel anders zijn. Voor de functionaliteit van de App zal namelijk zijn vereist dat gebruikers gegevens over de personen binnen hun sociale netwerk (‘social graph’) invoeren waarna deze gegevens in de analyse worden betrokken. De App heeft daarmee ook implicaties voor de privacy van degenen die niet zelf gebruiker zijn. Niet alleen gezondheids- en andere gegevens van deze personen worden verwerkt, ook hun positie en daarmee gedrag wordt beïnvloed (immers, contact met hen wordt mogelijk gemeden). In de door ons voorgestelde benadering zal de belangenafweging uitvallen in het voordeel van deze derden indien de aanbieder van de App geen nadere maatregelen heeft getroffen om ook de privacy van hen te beschermen en zal de applicatie de toets van gerechtvaardigd belang niet doorstaan. Dit oordeel zal anders uitvallen wanneer de aanbieder van de App de personen in het sociale netwerk van de App-gebruiker nader informeert over de toepassing en hen expliciet om toestemming voor de verdere data-analyse vraagt, bijvoorbeeld via een push up mededeling gekoppeld aan een OK-verzoek.

Een minder stringente uitkomst

Stel een startup heeft een algoritme ontwikkeld voor de diagnose van de ernst van hersenbloedingen en de beste behandelmethode. De bedoeling is de App te verkopen aan ziekenhuizen ter ondersteuning van de diagnoses door de betreffende specialisten. Voor de ontwikkeling van de app is vereist dat het algoritme wordt ’getraind’.

Hiervoor is een groot aantal hersenscans met bijbehorende diagnoses nodig, meer dan bij een individueel ziekenhuis voorhanden zijn. Door deze scans en diagnoses door het algoritme te halen, wordt het algoritme verbeterd en kan de App bij een nieuwe hersenscan een berekening maken van de ernst van de betreffende bloeding en de beste behandelmethode. De scans en diagnoses betreffen gezondheidsgegevens die zijn verzameld door de specialisten in het kader van hun behandelingsovereenkomst (het doel is behandeling van de patiënt). Deze gegevens mogen echter niet worden verstrekt aan de startup voor het 'trainen' van het algoritme. Het verstrekken van de gegevens aan een derde partij (de start up) voor gebruik voor commerciële doeleinden (het ontwikkelen van een commerciële app) betreft namelijk een ander doel dan het doel waarvoor de gegevens oorspronkelijk waren verzameld (geneeskundige behandeling). Daarmee is deze verstrekking niet verenigbaar met het oorspronkelijk doel en niet toegestaan. Deze verwerking voldoet dus niet aan het doelbindingsvereiste, terwijl er een duidelijk 'gerechtvaardigd belang' is bij het ontwikkelen en op de markt brengen van de betreffende applicaties. De ziekenhuizen hebben zelf niet de technische vaardigheden om een dergelijke App te kunnen ontwikkelen, niet genoeg scans en diagnoses voorhanden om het algoritme te kunnen trainen en de ontwikkelingskosten van een dergelijke App zijn te hoog voor een individueel ziekenhuis om te dragen. Dit terwijl de gezondheidszorg gebaat is bij een dergelijke applicatie (specialisten krijgen toegang tot gedeelde kennis en kunde; specialisten kunnen de eigen diagnose toetsen waarmee missers kunnen worden voorkomen, etc.). Op voorwaarde dat het analyse-proces goed wordt beveiligd, gegevens zoveel als mogelijk worden geanonimiseerd (privacy-by-design) en patiënten worden geïnformeerd en een opt-out mogelijkheid hebben, valt de gerechtvaardigd belang-toets in het voordeel van de geschetste ontwikkeling van de App uit. Relevant voor dit oordeel is ook dat de scan- en diagnosegegevens uitsluitend worden gebruikt voor het trainen van het algoritme.

Met in onze rugzak het voorstel om de gerechtvaardigd belang-grondslag aan te wijzen als de enige toets voor de verschillende fasen van de levenscyclus van gegevens, presenteren we in het navolgende eveneens voorstellen hoe om te gaan met **a.** het speciale regime voor de verwerking van bijzondere gegevens (paragraaf 4.2), **b.** de wettelijke vereisten voor transparantie (paragraaf 4.3) en **c.** de kwaliteit van gegevens (paragraaf 4.3).

4.2. Regime voor bijzondere persoonsgegevens knelt en is onnodig ingewikkeld

Onder het huidig wettelijk regime is de verwerking van bijzondere categorieën persoonsgegevens (medische gegevens, geloof, ras, etc) verboden

tenzij hiervoor een specifieke wettelijke grondslag bestaat.[218] In de inleiding stelden we al dat steeds vaker niet alleen relevant is of gegevens (als zodanig) gevoelig zijn. Meer en meer gaat het om gebruik dat gevoelig is. Bedrijven en overheid benutten in aanleg 'onschuldige' gegevens (die deels beschikbaar zijn in het publieke domein) om tot onderscheidingen (discriminatie) tussen individuen te komen. Deze onderscheidingen kunnen bijzonder gevoelig zijn. We gaven als voorbeeld de Target-kwestie, maar er zijn natuurlijk talloze andere voorbeelden. Te denken valt aan Facebook. Het bedrijf blijkt op basis van analyse van niet-gevoelige gegevens die op de Facebookpagina van iemand staan diens seksuele voorkeur te kunnen voorspellen. Of de Amerikaanse data broker Acxiom, die op basis van koopgedrag individuen identificeert met (kennelijke) aanleg voor diabetes. Om het nog maar niet te hebben over de talloze bedrijven die meeprofiteren van de zgn. *tracking* cookies die websites als babyopkomst.nl of erectiestoornis.nl plaatsen.[219]

Ook blijkt de kwalificatie *bijzondere gegevens* gedurende de tijd aan verandering onderhevig. Er zijn diverse soorten gegevens die volgens de wet niet tot de categorie *bijzondere gegevens* behoren, maar die wel bijzonder gevoelig zijn omdat de impact op burgers bij verlies of diefstal groot is. Voorbeelden hiervan zijn wachtwoorden voor toegang tot IT-systemen en websites, credit card-gegevens, bsn-nummers, paspoortnummers, etc. Verder zit de gevoeligheid van gegevens vaak in de *combinatie* van gegevens omdat die bijvoorbeeld bij verlies kunnen worden gebruikt voor geloofwaardige *fishing emails*. Zo is een e-mailadres op zich niet een gevoelig gegeven, maar in combinatie met een wachtwoord wel. Dit omdat veel mensen hetzelfde wachtwoord gebruiken voor toegang tot verschillende websites. Verlies van deze combinatie levert dan risico's op. Een ander voorbeeld is de hack bij het Amerikaanse verzekeringsbedrijf Anthem, waarbij de gestolen gezondheidsgegevens werden gebruikt om ambtenaren bij de Amerikaanse overheid met *fishing emails* te benaderen, wat erin resulteerde dat de personeelsgegevens van 21.5 miljoen Amerikaanse ambtenaren werden gestolen.[220] Ook valt te denken aan situaties waarbij niet-gevoelige gegevens ineens gevoelig worden door deze te koppelen aan gegevens die indirect gevoelige informatie kunnen bevatten, zoals nationaliteit, land van herkomst, en postcode gebied. Tot slot is er ook de andere kant van de medaille: er zijn genoeg voorbeelden van speciale categorieën gegevens die voor het doel waarvoor ze worden verwerkt niet gevoelig zijn, en waarvoor het daarom onnodig is dat deze aan een zwaarder regime worden onderworpen. In de inleiding gaven

218. Deze grondslag kan onder meer worden gevonden in de uitvoering van een specifieke overeenkomst en toestemming van de betrokkene.
219. Jacobs, 2015.
220. Zie: http://www.bloomberg.com/news/articles/2015-07-12/hacked-in-the-u-s-a-china-s-not-so-hidden-infiltration-op.

we het voorbeeld van de pensioenadministratie waaruit indirect seksuele voorkeur kan blijken.

In feite blijkt met de komst van nieuwe analysetechnieken de discussie over welke categorieën gegevens nu wel of niet gevoelig zijn steeds irrelevanter. De praktijk laat zien dat gegevens (en vooral de combinatie van gegevens) in de ene context wel en de andere context niet gevoelig zijn. Het gaat kortom veeleer om de context van het gebruik en veel minder om het gegeven als zodanig. Gevolg hiervan is dat het huidige regime dat uitgaat van de verwerking van speciale categorieën gegevens zijn doel voorbij schiet. In het ene geval knelt het regime omdat de context waarin de bijzondere gegevens worden verwerkt geen specifiek privacygevoelige implicaties oplevert. In het andere geval biedt de wet niet de noodzakelijke extra bescherming omdat het regime voor bijzondere gegevens niet van toepassing is, terwijl de context van de gegevensverwerking wel een zwaardere toets zou rechtvaardigen.

Problematisch bij dit alles is – en hier ligt de verbinding met de centrale stelling van ons betoog – dat bij het regime voor het gebruik van bijzondere gegevens niet wordt getoetst of sprake is van een gerechtvaardigd belang bij dat gebruik. In het huidige regime vormt de grondslag van gerechtvaardigd belang geen wettelijk gelegitimeerde reden voor de verwerking van bijzondere persoonsgegevens. Zonder hier alle grondslagen voor de verwerking van de verschillende categorieën bijzondere gegevens te bespreken, bestaan die vooral uit de uitvoering van specifieke overeenkomsten (bijvoorbeeld gezondheidsgegevens mogen worden verwerkt voorzover noodzakelijk voor een verzekeringsovereenkomst), specifieke doeleinden (bijvoorbeeld gegevens betreffende iemands ras mogen worden verwerkt voorzover dit met het oog op identificatie onvermijdelijk is) en de toestemming van de betrokkene. Deze grondslagen vergen geen belangenafweging, waarbij tevens een factor is welke mitigerende maatregelen door de verantwoordelijke zijn getroffen om de negatieve gevolgen voor de persoonlijke levenssfeer te beperken. Deze afweging wordt geacht te zijn inbegrepen (al te zijn gemaakt door de wetgever) bij de vaststelling van de betreffende wettelijke grondslagen. In dat opzicht kan de gerechtvaardigd belang-grondslag, anders dan vaak gedacht, meer privacy bescherming bieden aan individuen. Dit wordt ook onderkend door de WP29 (zie het eerder opgenomen citaat).[221]

Wat betreft bijzondere persoonsgegevens heeft de WP29 dit ondervangen door aan te geven dat de bescherming van deze gegevens op grond van artikel 8 Privacy Richtlijn nooit lager mag uitvallen dan indien verwerking plaatsvindt op een van de grondslagen van artikel 7 Privacy Richtlijn. Volgens de WP29 zijn de grondslagen van artikel 7 Privacy Richtlijn *cumulatief* van toepassing als de bescherming op grond van arti-

221. Opinie WP29 06/2014, p. 9-10.

kel 8 Privacy Richtlijn lager uitvalt. De WP29 beoogt daarmee vooral in sommige gevallen alsnog de toets van een gerechtvaardigd belang bij de gegevensverwerking in te voeren (zie vetdruk in citaat hierna).

> "(…) it is clear that the policy objective is to provide additional protection for special categories of data. Therefore, the final outcome of the analysis should be equally clear: the application of Article 8, whether in itself or in a cumulative way with Article 7, aims at providing for a higher level of protection to special categories of data.
> In practice, while in some cases Article 8 brings stricter requirements (…) this is not true for all provisions. Some exceptions foreseen by Article 8 do not appear equivalent or stricter than the grounds listed in Article 7. It would be inappropriate to conclude for instance that the fact that someone has made special categories of data manifestly public under Article 8(2)(e) would be – always and in and of itself – a sufficient condition to allow any type of data processing, **without an assessment of the balance of interests and rights at stake as required in Article 7(f). (…)**.
> In conclusion, the Working Party considers that an analysis has to be made on a case-by-case basis whether Article 8 in itself provides for stricter and sufficient conditions, or whether a cumulative application of both Article 8 and 7 is required to ensure full protection of data subjects. In no case shall the result of the examination lead to a lower protection for special categories of data."
>
> Opinie WP29 06/2014, p. 15-16, vetdruk toegevoegd.

Hoezeer het standpunt van de WP29 ook is te billijken op grond van de beschermingsgedachte, het mag ook duidelijk zijn dat de wijze waarop dit wordt gerealiseerd niet optimaal is. In de eerste plaats zal de gerechtvaardigd belang-grondslag van artikel 7 niet altijd van toepassing zijn. Dit komt omdat sommige van de grondslagen onder artikel 8 en 7 Privacy Richtlijn dezelfde zijn. Bijvoorbeeld is een van de grondslagen voor gegevensverwerking in artikel 7 "uitvoering van een overeenkomst". Voor bijzondere gegevens zijn in artikel 8 de overeenkomsten hoogstens gespecificeerd (maar de toets zal dan niet anders uitpakken). In dit geval komt men aan toepassing van de gerechtvaardigd belang toets niet toe. Beide artikelen kennen verder de grondslag "toestemming". Bij bijzondere gegevens wordt deze grondslag vaak gebruikt voor het legitimeren van verwerkingen, terwijl deze verwerkingen de gerechtvaardigd belang-toets niet zouden doorstaan.

Voor de grondslag toestemming ondervangt de WP29 dit door te bepalen dat in dat geval de beginselen van art. 6 Privacy Richtlijn van toepassing zijn (persoonsgegevens dienen eerlijk en rechtmatig te worden

verwerkt, en de vereisten van noodzakelijkheid en proportionaliteit zijn van toepassing):[222]

> "... obtaining consent does not negate the controller's obligations under Article 6 with regard to fairness, necessity and proportionality, as well as data quality. For instance, even if the processing of personal data is based on the consent of the user, this would not legitimise the collection of data which is excessive in relation to a particular purpose."

De WP29 verwijst verder naar beginselen van consumentenrecht die consumenten beschermen tegen oneerlijke commerciële praktijken.[223]

> "In this respect the Working Party emphasises that consumer protection law, in particular, laws protecting consumers against unfair commercial practices, is also highly relevant here. If a controller hides important information regarding unexpected further use of the data in legalistic terms buried in the small print of a contract, this may infringe consumer protection rules concerning unfair contractual terms (including the prohibition against 'surprising terms'), and it will also not fulfil the requirements of Article 7(a) for a valid and informed consent, or the requirements of Article 7(f) in terms of reasonable expectations of the data subject and an overall acceptable balance of interests. It would of course also raise questions of compliance with Article 6 as to the need for a fair and lawful processing of personal data. For instance, in a number of cases, users of 'free' online services, such as search, email, social media, file storage or other online or mobile applications, are not fully aware of the extent to which their activity is logged and analysed in order to generate value for the service provider and therefore they remain unconcerned of the risks involved."
>
> _____
>
> Opinie WP29 06/2014, p, 44.

Onze conclusie is dat – evenals we bij het doelbindingsbeginsel hebben gezien – de WP29 extra toetsen uit de kast haalt om maar tot het juiste eindresultaat te komen. Dat resultaat komt er in feite op neer dat voor de verwerking een gerechtvaardigd belang moet bestaan.[224]

222. Zie Opinie WP29 06/2014, p, 13, voetnoot 27, onder verwijzing naar het arrest van de Hoge Raad van 9 september 2011, ECLI:NL:HR:2011:BQ8097, §3.3(e), waarin de Hoge Raad bepaalde dat het beginsel van proportionaliteit van toepassing blijft ook als toestemming voor een verwerking wordt gevraagd.
223. Zie Opinie WP29 06/2014, p, 44.
224. Samenvattend dient er voor bijzondere gegevens een grondslag te zijn conform art. 8 Wbp; een grondslag te zijn conform art. 7 Wbp (indien deze strenger uitvallen dan de toets onder art. 8 Wbp, hetgeen in de praktijk uitsluitend de gerechtvaardigd belang grondslag kan zijn); en als toestemming de grondslag is dan dienen de beginselen van art. 6 Wbp te worden getoetst (onderdeel is hier het vereiste van proportionaliteit, waarmee de verlangde belangenafweging kan worden vereist en waar een relevante factor is welke privacy mitigerende maatregelen door de verantwoordelijke zijn getroffen).

Met toepassing van de door ons voorgestelde gerechtvaardigd belang-toets is het regime voor bijzondere persoonsgegevens (medische gegevens, geloof, ras, etc.) niet langer nodig. Het schrappen van het regime is ook eenvoudig te realiseren, nu het noch in het EU Handvest noch in het Verdrag is opgenomen. In plaats hiervan zullen de aard van de gegevens en het potentiële misbruik daarvan relevante factoren moeten zijn bij de belangenafweging die onderdeel is van de beoordeling of sprake is van een gerechtvaardigd belang voor de verzameling en het gebruik. Meegenomen zal ook moeten worden welke mitigerende maatregelen dienen te worden getroffen om de privacy-implicaties te beperken.

Wie de Opinie van de WP29 er bovendien op na slaat, stelt vast dat de aard van de gegevens ook nu al onderdeel vormt van de gerechtvaardigd belang-toets:[225]

> "ii) Nature of the data
> It would first be important to evaluate whether the processing involves sensitive data, either because they belong to the special categories of data under Article 8 of the Directive, or for other reasons, as in the case of biometric data, genetic information, communication data, location data, and other kinds of personal information requiring special protection."

Onder de Verordening blijft het specifieke regime voor bijzonder categorieën gegevens gehandhaafd.[226] De hiervoor door ons gesignaleerde tekortkomingen (het gebrek bij sommige grondslagen aan belangenafweging en het ontbreken van de noodzaak tot het treffen van mitigerende maatregelen) wordt (deels) ondervangen door nieuwe voorwaarden. Zo worden verwerkers verplicht om een Data Protection Impact Assessment (**DPIA**) uit te voeren voor verwerkingen die een hoog privacyrisico hebben, waarbij expliciet is bepaald dat deze in ieder geval zal zijn vereist bij grootschalige verwerking van bijzondere gegevens.[227] Bovendien zijn verwerkers verplicht om, indien uit de DPIA inderdaad blijkt dat de verwerking (zonder mitigerende maatregelen) een hoog privacyrisico zal kunnen hebben, de toezichthouder vooraf te consulteren. Opvallend daarbij is dat de verplichte DPIA een contextuele beoordeling vereist, waaronder een beoordeling van de noodzakelijkheid en proportionaliteit van de verwerking, een analyse van de privacyimplicaties en de mitigerende maatregelen die de verwerker voorstelt om deze te beperken.[228] Deze analyse moet derhalve ook worden gemaakt indien de grondslag voor de verwerking van de bijzondere gegevens toestemming of een contractuele grondslag betreft. Op deze manier worden via de achterdeur van de DPIA deze eisen ingevoerd.

225. Zie Opinie WP29 06/2014, p, 38.
226. Artikel 9 en 9a Verordening Gegevensbescherming.
227. Artikel 33(2(b) Verordening Gegevensbecsherming.
228. Artikel 33(3) Verordening Gegevensbescherming.

Hoewel dit vanuit de beschermingsgedachte te begrijpen valt, geldt wat ons betreft ook hier dat de wijze waarop de Verordening dit doel tracht te bereiken niet aan het vereiste van goede wetgeving voldoet. Onze conclusie is kortom wederom dat de Verordening Gegevensbescherming op het punt van complexiteit geen verbetering gaat brengen. In tegendeel.

Compatible use WP29 (Privacy Directive)	**Legitimate interest WP29 (Privacy Directive)**	**Compatible use (Data Protection Regulation)**	**DPIA (Data Protection Regulation)**
the **relationship** between the purposes for which the personal data have been collected and the purposes of further processing		any between the purposes for which the data have been collected and the purposes of the intended further processing	
the **context** in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use		the **context** in which the data have been collected, in particular regarding the relationship between data subjects and the controller	an assessment of the **necessity and proportionality** of the processing operations **in relation to the purposes**
the **nature of the personal data** and the **impact of the further processing on the data subjects**	the **impact on the data subjects**, including: - the **nature of the data**, - the way data are being processed - the status of the data controller and data subject, including the balance of power between the ata subject and the data controller	- the **nature** of the personal data, in particular whether special categories of personal data are processed, - the **possible consequences** of the intended further processing for data subjects	an assessment of the **risks to** the rights and freedoms of **data subjects**
the **safeguards** adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects	additional **safeguards** to prevent undue impact on the data subjects	the existence of appropriate **safeguards**	the measures envisaged to address the risks, including **safeguards**, security measures and mechanisms to ensure the protection of personal data

Wat resteert is uiteraard de vraag of er nu nog bepaalde soorten data zijn die dermate gevoelig zijn dat we daarvoor toch nog een verbod of een bijzonder regime nodig hebben. Voor dergelijke gegevens zou dan moeten worden vastgelegd dat verwerking categorisch is verboden of in welke gevallen en onder welke omstandigheden ze mogen worden verwerkt. Ook kan worden gedacht aan de voorwaarde dat de verwerking vooraf ter goedkeuring moet worden voorgelegd aan de toezichthouder. 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. Deze situaties zullen zeer casuïstisch zijn en lastig vooraf te voorspellen, laat staan te duiden. Bovendien blijkt de context van de toepassing telkens weer relevant voor de uitkomst van de belangenafweging. Eerder gaven we het voorbeeld van een algoritme dat wordt ontwikkeld door een commerciële startup voor diagnose van hersenbloedingen. Goed mogelijk is dat met een big data-applicatie wordt geanalyseerd wat de correlatie is tussen een populatie individuen die een hartaanval hebben gehad en genetische kenmerken.[229] Daarmee kunnen bepaalde groepen mensen en hun medische behandelaars beter worden ingelicht. Mits wordt voldaan aan bepaalde aanvullende maatregelen (minimale herleidbaarheid via privacy-by-design, etc.) zou gebruik van dergelijke gegevens mogelijk moeten zijn. Feit is wel dat wat betreft gevoelige data (maar net zo goed: wat betreft kwetsbare groepen in de samenleving) de afweging van belangen vanuit de toets van gerechtvaardigd belang naar onze inschatting veelal in het nadeel van de gegevensverwerker (verantwoordelijke) zal uitvallen. Veelal, maar dus niet altijd. De situaties waarin een verwerking van gevoelige gegevens de gerechtvaardigd belang toets wel zal kunnen doorstaan, zijn zo contextafhankelijk dat dit naar onze mening niet op voorhand in een wettelijk regime te vangen is. Het zal aan de Europese en nationale toezichthouders zijn om richtsnoeren te geven hoe de normen in concrete gevallen uitwerken (zie paragraaf 5.1). De WP29 heeft daarvoor een voorzet gedaan in de Opinie over de grondslag van gerechtvaardigd belang, en daarin ook een lijst met voorbeelden gegeven hoe de normen in concrete gevallen uitwerken. In de gegeven voorbeelden blijkt dat bij verwerking van gevoelige

229. Zie ook de voorbeelden die Meyer Schönberger geeft in een interview in *Medisch Contact*, 25 september 2015.

gegevens voor commerciële doeleinden de toets in de regel negatief zal uitvallen. Dit zal in de toekomst nader moeten worden uitgewerkt.

4.3 Het recht op informationele zelfbeschikking is een illusie

Diverse bepalingen in de huidige wetgeving beogen het oogmerk van informationele zelfbeschikking te realiseren. Allereerst zijn dat de informatieverplichtingen voor verwerkers neergelegd in art. 33 en 34 Wbp.[230] Daarnaast zijn dat de rechten van betrokkenen op inzage, correctie, verwijdering en verzet,[231] alsmede het recht van het individu om niet onderworpen te zijn aan een voor hem/haar negatief besluit dat uitsluitend is gebaseerd op geautomatiseerde verwerking, daaronder begrepen profilering.[232]

In de Inleiding tot dit preadvies constateerden we dat, ondanks de hen toegekende rechten, individuen nauwelijks in staat zijn informationele zelfbeschikking daadwerkelijk vorm en inhoud te geven. Ze blijken steeds transparanter te worden, behalve voor zichzelf. De realiteit van onze huidige datadreven samenleving is dat ze niet weten welke gegevens (en met name afgeleide informatie) er over hen worden verwerkt, in welke categorie ze zijn ingedeeld en wat voor hen de gevolgen zijn als op basis daarvan voorspellingen worden gedaan die hun toekomstige opties beperken.[233] In het huidige systeem worden de informatierechten als hoeksteen van de privacywetgeving beschouwd. Maar de aanname is dan wel dat een individu zijn/haar rechten op inzage, verzet, correctie en verwijdering daadwerkelijk kan uitoefenen omdat hij/zij ook weet dat er gegevens en informatie over hem/haar worden verwerkt en door wie.[234] De Verordening Gegevensbescherming gaat voort op de ingeslagen weg en versterkt de informatieverplichtingen en de rechten van individuen,[235] eveneens met de

230. Formeel kan men redeneren dat de informatieverplichtingen van verwerkers niets met informationele zelfbeschikking in de klassieke zin van het concept te maken hebben. Wij betrekken deze verplichtingen hier desalniettemin in het betoog omdat transparantie over de gegevensverwerking (die gestalte krijgt via de informatieplichten) cruciaal is voor het realiseren van informationele zelfbeschikking.
231. Zie artikelen 35-41 Wbp.
232. Artikel 42 Wbp.
233. Commission Communication on the Proposed Regulation, n 10, p. 4: constateert dat Europese burgers "feel they are not in control of their data. They are not properly informed of what happens to their personal information to whom it is transmitted and for what purposes. Often, they do not know how to exercise their rights online."
234. Zie Considerans 38 Privacy Richtlijn en Dammann, Simitis, 1979, p. 179.
235. Europese Commissie, 2012, p. 6; Considerans 6 Verordening Gegevensbescherming.

gedachte dat dit bijdraagt aan de autonomie van het individu en hem/haar betere controle over gegevensverwerkingen biedt.[236]

Onze stelling is dat de informatieverplichtingen zoals die nu gelden onvoldoende effectief zijn in horizontale verhoudingen.[237] Eenvoudig gezegd zijn de gegevensverwerkingen, de onderliggende logica en de doeleinden waarvoor de gegevens worden toegepast, zodanig gecompliceerd geworden dat de beschrijving daarvan in zgn. *privacy policies* voor velen simpelweg een brug te ver is. En dus lezen velen ze niet.[238] Daarbij, als een consument deze horde al zou nemen, wil dat nog niet zeggen dat hij of zij in staat is om de privacygevolgen van een eventueel akkoord op de *privacy policy* van de App of de sociale netwerkdienst te overzien.[239] Bovendien wijzigen bedrijven als Facebook met de regelmaat van de klok de privacyinstellingen, zijn de *default-settings* veelal ingericht op het openbaar maken van informatie over de gebruiker, in plaats van het beheren van deze informatie door de gebruiker zelf en is het voor gebruikers kortom moeilijk, zo niet onmogelijk, te achterhalen welke sporen ze achterlaten en wat daar vervolgens precies mee wordt gedaan.[240]

Hoewel de Verordening nadere eisen stelt aan onder meer de begrijpelijkheid van de te verstrekken informatie[241] en het gebruik van standaard

236. Europese Commissie, 2012, p. 2: "In this new digital environment, individuals have the right to enjoy effective control over their personal information" Zie verder Considerans 6 Verordening Gegevensbescherming: "Individuals should have control over their own personal data".
237. Dit ligt wat ons betreft anders in de relatie tussen overheid en burgers. Gegeven de specifieke kenmerken van deze relatie zou transparantie juist met behulp van digitalisering beter invulling moeten kunnen krijgen, al was het maar omdat het voor de overheid mogelijk is om, naar voorbeeld van de eigen elektronische dienstverlening, te streven naar een één-loket gedachte (al dan niet in de vorm van een digitale kluis voor de burger). Zie hierover WRR, 2011, p. 231.
238. Zie TNO 2015. Tevens: Moerel, 2014, p. 47-50. World Economic Forum Report, 2013, p. 11 rapporteert dat: "The torrent of data being generated from and about data subjects imposes an undue cognitive burden on individual data subjects. Overwhelming them with notices is ultimately disempowering and ineffective in terms of protection – it would take the average person about 250 working hours every year, or about 30 full working days – to actually read the privacy policies of the websites they visit in a year."
239. Zie Mcdonald, Reeder, Kelley en Cranor, 2009.
240. WRR, 2011, p. 43.
241. Artikel 12 Verordening Gegevensbescherming.

icoontjes stimuleert,[242] zal de verzwaring van deze verplichtingen onder de Verordening Gegevensbescherming individuen uiteindelijk geen betere positie geven, laat staan een gevoel van controle over hun gegevensverwerkingen. Overigens is dit niet een nieuw fenomeen. Toenmalig AFM bestuurder Kockeloren[243] merkte hierover op:

> "Aanvankelijk geloofde de toezichthouder dat meer openheid en betere productinformatie de consument zouden beschermen tegen misstanden. Maar daar is de toezichthouder van teruggekomen. "Transparantie alleen is niet genoeg". (…) Mensen lezen de financiele bijsluiters niet, omdat ze die te ingewikkeld vinden. (…) mensen vertonen ook allerlei ingebakken patronen, zoals verliesaversie. Daarom werken we niet alleen aan verbetering van informatie die klanten krijgen aangeboden, maar hebben we een paar jaar geleden ook gezegd dat toezicht nodig is op productontwikkeling."

Als we de observatie van Kockeloren vertalen naar de privacy-omgeving moeten we concluderen dat het ook hier niet zinvol is te denken dat als we mensen beter informeren over welke gegevens voor wat voor doeleinden worden verwerkt, ze in staat zijn om rationele keuzes te maken en hun rechten te kunnen uitoefenen.[244] We moeten af van het systeem waarbij verantwoordelijken zich voor legitimering van hun verwerkingen kunnen verlaten op het informeren van individuen en het door hen laten uitoefenen van hun rechten.

De lengte en gecompliceerdheid van de te verschaffen informatie is overigens niet de enige reden waarom deze verplichtingen in de nieuwe datagedreven samenleving niet meer werkbaar zijn. Specifiek voor big data en het Internet of Things geldt aanvullend dat het informeren van individuen over de via deze applicaties verwerkte gegevens praktisch problematisch is. Illustratief zijn de diensten verbonden aan het groeiend aantal intelligente en vernetwerkte apparaten – tv, koelkast en verwarming – dat een plekje in onze woning verovert. Bij veel van deze diensten zijn meer aanbieders betrokken, terwijl er niet altijd een logisch centraal kanaal

242. Artikel 12(4b) Verordening Gegevensbescherming.
243. "Consumenten zijn niet opgewassen tegen de groeidrift van de financiële sector", Volkskrant 31 Augustus 2013.
244. Zie hierover uitgebreid Moerel, 2014, p. 47-50. World Economic Forum Report, 2013, p. 17: dat het beginsel van 'notice and consent' als kandidaat voor hervorming aanmerkt: "In particular, reliance on mechanisms of "notice and consent" to ensure individual participation is seen as increasingly anachronistic. The current manifestation of the principles through notice and consent as a binary, one-time only involvement of the individual at the point of data collection was identified in the dialogue as an area ripe for reconsideration to better empower individuals, build trust in the system, and encourage the reliable, predictable and more valuable flow of data into and within the system."

voorhanden is om over de privacy-voorwaarden met bewoners te communiceren. De apparaten hebben vaak ook geen scherm om deze informatie over te dragen. Hoogstens kan via bijvoorbeeld stickers op het apparaat worden gewaarschuwd dat het een *connected device* betreft. Informatie over welke gegevens vervolgens door wie worden verwerkt, zal dan via andere kanalen (bijvoorbeeld de websites van de verschillende aanbieders) opzoekbaar moeten zijn, in plaats van rechtstreeks te worden gecommuniceerd aan het individu.

Verder gaat transparantie bij big data over meer dan alleen de gegevens die worden gebruikt. Ook de onderliggende logica van de in te zetten algoritmen is in dit opzicht relevant. Maar nu deze algoritmen in toenemende mate zelflerend zijn wordt het steeds lastiger op een willekeurig moment de precieze onderliggende logica vast te leggen en te communiceren. Het zou ons niet verbazen als Google bijvoorbeeld niet kan uitleggen wat op moment X precies het algoritme is dat tot een bepaald zoekresultaat voor een specifiek individu leidt. De Wbp en de nieuwe Verordening Gegevensbescherming bieden individuen het recht op informatie over de logica die ten grondslag ligt aan de geautomatiseerde verwerking van zijn/haar gegevens. Indien deze logica echter ondoorgrondelijk wordt is de vraag wat de toegevoegde waarde is voor het individu om daarvan kennis te hebben.[245]

Niet alleen de informatieplichten komen bij big data en het Internet of Things onder druk te staan. Dat geldt ook voor de rol van inzage, correctie en andere rechten van het individu. Zo zagen we in paragraaf 2.4 dat het voor veel diensten niet nodig is dat de aanbieder de opzoek-identiteit van iemand kent, met andere woorden iemand kan herleiden naar zijn/haar burgerlijke of unieke identiteit. Vaak kan worden volstaan met verwerking van de herken-identiteit. De betreffende persoon is daarmee wel te onderscheiden van anderen, maar de aanbieder kan geen link leggen naar diens burgerlijke dan wel unieke identiteit. Toch, ook hier blijken de zaken te gaan wringen. Enerzijds wordt het individu minder in zijn/haar privacy geraakt wanneer bedrijven slechts gebruik maken van de herken-identiteit (er worden immers minder privacygevoelige gegevens verzameld). Anderzijds, blijkt dat door te volstaan met de herken-identiteit, individuen minder bescherming wordt geboden. De Verordening Gegevensbescherming bepaalt namelijk dat in dat geval de verantwoordelijke niet kan worden verplicht nadere gegevens te gaan verzamelen om de

245. Artikel 35 lid 4 en 42 Wbp; vergelijk artikelen 14(1a) sub (h) en 14a(2) sub (h) en 20 Verordening Gegevensbescherming.

betrokkenen inzage, correctie, etc te kunnen bieden.[246] Het gevolg hiervan is dat in steeds meer gevallen de betrokkenen geen gebruik meer kunnen maken van hun rechten op inzage, correctie en verwijdering en dus in zoverre geen **'controle'** over hun verwerkingen hebben.

Illustratief voor de geringe effectiviteit van het recht op inzage, correctie en verwijdering is ook de dagelijkse realiteit in het geval individuen een beroep op deze rechten doen. Voor het uitoefenen daarvan moeten zij veelal een brief of email sturen naar een verantwoordelijke. Als deze al op een verzoek tot inzage van consumenten reageert, is dit uiterst summier dan wel door de verzoeker een onoverzichtelijk pak papier met prints of cd met bestanden te sturen. In de praktijk wordt dit recht dan ook nauwelijks uitgeoefend, en als burgers hier al toe over gaan, zullen ze met de uitdraai in de hand geen werkelijk inzicht verkrijgen in hun verwerkingen, laat staan (een gevoel van) controle daarover.[247] Het recht op inzage is daarmee een papieren tijger en archaïsch in het licht van de geavanceerde wijze waarop verantwoordelijken zelf de gegevens verwerken. Innovatie waarbij individuen wel real-time online inzage hebben in de over hen verwerkte gegevens en hun instellingen en voorkeuren kunnen wijzigen via een dashboard is (uiteraard) mogelijk, maar de huidige wettelijke verplichtingen van de verantwoordelijke om inzage, etc te verschaffen, dwingen de verantwoordelijke hier niet toe. Erger, de realiteit is dat veel verantwoordelijken de inzage mogelijkheden opzettelijk archaïsch houden (bijv. door ook van online klanten te eisen dat het inzagerecht per brief moet worden uitgeoefend), om zo uitoefening van deze rechten te ontmoedigen.

Het moet en kan anders

Wij verbinden informationele zelfstandigheid aan het, met name in Duitsland, prominent ontwikkelde recht op informationele zelfbeschikking. Dit

246. Artikel 10 Verordening Gegevensbescherming. Andersom kunnen verantwoordelijken gebruikers ook niet verbieden een pseudoniem te gebruiken, zie een recente uitspraak van de toezichthouder in Hamburg, die Facebook verplichtte Duitse gebruikers de mogelijkheid te bieden om een account aan te maken en te gebruiken onder een pseudoniem, gerapporteerd door Bloomberg http://www.bloomberg.com/news/articles/2015-07-28/facebook-ordered-by-hamburg-regulator-to-allow-pseudonyms.

247. Koops, 2014, p. 5, merkt hier het volgende over op: "As is the case with consent, the exercise of data subject rights is highly theoretical (…) The case against Facebook brought by Austrian law student Max Schrems is an eminent example of how useful the exercise of data subject rights can be to influence data controllers, but the example tells us nothing about data subjects having effective control over how their personal data are being processed. Your average Internet user simply is not Max Schrems, and your average data controller does not neatly send you a 1,222-page cd with all the data they process about you (as Facebook sent to Mr. Schrems). Not even the firmest believers in informational self-determination can claim, at least not with dry eyes, that they actually know which of their data are being processed in what ways by data controllers, or that they have effective control on most data-processing operations they are subjected to."

recht is door het Duitse Constitutioneel Hof omschreven als 'het recht van het individu om in beginsel zelf te beschikken over de openbaarmaking en het gebruik van persoonlijke gegevens'.[248] In de woorden van Rouvroy en Poullet impliceert informationele zelfbeschikking dat een individu de controle moet kunnen hebben over de inzake hem/haar beschikbare gegevens en in het bijzonder de implicaties van het gebruik daarvan om zo een bestaan te kunnen leven dat zelfbepaald is.[249] Hiervoor stelden we echter vast dat de huidige rechten en plichten die informationele zelfbeschikking vorm moeten geven in dit opzicht onvoldoende effectief zijn. Bovendien zijn deze rechten gericht op het realiseren van een zekere controle op het verzamelen en gebruiken van gegevens, terwijl het steeds meer gaat om controle op **de implicaties** van dat gebruik (wel of niet een aanbieding van een dienst, al dan niet sturen op gedrag van consumenten, etc.). In paragraaf 2.4 maakten we al duidelijk dat het ontnemen van opties (uitsluiting van een verzekering, het afwijzen van een lening) via *preemptive* voorspellingen over het algemeen meer implicaties voor de positie van een individu heeft dan wanneer iemand op basis van eerdere aankopen een volgende aanbieding krijgt.

Wanneer we ook hier de wetgeving beoordelen vanuit werkelijkheids- en mogelijkheidszin, zullen we moeten afstappen van het opleggen van informatieverplichtingen aan verwerkers als zelfstandige voorwaarde voor de legitimatie van gegevensgebruik. In plaats van het *sec* stellen van de informatieverplichting, dient onderdeel van de gerechtvaardigd belang-toets te zijn in hoeverre betrokkenen aantoonbaar een daadwerkelijke vorm van *controle* worden gegeven over de verwerking van hun gegevens, in het bijzonder de toepassingen en implicaties daarvan. Dit kan in talloze denkbare en ook nu nog niet-denkbare varianten. De wetgever dient hier niet op voorhand sturend op te treden maar open te staan van allerhande vormen van controle die worden ontwikkeld en geboden alsmede innovatie op dit punt te stimuleren, bijvoorbeeld door zelf het voorbeeld te geven en bij het ontwikkelen van diensten en applicaties als *launching customer* op te treden.[250]

Ter illustratie van de mogelijkheden bij commerciële toepassingen, geven we een paar voorbeelden.[251] Op dit moment is op grond van de Telecommunicatiewet voorafgaande toestemming vereist voor het plaatsen van onder meer *tracking* cookies waarmee bezoekers van website ook op andere websites worden gevolgd voor reclame doeleinden (zgn.

248. Bundesverfassungsgericht, 15 December 1983, BVerfGE, 65, 1 (43).
249. Rouvory, Poullet, 2009, p. 51.
250. Onder meer door dergelijke maatregelen in de specificaties bij een aanbesteding op te nemen. Zie Overweging 61 Verordening voor een aanmoediging daartoe aan de Lidstaten.
251. Zie eerder Moerel, 2014, p. 35-36 en 60.

behavioural targeting). Hoewel de meeste mensen bezwaar hebben tegen deze vorm van commercieel 'volgen', klikt vrijwel iedereen automatisch op "OK" voor "accepteer alle cookies". Dit omdat het praktisch lastig en te veel tijd kost om de cookie-informatie te lezen en per soort cookie de instellingen te veranderen. Ons inziens zijn de cookie-regels overbodig en kan een beter resultaat worden bereikt op grond van toepassing van de gerechtvaardigd belang-toets. De gerechtvaardigd belang-toets zal per soort cookie moeten worden toegepast en verschillend kunnen uitwerken. Richtsnoeren kunnen hier worden gegeven door de WP29 middels een Opinie. Een concrete uitwerking van de belangenafweging geven we ter illustratie in het navolgende kader.

Indien de met behulp van cookies verzamelde gegevens worden gebruikt voor het doen van website analytics, fraudebestrijding of het aanpassen van de bezochte website aan de voorkeuren van de bezoeker (*in-site behavioural targeting*) zal de afweging wat ons betreft (mits de verwerking privacy-by-design is ingericht en gegevens niet te lang worden bewaard) in het voordeel van de websitehouder uitvallen. Indien de gegevens worden aangewend voor *cross-site behavioural targeting* zal de afweging in het voordeel van de bezoekers uitvallen. De verwerking zal niet zijn toegestaan tenzij de websitehouder als mitigerende maatregel bezoekers een opt-in of opt-out mogelijkheid biedt. In dit geval zal waarschijnlijk het plaatsen van een duidelijke "*do not track*"-button afdoende zijn. Juridisch gezien is dit een 'opt-out', maar onze inschatting is dat veel bezoekers dan op deze button zouden klikken. Een dergelijke gerichte opt-out zou meer 'controle' en daarmee bescherming bieden dan de huidige opt-in voor alle soorten cookies. Immers, consumenten maken nu geen onderscheid meer.

De vraag blijft hier uiteraard: wat als bij websitehouders de wil ontbreekt om de cookie-instellingen zodanig in te richten dat bezoekers daadwerkelijke controle krijgen. Ook onder de huidige cookie-regels bestaat (uiteraard) de mogelijkheid om deze op verantwoorde wijze in te richten, maar daartoe is bij aanbieders momenteel overduidelijk de wil niet aanwezig.[252] Het is onze stellige mening dat met de gerechtvaardigd belang-toets een resultaat met meer effectiviteit en legitimiteit valt te realiseren. Dat is allereerst het geval omdat deze toets niet overreguleert door verwerkingen toe te staan die **geen wezenlijke implicaties** voor de privacy hebben. De huidige cookie-regels vormen een duidelijk geval van overregulering, nu ook voor cookies die geen wezenlijke gevolgen voor de privacy hebben toch toestemming is vereist. De dagelijkse realiteit is dat deze situatie de acceptatie van de regels in de weg staat en omzeiling in de hand werkt. Daarbij komt dat de commerciële belangen van websitehouders bij het

252. Leenes en Kosta, 2015.

inzetten van cookies voor gegevensverzameling dermate groot zijn, dat een creatieve invulling van de regels op de loer ligt. In de Inleiding betoogden we reeds dat waar opportuun de verplichting om de juiste infrastructuur te realiseren voor het informeren van individuen en verkrijgen van hun toestemming, veeleer gelegd zou moeten worden bij partijen die geen eigen belang hebben bij het omzeilen van de regels. In dit geval is duidelijk sprake van zo'n situatie. De effectiviteit van de regelgeving zou zijn gediend door de cookie-instellingen te laten aanbieden via browsers (waarvan er momenteel vijf zijn).[253] De leveranciers hebben geen eigen commercieel belang bij de cookie-instellingen en verder is effectief toezicht op vijf aanbieders realistischer dan toezicht op de talloze websitehouders die ieder voor zich een creatieve invulling aan de regels geven.[254]

Een ander voorbeeld van het bieden van 'controle' is wanneer bij *behavioural targeting* de gepersonaliseerde advertenties die aan de bezoeker worden gepresenteerd worden voorzien van een *icoontje* dat aan te klikken is. Op dat moment worden de indicatoren getoond die de dienstaanbieder gebruikt voor het selecteren van de betreffende advertentie (man, leeftijdscategorie, inkomenscategorie, geïnteresseerd in plezierboten). Indien de bezoeker deze indicatoren ter plekke kan aanpassen omdat ze naar zijn/haar mening irrelevant of onjuist zijn, of op zich juist, maar niet langer relevant (bijvoorbeeld omdat de plezierboot inmiddels is gekocht), wordt aan de bezoeker meer controle gegeven over de implicaties van de verwerking, in dit geval welke advertenties hij/zij krijgt. Dergelijke systemen zijn al in de VS in ontwikkeling.[255] In het laatste geval is informeren wellicht achteraf, maar geeft het de betrokkenen wel controle, terwijl de informatie vooraf in feite weinig tot nietszeggend is.[256]

Bij het oordeel – via de gerechtvaardigd belang-toets – in hoeverre de verwerker aan consumenten *controle* geeft over de verwerking van hun gegeven en in het bijzonder de implicaties daarvan, kan kortom worden betrokken welke maatregelen de aanbieder heeft getroffen om de verwerkingen *privacy-by-design* in te richten.[257]

Het voorgaande zou ook moeten gelden voor de inrichting van de huidige rechten op inzage en correctie. Deze geven, zoals we al hebben geconstateerd, individuen geen daadwerkelijk inzicht en controle over gegevensverwerkingen. Het vereiste van inzage zou moeten worden omgezet in het

253. Internet Explorer, Mozilla Firefox, Google Chrome, Safari en Opera.
254. Zie met een vergelijkbaar voorstel maar op een andere grondslag Cofone, 2015, par. 225.
255. Zie hiervoor Interactive Advertising Bureau (IAB) Self-Regulatory Program for Online Behavioral Advertising, July 2009, te vinden op http://www.iab.net/media/file/ven-principles-07-01-09.pdf.
256. Borgesius, 2014, paragraaf 9.7 geeft een overzicht van mogelijke wettelijke maatregelen (waaronder verplichte default-instellingen) om *behavioural targeting* beter te reguleren.
257. In paragraaf 5.2 gaan we nader in op privacy-by-design.

verschaffen van controle, waarbij het individu zelf real-time inzage heeft in welke gegevens van hem/haar worden verwerkt en individuen zelf aan de knoppen zitten wat betreft de gegevens die worden verwerkt (d.w.z. zelf via een keuzemenu de betreffende gegevens kunnen wissen en corrigeren) en ook opgegeven voorkeuren (wel of geen nieuwsbrief, wel of geen tracking cookies) kunnen worden aangepast. Ook hiervan zijn in de praktijk al diverse voorbeelden beschikbaar.[258] Natuurlijk beseffen wij dat dergelijke instrumenten – gegeven de huidige complexiteit van het gegevensgebruik, waarbij dezelfde gegevens op talloze plaatsen door ontelbare partijen tegelijkertijd worden verwerkt – slechts een druppel op de gloeiende plaat zijn. Vandaar ook dat wij verderop zullen bepleiten dat handhaving van de regels niet langer primair een verantwoordelijkheid van consumenten kan zijn (paragraaf 5.1). Maar juist omdat het een druppel op de gloeiende plaat betreft, en daarmee slechts een onderdeel van het bredere palet aan noodzakelijke maatregelen, vormt het bieden van controle één element bij het beoordelen van gerechtvaardigd belang. Inmiddels heeft ook de WP29 aangegeven dat het geven van controle aan individuen een belangrijke privacy mitigerende-maatregel kan zijn.

> "In connection with these safeguards – and the overall assessment of the balance – the Working Party wishes to highlight three specific issues that often play a crucial role in the context of Article 7(f):
> (…)
> - empowering data subjects: data portability and the availability of workable mechanisms for the data subject to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data."
>
> WP29 Opinion 06/2014, p. 43.

Zoals gezegd, we beogen met ons voorstel niet te zeggen dat het informeren van het individu, het bieden van inzage, de mogelijkheid tot correctie, het vragen van toestemming of het bieden van een opt-out mogelijkheid niet langer een rol spelen. De gerechtvaardigd belang-toets zal mede dienen te omvatten factoren als: is het individu geïnformeerd, in hoeverre biedt de verwerker het individu "controle" over zijn/haar gegevens, de verwerking daarvan en implicaties van het gegevensgebruik. Ons punt hier is wel dat het enkele informeren – d.w.z. ongeacht wat de daadwerkelijke informatiepositie is van het individu – geen betekenis kan hebben. De

258. Zie bijvoorbeeld de privacy settings dashboard op Facebook en het persoonlijke dashboard geboden op de Albert Heijn website waar gegevens kunnen worden gewijzigd of gewist en voorkeuren kunnen worden veranderd.

wijze van informeren en de bijdrage die het kan leveren aan de informatiepositie van de betrokkene vormen beoordelingsfactoren binnen de gerechtvaardigd belang-toets. Datzelfde geldt voor de wijze waarop aan inzage en correctie vorm wordt gegeven. Ook hier is het enkel bieden van de mogelijkheid van inzage en correctie niet voldoende. Dit levert immers geen "controle" op. Hoe de verantwoordelijke deze rechten heeft vormgegeven kan wel een beoordelingsfactor zijn binnen de gerechtvaardigd belang-toets.

4.4 Kwaliteit is betrekkelijk

Wie persoonsgegevens verwerkt moet de kwaliteit, dat wil zeggen juistheid en nauwkeurigheid, van de gebruikte persoonsgegevens garanderen. Artikel 11 lid 2 Wbp merkt daarover op: "De verantwoordelijke treft de nodige maatregelen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn." 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. Relevante overwegingen zijn hierbij het soort gegevens (betreft het krediet- dan wel medische gegevens of gaat het om NAW-gegevens), de doeleinden waarvoor deze worden verwerkt (uitvoeren van een betalingsopdracht dan wel bestrijding winkeldiefstal), stand van de techniek (kan een filterprogramma voor het opschonen van het gegevensbestand worden toegepast) en kosten die met de controlemaatregelen zijn gemoeid.

Wie even stilstaat bij zelfs de meest eenvoudige gegevenscyclus, weet dat een absolute garantie afgeven voor de juistheid van gebruikte gegevens ook geen realistische optie is. Zeker niet in situaties waarin veel gegevens samenkomen. En nog minder voor gevallen waarin het om tienduizenden zo niet miljoenen klanten gaat en gegevens steeds vaker worden verkregen buiten een direct persoonlijk contact met het betreffende individu om. De complexiteit van hedendaagse gegevensverzamelingen vormt in feite een afspiegeling van de complexiteit van onze vernetwerkte samenleving en globaliserende economie. En daarmee is een omvattend overzicht van de wijzigingen die gegevens lopende de tijd in detail ondergaan onmogelijk te realiseren.

Bij de juistheid van de gegevens gaat het om twee vormen: formele en materiële juistheid. Formeel juist wil zeggen dat een bedrijf of organisatie de nodige maatregelen heeft getroffen om de integriteit van de gegevens te garanderen. Heel concreet betekent dit bijvoorbeeld dat het optreden van fouten bij het invoeren van gegevens vermeden moeten worden. Wanneer een beperkt aantal gegevens handmatig wordt ingetypt is formele juistheid

nog wel te realiseren (hoewel dat soms ook kan tegenvallen). In situaties waarin duizenden gegevens volautomatisch vanuit meerdere bronnen bijeen worden gebracht is het doorvoeren van een integriteitsbeleid lastiger. Toch zal de formele juistheid ook bij het geautomatiseerd koppelen van gegevens grotendeels zijn te garanderen via bijvoorbeeld de inzet van een geautomatiseerde invoer- en koppelingsvalidatie. Ingewikkelder wordt het als het op de materiële juistheid aankomt. Dan is de toets of de gegevens aansluiten bij de werkelijkheid, kortom of de persoonsgegevens een juiste weergave bieden van de feiten. Anders geformuleerd: hier gaat het niet om de vraag of de gegevens juist zijn ingevoerd of gekoppeld, maar of het juiste gegeven is ingevoerd en gekoppeld. Beoordeeld moet bijvoorbeeld worden of gegevens niet zijn verouderd dan wel of de context waarin de gegevens worden gebruikt, hergebruikt en geduid wel overeenstemt met de werkelijkheid.

Zeker in situaties waarin gegevens aan derden worden verstrekt en daarmee vaak uit hun context worden gehaald (gedecontextualiseerd) om vervolgens in een geheel andere context te worden gebruikt (gehercontextualiseerd) staat materiële juistheid al snel op de tocht. Illustratief is de situatie waarin van Internet Service Providers wordt verlangd dat ze aan opsporingsinstanties gegevens verstrekken over bezoekers van op radicalisering gerichte websites. Als één van deze bezoekers een wetenschapper blijkt te zijn die onderzoek verricht naar dit fenomeen, zal de betreffende opsporingsinstantie de nodige maatregelen moeten treffen om het IP-adres en de gegevens over het zoekgedrag van deze persoon te verwijderen uit het bestand. Dat zal een lastige opgave zijn. Zoals gezegd: een 100%-controle op de juistheid en nauwkeurigheid wordt niet verlangd en daarmee zal de betreffende opsporingsinstantie de nodige argumenten ter vrijwaring kunnen aandragen. Echter, als de betreffende wetenschapper aan de bel heeft getrokken dan wel de instantie om andere redenen kon weten dat de onderzoeker niet in het bestand thuishoort, zijn maatregelen aan de orde om zowel de gegevens te verwijderen als te voorkomen dat in de toekomst de gegevens wederom in de systemen voorkomen.

Toch, in de meer klassieke vormen van geautomatiseerde gegevensverwerking is het borgen van kwaliteit een aangelegenheid die nog ‘te doen’ valt. Maar met name materiële juistheid wordt met meer innovatieve vormen van gegevensverwerking een lastiger te hanteren vereiste. Kenmerkend voor big data-toepassingen is dat grote hoeveelheden gegevens bij elkaar worden gebracht om daarin met behulp van data-analyse patronen te ontwaren die voldoende interessant blijken om aan de hand daarvan (al dan niet commerciële) toepassingen te ontwikkelen. Hoe kun je de materiële juistheid van de gegevens beoordelen als de context waarin deze worden gebruikt nog onbekend is? Hoewel diverse toepassers de zgn. *Veracity* – waarheidsgetrouwheid – van big data claimen omdat de

toepassingen gebaseerd zijn op verifieerbare gegevens,[259] zetten wij hier onze vraagtekens bij.

Inherent aan een fenomeen als big data is namelijk dat de kwaliteit van gegevens er op voorhand lang niet altijd toe doet. Bij aanvang van het analyseproces gaat het gebruikers immers niet altijd om detailkennis, maar om inzichten die een eerste indruk geven van 'wat er uit de berg aan te combineren gegevens te halen valt'. Met andere woorden, het gaat allereerst om inzichten in de patronen en daarmee het macroniveau van type consument (geïnteresseerd in verre reizen), type patiënt (behept met bepaalde risicofactoren in combinatie met levensstijl) en type burger (hoogte van het inkomen, fiscale historie en type aftrekposten). Veel minder relevant in deze fase zijn de details – het microniveau van de individuen die voldoen aan de patronen. Daarmee kunnen bedrijven **in deze fase** volstaan met een aanzienlijk afgezwakte nauwkeurigheid van de te gebruiken gegevens. Bovendien, gegeven de grote aantallen gegevens, de variëteit in herkomst van de gebruikte databestanden (deels openbare online bronnen) en de talrijke partijen van wie de data afkomstig zijn, is het vergroten van de nauwkeurigheid een kostbare en soms ook onmogelijke opgave. Voor gebruikers zullen de investeringen die gemoeid zijn met het kunnen garanderen van een relatief hoog niveau van juistheid daarom bij bepaalde toepassingen niet opwegen tegen de meerwaarde die een kwaliteitsslag hen oplevert. Immers: precisie komt in dat geval later wel.

Inherent aan big data is dan ook dat de wijze waarop we naar gegevenskwaliteit kijken verandert. Dit heeft alles te maken met de verschuiving van de aandacht van het primaire doel waarvoor gegevens werden verzameld (bijvoorbeeld gegevens die door Google worden verzameld voor het afhandelen van de geleverde zoekopdrachten) naar innovatief hergebruik van deze gegevens (het benutten van gegevens van de oude zoekopdracht voor nieuwe diensten dan wel verkopen van deze gegevens aan andere bedrijven). De verandering valt goed te illustreren met de overname in 2014 van de kleine Amerikaanse online bank Simple door een grote Spaanse bank (Banco Bilboa Vizcaya Argentaria). De Spaanse bank telde 117 miljoen dollar neer voor in totaal 100.000 klanten van de Amerikaanse bank.[260] Maar het ging de Spaanse bank niet om deze klanten, maar om het bedrijfsmodel van Simple. Deze benut namelijk rekeninginformatie van klanten over hun inkomsten en uitgaven in combinatie met demografische gegevens en andere openbare data, om klanten – deels visueel m.b.t. grafieken – real-time van advies te dienen. Gegeven het type individu dat

259. Zie onder meer http://www-01.ibm.com/software/data/bigdata/images/4-Vs-of-big-data.jpg en de claims opgetekend in http://issuu.com/brunovdberg/docs/big_data_big_possibilities
260. http://www.newyorker.com/currency-tag/the-bank-and-the-anti-bank

rekeninghouder X is, zijn/haar bestedingspatroon en lopende verplichtingen: moet hij/zij vandaag zijn/haar spaartegoed ophogen, mag die vakantie wel of niet worden geboekt en voor welk bedrag mag hij/zij aankomend weekend uit zijn/haar dak gaan? Bovendien: de dienst wordt gepresenteerd als ware het afhandelen van bankzaken een spel: "... what Simple actually wants to do is get you to play a game. The game is called 'Master Your Finances,' and you are Player 1." Bij klassieke vormen van financiële gegevensverwerking hebben transactiegegevens nadat het primaire doel waarvoor ze zijn verzameld is afgehandeld (de overboeking), nauwelijks meer gebruikswaarde. Maar het voorbeeld van Simple laat zien dat recycling van gegevens, door deze te combineren met andere gegevens en op zoek te gaan naar onontdekte verbanden, *booming business* is. In feite is het hoofddoel van de gegevens niet langer statisch maar dynamisch: afhankelijk van het hergebruik verandert het lopende de tijd van gedaante. De consequentie is echter dat als de juistheid van gegevens moet worden beoordeeld als 'een juiste weergave van de feiten in het licht van de werkelijkheid', kwaliteit niet of nauwelijks op voorhand is vast te stellen. Er is immers een potentieel ontelbaar aantal secundaire toepassingen en daarmee werkelijkheden waar de gegevens bij moeten aansluiten.

Hoe verder?

Het beoordelen van kwaliteit en kwaliteitsbeleid is geen eenvoudige opgave, zo laten eerdere NJV-preadviezen 2015 zien. Kwaliteit is de geschiktheid van iets – persoonsgegevens – voor een bepaalde verwerking, maar kwaliteitsbeleid hangt onder meer af van hoe men de ambitie definieert en welke accenten men daarbij legt.[261] Wat dient kwaliteitsbeleid heel concreet te omvatten in de gevallen waarin individuen zonder dat ze dit weten worden onderworpen aan voorspellingen die hun toekomstige opties beperken en dit wordt gedaan met behulp van gegevens die niet logisch kunnen worden afgeleid uit de beschikbare combinatie van gegevens? Bovendien gaat het hierbij niet uitsluitend om de kwaliteit van de gegevens. Vaak gaat het bij big data ook om de kwaliteit van de selectiecriteria die bij de data-analyse worden gehanteerd. Voor de kwaliteit daarvan zal hebben te gelden dat ze doeltreffend en doelmatig zijn. Aandacht zal er ook moeten zijn voor de fundering (*evidence based*) van de keuze voor de gehanteerde criteria en daarmee indirect ook de rechtmatigheid van het gebruik van die criteria. Waar bij gegevens – juist omdat de duiding in de context zo belangrijk is – een kwaliteitsoordeel aan de hand van min of meer objectiveerbare criteria moeilijk is, zal dat voor het oordeel over de kwaliteit van de selectiecriteria eerder mogelijk zijn.

261. Van Lochem, Van Gestel, De Bock, 2015, p. 18.

Ook bij de inzet van big data-toepassingen zijn kortom concrete kwaliteitseisen te stellen. Belangrijk is echter te erkennen dat binnen het totale verwerkingsproces verschillende standaarden zullen gelden. Een kwaliteitsstandaard voor de fase waarin de gebruiker datamining toepast om interessante profielen te detecteren. En een standaard voor de fase waarin op basis van vastgestelde profielen persoonsgegevens worden gebruikt met het oog op een concrete toepassing. Zeker in deze fase moeten maatregelen worden getroffen die garanderen dat de persoonsgegevens een juiste weergave bieden van de feiten. Gevolg hiervan is dat het oordeel op de vraag of een verantwoordelijke voldoende maatregelen heeft genomen om de kwaliteit van de gegevens en gehanteerde selectiecriteria te garanderen, geen eigenstandig oordeel kan zijn, maar onderdeel is van de bredere toets van een gerechtvaardigd belang. Zeker bij kwetsbare toepassingen van big data die we eerder in dit preadvies bespraken (paragraaf 2.3) moet het bij beleid voor gegevenskwaliteit immers om meer gaan dan uitsluitend procedurele regels en *tools* voor het beoordelen van kwaliteit. Uiteindelijk zal het moeten gaan om het afleggen van verantwoording of de gegevens en gehanteerde criteria zodanig zijn gekozen dat het gebruik is gelegitimeerd met het oog op de toepassing waarvoor ze worden ingezet en de risico's die daarmee zijn gemoeid.

4.5 De gerechtvaardigd belang-toets concreet gemaakt

Als we alle hiervoor gepresenteerde touwtjes aan elkaar knopen, staan we voor de vraag wat een en ander nu betekent als we de gerechtvaardigd belang-toets concreet maken. Natuurlijk beseffen wij dat het niet mogelijk is om vooraf aan te geven wat dan een 'goede' principiële afweging over gerechtvaardigd belang inhoudt, of hoe die in alle specifieke gevallen dient uit te pakken. Los van een specifieke context kan die uitkomst ook niet op voorhand worden voorgeschreven. Toch, alhoewel niet op voorhand is aan te geven hoe een oordeel over gerechtvaardigd belang zal uitpakken, is wel veel te zeggen over de randvoorwaarden van die afweging en de wijze waarop invulling dient te worden gegeven aan het zoeken en bediscussiëren van de balans tussen de verschillende belangen door een verwerker.
Eerder stelden we al dat zoals bij zoveel andere open normen (denk aan het verbod op **misleidende reclame**), deze norm uiteindelijk via handhaving zal moeten uitkristalliseren waardoor duidelijk wordt hoe de afweging in nieuwe gevallen uit zou moeten pakken. De WP29 heeft verder een uitgebreide voorzet gedaan hoe de gerechtvaardigd belang-toets dient te worden toegepast in de Opinie over de grondslag van gerechtvaardigd belang, en daarin ook een lijst van illustratieve voorbeelden gegeven hoe de normen in concrete gevallen uitwerken. Gezien de snelle ontwikkelingen is niet aan te bevelen deze beleidslijnen in wetgeving te verankeren, om zo te zorgen dat deze zich snel aan de veranderende omstandigheden en nieuwe

inzichten kunnen aanpassen.[262] Onze aanbeveling is wel om de WP29 (onder de Verordening omgevormd tot de European Data Protection Board) nader te laten bepalen wat de ondergrenzen van verwerkingen op grond van het gerechtvaardigd belang zijn, met andere woorden specifieke gegevensverwerkingen aan te wijzen die niet zijn toegestaan omdat deze een te vergaande inbreuk op de fundamentele rechten en vrijheden van individuen opleveren (zie ook paragraaf 5.1).[263]

Overigens is opvallend dat de wijze waarop de WP29 de gerechtvaardigd belang-toets vormgeeft in feite al nauw aansluit bij de wijze waarop wij hier voorstellen dat deze toets dient te worden toegepast. Zonder het werk van de WP29 hier over te willen doen, zijn onze belangrijkste voorstellen ten aanzien van de toets de navolgende.

a. Collectief belang

Belangrijk is allereerst dat bij de toetsing van het gerechtvaardigd belang ook het collectief belang dient te worden betrokken. De WP29 heeft inmiddels herhaaldelijk aangegeven, dat bij de toetsing van de gerechtvaardigd belang-grondslag en de toetsing of een verdere verwerking voldoet aan het verenigbaarheidsvereiste, niet uitsluitend de potentiële negatieve implicaties voor betrokkenen dienen te worden betrokken. Ook zal een bredere kosten/batenanalyse gemaakt moeten worden, waarin de implicaties voor privacy **en andere risico's** voor zowel het individu **als de samenleving** worden betrokken en een afweging wordt gemaakt met de mogelijke **voordelen** van de verwerking voor het individu, bedrijven en de maatschappij als geheel.[264]

262. Dit is geen nieuw inzicht, maar is ook de conclusie voor andere rechtsgebieden. Zie eerder Moerel, 2014, p. 177, met verwijzing naar *The Report of the High Level Group of Company Law Experts on a Modern Regulatory Framework for Company Law in Europe*, Brussels, 4 November 2002, beschikbaar via <http://ec.europa.eu/internal_market/company/modern/index_en.htm>, at para. 2: "We noted that the system of harmonising company law through Directives – that have to be implemented by Member states – may have led to a certain "petrifaction". Once Member States have agreed to an approach in an area of company law and have implemented a Directive accordingly, it becomes very hard to change the Directive and the underlying approach. Simultaneously however, there is a growing need to continuously adapt existing rules in view of rapidly changing circumstances and views (…) Secondary regulation by the government, based on primary legislation in which broad objectives and principles are laid down; the secondary regulation can be amended more quickly when circumstances require change. (This process also often enables more effective consultation and reflection of an expert consensus)."
263. Het ASNEF-FEMCED arrest van 24 november 2011 (zaken C-468/10 en C-469/10) verbiedt dat dergelijke nadere regels op nationaal niveau worden gesteld. Ook onder de Verordening is daar geen ruimte voor. Nadere richtsnoeren (uitleg) kunnen wel worden gesteld door de nieuwe European Data Protection Board (de opvolger van WP29, zie artikel 64 ev. Verordening).
264. Zie ook het HvJ in de zaak Schrems, Zaak C-362/14, 6 oktober 2014, EU:C:2015:650

"In assessing the impact of the processing, both positive and negative consequences should be taken into account. These may include potential future decisions or actions by third parties, and situations where the processing may lead to the exclusion of, or discrimination against, individuals, defamation, or more broadly, situations where there is a risk of damaging the reputation, negotiating power, or autonomy of the data subject.

In addition to adverse outcomes that can be specifically foreseen, broader emotional impacts also need to be taken into account, such as the irritation, fear and distress that may result from a data subject losing control over personal information, or realising that it has been or may be misused or compromised, – for example through exposure on the internet. The chilling effect on protected behaviour, such as freedom of research or free speech, that may result from continuous monitoring/tracking, must also be given due consideration.

The Working Party emphasises that it is crucial to understand that relevant 'impact' is a much broader concept than harm or damage to one or more specific data subjects. 'Impact' as used in this Opinion covers any possible (potential or actual) consequences of the data processing."

_____

Opinie WP29 06/2014, p. 37.

b. Aard van de gegevens

Het tweede voorstel is het verlaten van een afzonderlijk regime voor bijzondere persoonsgegevens. Het is de aard van de gegevens (waaronder de mate van gevoeligheid in de betreffende context) die een factor dient te zijn in de afweging of is voldaan aan de gerechtvaardigd belang-toets. Ook de WP29 heeft inmiddels aangegeven dat de aard van de betreffende gegevens (de mate van gevoeligheid) een van de factoren is die een rol speelt bij de belangenafweging als onderdeel van de gerechtvaardigd belang-toets.

"It would first be important to evaluate whether the processing involves sensitive data, either because they belong to the special categories of data under Article 8 of the Directive, or for other reasons, as in the case of biometric data, genetic information, communication data, location data, and other kinds of personal information requiring special protection."

_____

Opinie WP29 06/2014, p. 38.

c. Contractuele relatie en toestemming niet langer als zelfstandige grondslag

Wat betreft toestemming menen wij dat toestemming en contractuele relatie niet langer als zelfstandige grondslagen voor de verwerking van gegevens moeten fungeren, maar slechts als een factor bij de beoordeling van de vraag of sprake is van een gerechtvaardigd belang. Ook op dit punt heeft de WP29 inmiddels aangegeven dat de *contractuele relatie* inderdaad een factor is bij het maken van de belangenafweging. Dit uit zich in een aantal door de WP29 relevant geachte (en reeds in paragraaf 4.1 besproken) factoren voor de afweging of voldaan is aan de gerechtvaardigd belang-toets (zoals status van het individu, de verantwoordelijke en de implicaties voor het individu en diens gerechtvaardigde verwachtingen). Daarbij geldt dat hoe specifieker de relatie is, hoe meer beperkingen er waarschijnlijk voor het gebruik van de data zullen zijn.

> "The reasonable expectations of the data subject with regard to the use and disclosure of the data are also very relevant in this respect. As also highlighted with regard to the analysis of the purpose limitation principle, it is 'important to consider whether the status of the data controller, the nature of the relationship or the service provided, or the applicable legal or contractual obligations (or other promises made at the time of collection) could give rise to reasonable expectations of stricter confidentiality and stricter limitations on further use. In general, the more specific and restrictive the context of collection, the more limitations there are likely to be on use. Here again, it is necessary to take account of the factual context rather than simply rely on text in small print."
>
> Opinie WP29 06/2014, p 38.

Wat toestemming betreft geldt hetzelfde. Het enkel vragen van toestemming is onvoldoende, maar (*opt-in* of *opt-out*) toestemming kan wel een sluitstuk zijn bij de gerechtvaardigd belang-toets.

> In connection with these safeguards – and the overall assessment of the balance – the Working Party wishes to highlight three specific issues that often play a crucial role in the context of Article 7(f):
> (…)
> – the right of the data subject to object to the processing, and beyond objection, the availability of an opt out without the need for any justification;(…)"

d. Informatieverplichtingen en inzage- en correctierechten

In plaats van de informatieverplichtingen dient onderdeel van de gerechtvaardigd belang-toets te zijn in hoeverre betrokkenen *controle* wordt gegeven over de verwerking van hun gegeven en de toepassingen daarvan. Ook

op dit punt heeft de WP29 aangegeven dat het geven van controle aan individuen een belangrijke privacymitigerende maatregel kan zijn.

> "In connection with these safeguards – and the overall assessment of the balance – the Working Party wishes to highlight three specific issues that often play a crucial role in the context of Article 7(f):
> (…)
> – empowering data subjects: data portability and the availability of workable mechanisms for the data subject to access, modify, delete, transfer, or otherwise further process (or let third parties further process) their own data."
>
> Opinie WP29 06/2014, p. 38.

e. Accountability en transparantie vereiste

Voorwaarde is verder dat verantwoordelijken de verplichting krijgen hun afwegingen met betrekking tot ieder van de fasen van de levenscyclus van gegevens transparant te maken.[265] De vaak impliciete afwegingen die verwerkers van gegevens momenteel maken (of soms in het geheel niet maken) dienen vanuit de gerechtvaardigd belang-toets veel meer inzichtelijk, navolgbaar en aanvechtbaar te worden gemaakt.[266] Het transparantiebeginsel blijkt over het algemeen een goed reguleringsinstrument voor het disciplineren van bedrijven.[267] Indien zij hun afwegingen en keuzes bekend moeten maken leidt dit veelal tot duidelijke beleidslijnen die een bedrijf bereid is openbaar te maken en voor een breder publiek te verdedigen. Wat ons betreft geldt hier: "sunlight is the best of disinfectants".[268] Aldus kan het normenkader daadwerkelijk grensstellend werken en is het meer dan het huidige *tick de box* mechanisme van informeren en toestemming. Verantwoordelijken kunnen zich immers niet langer verschuilen achter (zogenaamd) geboden 'transparantie' en verkregen toestemming dan wel geaccepteerde contractuele voorwaarden. Zie in die zin ok de WP29.

265. Zie eerder Moerel, 2014, p. 60, onder verwijzing naar Hildebrandt, 2014, p. 21 voor een vergelijkbare suggestie, maar vanuit een ander perspectief, namelijk over de vraag welke informative en keuzes in de "limelight" moeten worden geplaatst en welke in de duisternis moeten blijven, omdat de huidige informatie- en toestemmingsvereisten in een "buffer overflow" resulteren.
266. Zie soortgelijk voor afwegingen binnen een overheidscontext: WRR, 2011.
267. Zie eerder Moerel, 2014, p. 60, onder verwijzing naar Thaler, Sunstein, 2008, p. 245.
268. Deze quote is toegeschreven aan US Supreme Court Justice Louis Brandeis, zie Sunstein, 2001, p 174.

"In that sense, Article 7(f) is based on the accountability principle. The controller must perform a careful and effective test in advance, based on the specific facts of the case rather than in an abstract manner, taking also into account the reasonable expectations of data subjects. As a matter of good practice, where appropriate, carrying out this test should be documented in a sufficiently detailed and transparent way so that the complete and correct application of the test could be verified – when necessary – by relevant stakeholders including the data subjects and data protection authorities, and ultimately, by the courts.
(…)
The notion of accountability is closely linked to the notion of transparency. In order to enable data subjects to exercise their rights, and to allow public scrutiny by stakeholders more broadly, the Working Party recommends that controllers explain to data subjects in a clear and user-friendly manner, the reasons for believing that their interests are not overridden by the interests or fundamental rights and freedoms of the data subjects, and also explain to them the safeguards they have taken to protect personal data, including, where appropriate, the right to opt out of the processing."

_____
Opinie WP29 06/2014, p. 38.

De toets samengevat

Kortom, en samengevat in onze eigen formulering, persoonsgegevens zouden moeten kunnen worden verzameld, gebruikt (profilering daaronder begrepen), samengevoegd, doorgegeven of vernietigd:

> "indien de betreffende gegevensverwerking noodzakelijk is voor de behartiging van een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer prevaleert".

Het is in eerste instantie de verwerker van persoonsgegevens die de belangenafweging vanuit de bovenstaande opdracht vorm en inhoud moet geven. Reële en toetsbare argumenten en afwegingen zijn hier cruciaal. Dat betekent dat de gemaakte afwegingen moeten worden geëxpliciteerd en publiekelijk dienen te worden verantwoord. Alleen een stevige, geloofwaardige en procesmatig vormgegeven invulling van de afweging kan immers de realiteitswaarde van de gerechtvaardigd belang-toets garanderen. De door bedrijven op te stellen en te publiceren Data protection Impact Assessment (DPIA) is niet alleen voor hen het instrument om op alle vitale momenten in het proces van gegevensverwerking de belangenafweging concreet invulling te geven. Het moet ook de samenleving – individuen, toezichthouders en de rechter – in staat stellen

indien noodzakelijk een *countervailing power* te zijn en reëel toezicht te houden.[269] Daarover komen wij in paragraaf 5.2 nog te spreken.

Overigens reikt het in de Verordening Gegevensbescherming verankerde instrument van de DPIA[270] slechts ten dele het noodzakelijke instrumentarium aan. De verplichting een DPIA uit te voeren ziet alleen op verwerkingen die een hoog risico voor privacy hebben en verplicht verantwoordelijken niet de DPIA (of in ieder geval de gemaakte keuzes en afwegingen daaromtrent) openbaar te maken. Wel bevat de Verordening een cryptische bepaling die verwerkers verplicht om "waar gepast" de betrokkenen of hun vertegenwoordigers te consulteren.[271] Bij voorgenomen verwerkingen van gegevens van werknemers ligt het voor de hand dat de Ondernemingsraad wordt geconsulteerd. Dit is nu ook al verplicht.[272] Volstrekt onduidelijk is wanneer het gepast zal zijn om ook consumenten (bijvoorbeeld via een consumentenbond) te consulteren over voorgenomen verwerkingen. De Europese wetgever heeft hier niet de aanbevelingen van de WP29 gevolgd, hetgeen wat ons betreft een gemiste kans is.

Recapitulerend: elk van de fasen van de levenscyclus van gegevens zal, kijkend vanuit de specifieke context die aan de orde is, door de verwerker van persoonsgegevens moeten worden beoordeeld. Deze specifieke context wordt mede bepaald door factoren als[273]:

- De hoedanigheid van de verantwoordelijke (betreft het de dokter, Facebook of de NSA);
- De hoedanigheid van het individu (patiënt, student, consument, werknemer);
- De wijze waarop de gegevens worden verkregen (betreft het gegevens vertrekt door het individu of zijn deze afkomstig van derden, werd het individu zonder diens medeweten geobserveerd of geanalyseerd);
- De aard van de gegevens (betreft het gezondheidsgegevens, WhatsApp-berichten of bezoekersgegevens van een site);
- Het belang voor de verwerking (ziet de verwerking op uitsluitend een commercieel belang van de verwerker, kent het mogelijke voordelen voor het individu dan wel de samenleving, wordt een breder maatschappelijk belang beoogd en gediend);
- Het kanaal waarmee de gegevens worden verzameld (via een mobiele app, via een online *scraper* of in een 1-op-1 gesprek);
- De implicaties voor het individu (kreeg het individu in ruil een relatief onschuldige gratis dienst, is de al dan niet toekomstige (maatschappelijke dan wel economische) positie van het individu in het geding).

269. Zie over handhaving paragraaf 5.2.
270. Artikel 33 ev. Verordening Gegevensbescherming.
271. Artikel 33(4) Verordening Gegevensbescherming.
272. Artikel 27(1) sub k Wet op de ondernemingsraden.
273. Zie hierover ook: World Economic Forum Report, 2013, p.11.

Zoals nu ook al het geval, impliceert de belangenafweging tevens een proportionaliteits-test. Concreet betekent dit onder meer dat in elke fase van de verwerking mitigerende maatregelen moeten worden getroffen. Bij big data-toepassingen zullen grote hoeveelheden gegevens worden verwerkt (data minimalisatie is dan niet noodzakelijkerwijs van toepassing). Het proportionaliteitsbeginsel zal dan echter wel verlangen dat de gegevens bij de bron worden gepseudonimiseerd, waarbij de sleutel slechts in een zeer beperkt aantal situaties en voor een zeer limitatief aantal personen beschikbaar is. Aldus worden de effecten van de analyse op het niveau van concrete individuen zoveel als mogelijk beperkt, zo niet geëlimineerd. Wat betreft de "toepassingsfase" kan vervolgens de conclusie zijn dat de uitkomsten van de analyses niet mogen worden benut voor het nemen van beslissingen met negatieve consequenties voor de concrete individuen. Zijn de implicaties echter verwaarloosbaar, neutraal of positief voor individuen of wegen de belangen van de samenleving als geheel zwaarder, dan zou de belangenafweging naar de andere kant kunnen doorslaan. Afhankelijk ook van de uitkomst van de belangenafweging kan de conclusie zijn dat het bieden van een opt-out of het vragen van een opt-in is aangewezen.[274]

5. Grenzen stellen en handhaven

Wat ons betreft liggen er nog twee cruciale vragen op tafel: in hoeverre dient de overheid toch nog op voorhand grensstellend op te treden (paragraaf 5.1) en op welke wijze moet handhavend worden opgetreden mochten verwerkers een loopje nemen met het voorgestelde afwegingskader (paragraaf 5.2)?

5.1 Grenzen aan gerechtvaardigd belang

Wat ons betreft zijn er inderdaad grenzen, zelfs als naar het oordeel van verwerkers en derden sprake is van een gerechtvaardigd belang. Om het simpel te verwoorden: aan bepaalde diensten heeft een democratische en op een zekere solidariteit gestoelde samenleving nu eenmaal geen behoefte. Te denken valt aan aanvullende pakketten bij ziektekosten- of arbeidsongeschiktheidsverzekeringen waarbij de premie is gebaseerd op data-analyse met behulp van onder meer genetische informatie. We

274. Een voorbeeld hier is het verzamelen van gegevens door middel van cookies. Indien de gegevens worden gebruikt voor het doen van website analytics, fraudebestrijding of het aanpassen van de bezochte website van de voorkeuren van de bezoeker zal er een gerechtvaardigd belang zijn. Indien de gegevens worden aangewend voor cross-site behavioural targeting zal de uitkomst waarschijnlijk zijn dat hiervoor de voorafgaande toestemming van het individu nodig is. Zie hiervoor in paragraaf 4.3.

maakten eerder in dit preadvies al melding van farmaceutische bedrijven die volgens berichten in de media inmiddels intensief optrekken met bedrijven als Google en Apple in de zoektocht naar waardevolle genetische kennis om die commercieel te benutten.[275] Zolang hun data-analyse zich beperkt tot het genereren van abstracte inzichten en modellen (en mitigerende maatregelen zijn getroffen, zoals het inrichten van een aparte analyse-omgeving, de gegevens worden gepseudonimideerd en er strikte toegangscontrole is), zal voor het doen van de analyses heel wel 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. Ziektekostenverzekeraars benutten momenteel de bij hen beschikbare gegevens in geanonimiseerde vorm in hun zoektocht naar mogelijke vroege indicatoren voor dementie. Weinigen zullen in deze geanonimiseerde vorm fel tegenstander zijn. Het andere uiterste is de App 'die elk uur test of er al dementie in aantocht is'.[276] Ingewikkeld wordt het echter wanneer de data-analyse sterke aanwijzingen oplevert dat bij een bepaald patroon mogelijk sprake is van een aanleg voor dementie. Achten we het vervolgens aanvaardbaar of wellicht zelfs wenselijk dat ziektekostenverzekeraars deze kennis koppelen aan persoonsgegevens, bijvoorbeeld om proactief een signaal richting de betreffende individuen of de huisarts te geven?[277]

Bij big databestanden zullen inzichten en andere kennis vrijwel altijd zijn te herleiden tot een concrete persoon. De tijd is voorbij waarin het volstond dat de wetgever criteria formuleerde voor situaties waarin een individu wel of niet geïdentificeerd *kan* worden.[278] Bescherming zal moeten aanknopen bij het oordeel of de kennis wel of niet tot een persoon *mag* worden herleid. Voor bepaalde inzichten zal dan hebben te gelden dat deze niet mogen worden benut voor geïndividualiseerde toepassingen. Dat zal wat ons betreft zeker het geval zijn bij voorspellende kennis over de 'winnaars' en 'verliezers' in onze samenleving.[279] Ook valt te denken

275. http://www.wired.com/2015/07/another-personal-genetics-company-selling-client-data/
276. Aldus medische specialist en bestuursvoorzitter van het AMC, Marcel Levi, in een column in Medisch Contact (10 september 2015).
277. Zie eerder over deze discussie Buruma, Prins, 2009, p. 1374-1387.
278. Zie onder meer de studie waarin werd aangetoond dat aan de hand van een geanonimiseerd databestand waarin gegevens waren opgenomen over de locatie van (geanonimiseerde) personen en hun verplaatsing per uur geregistreerd, deze personen met een 95% zekerheid uniek waren te identificeren. De Montjoye, Hidalgo, Verleysen, Blondel, 2013, p. 1376.
279. Zie over de ontwikkeling dat de digitale samenleving het onderscheid tussen rijk en arm vegroot en het feit dat de gevestigde klassen profiteren van de big data analyses (die goede kredietbeoordelingen hebben en een goed consumptieprofiel) en de lagere klassen en kwetsbare groepen (die vatbaar voor ziektes, misdaad of andere sthmatiserend gedrag zijn) eerder de negatieve implicaties van de analyses zullen ervaren: Moerel, 2014, p. 14-16 en p. 42-43 en de daar opgenomen literatuur.

aan situaties waarin burgers zich in het maatschappelijk leven niet langer in vrijheid blijken te kunnen ontplooien, bijvoorbeeld als sprake is van machtsongelijkheid tussen commerciële bedrijven en individuen in combinatie met zeer ingrijpende implicaties van de inzet van data-analyse, zoals in het besproken voorbeeld van 'pay-how-you-drive' verzekeringen.

> "In the end the worry may not be so much about having information gathered about us, but rather being sorted in the wrong or disfavoured bucket."
>
> Jerome 2013, p 50-51.

Kortom, ons inziens heeft de overheid zich een verantwoordelijkheid aan te meten vanuit de taak haar burgers te beschermen tegen bepaalde voorzienbare en onvoorzienbare effecten van data-innovatie. De noodzaak tot het doordenken van een grensstellend kader dat op voorhand is gegeven vloeit ook voort uit de zeer fluïde grenzen tussen de private en publieke sector als het om gegevensuitwisseling gaat. Veel gegevens worden over de grenzen van beide sectoren heen gedeeld, waarbij de private sector lang niet altijd in de positie is de publieke sector te beteugelen wat betreft het opvragen van informatie. Dankzij digitalisering en gelegitimeerd door wetgeving die de private sector verplicht tot het verstrekken van informatie aan de overheid, vervloeien de – toch al niet scherp afgebakende – grenzen tussen de private en publieke sector. En eenmaal aan de overheid verstrekt, is de informatie in handen van een monopolist hetgeen de situatie anders maakt dan wanneer de private sector zich geen betrouwbare partner van een consument toont.

Belangrijk is ten slotte de blinde vlek op macroniveau die de inherente consequentie is van een gerechtvaardigd belang-toets die op microniveau door de verwerker moet worden uitgevoerd. Weliswaar zal de toets plaats moeten vinden vanuit een breder perspectief dan de geambieerde innovatie in de geïsoleerde context. Toch, verantwoordelijken zullen niet in staat zijn de toepassing te beoordelen op de meer omvattende veranderingen die, onder invloed van het benutten van bepaalde data, uiteindelijk de samenleving als geheel raken. Dit heeft tot gevolg dat de bredere maatschappelijke belangen en daarmee afbreukrisico's op macroniveau die juist op de langere termijn en bij het samenkomen van verschillende ontwikkelingen naar voren treden, onvoldoende door individuele bedrijven kunnen worden gezien en erkend.

Vanuit de noodzaak om ook waar het de private sector aangaat te kunnen sturen op de meer omvattende veranderprocessen die in de samenleving plaatsvinden, menen wij dat de wetgever van sommige vormen van gegevensgebruik zal moeten zeggen: "die (nog) niet". Daarbij valt in ieder

geval te denken aan het verwerken van genetische informatie op gepersonaliseerd niveau. Een ander voorbeeld zijn de "*pay-how-you-drive*" en "*pay-how-you-live*" verzekeringsvormen. De vormgeving van de begrenzing die wij bepleiten zal niet die van een *ex-ante* toetsing moeten zijn, zoals die momenteel onder de Wbp voor bepaalde typen van gegevensverwerking geldt (en die we ook in de Verordening Gegevensbescherming terugzien). De praktijk wijst uit dat procedurele regels en argumenten hier veelal in de weg staan aan het realiseren van een materiële toetsing. Bovendien biedt de waarborg van de ex-ante toetsing uiteindelijk slechts beperkte bescherming. Ook in dit geval geschiedt beoordeling en daarmee rechtsbescherming immers van geval tot geval (net als de handhaving door de privacytoezichthouder), waarmee deze niet vanuit een macro-beoordeling het noodzakelijk tegenwicht kan bieden. Idealiter zou een soort ondergrens voor gerechtvaardigd belang moeten worden geformuleerd gebaseerd op bepaalde typen gegevens en vormen van gegevensgebruik. Gekozen kan bijvoorbeeld worden dit kader te laten expliciteren door de WP29, om het vervolgens door de (nationale) toezichthouder en de rechter stapsgewijs en contextafhankelijk nader te ontwikkelen. Het formuleren van deze ondergrens is uiteindelijk ook een politieke opdracht. En uiteraard is de uitkomst daarvan altijd gekleurd en omstreden. Toch, er zal moeten worden geprobeerd een soort *common ground* te formuleren voor de zaken waar een overheid in de digitale samenleving garant voor moet staan. Deze systeemverantwoordelijkheid kan niet zonder meer terzijde worden geschoven.[280]

5.2 Handhavingsopties

Nu de digitalisering in de haarvaten van onze samenleving is doordrongen en er een dermate verscheidenheid van verwerkingen is, zal het niet verbazen dat er niet een *one fits all* optie voor handhaving is. Zo caleidoscopisch de verwerkingen, zo caleidoscopisch de wijze waarop handhaving het beste kan worden vormgegeven om het gewenste resultaat te borgen. Dat geldt ook voor de handhaving van het door ons voorgestelde toetsingskader. Bovendien, ook het terrein van de gegevensbescherming zal niet immuun zijn voor de veranderingen die zich op dit moment in onze meerlagige rechtsorde voltrekken. Onherroepelijk zullen ontwikkelingen als de constitutionalisering van het privaatrecht (de doorwerking van fundamentele rechten in het privaatrecht), de aandacht voor de rol van het privaatrecht als instrument van (overheids)beleid, de groeiende populariteit van *public interest litigation* en de toenemende invloed van niet-statelijke regels hun uitwerking hebben op vorm en inhoud van zowel privacynorm-

280. WRR, 2011, p. 237-240.

stelling als -handhaving.[281] We staan daarom in dit preadvies niet uitgebreid stil bij de verschillende handhavingsopties. In ieder geval is het onze verwachting dat met het sterk vereenvoudigde kader dat wij hiervoor hebben gepresenteerd ook de bereidheid tot naleving van de regels zal verbeteren. Daar waar die bereidheid er niet is, zijn de sancties aanzienlijk groter dan in het verleden nu de boetes zeer fors omhoog zijn gegaan en in de miljoenen euro's kunnen lopen.

Belangrijk is wel dat we als samenleving niet langer mogen verwachten dat individuele burgers primair verantwoordelijk zijn voor de handhaving van gegevensbescherming en daarmee borging van privacy voor onze samenleving. De realiteit van onze datagedreven samenleving is dat individuen ondanks de hen toegekende rechten, nauwelijks tot niet in staat zijn tot effectieve handhaving. Bij gegevensverwerkers krijgen ze veelal nul op rekest, de toezichthouder pakt individuele klachten van consumenten niet of slechts in uitzonderlijke situaties op en effectieve rechtsbescherming via een (civiele) procedure is illusoir. Niet alleen zullen de kosten van de laatstgenoemde route nogal in de papieren lopen. Ook is het voor individuen lastig aan te tonen wie verantwoordelijk is voor de betreffende inbreuk, in welke mate zij in hun individuele privacybelang zijn geschaad en wat de schade is waarin het onrechtmatige gegevensgebruik resulteert.[282] Hoewel het voor privacybescherming gunstig is dat bij het personenschaderecht voorzichtig wordt losgekomen van het idee dat het enkel gaat om financiële 'terugkeer in oude toestand', maar steeds meer om de vraag 'hoe nu verder?',[283] is de sterke afhankelijkheid van handhaving door individuen onwenselijk. Het gaat immers, zeker bij een ontwikkeling als big data, om maatschappelijke kwesties en de bescherming van publieke en ideële belangen. Wij betogen niet dat we af moeten van de handhaving door burgers zelf. Die ruimte moeten ze zeker behouden, en daartoe bepleiten wij ook een veel sterkere nadruk op daadwerkelijke controle voor individuen. Belangrijk daarbij is dat het ons dan niet zozeer gaat om de controle op het verzamelen van gegevens als zodanig. Nieuwe vormen van gegevensgebruik noodzaken daarentegen veeleer tot controle op de verwerking van gegevens en daarmee de implicaties die het gegevensgebruik voor het individu heeft. Los hiervan staat voor ons vast dat handhaving van gegevensbescherming niet langer primair de verantwoordelijkheid van individuele burgers kan zijn.

281. Zie hierover: Van Gestel, Loth, 2015, p. 2602-2603.
282. Cofone 2015, par. 2.4.4. Steeds vaker zal een privacyschending in een grensoverschreidende context plaatsvinden, hetgeen extra belemmeringen meebrengt, zie Moerel 2012, para. 4.3.
283. Zie Hartlief, 2015, p. 2003. Akkermans e.a., 2015; Loth, Beumers/Van Boom, 2015.

Veel intensiever dan momenteel, zal de privacytoezichthouder daarom op eigen initiatief tot snelle en effectieve handhaving moeten overgaan. Zeker, we erkennen dat de toezichthouder ook nu al handhavend optreedt. Maar wat ons betreft kan er nog wel een schepje bovenop. Daartoe krijgen de toezichthouders in de EU-lidstaten ook de mogelijkheden: met de Verordening wordt hun rol verzwaard en krijgen ze de nieuwe bevoegdheden. Wel zullen de nationale overheden hun verantwoordelijkheid moeten nemen om de toezichthouder ook de benodigde financiële middelen te geven om deze rol waar te maken.[284] Overigens kunnen ook andere toezichthouders handhavend optreden. Zo kan de ACM de regels van het consumentenrecht benutten.[285] Belangrijk is dat de verschillende toezichthouders tot een goede onderlinge afstemming komen.

Maar handhaving zal niet aan de toezichthouders alleen kunnen worden overgelaten. In lijn met de hiervoor genoemde tendens dat in onze meerlagige rechtsorde zich ook langs andere wegen de noodzakelijke maatschappelijke zorgvuldigheidsnormen ontwikkelen en eventuele schendingen worden getoetst, zijn zeker ook andere, waaronder civiele, instrumenten in te zetten. Veel meer nog dan nu het geval is, zou een beroep op de civiele rechter gedaan kunnen worden door maatschappelijke organisaties die een rechterlijke uitspraak benutten als breekijzer voor een scherpere demarcatie van de grenzen van gegevensgebruik. Een dergelijke stap zou passen bij de opkomst van zogeheten *public interest litigation*, waarbij acties op grond van artikel 3: 305a BW worden ingesteld omdat publieke belangen in het geding zijn.[286] Duidelijk is in ieder geval dat er op het terrein van privacy en persoonsgegevensbescherming een groeiende belangstelling is voor het instrument van collectieve acties en *class actions*.[287]

284. Daartoe is de Nederlandse regering kennelijk niet bereid: "Ik ben er niet in geslaagd om het ministerie te overtuigen van extra menskracht voor die nieuwe taken", aldus de voorzitter van de Autoriteit Persoonsgegevens, Kohnstamm, in NRC Handelsblad (30 december 2015, p. 2).
285. Consumenten moeten onder meer op een niet misleidende, eerlijke manier worden geïnformeerd over de voornaamste kenmerken en de prijs van een product. Zie hierover de minister van Economische Zaken: "Ook mag niet op een oneerlijke manier gebruik worden gemaakt van het begrip «gratis» of bewoordingen van gelijke strekking. Hiervan zou sprake kunnen zijn als apps of diensten als gratis worden geadverteerd terwijl in wezen sprake is van een uitruil doordat de gegevens van de consument worden uitgelezen. Ook moet de aanbieder van een digitale dienst de consument informeren of de digitale inhoud wordt gebruikt voor het in kaart brengen van consumentengedrag (ook wel bekend als tracking). De ACM ziet toe op de naleving van deze regels." Kamerstukken II, 2014/15, 32761, nr. 78, p. 4.
286. Zie hierover: Van Gestel, Loth, 2015, p. 2602-2603.
287. Zie over de recente ontwikkelingen de preadviezen voor de Vereniging voor Burgerlijk Recht over collectieve acties: Faure, Visscher, Tzankova 2015. Illustratief is de uitspraak van het 3rd District (New York) van 13 november 2015 in een zaak die tegen Google was aangespannen en waarin de rechtbank oordeelde dat een privacy-inbreuk als 'tort' kwalificeert en individuen schadevergoeding kunnen claimen.

Relevant in dit verband is de bepaling in de Verordening dat immateriële schade voor vergoeding in aanmerking dient te komen.[288] En, afgezien van het nieuwe boeteregime onder de Verordening dat werkt met een percentage van de wereldwijde omzet, zou bij handhaving langs de privaatrechtelijke weg overwogen kunnen worden te werken met een forfaitaire boete. Het zou dan kunnen gaan om een forfaitair bedrag per inbreuk per individu, wat kan oplopen bij groepsacties en kan variëren al naar gelang de ernst van de overtreding.[289]

Wij roepen ook op tot innovatie in handhaving, zowel in het instrumentarium als op institutioneel niveau. Naar voorbeeld van Duitsland kan worden gedacht aan de mogelijkheid voor concurrenten om elkaar op naleving van de privacyregels aan te spreken (zoals ook bijvoorbeeld bij misleidende reclame het geval is).[290] Inspiratie biedt eveneens de eind 2015 door de Duitse *Bundestag* aangenomen wetgeving die het voor consumentenorganisaties en kamers van koophandel mogelijk maakt om bedrijven voor de rechter te dagen indien in strijd met de privacywetgeving wordt gehandeld.[291] Richting de bedrijven zelf doen we de suggestie om te verkennen in hoeverre op co-regulering gestoelde modellen mogelijkheden bieden om op sectorniveau tot het afhandelen van privacyklachten te komen. Juist voor het afhandelen van grote hoeveelheden klachten laten voorbeelden in het buitenland zien dat er kansen liggen. In het Verenigd Koninkrijk bijvoorbeeld, handelt de UK Financial Ombudsman Service jaarlijks enkele honderdduizenden klachten af. Uit de annual review 2014/15 blijkt dat op welgeteld 1.786.973 vragen van consumenten werd gereageerd, waarvan 329.509 klachten die werden afgehandeld.[292]

288. Zie in dit verband ook het preadvies van Erik Tjong Tjin Tai. Zie artikel 77(1) Verordening Gegevensbescherming. Zie verder de recente uitspraak in het VK, waar schadevergoeding werd toegewezen ter compensatie van het enkele feit dat een inbreuk had plaatsgevonden, zonder dat daadwerkelijk schade werd aangetoond. Decision in Gulati & Ors v MGN Limited [2015] EWHC 1482 (Ch), r.ov. 132.
289. Een systeem van winstafdracht, zoals onder meer mogelijk bij inbreuk op intellectuele eigendomsrechten, is problematisch omdat het hier moet gaan om de daadwerkelijk aan de inbreuk toerekenbare winst, en die is niet noodzakelijk groot en bij misbruik van persoonsgegevens lastig te berekenen. Welke winst heeft een bedrijf gemaakt met bijvoorbeeld het welbewust niet goed informeren van consumenten? Ook bij een forfataire boete blijft het overigens lastig als we de hoogte daarvan zouden willen relateren aan daadwerkelijke schade/winst door inbreuk (met name nu het om zeer verschillende inbreuken kan gaan: binnenskamers verwerken van gegevens levert potentieel schade op/waarde van databank maar is lastig te begroten, schade met concreet gebruik is eenvoudiger maar niet altijd het belangrijkst of erg waardevol).
290. LG Frankfurt a.M., Urteil v. 18.02.2014, Az. 3-10 O 86/12; OLG Hamburg, Urteil v. 27.06.2013, 3 U 26/12.
291. Zie voor deze op 17 december 2015 aangenomen wetgeving: http://dip21.bundestag.de/dip21/btd/18/046/1804631.pdf
292. http://www.financial-ombudsman.org.uk/publications/ar15/ar15.pdf

Ter afsluiting van de handhavingsopties staan we kort stil bij een voor privacybescherming specifieke mogelijkheid*: privacy-by-design*.

Privacy-by-design

Belangrijk onderdeel bij toepassing van de beginselen van *privacy-by-design* of *privacy-by-default* (paragraaf 4.2.) is dat de grenzen aan en voorwaarden voor gegevensverwerking in de technologie zelf worden ingebouwd, waarmee additionele handhaving op de door de technologie gereguleerde onderdelen wordt gefaciliteerd en soms niet langer nodig is. Voorbeelden zijn de software waarmee de toegang tot bepaalde gegevens wordt afgesloten voor bepaalde functies en rollen van werknemers, of technisch gefaciliteerde protocollen op basis waarvan gegevens automatisch worden gewist na verloop van een bepaalde tijd. Illustratief is ook het automatisch versleutelen of pseudonimiseren van gegevens. In feite is met deze toepassingen ook de handhaving van de regels in handen van de technologie gelegd. Eerder in dit preadvies wezen we op de mogelijkheid om gepersonaliseerde advertenties die aan de bezoeker worden gepresenteerd te voorzien van een *icoontje* dat aan te klikken is, waarna de indicatoren worden getoond die de dienstaanbieder gebruikt voor het selecteren van de betreffende advertentie en die de bezoeker kan aanpassen al naar gelang hij/zij deze irrelevant of onjuist acht. Een wezenlijk verschil in niveau van privacybescherming valt ook te realiseren door als standaardinstelling (*default*) voor de gegevensverzameling en – verstrekking via websites, Apps en andere applicaties op smartphones **OFF** in plaats van **ON** te hanteren. Ook voor authenticatie en zoekmachines zijn inmiddels diverse toepassingen van privacy-by-design in ontwikkeling.[293]

Alhoewel diverse wettelijke vereisten zeker in applicaties zijn in te bouwen (zoals het afschermen van gegevens voor onbevoegden), hebben Koops en Leenes terecht opgemerkt dat privacy-by-design lang niet altijd valt te omarmen voor het afdwingen van privacyregels met behulp van technologie:

> "The idea of encoding legal norms at the start of information processing systems is at odds with the dynamic and fluid of many legal norms, which need a breathing space that is typically not something that can be embedded in software."[294]

Privacy-by-design dient, aldus de auteurs, veeleer opgevat te worden als een benadering waarbij leidende privacywaarden als dataminimalisatie, controle over gegevens, het opschonen van bestanden, etc. wezenlijke

293. Zie bijvoorbeeld: https://www.qiyfoundation.org/nl/ en de zoekmachine ixquick (https://www.ixquick.com/).
294. Koops, Leenes, 2014, p. 166.

ontwerpprincipes vormen.[295] Ook voor een beschermingsregime dat is gestoeld op een oordeel over gerechtvaardigd belang zal gelden dat privacy by design meer omvat dan een technologie-georiënteerde benadering bij het ontwerpen van de applicaties. Maar zeker voor apparaten en gebruiksvoorwerpen die gegevens verzamelen en doorsturen (Internet of Things) geldt dat er nog veel te winnen valt bij privacyvriendelijke productstandaardisatie. Daar waar momenteel wordt gewerkt aan Internet of Things-productstandaardisatie is privacy jammer genoeg uitsluitend aan de orde vanuit een beveiligingsoptiek.[296]

De Verordening bevat een verplichting voor de verwerker om verwerkingen privacy-by-design in te richten. Anders dan wij voorstaan bevat de Verordening echter geen verplichting voor leveranciers van software en digitale infrastructuur waarmee gegevens worden verwerkt om hun producten privacy-by-design in te richten. Het behoeft weinig betoog dat dit een gemiste kans is. De individuele verwerkers zullen nu ieder voor zich specifiek de leveranciers moeten vragen hun software privacy-by-design in te richten om zo aan hun verplichtingen te kunnen voldoen. Het had voor de hand gelegen om softwareleveranciers van met name standaardproducten een verplichting op te leggen deze privacy-by-design in te richten. Een dergelijke verplichting is effectiever te handhaven bij de leveranciers van software dan telkens de individuele gebruikers van software hierop aan te spreken. De leveranciers hebben verder geen eigen commercieel belang om bijvoorbeeld de inrichting van het vragen van een opt-in te omzeilen, waar dat voor individuele gebruikers anders kan liggen. Overweging 61 van de Verordening bevat wel een aanbeveling aan de lidstaten om de producenten “aan te moedigen” hun producten privacy-by-design in te richten. Onze aanbeveling aan de Nederlandse overheid is hieraan inderdaad opvolging te geven.

Afrondend over privacy-by-design nog het volgende. In feite zal aandacht hiervoor een onlosmakelijk onderdeel moeten zijn van de bredere opdracht binnen bedrijven om een goede impact assessment te maken telkens wanneer ze een nieuwe technologie invoeren (Technology Impact Assessment). Nieuwe technologieën brengen niet alleen privacy issues mee, maar ook ethische dilemma’s die op dit moment nog niet altijd even zichtbaar zijn en waarvoor we nog geen pasklare antwoorden hebben. Organisaties zullen ook dergelijke issues dienen te evalueren en in het ontwerp en aanbod van hun producten en diensten dienen te betrekken (ethics-by-design). Veel meer dan momenteel het geval is zullen de productontwikkelaars, bedrijfsjuristen, compliance officers, security officers, risk officers, en de e-business en IT-strategie verantwoordelijken met

295. Hoepman, 2012.

296. Zie bijvoorbeeld de augustus 2015 gepresenteerde raamwerk (versie 1.0) ontwikkeld door The Open Interconnect Consortium (http://openinterconnect.org/developer-resources/specs/).

elkaar in gesprek moeten gaan. Een oriëntatie alleen op privacy-by-design is te beperkt. De toekomst is wat ons betreft gelegen bij het uitvoeren van al omvattender Technology Impact Assessments.[297]

6. Afronding

In een van zijn columns pleitte de schrijver Arnon Grunberg vorig jaar voor de introductie van het recht op onwetendheid als mensenrecht.[298] Natuurlijk kan een democratie alleen bestaan als burgers geïnformeerde en beredeneerde keuzes kunnen maken, aldus de schrijver. Tegelijkertijd vereist ware kennis een specialisatie en tijdsinvestering die veel burgers niet kunnen opbrengen. "Een fatsoenlijke samenleving geeft zijn burgers in ieder geval de mogelijkheid om onwetend te zijn zonder dat die onwetendheid tot de beschuldiging van immoreel gedrag hoeft te leiden." Alhoewel Grunberg in zijn column de relatie tussen kennisverwerving en morele deugdzaamheid ter discussie stelde, willen wij zijn punt doortrekken naar een essentieel kenmerk van de ontwikkelingen die in dit preadvies zijn geagendeerd. De gedachte dat individuen in de huidige samenleving nog met voldoende kennis zorg kunnen dragen voor de bescherming van hun persoonsgegevens, is naïef. Kennis is niet langer een werkbaar instrument voor het realiseren van een geïnformeerde positie en daarmee de weg naar bewuste privacykeuzes. En dus mag onwetendheid van burgers – voor wie aanklikken van de OK-button in de praktijk veelal nog de enig resterende optie is – niet impliceren dat hen steeds meer privacypositie wordt ontzegd. Een fatsoenlijke samenleving geeft ook op dit vlak zijn burgers de mogelijkheid om onwetend te zijn, maar stelt hen tegelijkertijd in staat eigen levenskeuzen en levensstijlen vorm te geven. Het gaat, zoals we eerder in dit preadvies betoogden, om capabilities waarmee mensen in staat blijven mee te kunnen beslissen over de inrichting van de eigen sociale en informationele leefomgeving, relaties aan te gaan en vorm te geven, een veilig leven te leiden, zich intellectueel in vrijheid te kunnen ontwikkelen en eigen afwegingen te maken over wat goed en niet goed is. We zullen met andere woorden de stap moeten zetten naar een meer hedendaags beschermingsregime dat individuen ondanks onwetendheid, hun rechtmatige privacypositie garandeert zodat ze nog steeds in staat zijn zich in vrijheid te ontwikkelen en eigen afwegingen te maken.

Tegelijkertijd, daar waar individuen wel controle over hun gegevens wensen uit te uitoefenen, zal het beschermingsregime hen hier nog steeds in moeten faciliteren. En meer dan dat alleen. De wetgever zal het normen-

297. Zie eerder Moerel, 2014, p. 61 – 62, onder verwijzing naar European Commission, 2012, p. 9, 12 en 30.
298. Grunberg, 2015, p. 15.

kader zo moeten inrichten dat burgers aan hun gerechtvaardigde privacy-aanspraken ook daadwerkelijk invulling kunnen geven. Terugkerend naar de gezondheidsapp waar we dit preadvies mee begonnen: voor sommigen onder ons zal deze gerechtvaardigde privacy-aanspraak erop neerkomen dat ze zoveel als mogelijk over zichzelf te weten komen. Voor anderen betekent het daarentegen dat ze niets over hun gezondheidstoestand te weten behoeven te komen. Het betoog in de voorgaande paragrafen toont echter dat voor het realiseren van deze privacy-aanspraken de huidige – veelal procedureel benaderde – gegevensbescherming onvoldoende garanties biedt. Om gegevensbescherming naar de kern gestalte te kunnen geven, zal individuen niet alleen in formele, maar ook in materiële zin invloed op het gebruik van hun gegevens moeten worden geboden.

Maar ook verwerkers van gegevens mogen er op kunnen rekenen dat het de wetgever om meer te doen is dan het afkondigen en handhaven van een set rechtsregels die in de praktijk de beoogde doelstelling toch niet kunnen realiseren. Hier evenzeer dient het materieelrechtelijke oogmerk en niet de procedurele regel voorop te staan. Vanuit dit vertrekpunt en daarmee de gerechtvaardigde aanspraak van alle betrokken partijen – namelijk dat in *materiële* zin recht wordt gedaan aan een weging van de belangen die in een specifieke context voorliggen – zullen de procedurele regels hebben aan te sluiten bij zowel de ontwikkelingen in gegevensgebruik als de realiteit van degenen die aan deze regels hun positie ontlenen.

Kijkend naar de ontwikkelingen in gegevensgebruik die we in dit preadvies hebben geschetst en duiding hebben gegeven, is het onze stellige overtuiging dat het regelgevend kader dat ten dienste staat van gegevensbescherming niet primair gericht moet zijn op een beoordeling vanuit de in het betreffende geval betrokken individuele belangen (van zowel verwerkers als consumenten). Het huidige informatietijdperk veronderstelt dat bij de toetsing of een gegevensverwerking gerechtvaardigd is, ook het collectief belang wordt betrokken. Dat is ook het signaal dat de EU-wetgever destijds heeft afgegeven: de grondwettelijk verankerde opdracht geldt niet alleen voor de eerbiediging van het privéleven (art. 7 EU Handvest) maar evenzeer voor de bescherming van persoonsgegevens (art. 8 EU Handvest). De gerechtvaardigd belang-toets lijkt deze beoordeling bij uitstek te kunnen operationaliseren en kan ons inziens worden gezien als een species van het element van 'fairness' dat in dit artikel 8 EU Handvest staat. Daarbij wordt op Europees niveau inmiddels expliciet erkend dat de gerechtvaardigd belang-toets mede een beoordeling vanuit een breder, maatschappelijk, belang omvat. Zo heeft de WP29 herhaaldelijk aangegeven, dat bij de toetsing van de gerechtvaardigd belang-grondslag en de beoordeling of een verdere verwerking voldoet aan het verenigbaarheidsvereiste, niet uitsluitend het potentiële negatieve effect op betrokkenen mag worden betrokken, maar ook dat een kosten/batenanalyse dient te worden gedaan, waarbij de effecten op de privacy en andere risico's moe-

ten worden afgewogen tegen de mogelijke voordelen van de verwerking voor het individu, bedrijven en de maatschappij als geheel.[299]

Vanuit deze benadering bepleiten wij daarmee ook een andere functie en rol voor het regelgevend kader dat gegevensverwerking al dan niet legitimeert. Kort samengevat betekent het abstraheren van belangen en effecten op individueel niveau ook dat de privacyhouding van individuen (laks, naïef, argwanend, etc.) niet bepalend kan zijn voor het realiseren van materieelrechtelijke aanspraken. Concreet impliceert dit dat toestemming en contractuele relatie niet langer als zelfstandige grondslagen voor de verwerking van gegevens kunnen fungeren, maar slechts als een factor bij de beoordeling van de vraag of sprake is van een gerechtvaardigd belang. Ook betekent het dat de wetgever afstapt van de zelfstandige betekenis van informatieplichten voor verwerkers en rechten van betrokkenen (recht op inzage, correctie, verzet en verwijdering). In plaats daarvan is een beoordeling hiervan onderdeel van de gerechtvaardigd belang-toets. Centraal moet dan staan de vraag in hoeverre individuen realistische *controle* wordt gegeven over de verwerking van hun gegevens en de toepassingen daarvan.[300] Met andere woorden, wordt hen niet alleen de postbus voor inzage geboden, maar ook de route die naar een beter geïnformeerde privacypositie leidt?

Winst van ons voorstel zal uiteindelijk moeten zijn dat de vaak impliciete afwegingen die verwerkers van gegevens momenteel maken (of soms in het geheel niet maken) met de gerechtvaardigd belang-toets inzichtelijk, navolgbaar en aanvechtbaar worden gemaakt.[301] Aldus kan het normenkader daadwerkelijk grensstellend gaan werken en is het meer dan het huidige *tick de box*-mechanisme van informeren en toestemming waar verwerkers zich vaak al te gemakkelijk achter verschuilen. Met het aanscherpen van de noodzaak tot expliciteren en verantwoorden, komt tegelijkertijd een reductie van de complexiteit van het systeem voor de beoordeling van de rechtmatigheid van een gegevensverwerking. Zo kan het regime voor bijzondere persoonsgegevens worden afgeschaft omdat de aard van de gegevens (waaronder in ieder geval de mate van gevoeligheid in de betreffende context) een factor dient te zijn in de afweging of is voldaan aan de gerechtvaardigd belang-grondslag. Zoals hiervoor al opgemerkt, de bereidheid tot naleving van de regels zal winnen met het vereenvoudigde toetsingskader.

Ten slotte: wij realiseren ons dat de Verordening Gegevensbescherming is afgerond en onze voorstellen daarin niet kunnen worden meegenomen. In de inleiding hebben we aangegeven waarom we toch denken dat de

299. Opinie WP29 06/2014, p. 37.
300. WP29 heeft aangegeven dat het geven van controle aan individuen een belangrijke privacymitigerende maatregel kan zijn.
301. Zie soortgelijk voor afwegingen binnen een overheidscontext: WRR, 2011, paragraaf 2.4.

uitgewerkte gedachten relevant kunnen zijn. Samengevat hebben we gezien dat de criteria waaraan moet worden getoetst of sprake is van een gerechtvaardigd belang en/of voldaan is aan het verenigbaarheidsvereiste, nagenoeg overlappen. Beide vergen een contextuele beoordeling van de betreffende verwerking waarbij de proportionaliteit van het belang bij de verwerking wordt beoordeeld in het licht van de impact van de verwerking op de privacy van betrokken individuen, en de in dat kader van de verwerker te vergen mitigerende maatregelen. Mede gezien de objectivering van de betreffende toetsen in de Verordening, is dan ook de verwachting dat in de praktijk de twee toetsen tot hetzelfde resultaat zullen leiden. Gezien de additionele eisen die de WP29 inmiddels aan de overige grondslagen zoals toestemming, uitvoering overeenkomst en de verwerking van gevoelige gegevens stelt, in combinatie met het vereiste onder de Verordening voor verwerkingen met een hoog risico om een DPIA uit te voeren, is voor verwerkers in de praktijk de meest veilige (en daarmee rechtszekere) weg om door middel van een eenvormig protocol een contextuele beoordeling uit te voeren van de implicaties van het gebruik en hergebruik van gegevens. Via deze beoordeling wordt de verwerking langs de lat van alle criteria van de gerechtvaardigd belang-toets/verenigbaarheids-toets gelegd en worden de uitkomsten van de beoordeling alsmede de gemaakte afwegingen gedocumenteerd. Op deze manier wordt tegelijkertijd aan de nieuwe vereisten onder de aankomende Verordening voldaan.[302]

De stap naar een beoordeling primair vanuit gerechtvaardigd belang, is wat ons betreft de eerste in een ontwikkeling naar een andere benadering van gegevensbescherming. Ook het reguleren van gegevensverwerking aan de hand van de gerechtvaardigd belang-toets zal uiteindelijk onvoldoende stringent en tegelijkertijd flexibel blijken te zijn. In plaats van te trachten vooraf regels te stellen waaraan verwerkingen dienen te voldoen, zal op termijn een systeem waarbij achteraf misbruik wordt gestraft de vervolgstap moeten zijn. De vergelijking met de regulering van reclame en verkoopmethoden van bedrijven dringt zich op. Iedereen mag reclame maken en zijn/haar producten verkopen, maar misleidende reclame en oneerlijke handelspraktijken worden gestraft. Het is immers ondoenlijk om alle denkbare vormen van reclame en handelspraktijken (die bovendien voortdurend wijzigen) in regels voor toegestane reclame te vatten. Wanneer precies reclame als misleidend en handelspraktijken als oneerlijk worden beoordeeld, heeft zich in de loop der tijd in de rechtspraak ontwikkeld. Deze benadering toegepast op gegevensverwerkingen zou resulteren

302. Zoals de *accountability*-verplichting, waarbij dient te kunnen worden aangetoond dat verwerkingen overeenkomstig de wet worden verwerkt (artikel 22); de verplichting verwerkingen te documenteren (artikel 28), en de verplichting om voor specifieke verwerkingen die mogelijk een hoog privacyrisico vormen een 'Data Protection Impact Assessment' (DPIA) uit te voeren en indien inderdaad blijkt dat er een hoog risico bestaat over deze verwerking vooraf de toezichthouder te consulteren (artikel 33 en 34).

in een regelgevend kader waarbij gegevensverwerking is toegelaten tenzij deze als "oneerlijk" of "ongerechtvaardigd" kwalificeert (als een "unfair processing" moet worden aangemerkt) en aldus onrechtmatig is. Ook deze benadering noodzaakt gegevensverwerkers tot een contextuele beoordeling en afweging van belangen, en wel vanuit een mogelijke oneerlijke of ongerechtvaardigde verwerking. En wederom zal voor dat oordeel relevant zijn hoe wordt omgegaan met de rol en invloed van consumenten en welke mitigerende maatregelen zijn genomen om de privacy-implicaties zo beperkt mogelijk te houden. Mocht een rechter een bepaalde praktijk van gegevensverwerking als oneerlijk dan wel ongerechtvaardigd aanmerken, dan hebben consumenten recht op schadevergoeding (strikte aansprakelijkheid). Op de lange termijn zou een dergelijke benadering wel eens beter uit kunnen werken voor individuen dan het huidige systeem waarbij in feite vooraf een 'vergoeding' voor gegevensgebruik kan worden geboden (namelijk de online dienst, de korting op een verzekeringspremie, etc.), maar in deze vergoeding de uiteindelijk werkelijk schadelijke gevolgen van dat gebruik niet of nauwelijks zijn te verdisconteren.[303] Ook het bredere belang van de samenleving zal met deze benadering kunnen winnen nu het zowel streng – in het belang van de waarden van onze democratische samenleving – als flexibel – in het belang van de evenzeer noodzakelijke innovatie – kan zijn.

Ten slotte. In dit preadvies hebben wij vanuit de overtuiging dat de effectiviteit en legitimiteit van de huidige gegevensbescherming toenemend onder druk staat, een alternatieve benadering willen ontwikkelen. Wij willen niet betogen dat er geen kwetsbaarheden schuilen in de door ons voorgestelde aanpak. Waar het ons om gaat is dat veel analyses van persoonsgegevensbescherming teruggrijpen op vertrouwde uitgangspunten die al decennia aan het wettelijk systeem ten grondslag liggen. Vasthouden aan deze uitgangspunten is echter veel te eenvoudig, zeker nu deze door de fundamentele veranderingen in het gebruik van gegevens steeds indringender ter discussie worden gesteld. Of het nu gaat om het principe van doelbinding, de rechtvaardigingsgrond van toestemming, de speciale bescherming voor bijzondere gegevens of de informatie- en transparantieverplichtingen: het blijken in de dagelijkse praktijk veelal tandeloze instrumenten te zijn. Bovendien, in plaats van onze pijlen te richten op de actoren (zowel bedrijven als consumenten) die kennelijk massaal onvoldoende vorm en inhoud weten te geven aan de huidige wettelijke verplichtingen, wilden wij de dieperliggende vraag aan de orde stellen of het huidige complexe kader hen wel voldoende in staat stelt hun positie wat betreft gegevensgebruik waar te maken. Over de uitwerking van de door ons voorgestelde gerechtvaardigd belang-toets kan men van mening verschillen. Hoe zwaar moet wegen dat een verzekeraar onvoldoende

303. Zie over de financiële trade-offs bij privacy bescherming: Cofone (2015), par. 3.

transparant is geweest over de mogelijkheden die verzekerden hebben om daadwerkelijke controle over het hergebruik van hun gegevens uit te oefenen? Hoe zwaar sanctioneren we hergebruik van gegevens indien blijkt dat hiervoor geen gerechtvaardigd belang gevonden kon worden? Maar het is juist het debat over deze en andere vragen dat we met elkaar moeten voeren en dat teruggaat tot de fundamentelere vraag waar de grenzen van gegevensgebruik in onze samenleving moeten liggen en welke maatstaf we willen hanteren bij het wegen van de verschillende belangen die in een bepaalde context aan de orde zijn.

7. Literatuur

Adviesraad Internationale Vraagstukken (2014), Rapport no. 92, *Het Internet: een wereldwijde vrije ruimte met begrensde staatsmacht*, http://aiv-advies.nl/download/7daceb03-a324-4204-8099-3dcbb44e3709.pdf

Akkermans e.a. (2015), *Je geld of je leven terug. Vergoeding in natura*, Vereniging van Letselschadeadvocaten, Boom juridische uitgevers

Alesenoy, B. Van, Kosta E., Dumortier J. (2014), "Privacy notices versus informational self-determination: Minding the gap", 28 *International Review of Law, Computers & Technology*.

Ariely, D. (2010), *Predictably irrational*, Harper Collings Publishers

Baesens, B. (2014), Analytics in a Big Data World: The Essential Guide to Data Science and its Applications, Wiley Publishers

Bamberger, Kenneth A., Mulligan, Deirdre K. (2013), "Privacy in Europe: Initial Data on Governance Choices and Corporate Practices", *George Washington Law Review*, Vol. 81, p. 1529.

Barocas, Solon, Selbst, Andrew D. (2016), "Big Data's Disparate Impact", 104 *California Law Review*, http://ssrn.com/abstract=2477899.

Blok, Peter (2002), *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*, diss. Tilburg.

Bodelier, Ralf (2012), *Kosmopoliet en krottenwijk*, diss. Tilburg.

Boer, Leo De (2015), "Vernieuwingen dagen verzekeraars uit", *Financiële Dagblad* 21 juli 2015, http://fd.nl/opinie/1112046/vernieuwingen-dagen-verzekeraars-uit.

Borgesius, F. (2014) "Improving data protection in the area of behavioural targeting", diss. Universiteit van Amsterdam.

Broeders D.W.J., Griffioen H., Prins J.E.J. (2012), "iGovernment: A new perspective on the future of government digitization", *Computer Law & Security Review* nr. 3 2012.

Brouwer, Evelien (2010), Chapter 14, "Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation", in: *The Eclipse of the Legality Principle in the European Union*, Leonard F.M. Besselink, Frans Pennings, Sacha Prechal (eds.), Kluwer.

Burton B., Willis D.A. (2014), *Gartner's Hype Cycle Special Report for 2014*, www.gartner.com.

Burton C., Boel L. De, Kuner C., Pateraki A., "The Proposed EU Data Protection Regulation Three Years Later: The Council Position", *BNA Privacy & Security Law Report*, 29 June 2015.

Buruma, Y. Prins, J.E.J. (2009), "Humane biotechnologie en recht", *Nederlands Juristenblad (NJB)*, afl. 22 2009.

Carr Nicholas (2013), *The Big Switch, Rewiring the World from Edison to Google*, W. W. Norton & Company.

Centre for Information Policy leadership - CIPL (2013), *Big Data and Analytics, Seeking Foundations for Effective privacy Guidance*, http://www.hunton.com/files/Uploads/Documents/News_files/Big_Data_and_Analytics_February_2013.pdf

Centraal Plan Bureau (2014), *Kiezen voor privacy. Hoe de markt voor persoonsgegevens beter kan*, CPB Policy Brief 2014/4.

Clarke R. (2000), *Beyond the OECD Guidelines: Privacy Protection for the 21st Century*, Xamax Consultancy, http://www.rogerclarke.com/DV/PP21C.html.

Cofone Ignatio Nicolas (2015), *Privacy Tradeoffs in Information Technology Law*, diss. Erasmus Universiteit Rotterdam

College Bescherming Persoonsgegevens (2014), *Definitieve bevindingen naar de verwerkingen van persoonsgegevens met cookies door de publieke omroep (NPO),* Den Haag.

Commission of the European Communities (2003), *First Report on the implementation of the Data Protection Directive (95/46/EC)*, COM/2003/265 final.

Cuijpers C.M.K.C., Purtova N., Kosta E. (2014): "Data Protection Reform and the Internet: The Draft Data Protection Regulation", in: *Research Handbook on EU Internet Law*, Savin, A., Trzaskowski, J., (eds), Edward Elgar; Tilburg Law School Research Paper No. 03/2014 (n 35).

Dammann Ulrich, Simitis Spiros (1979), *EG-Datenschutzrichtlinie*, Nomos Verlagsgesellschaft.

Deloitte (2012), *Digital Age Transportation,* http://dupress.com/articles/digital-age-transportation/

Dorbeck-Jung B. (2015), *Bruggen tussen technologieregulering, wetenschap en kunst,* afscheidsrede Universiteit Twente.

Duhigg Charles (2012), "How Companies Learn Your Secrets", *NY Times* 16 februari 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

European Commission (2011), *Towards Responsible Research and Innovation in the Information and Communication, Technologies and Security Technologies Fields*, http://ec.europa.eu/research/science-society/document_library/pdf_06/mep-rapport-2011_en.pdf

Europese Commissie (2012), *Communication of the Commission to the European Council, the European Economical and Social Committee of the Regions, Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century*, COM(2012) 9 final.

Executive Office of the President (2014), *Big Data: Seizing Opportunities, Preserving Values*, http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

Faure M.G., Visscher L.T., Tzankova I.N.(2015), "Collectieve acties", *Preadviezen voor de Vereniging voor Burgerlijk Recht*, Zutphen Uitgeverij Paris.

Ferretti F. (2014),"Data protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights?" *Common Market Law Review* 51.

Finn R., Wright D., Friedewald M. (2013), "Seven Types of Privacy", in: *European Data Protection: Coming of Age?*", S. Gutwirth, R. Leenes, P. De Hert et al. (eds.), Springer.

Floridi L. (2005), "The ontological interpretation of information privacy", *Ethics and Information Technology.*

Fuller Lon L. (1969), *The Morality of Law*, herziene druk, New Haven: Yale University Press.

Galetta Antonella, Hert Paul De (2014), "Completing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance", *Utrecht Law Review*, January.

Gangadharan Seeta Peña et al. (2014), "Room for Debate: Is Big Data Spreading Inequality?", *N.Y. TIMES*, http://www.nytimes.com/roomfordebate/2014/08/06/is-big-data-spreading-inequality/the-dangersofhigh-tech-profiling-using-big-data.

Gestel R. Van, Loth Marc (2015), "Urgenda: roekeloze rechtspraak of rechtsvinding 3.0?", *Nederlands Juristenblad* no. 37.

Goslinga Maaike (2015), "Zo houden datahandelaren ons in de gaten (maar wie controleert hen?)", *De Correspondent*, 13 oktober.

Grijpink J.H.A.M., Prins J.E.J. (2001a), "Digital Anonymity on the Internet", *The Computer Law and Security Report*, 17(6).

Grijpink J.H.A.M., Prins J.E.J. (2001b), "Nieuwe rechtsregels voor anoniem rechtsverkeer? en verkenning van de privaatrechtelijke gevolgen van digitale anonimiteit", *Nederlands tijdschrift voor burgerlijk recht* (NTBR), 18(3).

Grunberg Arnon (2015), "Kennis", *Wordt Vervolgd*, september.

Hartlief T. (2015), "Waar ligt de toekomst van het personenschaderecht?", *Nederlands Juristenblad* no. 40.

Hert, P De (2009), *In het licht van de technologie. Pleidooi voor continuïteit en verandering bij gegevensbescherming*, College Bescherming Persoonsgegevens, Den Haag.

Herz Noreena (2013), *Eyes Wide Open, How to Make Smart Decisions in a Confusing World*, William Collins Publishers.

Hijmans H. (2012), "Nieuwe Europese regels voor privacy: commissie stelt pakket voor om gegevens ook in het informatietijdperk te beschermen", *Nederlands tijdschrift voor Europees recht*, 2012/4.

Hijmans H. (2014), "Right to have links removed: Evidence of effective data protection", *Maastricht Journal of European and Comparative Law*, 3.

H. Hijmans (2016), *What the EU does and should do to make Article 16 TFEU work, by means of judicial review, legislation, supervision by independent authorities, cooperation of the authorities and external action*, diss. Universiteit van Amsterdam (handelseditie te verschijnen bij Springer Verlag).

Hildebrandt Mireille (2013), "Slaves to Big Data. Or Are we?", http://works.bepress.com/mireille_hildebrandt/52

Hirsch Ballin E.M.H. (1993), *De staat van Nederland*, Tilburg: Tilburg University Press.

Hoepman J.H. (2012), "Privacy design strategies", http://arxiv.org/pdf/1210.6621.pdf

Hof S. van der, Prins J.E.J. (2008), "Personalisation and Its Influence on Identities, Behaviour and Social Values", in: *Profiling the European Citizen, Cross-disciplinary Perspectives*, M. Hildebrandt, S. Gutwirth (eds.), Springer.

Hustinx Peter (2013), "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", *Collected Courses of the European University Institute's Academy of European Law*, 24th Session on European Union Law, 1-12 July 2013

Issenberg Sascha (2012), "How President Obama's campaign used big data to rally individual voters, Part 1", *MIT Technoloy Review*, http://www.technologyreview.com/featuredstory/508836/how-obama-used-big-data-to-rally-voters-part-1/

Jacobs Bart, "Klantverraders", http://pilab.nl/index.php/2015/12/13/nederlands-klantverraders/?lang=nl#more-1543

Jerome Joseph (2013), "Buying and Selling Privacy: Big Data's Different Burdens and Benefits", 66 *Standford Law Review Online* 47.

Jong A. de (2014), "Big Data – Fundamentele rechten in een fundamenteel veranderde wereld", *pre-advies jonge VAR*.

Kapitein M.C. (2012), *Personalized Persuasion in Ambient Intelligence*, diss. TU/e Eindhoven.

Keats Citron Danielle, Pasquale Frank (2014), "The Scored Society: Due Process for Automated Predictions", 89 *Washington Law Review*, 1.

Kerr Ian, Earle Jessica (2013), "Prediction, Preemption, Presumption: How Big Data Threatens Big Picture", 66 *Stanford Law Review Online*.

Keymolen E., Prins J.E.J. (2011), "Jeugdzorg via systemen. de verwijsindex risicojongeren als spin in een digitaal vangnet", in: *De Staat van Informatie*, Dennis Broeders, Colette (M.K.C.) Cuijpers & Corien (J.E.J.) Prins (red.), Amsterdam University Press.

Keymolen E. (2007), *Onzichtbare zichtbaarheid. Plessner ontmoet profiling*, scriptie Erasmus Universiteit Rotterdam.

Khouri Andrew (2015), "Insurance start-up Oscar seeks to shake-up healthcare through its app", Los Angeles Times, http://www.latimes.com/business/la-fi-cutting-edge-oscar-20151018-story.html.

Klink B.M.J. van, Prins J.E.J. Prins, Witteveen W.J. (2001), "Het conceptuele tekort: een survey-onderzoek naar de wisselwerking tussen ICT en het recht", in: *De invloed van ICT op maatschappij en overheid. Naief vooruitgangsgeloof of harde werkelijkheid?*, R. van der Ploeg & C. Veenemans (red.), Amsterdam University Press.

Kluemper Donald, Rosen Peter, Mossholder Kevin (2012), "Social Networking Websites, Personality Ratings, and the Organizational Context, More than Meets the Eye?", *Journal of Applied Social Psychology*, Vol. 42, issue 5, http://onlinelibrary.wiley.com/doi/10.1111/j.1559-1816.2011.00881.x/full.

Kohnstamm Jacob (2015), "Grenzen aan verzamelhonger big data noodzakelijk", *Financiële Dagblad* 22 januari 2015.

Koops B.J., Lips A.M.B., Prins J.E.J., Schellekens M.H.M. (2006), *Starting Points for ICT Regulation* (IT & Law Series no. 9). TMC Asser Press.

Koops B.J., Leenes R.E. (2014), "Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law", *International Review of Law, Computers & Technology*, no. 2.

Koops B.J. (2014), "The trouble with European Data Protection Law", *International Data Privacy Law*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692.

Kranenborg H.R., Verhey L.F.M. (2011), *Wet bescherming persoonsgegevens in Europees perspectief,* Kluwer.

Kranenborg H.R. (2014) in "Protection of Personal Data", in: *The EU Charter of Fundamental Rights, A Commentary*, Steve Peers, Tamara Hervey, Jeff Kenner, Angela Ward (eds.), Hart Publishing.

Kuner Christopher (2010), "Internet Jurisdiction and Data Protection Law: An International Legal Analysis (Part 2)", *International Journal of Law and Information Technology*, Vol. 18.

Kuner Christopher (2012), "The European Commission's Proposed Data Protection Regulation", *Bloomberg BNA Privacy & Security Law Report*, 6 February.

Kurzweil Ray, interview by Keith Kleiner, http://www.youtube.co/watch?v=YABUffpQY9w

Leenes R.E. (2007), "Do they know me? Deconstructing Identifiability", *University of Ottawa Law & Technology Journal*, no. 4, https://pure.uvt.nl/portal/files/1310856/Leenes_Do_they_know_me_110216_publishers_immediately.pdf

Leenes Ronald, Kosta Eleni (2015), "Taming the cookie monster with Dutch law. A tale of regulatory failure", 31 *Computer Law & Security Review*.

Leskovec J., Ramarajam A., Ulman J.D. (2014), *Mining of Massive Data Sets*, Cambridge University Press, 2nd ed.

Lochem P.J.P.M van, Gestel R.A.J. van, Bock R.H. de(2015), "Kwaliteit als keuze in rechtspraak, wetgeving en rechtswetenschap", Handelingen Nederlandse Juristen-Vereniging.

Lodder Arno (2015), *Financiële Dagblad* 21 januari.

Loth M., Beumers Th., Boom W. van (2015), *Maatmens-benadeelde*, *Preadviezen Vereniging voor Aansprakelijkheids- en schadevergoedingsrecht*.

Mcdonald A.M., Reeder R.W., Kelley P.G., Cranor L.F. (2009), "A comparative study of online privacy policies and formats", in: *Privacy enhancing technologies*, Springer, http://www.springer.de/comp/lncs/index.html

Mayer-Schönberger V., Cukier K. (2013), *Big Data: A Revolution that will Transform How We Live, Work, and Think*, John Murray.
Mertens Thomas (2012), *Mens en Mensenrechten*, Boom.

Milne George, Culnan Mary (2004), "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices", 18 *Journal of Interactive Marketing* 15.

Moerel Lokke (2012), *Binding Corporate Rules, Corporate Self-Regulation of Global Data Transfers*, Oxford University Press.

Moerel Lokke (2014), *Big Data Protection, How to Make the Draft EU Regulation on Data Protection Future Proof*, Oratie Universiteit Tilburg, http://www.mondaq.com/x/298416/data+protection/Big+Data+Protection+How+To+Make+The+Draft+EU+Regulation+On+Data+Protection+Future+Proof al Lecture.

Moerel L. (2015a), "Zo behouden alleen de rijken hun privacy", *NRC Handelsblad* 28/29 november 2015, p.O&D7

Moerel L. (2015b),"Werken met big data is lang niet altijd big mistake, College Bescherming Persoonsgegevens moet erkennen dat analyse van big data wettelijk is toegestaan", *Financiële Dagblad* 20 januari 2015.

Moerel L., Prins J.E.J., (2015a), "On the death of Purpose Limitation", IAPP Privacy Perspectives 2015, https://iapp.org/news/a/on-the-death-of-purpose-limitation/

Moerel L., Prins J.E.J. (2015b), "Further processing of data based on the legitimate interest ground: the end of purpose limitation?",https://www.tilburguniversity.edu/upload/bcbd911e-9902-485a-9de9da88eae5042c_Prins_Moerel_Collection%20and%20further%20processing%20of%20data%20%28with%20foornotes%29%20doc.pdf.

Montjoye Y. De, Hidalgo C.A., Verleysen M., Blondel V.D. (2013), "Unique in the crowd: the privacy bounds of human mobility", 2013 *Scientific Reports* 3: 1376, http://www.ncbi.nlm.nih.gov/pubmed/23524645

Morozov Evengy (2013), "To Save Everything Click Here. The Folly of Technological Solutionism*", PublicAffairs*.

Mundie Craig (2014), "Privacy Pragmatism, Focus on Data Use, Not Data Collection", https://www.foreignaffairs.com/articles/2014-02-12/privacy-pragmatism.

Nationale Denktank (2014), "Big Data In Zicht: 10 oplossingen voor maatschappelijke impact met Big Data", http://www.nationale-denktank.nl/jaarlijkse-denktank/eindrapport-2014/

Naughton John (2010), "The internet. Everything you ever need to know", The Guardian, 20 juni 2010.

Nissenbaum Helen (2004), "Privacy as contextual integrity", 19 *Washington Law Review* 119.

Nissenbaum Helen (2011) "A Contextual Approach to Privacy Online", *Daedalus*, 140/4, 32-48.

NOREA (2015), *Privacy Impact Assessment, Introductie, Handreiking, Vragenlijst*, versie 1.1., juli 2015.

Nussbaum Martha C. (2007), *Frontiers of Justice: Disability, Nationality, Species Membership*, Harvard University Press.

OECD (1980), *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, 23 September.

OECD Working party on Security and Privacy in the Digital Economy (2014a), "Summery of the OECD Expert Roundtable Discussion Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking", http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg(2014)3&doclanguage

OECD (2014b), Data-driven Innovation for Growth and Well-being.
Pariser E. (2012), *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*, Pengiun Books.

Pentland A. (2014), *Sociale Big Data. Opkomst van de datagedreven samenleving*, Maven Publishing.

Robert Post Robert (2000), "Three concepts of privacy", 89 *Georgetown Law Journal* 2087.

Prins J.E.J., Donk W.B.H.J. van de, Duivenboden H.P.M. van, Nouwt J., Have K. Ten, Vorselaars H.A.C.M., Zouridis S. (1995), *In het licht van de Wet persoonsregistraties : zon, maan of ster? Verslag van een sociaal wetenschappelijke evaluatie van de Wet Persoonsregistraties*. Alphen aan den Rijn: Samsom.

Prins J.E.J. (2007a), "Nalaten in Cyberspace", *Nederlands Juristenblad*, no. 6.

Prins J.E.J. (2007b), "Technocratie en de toekomstagenda van de Nationale Ombudsman", in: *Werken aan behoorlijkheid. De Nationale Ombudsman in zijn context (jubileumbundel 25 jaar Nationale Ombudsman)*, Den Haag: Boom Juridische Uitgevers.

Prins J.E.J. (2008), "Export van lichaamsmateriaal", *Nederlands Juristenblad*, no. 10.

Prins J.E.J. (2011), "Function creep: over het wegen van risico's en kansen", *Justitiële Verkenningen*, nr. 8.

Prins J.E.J. (2015a),"Mijn intelligente koelkast", *Nederlands Juristenblad*, no. 23.

Prins J.E.J. (2015b), "Heeft u nog de controle over uw auto?", *Nederlands Juristenblad*, no. 33.

Provost Foster, Tom Fawcett Tom (2013), *Data Science for Business: What you need to know about data mining and data-analytic thinking*, O'Reilly Media.

Rauhofer J. (2014), 'Look to yourselves, that we lose not those things which we have wrought. "What do the proposed changes to the purpose limitation principle mean for public bodies" rights to access third-party data?', *International Review of Law, Computers & Technology*, 28(2).

Richtel Matt (2013), "I Was Discovered By An Algorithm", *N.Y. TIMES*, April 28, BU1.

Rouvory A., Poullet Y. (2009), "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy", in: *Reinventing Data Protection*, S. Gutwirth e.a (eds).

Schrage Michael (2014) "Big Data's Dangerous New Era of Discrimination" *Harvard Business Review* January 29.

Selznick Philip (1992), *The Moral Commonwealth*, Berkeley: University of California Press.

Siegel Eric (2013), *Predictive Analysis. The Power to Predict who will Click, Buy, Lie or Die*, John Wiley & Sons.

Smidt Eric, Cohen Jared (2013), The New Digital Age, Alfred A. Knopf publishers.

Solove D.J., (2008) *Understanding Privacy*, Cambridge, MA: Harvard University Press.

Solove D.J. (2013), "Introduction: Privacy Self-management and the Consent Dilemma", *Harvard Law Review*, 126.

Somsen Han (2009), "Rechtvaardige en doelmatige regulering van medische biotechnologie", *Handelingen Nederlandse Juristen-Vereniging*.

Sprague Robert (2015), "Welcome to the Machine: Privacy and Workplace Implications of Predictive Analytics", *21 Richmond Journal of Law & Technology*.

Staatscommissie Grondwet (2010), *Rapport Staatscommissie Grondwet*, Den Haag.

Sunstein Cas (2001), *Republic.com*, Princeton University Press.

Tene Omer, Polonetsky Jules (2012), "To Track or 'Do Not Track': Advancing Transparency and Individual Control in Online Behavioral Advertising" *Minnesota Journal of Law, Science & Technology*, No. 1 https://ssrn.com/abstract+1920505

Thaler Richard H., Sunstein (2008), *Nudge, Improving Decisions About Health, Wealth, and happiness*, Yale University Press.

Tiemeijer W.L. (2012), *Hoe mensen keuzes maken: de psychologie van beslissen*, Amsterdam University Press.

Timmer, T., Elias I., Kool L, Est R. van (2015), *Berekende risico's. Verzekeren in de datagedreven samenleving*, Den Haag, Rathenau Instituut.

TNO (2015), *Privacybeleving op het internet in Nederland*.

Tucker Joanne (2014), "Telematics ROI Beyond Fuel Savings", *Automotive Fleet magazin*, http://www.automotive-fleet.com/article/story/2014/10/telematics-roi-beyond-fuel-savings.aspx.

United Kingdom's Information Commissioner's Office (2014), "Big Data and data protection", https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf. p. 21

US Department of Commerce (2014), *Big Data and Consumer Privacy in the Internet Economy*, 79 Federal Register 32714.

Verbond van Verzekeraars (2014), *Het Innovatielab, aanjager voor innovatie in de verzekeringssector*, https://www.verzekeraars.nl/verzekeringsbranche/publicaties/Publicaties/Brochure%20Innovatielab.pdf

Verhey L.F.M. (1992), *Horizontale werking van grondrechten, in het bijzonder het recht op privacy*, Tjeenk Willink, Zwolle.

Vodafone Institute, Big Data. A European Survey on the Opportunities and Risks of Data Analytics, 2016, beschikbaar via: http://www.telecompaper.com/news/only-18-of-europeans-trust-operators-on-personal-data--1123558

Vos B.J. de (2010), *Horizontale werking van grondrechten. Een kritiek*, diss. Leiden, Maklu

Voorstel voor een verordening betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Verordening Gegevensbescherming), COM(2012)/11 final, 25 januari 2012.

Warren S.D., Brandeis L.D. (1890), "The Right to Privacy", *Harvard Law Review*.

Wetenschappelijke Raad voor het Regeringsbeleid (2011), *iOverheid*, Den Haag.

Wetenschappelijke Raad voor het Regeringsbeleid (2014), *Met kennis van gedrag beleid maken*, Den Haag.

Wetenschappelijke Raad voor het Regeringsbeleid (2015), *De publieke kern van het internet. Naar een buitenlands internetbeleid*, Den Haag.

Wijnberg Ron (2015), "Hoe onze risicomijdende cultuur de solariditeit ondermijnt", *De Correspondent,* https://decorrespondent.nl/1453/Hoe-onze-risicomijdende-cultuur-de-solidariteit-ondermijnt/37240390-6d43a6ee

Witteveen Willem (2010), Het wetgevend oordeel. Boom Juridische uitgevers, Den Haag.

Witteveen Willem (2014), *De wet als kunstwerk*, Amsterdam: Uitgeverij Boom.

WP29 Recommendation 2/2001, *On certain minimum requirements for collecting personal data on-line in the European Union*, Brussel 2001.

WP29 Opinion 04/2007, *On the concept of personal data*, Brussel 2007.

WP29 Opinion 15/2011, *Consent*, Brussel 2011.

WP 29 Opinion 03/2013, *On purpose limitation*, Brussel 2013.

WP29 Opinion 03/2014, *On Personal Data Breach Notification*, Brussel 2014.

WP29 Opinion 06/2014, *On the notion of legitimate interest of the data controller under Article 7 of Directive 95/46/EC*, Brussel 2014.

WP29 Opinion 8/2014, *On the Recent Developments on the Internet of Things*, Brussel 2014.

World Economic Forum Report (2013), *Unlocking the Value of personal data: From Collection to Usage*, http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf

Wright David, Raab Charles (2014), "Privacy principles, risks and harms", *Law Computers & Technology*, no. 3.

Zarsky Tal S. (2014), "Understanding Discrimination in the Scored Society", 89 Washington Law Review, 1375.

Data-Gestuurde Intelligentie in het strafrecht[1]

Mireille Hildebrandt

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

1. Homo digitalis in het strafrecht

> We cannot doubt everything, but we should be open to doubt anything.[2]
> *after Putnam*

> We cannot suspect everybody, but should we be open to suspect anybody?[3]
> *Homo digitalis in het strafrecht*

1.1 Waar gaat dit over?

Het recht is gebouwd op de idee dat de geest actief is en de materie passief. Dit eenvoudige schema, dat het leven overzichtelijk maakte, gaat niet meer op. Dit preadvies beperkt zich dan ook niet tot gegevensverwerking, hoe belangrijk ook. In het eerste hoofdstuk wordt besproken dat en hoe de samenleving zich beweegt van een informatiesamenleving (waar meer informatie gelijk staat aan betere kennis) naar een data-gestuurde samenleving (waar de kunst is om de relevante datapunten te vinden, te verbinden en daarop te sturen). Het centrale begrip is hier dan ook niet langer data of big data, maar *agent* (een data-gestuurd intelligent systeem). Dat betekent dat de nadruk niet ligt op gegevensverwerking maar op computersystemen die 'handelend optreden', waarbij de mate van aansturing door menselijke *agents* van geval tot geval verschilt. In het eerste hoofdstuk wordt uiteengezet hoe we ons de *homo digitalis* kunnen voorstellen in een omgeving waarin *agents* een hoofdrol spelen. Wie behoefte heeft aan een handzame introductie op data gestuurde intelligentie in combinatie met theoretische reflectie leze dus het eerste hoofdstuk. Wie liever direct naar de implicaties voor materieel en formeel strafrecht gaan kunnen door naar hoofdstukken twee en drie. Wie direct kennis wil nemen van mogelijke oplossingen begint bij hoofdstuk vier.[4]

In het tweede hoofdstuk ga ik in op enkele materieelrechtelijke implicaties van de verschuiving van informatievergaring naar data-gestuurde *agents*. In het derde hoofdstuk ga ik – na een korte bespreking van de doelen van het strafrecht – in op de aard van de *agents* die worden ingezet bij de strafrechtelijke handhaving van de rechtsorde. Daarna onderzoek ik hoe dit de aantasting van een aantal grondrechten beïnvloedt, met nadruk

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

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

1.2 Nieuwe agenten in het strafrecht

Dit preadvies richt zich dus specifiek op de gevolgen van data-gestuurde intelligentie voor het strafrecht, met nadruk op de toenemende inzet van kunstmatig intelligente *agents*. Het gaat daarbij niet alleen over software *agents* maar juist ook over de voortgaande vermenging van software en hardware; de opkomst van het Internet van de Dingen, cloud robotica en allerhande slimme infrastructuur. Bovendien gaat het niet alleen om *agents* die min of meer zelfstandig voorgeprogrammeerde taken uitvoeren (een eenvoudige thermostaat is in die zin al een *agent*), maar ook om *agents* die in staat zijn min of meer zelfstandig te leren op basis van de feedback die ze oppikken uit hun omgeving en die juist op basis daarvan hun gedrag aanpassen (bijvoorbeeld de zelfrijdende auto).[5] Het Nederlandse woord 'agent' heeft een andere lading dan het Engelse woord *agent*, dat zowel een term is uit de computerwetenschappen (*intelligent agent*, *multi agent systems*),[6] als de

5. De software *agents* die Schermer (2007) in zijn proefschrift besprak zijn nog steeds relevant, maar de grootschalige opkomst van machinaal lerende cyberfysieke systemen gaat veel verder, met name in de mate waarin deze systemen ingrijpen in de werkelijkheid.
6. *Agents* spelen een belangrijke rol in kunstmatige intelligentie (KI), zie Russell en Norvig (2009) en Mitchell (1997). Bij KI verwijst de term *agent* naar een systeem dat de omgeving waarneemt (via sensoren) en erop ingrijpt (via actuatoren). In de informatica wordt een software *agent* vaak gedefinieerd als een programma dat handelt in opdracht van de gebruiker of een ander programma. Zie in die laatste zin Schermer (2007: hoofdstuk 2).

(rechts)filosofie (*human agency*),[7] als het recht (*agent-principal*).[8] Voor dit preadvies zijn alle drie betekenissen relevant. Hierna zal ik de term *agent* gebruiken voor data gestuurde systemen. Denk aan een zoekmachine, een drone, een computervirus, of een slim energiesysteem dat de levering van energie afstemt op de spanning van het energienetwerk. Meer toegespitst op de strafvordering kunnen we bijvoorbeeld denken aan een systeem van slimme sensoren (camera's en microfoons) in een smart city die detecteren of de bezoekers van een voetbalwedstrijd of uitgaansgebied op het punt staan geweld te gebruiken.

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

Nu het om data-gestuurde *agents* gaat impliceert dit tegelijk een overgang van de *informatie*samenleving naar een *data-gestuurde* samenleving. Meer data staat niet (meer) gelijk aan meer informatie, integendeel. We zijn op het punt aangekomen dat een toenemende data-obesitas ons het zicht beneemt op de juistheid en de mogelijke relevantie van data; de uitdaging ligt niet meer in het verzamelen van zoveel mogelijk data maar in de slimme selectie en intelligente verwerking daarvan. In tijden van data-zwaarlijvigheid gaat het niet meer om de calorische waarde maar om de voedingswaarde en zelfs dan *niet* om meer van hetzelfde maar om de juiste verhoudingen. Zoals bekend spelen sporenelementen daarbij een cruciale rol; het ontbreken (of een teveel) van minieme hoeveelheden vitaminen en mineralen kan tot ondervoeding (of ziekelijke ontwikkeling) leiden, ondanks inname van voldoende energierijk voedsel. Zo is het ook met data; de kunst is om de juiste datapunten te vinden en dat kan niet altijd door zoveel mogelijk data te verzamelen.[9] Maar ook adequate selectie en verwerking vormen niet de kern van wat ons te wachten staat. De crux ligt in onze nieuwe – *geestloze* – huis-, land- en wereldgenoten: systemen die in staat zijn hun omgeving waar te nemen, erop in te grijpen en vervolgens te leren van de feedback die zij ontwaren, zodat zij hun gedrag

7. Over *moral* en *legal agents* Duff (2009). Bij morele of juridische *agents* gaat het om mensen die – anders dan computer systemen – bewustzijn hebben en zich – anders dan dieren – bewust zijn van dat bewustzijn. Morele *agents* zijn dankzij hun zelfbewustzijn in staat tot reflectie op de normatieve implicaties van hun eigen gedrag. Alleen *moral agents* kunnen onrechtmatig en verwijtbaar handelen.
8. Hier gaat het om het leerstuk van vertegenwoordiging (Dowrick 1954), in Nederland geregeld in 3:60 BW (volmacht), waarbij het vertrouwensbeginsel een belangrijke rol speelt.
9. Soms is dat overigens wel zo. Helaas generaliseren sommige auteurs ten onrechte specifieke leerstukken uit de statistiek die inderdaad aanleiding zijn om aan te nemen dat foutmarges afnemen als maar extreem veel data verzameld worden. Mayer-Schönberger en Cukier (2013) lijken in die valkuil te trappen. Zie bijvoorbeeld boyd en Crawford (2012) voor relativering.

in lijn met te bereiken doelen kunnen aanpassen. Ik mag er alvast op wijzen dat deze *agents* zich weliswaar gedragen, maar (nog?) niet handelen. Zo zij al intenties hebben is er geen bewustzijn van die intenties, laat staan zelfbewustzijn. Zo zij al betekenis toekennen aan hun eigen of andermans gedragingen, is dat een metafoor voor hun vermogen om op basis van machinaal leren (ML) inferenties af te leiden en toe te passen. Voor deze *agents* zijn wij geen *homines sapientes*, maar *homines behaviorales*, min of meer voorzienbaar en ondervangbaar op basis van de mechanismen die uit ons gedrag worden afgeleid.[10] In dat kader passen drie caveats. Ten eerste moeten we ons niet verslikken in metaforen die termen als waarneming, betekenis, intentie en gedrag verbinden met het (zelf)bewustzijn dat ons eigen is. *Agents* nemen waar, ze 'hebben' vaak (door ons bepaalde) intenties en ze gedragen zich; bovendien kunnen ze computationele 'betekenis' toekennen aan wat ze waarnemen. Maar dat doen ze allemaal zonder enige vorm van bewustzijn, laat staan zelfbewustzijn. Wie de ontwikkelingen binnen de neurowetenschappen volgt zal zien dat steeds duidelijker wordt dat grote delen van ons gedrag gestuurd wordt door processen waar we ons niet van bewust zijn, terwijl sommigen zelfs concluderen dat ons zelfbewustzijn een zogenaamd 'epifenomeen' is – een neveneffect waar we eerder de lasten dan de lusten van smaken. We moeten echter, ten tweede – juist in het recht, en precies in het strafrecht – de verleiding weerstaan om het kind al te snel met het badwater weg te gooien door het zelfbewustzijn als een illusie bij het groot vuil te zetten.[11] Met Damasio (2011: 280, 287, 293) meen ik dat het flintertje zelfbewustzijn waarmee we zijn begiftigd er toe doet, en de grondslag vormt van het vermogen onszelf (als persoon en als samenleving) de wet te stellen. Ten derde impliceert het feit dat *agents* geen zelfbewustzijn hebben, en in die zin geestloos zijn, niet dat ze gelijkgesteld kunnen worden met om het even welk type informatiesysteem. *Agents* nemen hun omgeving waar en zijn in toenemende mate zo ontworpen dat ze in kunnen grijpen en hun gedrag vervolgens aan kunnen passen naar aanleiding van de feedback die ze ontwaren. Het zijn geen mensen (geen zelf-bewustzijn), geen dieren (geen bewustzijn), maar zijn niet noodzakelijkerwijs puur reactieve informatiesystemen.

10. *Homo behavioralis* is het verdwijnpunt (de verzwegen premisse) van Kahneman en Tversky's (1979) cognitieve psychologie (en daarmee van de gedrageconomie). Het begrip *homo behavioralis* is gemunt door Binmore (1988) als tegenhanger van *homo economicus*. De *homo behavioralis* is volgens Binmore de 'mythische hominoide' van de gedragseconomie, volledig door genen, omgeving en evolutie gedetermineerd: 'Both species are modeled as stimulus-response machines, but *homo behavioralis* is programmed directly with behavior, like a chocolate-dispensing machine (Binmore 1988:4).'
11. Zoals op sjabloonachtige wijze min of meer bepleit door Swaab (2010) en Lamme (2011), maar zie Slors (2015) of Van de Laar en Voerman (2011); voor het recht *NJB* (2013) special issue 'Neurolaw in Nederland'. Voor de internationale discussie Damasio (2011) en meer specifiek voor het recht Morse (2008) en Vincent (2013).

Om de gedachten te bepalen vangen we aan met een korte bespreking van *agents*. Doel is niet om de daarmee opgeroepen problemen juridisch-technisch 'op te lossen', maar om de relevante vragen die *agents* oproepen scherper op het netvlies te krijgen. Pitlo zei het al: 'zoeken is ons doel. Vinden zou ons met lege handen laten staan'.[12] Hierna bespreek ik: (1) een botnet, (2) een zorgrobot die online is verbonden met de cloud, (3) slimme energienetwerken (smart grids) en (4) een smart city project in Eindhoven. Sommige *agents* zijn duidelijk herkenbaar als een identificeerbare, duurzame eenheid van actie, waarneming en reactie (bijvoorbeeld een drone), anderen vertonen waarneming en gedrag zonder dat sprake is van een eenvoudig te identificeren eenheid (denk aan een smart grid infrastructuur).[13] Interessante vraag is natuurlijk of de duurzame identificeerbaarheid een kwestie is van (1) hoe het systeem zich gedraagt (de ontologische vraag) ofwel van (2) de mate waarin wij het als eigenstandige *agent* herkennen (de kennistheoretische vraag). Mij dunkt dat dit van geval tot geval en in de loop van de tijd zal verschillen. Punt is dat systemen die zich herkenbaar als *agent* gedragen ook als zodanig geadresseerd kunnen worden, terwijl gedistribueerde systemen allerlei toerekeningsproblemen oproepen. Men bedenke echter dat juist de opkomst van cloud robotica impliceert dat veel herkenbare systemen feitelijk gedistribueerd zijn (de 'hersenen' van de zorgrobot 'hangen' wellicht deels in de cloud). Door consequent te spreken van *agents* wil ik het actiepotentieel van al deze systemen benadrukken. Het gaat niet alleen om gegevensverwerking.

Eerste voorbeeld. Wie kwaad wil kan haar[14] hart ophalen in de catacomben van het internet (over het zogenaamde 'darknet' zie Morozov 2011). Zij kan daar een botnet inhuren om geautomatiseerde DDOS (distributed denial of service) aanvallen te laten uitvoeren met als gevolg dat de beschikbaarheid van het doelwit ernstig te lijden heeft. Dit is zonder meer

12. Dit citaat van Pitlo e.a. (1995) hing jarenlang in mijn werkkamer bij de Erasmus Universiteit. Helaas heb ik de juiste pagina niet kunnen achterhalen. Met zijn uitspraak is niet gezegd is dat oplossingen niet interessant zijn; het gaat er meer om kortsluiting te voorkomen door oplossingen te gaan zoeken voordat de problemen verkend zijn.
13. Over verschillende typen kunstmatige *agents* Pfeifer en Bongard (2007), Floridi en Sanders (2004) en voor de geschiedenis van kunstmatige intelligentie zie Hayles (1999), Varela, Thompson en Rosch (1991).
14. In dit advies wordt consistent met een vrouwelijk verwijswoord terugverwezen naar termen die zowel naar mannelijke als vrouwelijke personen kunnen verwijzen, zoals bijvoorbeeld persoon, gebruiker, dader, verdachte. Dit om de leesbaarheid te bevorderen (geen hij/zij of zijn/haar) en om niet te vervallen in 'hij' of 'zijn', het gebruikelijke pars pro toto. Zie bijvoorbeeld <http://taaladvies.net/taal/advies/tekst/110/verwijzingsproblemen_met_voornaamwoorden_van_de_derde_persoon_enkelvoud_algemeen/> of <http://www.learnersdictionary.com/qa/the-he-or-she-dilemma> (in Nederland valt dit waarschijnlijk onder radicaal feminisme).

een strafbaar feit (art. 138b Sr als formeel omschreven delict),[15] en afhankelijk van het type en de distributie van de schade ook nog te kwalificeren in termen van art. 161 sexies Sr (een materieel omschreven delict dat 'gemeen gevaar voor goederen of verlening van diensten' als delictsbestanddeel heeft).[16] Zij is bij het uitvoeren van die aanval niet gebonden aan landsgrenzen en 'zij' kan ook een staat zijn, een terroristische organisatie of een bedrijf. Ze kan – in plaats van een botnet – ook een virus of andere malware aanschaffen of zelf (laten) ontwikkelen die zelfstandig een pad kiest om binnen te dringen in specifieke systemen ten einde daar informatie te kopiëren, instructies te verbergen of gewoon de werking van een of meer systemen te saboteren. Het klinkt eenvoudiger dan het is,[17] maar het kan wel en is in beginsel strafbaar ex art. 138ab WvSr (formeel omschreven delict: hacken) en eventueel ook 350a WvSr (materieel omschreven: veranderen, wissen, onbruikbaar of ontoegankelijk maken van gegevens). De mogelijkheid om dit soort aanvallen relatief eenvoudig vanuit een andere locatie en jurisdictie te organiseren roept vragen op rond extraterritoriale handhavingsjurisdictie (Koops en Goodwin 2014). In combinatie met de ernst van de gevolgen, bijvoorbeeld wanneer het om aanvallen op kritische infrastructuur gaat, roept dit alles bovendien vragen op rond het onderscheid tussen oorlog, criminaliteit, internationaal terrorisme en illegale extraterritoriale handhaving die niet als oorlogsvoering gekwalificeerd kan worden maar wellicht ook niet als strafrechtelijk optreden (Hildebrandt 2013).

Tweede voorbeeld. Het zou zomaar kunnen dat hoogbejaarden binnen 10 jaar geen verpleger van vlees en bloed aan hun zijde vinden, maar een intelligente, met emotie-detectie uitgeruste, vriendelijke maar ook robuuste zorgrobot. Deze voedt zich met data en programmatuur uit de cloud, en leert op basis van de interactie met de 'eigen' patient of cliënt. De zorgrobot kan dag en nacht doorwerken, heeft een ijzersterk geheugen en gecalculeerd inzicht in de eigenaardigheden van de cliënt, en onderhoudt directe verbindingen met apotheek, huisarts, medisch specialisten en

15. Een formeel omschreven delict stelt een bepaald handelen strafbaar, in dit geval het 'opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmer[en] door daaraan gegevens aan te bieden of toe te zenden'.
16. Een materieel omschreven delict stelt het veroorzaken van een bepaald gevolg strafbaar, in dit geval gaat om het 'opzettelijk enig geautomatiseerd werk of enig werk voor telecommunicatie verniel[en], beschadig[en] of onbruikbaar ma[ken], stoornis in de gang of in de werking van zodanig werk veroorza[ken], of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdel[en], indien daarvan gemeen gevaar voor goederen of voor de verlening van diensten te duchten is', met nog een aantal strafverzwarende gevolgen (levensgevaar en de dood van een ander). Zie HR 22 februari 2011, ECLI:NL:HR:2011:BN9287.
17. Over transnationale cybercriminaliteit Koning (2012), over cyberoorlog of spionage Hijink (2012).

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

Derde voorbeeld. Slimme energiesystemen (smart grid) moeten niet worden verward met een slimme meter. De laatste is slechts een onderdeel van zo'n systeem.[18] Een smart grid betekent een omwenteling in de afstemming van vraag en aanbod in de levering van energie, waarbij huishoudens, bedrijven en overheden niet alleen energie afnemen maar ook produceren, uitruilen en/of uploaden naar het distributie netwerk. De komst van de elektrische auto en de exponentieel toenemende inzet van elektronica in huis, kantoor, verkeer, sport, fabriek, gezondheidszorg, en detailhandel leidt tot een sterk wisselende energiebehoefte die zonder predictieve (voorspellende) en pre-emptieve (ondervangende) data-analyse tot een onbeheersbaar netwerk zou leiden – met voortdurende systeembreuken en uitval als gevolg. De idee is dat toegang tot gedetailleerde gebruiksgegevens redelijk nauwkeurige voorspellingen mogelijk maakt,

18. Over de privacy implicaties van de slimme meter Cuijpers en Koops (2013); over de implicaties van een slimme energie infrastructuur voor een aantal grondrechten Hildebrandt (2013b).

die in samenhang met *sturing van* en zelfs *controle over* energieverbruik van de eindgebruikers tot een verantwoorde energiehuishouding kan leiden. Zo kan de netbeheerder die de juiste spanning op het net moet garanderen besluiten dat wie tijdens een veelbekeken voetbalwedstrijd ook nog een was wil draaien daar een extreem hoge prijs voor moet betalen (sturing door middel van flexibele prijsstelling) of beslissen dat bepaalde huishoudens die was niet kunnen draaien (remote control). Die laatste ingreep zal waarschijnlijk alleen mogelijk zijn als de klant korting accepteert in ruil voor een contract dat dit type ingrepen onder bepaalde voorwaarden toelaat. Het smart grid – dat in Europa op initiatief van de EU wordt uitgerold – bestaat uit een veelheid van kleine en grotere systemen, die voortdurend met elkaar in gesprek zijn middels machine-tot-machine communicatie. Sommige systemen zullen kunstmatige intelligentie (KI) toepassen, bijvoorbeeld machinaal leren, om snel inzicht te krijgen in te verwachten energieverbruik en – via simulaties – in de gevolgen van dynamische aanpassing van de prijs, dosering op afstand en andere ingrepen bedoeld om het energieverbruik te beïnvloeden. Hier is evident sprake van *agency*, nu deze systemen niet alleen hun omgeving waarnemen (zowel ons energieverbruik als weersomstandigheden, verkeerspieken, relevante evenementen, dag- en nachtritmes en zo meer) maar hun gedrag daar bovendien op aanpassen (prijsstelling, remote control, dosering) en vervolgens ook leren van de impact van het eigen gedrag op dat van de omgeving. Strafrechtelijk kan dit alles tot een nieuwe dynamiek leiden:[19] (1) deelsystemen kunnen uit de pas gaan lopen en grote schade veroorzaken nu het hier gaat om kritische infrastructuur, (2) de afstemming tussen systemen kan tot soortgelijke of nog omvangrijker problemen leiden, (3) systemen kunnen worden gehackt en gemanipuleerd door individuele personen of organisaties binnen of buiten de relevante strafrechtelijke jurisdictie, (4) bedrijven en overheden kunnen toegang krijgen tot energieverbruiksgegevens van huishoudens en daar – eventueel in samenhang met andere gegevens – conclusies uit trekken met betrekking tot religie, werkloosheid, gezondheid, feitelijke gezinssamenstelling, fraude met sociale zekerheid of belastingen en zo meer. Daarbij zij opgemerkt dat deze agents wel eens iets anders zouden kunnen doen dan de gebruiker is verteld, denk bijvoorbeeld aan het voorbeeld van Volkswagen, waar volautomatisch valse informatie over vervuilingswaarden werd verstrekt. Zoals Jensma (2015) opmerkt lijkt hier sprake van strafbaar bedrog, waarbij vooral ook de oplossing die hij aandraagt tot nadenken stemt: een cyberfysieke infrastructuur die real-time monitort hoeveel vervuiling de auto produceert (en, ik voeg daar maar aan toe, gelijk de

19. Over de kwetsbaarheid van de huidige kritische infrastructuur Nationaal Coordinator Terrorismebestrijding en Veiligheid (2015).

belastingdienst op de hoogte houdt van eventuele fraude met de lease auto).

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

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

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

Zoals hierboven aangestipt kan het doorsluizen van energieverbruiksgegevens vanuit de private sector (energieleveranciers, aanbieders van applicaties bij de slimme meter) naar justitie of de belastingdienst voor soortgelijke grensoverschrijdende uitwisseling leiden. Nog los van bijvoorbeeld de onschuldpresumptie roept dit de vraag op wanneer dit gaat leiden tot maatregelen die de essentie van het recht op privacy en gegevensbescherming aantasten.[20]

1.3 De cyber in cyberspace

Hoewel de notie 'digitaal' interessant is omdat die de aandacht vestigt op de bijzondere aard van door computers verwerkte data,[21] is van belang om digitaal te bezien in relatie tot 'cyber'. Het onderscheid tussen computer en cyber verwijst meestal naar de overgang van op zichzelf staande computersystemen naar online verbonden computersystemen en valt dus samen met de komst van het internet en het world wide web (www). Interessanter is echter dat de digitalisering van de werkelijkheid en de daarmee samenhangende informatica van begin af aan nauw was verbonden met de cybernetica, de door Wiener (1988) geïntroduceerde wetenschap van het besturen op afstand (de oud-Griekse term *kyber* kan worden vertaald met navigeren of sturen).[22]

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

Machinaal leren (ML) is op dit moment een van de meest gebruikte vormen van KI; het wordt bijvoorbeeld ingezet bij beeldherkenning, tekstanalyse, de ondersteuning van medische diagnostiek, cloud robotica

20. Nog los van de proportionaliteitstoets van art. 8 EVRM kan toetsing aan art. 52 lid 1 van het Handvest van de Grondrechten in de EU (Hv) leiden tot een onrechtmatigheidsoordeel (het gaat dan om aantasting van de essentie van het recht), cf. HvJEU 8 April 2014, C-293/12 and C-594/12 (Digital Rights Ireland/Ierland), r.o. 38, 39 (geen aantasting essentie, maar wel disproportioneel en dus ongeldig) ofwel HvJEU, 6 October 2015, C-362/14 (Schrems/Data Protection Commissioner Ireland), r.o. 94-95 (wel aantasting essentie en daarmee ongeldig).
21. Over de wiskundige aard van de informatietheorie die ten grondslag ligt aan informatie in het tijdperk van digitalisering, alsmede de relevantie daarvan voor het recht Hildebrandt (2016a te verschijnen).
22. In de 19e eeuw gebruikte de natuurkundige Ampère (2012:143) de term cybernetica: 'qui est, à l'égard du gouvernement des nations, ce qu'est la stratégie relativement à la conduite d' une armée.' Men zou kunnen vertalen met administratie of bestuur, een soort bestuurskunde *avant la lettre*.

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

Terug naar de cyber in cyberspace. Internet maakte computernetwerken mogelijk, waarop allerhande applicaties gebouwd kunnen worden, in de eerste plaats het www. De hyperconnectiviteit en het netwerkeffect die hiermee in gang werden gezet bepalen de contouren en eigenschappen van cyberspace. Op het niveau van hardware zien we een verschuiving richting de cloud, waardoor de wettelijke term 'randapparatuur' opnieuw actueel is. Onze schermen (toepasselijk monitor geheten) zijn steeds meer een interface naar grootschalige, dynamische computersystemen die op servers 'draaien' die zich elders bevinden, vaak ook in andere jurisdicties. Opslag van data, software en zelfs besturingssystemen vindt plaats waar en hoe het

efficiënt is, wat ook kan betekenen dat data herhaaldelijk wordt verplaatst (en uit voorzorg zowel verspreid als dubbel wordt opgeslagen). Op het niveau van software applicaties hebben sociale media en 'online gaming' een enorme vlucht genomen, waar het delen van zogenaamde 'user generated content' of spel-interactie voorop staat en het koppel van hyperconnectiviteit en netwerkeffect een geheel nieuwe betekenis heeft gegeven aan de idee van cyberspace. In eerste instantie lijkt dit koppel de beste omschrijving te bieden van cyberspace: een online wereld waar de zwaartekracht niet geldt en vooral het leggen van verbindingen langs lijnen van elkaar kruisende netwerken voorop staat. Cruciaal is dat de communicatie niet is voorbehouden aan personen, maar vaak door eenvoudige of complexe kunstmatige *agents* wordt onderhouden, hetgeen samenhangt met de computationele achterkant van cyberspace, die het mogelijk maakt om alle 'gedrag' niet het alleen te meten maar ook op te slaan, te vergelijken en daar middels data-analyse nieuwe 'kennis' uit af te leiden.

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

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

worden met verwijzing naar cyberspace, juist omdat die leefwereld niet meer is opgedeeld in online en offline.[24]

1.4 ***Homo digitalis*** *in de onlife wereld*

Na deze preliminaire verkenningen van *agents* nu over naar de *homo digitalis*. Door te spreken van een *homo digitalis* erkent de NJV dat technologie de mens verandert die haar uitvindt en wordt de vraag opgeroepen hoe de *homo digitalis* zich verhoudt tot *homo sapiens*, *homo faber* en *homo ludens*. In hoeverre is de *homo digitalis* een ordinaire *homo economicus* of *behavioralis*, de droom van de economen en psychologen die zoeken naar de meest effectieve en efficiënte manier om mensen te beïnvloeden? Welke *huomo* ligt ten grondslag aan het mensbeeld in het strafrecht en hoe verhoudt de *homo digitalis* zich tot het – voor het strafrecht cruciale – onderscheid tussen gedrag (extern perspectief met nadruk op meetbaarheid) en handeling (gematigd intern perspectief met nadruk op betekenis)? Om de vraag te beantwoorden welk mensbeeld ten grondslag ligt aan het strafrecht kunnen we een survey organiseren, een literatuuronderzoek doen (ideeënhistorisch, analytisch, hermeneutisch, semiotisch), een computersimulatie ontwerpen die het gedrag van kunstmatige *agent*s registreert op basis van onderscheiden mensbeelden,[25] of alle actoren in de strafrechtsketen voorzien van een daartoe ontworpen App die op slimme wijze hun reactie toetst op het ermee verweven mensbeeld.[26] We kunnen ook – met dit alles in het achterhoofd – zelf nadenken en een beargumenteerde positie innemen. Ik zal het kort houden en verwijzen naar drie filosofen die relevante gedachten ontwikkelden, die naar ik hoop verhelderen waar de schoen wringt wat betreft het onderscheid tussen gedrag en handelen.

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

24. In mijn oratie heb ik bepleit om cyberspace ruimer op te vatten dan alleen in termen van de online wereld, maar gezien het taalgebruik is het misschien verstandiger een andere term te gebruiken om de vermenging van online en offline aan te duiden, zie Hildebrandt (2011b).
25. Dit zou dan een voorbeeld zijn van computationele rechtsociologie, zie Helbing (2012).
26. Dat zou een voorbeeld zijn van sociale strafrechtsfysica, zie Pentland (2014).

van de verdachte of dader (dus geen disciplinering) als aan de zijde van de straffende overheid (dus geen automatisme). Wat is dan gedrag en wat handelen?

In haar *The Human Condition* onderscheidt Arendt (1958) gedrag als een automatisch proces dat onderworpen is aan de wetten van causaliteit en dus ook causaal beïnvloedbaar is.[27] Handelen, daarentegen, is verbonden met vrijheid en onzekerheid. Zij situeert handelen buiten het domein van noodzaak en voorspelbaarheid, en legt de relatie met het spreken in een publieke context en het vermogen opnieuw te beginnen (zij spreekt van nataliteit). Voor het strafrecht is dit een buitengewoon relevante benadering, die de aanspreekbaarheid van de dader benadrukt in een publieke context, op basis van de vooronderstelling dat de dader anders had kunnen en moeten handelen en vooral ook uitgaat van de gedachte dat zij in de toekomst anders kan handelen (wanneer de staf is uitgezeten mag in beginsel niet meer gestigmatiseerd worden als ex-veroordeelde). Deze vooronderstellingen zijn hachelijk en niet evident, zeker wanneer we de statistiek erbij halen om te 'bewijzen' dat het meestal of toch vaak weer mis gaat. *Gedrag benoemen als handeling* is dan ook geen vanzelfsprekendheid en vraagt een specifieke maatschappelijke ordening die voorkomt dat dader en straffer zich in hun rol verliezen en zich beperken tot wat van hen wordt verwacht (statistisch gezien dan toch). Voor de dader ligt de uitdaging erin haar gedrag toe te eigenen als haar eigen handelen, waarvoor zij ter verantwoording kan worden geroepen wanneer zij daarmee anderen heeft beschadigd (of had kunnen beschadigen).[28] Voor de straffende instantie is de uitdaging om zich te weerhouden van straffen als automatische reactie – als zou het niet anders kunnen; ook het straffen zelf is een vorm van zich gedragen die pas betekenis krijgt als de straffer zich de concrete straf als eigen handeling toe-eigent.

In haar *Giving an Account of Oneself* stelt Butler (2005:10-17) – onder verwijzing naar Nietzsche (1969: 84) – dat het morele subject als zodanig geboren wordt bij het opleggen van de eerste straf. Het gaat om het moment waarop de ander mij aanspreekt op de gevolgen van mijn gedrag en straft vanwege het leed dat ik heb veroorzaakt met *mijn* handelen. Uit die eerste straf komt mijn anticipatie voort op de gevolgen van mijn gedragingen voor anderen;[29] die anticipatie geeft betekenis aan mijn gedrag en

27. De discussie is ook buitengewoon relevant voor de strijd rond *homo economicus* (rationele keuzemodel, speltheorie) en *homo behavioralis* (gedragseconomie, beperkte rationaliteit, 'bias'), een strijd die niet alleen in de economische wetenschap maar ook binnen 'law and economics' speelt, zie noot 10 hierboven. Over de relevantie voor het recht Gigerenzer en Engel (2006).
28. We onderscheiden gevaarzettings- en krenkingsdelikten.
29. Voor de strafrechtdogmatiek is dit natuurlijk een gruwel: Nietzsche stelt dat die eerste straf vooraf gaat aan het nemen van verantwoordelijkheid, in flagrante strijd met het legaliteitsbeginsel. Punt is dat het legaliteitsbeginsel het besef van die verantwoordelijkheid vooronderstelt en dat besef moet eerst gevestigd worden. In vergelijkbare zin neurowetenschapper en filosoof Damasio (2011: 280).

schept vrijheid om anders te handelen. De straf verleent betekenis aan mijn gedrag *als mijn handelen* en dwingt mij alternatieve gedragingen te overwegen. Het is die overweging die de straf onderscheidt van training, disciplinering, nudging en priming. Ik word niet gedwongen om mij anders te gedragen, maar om mij een voorstelling te maken van andere manieren van doen. We hebben het niet over Pavlov's hond of Pentland's sociale fysica; het gaat niet over gedrag als verklaarbaar en voorspelbaar mechanisme, maar over gedrag dat als handeling betekenis verkrijgt.

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

30. Ik kom hier in het kader de digitale toerekening van strafrechtelijke aansprakelijkheid nog op terug, zie paragraaf 2.4 hieronder.
31. Kort gezegd stelt Pentland voor om zeer grote groepen mensen – op vrijwillige basis – te voorzien van smartphones die zijn uitgerust met een veelheid van sensoren, die permanent fysiek en sociaal gedrag opmeten en doormeten. Deze gegevens zouden geaggregeerd en beveiligd worden, waarna onderzoekers vragen kunnen stellen aan de database, die door algoritmische *agents* worden verwerkt. De onderzoeker krijgt geen toegang tot de gegevens, maar wel 'safe answers'. Dit zou volgens Pentland een grote vooruitgang betekenen voor de sociale wetenschappen. Helbing werkt niet met gedragdata maar met software *agents* die op basis van speltheoretische of gedragseconomische instructies met elkaar interacteren. Op basis van dergelijke simulaties probeert hij crises in complexe sociale systemen te voorspellen en te testen welke alternatieven zulke crises kunnen voorkomen.

zijn ingebakken ongemerkt het mensbeeld in het strafrecht gaan bepalen. Laat de *homo digitalis* vooral ook een *homo ludens* zijn.[32]

Met betrekking tot de *homo digitalis* beperk ik mij verder tot enkele gedachten die relevant zijn voor *agents* in de context van het strafrecht. Onderzoek naar de eerste mensachtigen doet vermoeden dat (1) de inzet van gereedschappen, (2) gevoel voor causaal verband en (3) het spreken van een taal die tegenwoordig kan stellen wat niet aanwezig is, zich gelijktijdig hebben ontwikkeld (Ambrose 2010, Roby-Brami e.a. 2012). *Homo faber* en *homo sapiens* lijken 'gelijkoorspronkelijk', zoals de Duitsers het zo mooi kunnen zeggen. Hoewel sommige dieren wat voorhanden is in hun omgeving inzetten om een doel te bereiken (een dam te bouwen, een opening te maken) gaan ze er zelden toe over hun gereedschap zelf te maken. En hoewel sommige primaten op aandringen van hun menselijke trainers een aardige woordenschat kunnen bereiken, ontwikkelen zij geen grammatica die tot het benoemen van de verhouding tussen heden, verleden en toekomst leidt en het tegenwoordig stellen mogelijk maakt van wie of wat *voorbij* of *veraf* of zelfs *nog niet* zijn. Het vermogen om te denken (het internaliseren van de gesproken en gehoorde taal) en te weten (in de zin van het opslaan van expliciete kennis in ons geheugen of in externe dragers die het delen van kennis voorbij het hier en nu mogelijk maken) is kenmerkend voor de *homo sapiens.* Dat denkvermogen is intussen hecht verbonden met de *homo faber*, nu juist het fabriceren van dingen die inwerken op de omgeving tot leerprocessen leidt die zonder zulke feedbackmechanismen niet van de grond komen. *Homo faber* vindt technologie uit die haar toestaat zich als *homo sapiens* te heruitvinden. De technologie van het schrift is daarvan de meest evidente uiting; het hangt direct samen met ons vermogen tot abstractie Gleick (2010:37). *Homo ludens* gaat nog een stap verder, door het spel (dat op zich niet specifiek is voor de mens) te integreren met het vermogen om te maken en te denken. Daarbij is het onderscheid tussen 'play' en 'game' van belang (Mead en Morris 1962:153-54). Het eerste is ludieker dan het tweede, speelser en meer experimenteel, de regels worden er nog gaandeweg aangepast. Het tweede veronderstelt dat men in staat is te anticiperen op alle andere spelers (en dus ook op hoe zij zich tot elkaar verhouden). Daarmee gaat het bij 'game' al snel om een spel met regels die bepalen of iets als zodanig geldt: wie de regels van het schaakspel aanpast speelt geen schaak meer, wie haar echtscheiding niet inschrijft in de burgerlijke stand blijft getrouwd voor de wet. Je zou kunnen zeggen dat Wittgenstein's (1992) inzicht in het *taalspel* als constitutief voor

32. Dit is geen oproep tot 'gamification', maar een pleidooi voor het inbouwen van speelruimte in onze onlife wereld, bijvoorbeeld door het mogelijk te maken om algoritmische 'waarheden' aan te vechten met behulp van alternatieve algoritmen.

onderscheiden levensvormen op de grens van 'game' en 'play' staat. Taal is een spel met harde regels die we niet zonder schade kunnen negeren (dan begrijpt niemand wat we bedoelen); tegelijk wordt taal gemaakt en vermaakt steeds wanneer we haar gebruiken.[33] De regels van een taal zijn robuust maar buigzaam, en juist in taalgebruik dat zich buiten de regels stelt zonder het lijntje te breken, kunnen nieuwe paden worden ontgonnen. Zo kan ook worden geëxperimenteerd met een nieuwe benadering van de werkelijkheid.[34] Huizinga's (2010) *homo ludens* zag op de speelse mens, die zich een leefwereld schept en er tijdelijk in huist, grenzen verkent en verlegt en dan weer een ander spel verzint. Hoe belangrijk het serieuze spel ook mag zijn (bijvoorbeeld het recht als spel dat rechtsgevolg toekent aan ons handelen), de vrijheid van de mens (hoe fragiel en betwist die ook mag zijn) uit zich onder meer in de ruimte die zij neemt en schept om de zaken anders aan te pakken (de *homo faber*) en zich daartoe ook een andere werkelijkheid te denken (de *homo sapiens*). Paradoxaal maar pertinent is dat het recht (als 'game') de harde regels stelt die ruimte maken voor de vrijheid (als 'play').

Hoe nu met de *homo digitalis*? Is dat een verder doorontwikkelde *homo sapiens* (of juist een gedegenereerde versie)? Was de *homo sapiens* misschien een homo *analogus*? Voor dit preadvies gaat het vooral om de *homo digitalis* als verdachte dan wel handhaver van het strafrecht. Als we ervan uitgaan dat mensen worden wie ze zijn in het samenspel met de anderen waar ze op anticiperen, zal de intrede van *agents* gevolgen hebben voor wie wij zijn. Navigeren in de onli*f*e wereld betekent anticiperen op de ingrepen van data-gestuurde (digitale) *agents* en die anticipatie vraagt dat wij inspelen op de logica van machinaal lerende systemen. Het spel wordt dus anders gespeeld en de vraag is of deze systemen wel met zich laten spelen, of dat zij niet anders kunnen dan ons hun versie van de werkelijkheid opleggen. *Agents* opereren op basis van meetbare en doorrekenbare gedragsanalyse, zij nemen ons handelen waar als gedrag, liefst te vangen

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

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

in probabilistische patronen die voorspelbaarheid genereren, en zo nodig te ondervangen door machinale *nudging* (Thaler en Sunstein 2008) en *priming* (Ariely en Berns 2010). De verdachte als *homo digitalis* zal mogelijk roepen dat zij gedwongen werd zich te *gedragen* zoals zij deed, wanneer de idee dat mensen ter verantwoording worden geroepen voor hun *handelen* als een pijnlijke – zo niet megalomane – misvatting terzijde wordt gesteld. Justitie en politie zullen als *homines digitales* mogelijk antwoorden dat hun eigen gedrag is ingegeven door accurate berekeningen van effectiviteit en efficiency, die mag blijken uit grootschalige simulaties met gedragsdata. Dat alles onder de noemer van 'sociale fysica' (Pentland 2014) of 'computationele sociale wetenschappen' (Helbing 2012).

Het mag duidelijk zijn dat dit scenario mij niet aanspreekt. De *homo digitalis* die beter aan lijkt te sluiten bij het mensbeeld van het strafrecht in een democratische rechtsstaat neemt kunstmatige intelligentie serieus en begint te 'tinkeren' met de omgeving opdat en totdat die weer een juiste balans toelaat tussen play en game; het blijft dus een *homo faber* en *homo ludens*. Dat sluit aan bij de idee van juridische bescherming by design, bedoeld om de onlife wereld zo te verbouwen dat de *homo digitalis* ook een *homo sapiens* kan blijven. Dat wil zeggen een *agent*/subject in de ethische en juridische zin, die zowel moreel als ook in rechte ter verantwoording kan worden geroepen voor gedragingen die zij (h)er-kent als haar eigen handelen. Dat laatste veronderstelt uiteraard dat de *homines digitales* aan de zijde van de strafrechtelijke wetgever, justitie en politie de rechtshandhaving niet reduceren tot automatische handhaving van de bestaande orde.[35]

---

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

2.1 Introductie: onzichtbare 'remote control'

In deze inleiding eerst een korte uiteenzetting over het verschil tussen 'traditionele' criminaliteit en cybercriminaliteit, met nadruk op interventies van *agents*. Voorbeelden van strafbare interventies via *agents* zijn bijvoorbeeld DDOS aanvallen; botnets die toegang verkrijgen tot wachtwoorden, medische dossiers of vertrouwelijke emails; en ransom aanvallen waarbij de inhoud van de harde schijf wordt versleuteld en alleen tegen betaling van een 'ransom' weer vrij wordt gegeven. In deze gevallen is evident sprake van opzet. Het kan ook gaan om onverwachte of onverhoopte schade of letsel veroorzaakt door onvoorspelbaar gedrag van bona fide *agents*; strafrechtelijke aansprakelijkheid voor opzetdelicten is dan alleen aan de orde wanneer degene die het betreffende systeem heeft

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

ontworpen, ingekocht en/of degene die het gebruikt erop bedacht zou moeten zijn dat het onverwacht gevaarlijk gedrag kan gaan vertonen en vervolgens willens en wetens de aanmerkelijke kans aanvaardt dat een strafbaar gevolg intreedt. Daarnaast kan sprake zijn van een culpoos delict, wanneer sprake is van verwijtbaarheid zonder enigerlei vorm van opzet.

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

De ontwikkeling van computer- naar cybercriminaliteit hangt vooral samen met de hierboven aangegeven exponentieel gegroeide connectiviteit tussen computers, computersystemen, personen, diensten en zelfs goederen (denk aan RFID, het Internet van de Dingen en zo meer). Als gevolg daarvan kan het verschil tussen cyber- en 'traditionele' criminaliteit uit het computerloze tijdperk onder de noemer van zes factoren worden samengevat: afstand, schaal, snelheid, distributie, automatisering en onzichtbaarheid. Deze factoren veranderen de samenhang tussen gedrag en gevolg, evenals de voorzienbaarheid en de omvang van de gevolgen en het gemak waarmee schade kan worden veroorzaakt op grote afstand zonder noodzakelijkerwijs veel sporen achter te laten. Het mag duidelijk zijn dat precies deze implicaties ook weer grote gevolgen hebben voor de rechtshandhaving (waarover meer in het volgende hoofdstuk).

Afstand Met enige weemoed kijken we terug naar de tijd dat een strafrechtelijk relevante handeling werd omschreven als een 'gewilde spierbeweging', en naar het leerstuk van 'functioneel daderschap' waarmee het gevolg van een handeling verricht door de één aan een ander kan worden toegerekend op basis van de samenwerking tussen beide. Wie een ander opdracht geeft een derde te doden is *doen pleger* voor zover degene die de trekker overhaalt zelf niet strafbaar is, en *medepleger* als de opdrachtnemer zelf ook strafbaar is. De opdrachtgever kan bovendien strafbaar zijn wegens uitlokking. Het oordeel dat sprake is van plegen, doen plegen, medeplegen of uitlokken is altijd een kwestie is van toerekening. De vraag of iemand een strafbaar feit heeft gepleegd volgt niet automatisch uit een fysieke gedraging maar vraagt om kwalificatie van een samenstel en/of

samenspel van fysieke gedragingen, uitspraken, afspraken, houdingen en verrichtingen. Dat komt goed van pas als het gaat om cybercrime, want de afstand tussen fysiek gedrag en het strafbare gevolg kan hier extreme vormen aannemen. Niet alleen omdat de dader haar buurman in beginsel om het leven kan brengen via een *agent* die vanuit Verweggistan zijn zorgrobot hackt, maar ook omdat het mogelijk is die aanval te timen en dus ook afstand te creëren in de tijd. De vraag is of dit een fundamenteel verschil maakt, maar zolang we in verschillende jurisdicties leven met verschillende strafbaarstellingen en verschillende prioriteiten bij de handhaving zal dit soort afstand zeker tot problemen leiden. Dit houdt ook verband met de democratische component van de strafbaarstelling, die in beginsel door de wetgever als vertegenwoordiger van de rechtsgenoten binnen de eigen jurisdictie wordt vastgesteld.

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

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

Onzichtbaarheid Fysieke gedragingen zijn zichtbaar voor zover ze in nabijheid van anderen plaatsvinden, of middels CCTV camera's of drones worden opgenomen. Of een fysieke gedraging gekwalificeerd kan worden als deel uitmakend van een strafbare handeling hangt van velerlei factoren af. Het is zeker niet zo dat voor de komst van de computer strafbare feiten altijd in het volle zicht werden gepleegd of als zodanig herkend. Neem het

onderscheid tussen heterdaad en niet-heterdaad; vaak worden heimelijk verrichte misdrijven als ernstiger aantasting van de rechtsorde gezien en dus zwaarder bestraft. Cybercriminaliteit beweegt zich echter in een leefwereld die in toenemende mate wordt bepaald door een computationele achterkant die voor de 'gebruiker' of liever 'bewoner' van die onli*f*e wereld niet gemakkelijk kenbaar is. Dat heeft te maken met bedrijfsgeheimen en intellectuele rechten op software, maar ook los daarvan is de architectuur of grammatica van die achterkant lastig te doorgronden. Zelfs al zou iemand de algoritmes aanreiken en verklaren, dan zouden we daar waarschijnlijk vooral moe van worden, zonder dat duidelijk is hoe die algoritmes onze onli*f*e wereld configureren. Dat maakt cybercriminaliteit bij uitstek ondoorzichtig en onbegrijpelijk. Wie haar voordeur niet op slot draait mag niet verbaasd staan als ze wordt bestolen, we kunnen ons onmiddellijk een voorstelling maken van de dief die binnentreedt en waardevolle spullen meeneemt. Bij diefstal van wachtwoorden en identiteitsfraude is het al veel moeilijker te achterhalen wat er nu precies gebeurt en hoe we dat het beste kunnen voorkomen. Wanneer ML en DL hun intrede doen bij het fabriceren van kant-en-klare malware zal het echter nog veel lastiger worden om te doorzien tegen welke aanvallen of systeembreuken we ons moeten beschermen.

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

*2.2 De **agent** als rechtsubject?*

Onder huidig recht kan een *agent* niet worden aangemerkt als een rechtssubject; het kan uitsluitend object zijn van rechten. Juridisch-technisch is het niet meer en niet minder dan een instrument waarvan een dader zich bedient of waarvoor zij verantwoordelijk is. Zo kan zij bijvoorbeeld als hoteleigenaar een domotica systeem beheren dat onvoldoende is beveiligd en wordt gehackt met desastreuze gevolgen: diefstal van eigendommen omdat anderen toegang hebben tot de kamers, ontregeling van de warmwatervoorziening waardoor gasten brandwonden oplopen. In beginsel lijkt dat niet revolutionair, nu ernstig letsel sinds jaar en dag door allerlei technologie wordt veroorzaakt (denk aan auto's, treinen, vliegtuigen en allerhande elektrische en elektronische apparatuur). Verkeerd gebruik, verzuimd onderhoud, onverwachte samenloop van omstandigheden, bezuiniging op fabricage, en onjuiste of onvoldoende uitleg kunnen stuk voor stuk leiden tot schade of letsel en in een beperkt aantal gevallen zal dat naast privaatrechtelijke aansprakelijkheid aanleiding zijn voor straf-

vervolging. Ook doleuze delicten zullen vaak gepleegd worden met gebruik van technologie, bijvoorbeeld een mes, vuurwapen, gif of explosieven. Kortom, de inzet van apparaten en systemen kan al dan niet opzettelijk schade of letsel veroorzaken waarvoor enigerlei rechtssubject strafrechtelijk aansprakelijk is. Data-gestuurde *agents* onderscheiden zich echter van andere instrumenten doordat zij niet alleen instrument zijn maar daarnaast in staat zijn om op grond van hun leervermogen zelfstandig in te grijpen, hun gedrag te veranderen en daarbij rekening te houden met de manier waarop het mogelijke slachtoffer zich gedraagt. Daarmee dringt de vergelijking met een dier zich op, dat zoals dat zo mooi heet 'een eigen energie heeft' die in het privaatrecht tot risicoaansprakelijkheid leidt.[36] Strafrechtelijk is dat laatste niet aan de orde, nu daar behalve vervulling van de bestanddelen van een delictsomschrijving en wederrechtelijkheid altijd sprake moet zijn van verwijtbaar handelen (inclusief eventueel nalaten) van het rechtssubject. Het OM zal dus moeten aantonen dat de eigenaar of houder van een dier met opzet of in ieder geval verwijtbaar heeft gehandeld, bijvoorbeeld door het dier geen muilkorf te laten dragen, een hek niet te repareren of een giftige slang zonder toezicht buiten de kooi te laten. Hoewel wij niet precies kunnen voorzien hoe en wanneer een dier derden in gevaar zou kunnen brengen of verwonden, hebben we wel voldoende zicht op hoe de dieren die we 'houden' zich in het algemeen gedragen en wat van de houder verwacht mag worden om letsel of schade te voorkomen.

Dat ligt bij *agents* anders. Enerzijds omdat het ontwerp en de inzet van *agents* relatief nieuw en volop in ontwikkeling zijn, anderzijds omdat zij een aantal eigenschappen hebben waaraan wij niet gewend zijn, noch bij onze apparaten en machines, noch bij dieren en mensen. Het gaat daarbij om de bovengenoemde punten, te weten afstand, schaal, snelheid, distributie, automatisering, en onzichtbaarheid. Ik leid daar nog twee opvolgende punten uit af, die het bijzonder lastig maken om het gedrag van *agents* en de implicaties daarvan te voorzien: hun mobiliteit en polymorfe hoedanigheid. Karnow (1997) voorzag eind vorige eeuw al dat *agents* vaak over verschillende servers gedistribueerd zijn (denk ook aan cloud computing) en zich snel en voortdurend verplaatsen in functie van hun taken, waarbij ze dankzij hun vermogen om te leren bovendien in staat zijn hun eigen systeem opnieuw te configureren waardoor ook hun waarneembare vorm kan veranderen. Malware wordt niet voor niets betiteld als virus, worm of Trojaans paard. De combinatie van remote control, schaalvergroting, snel-

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

heid, decentrale opslag, automatisering, onzichtbaarheid, mobiliteit en morfologische veranderlijkheid kan het bijzonder lastig maken om een *agent* als zodanig te identificeren, blijvend te traceren en te adresseren. Karnow stelt dan ook de vraag of hier nog wel sprake is van een herkenbare eenheid die het mogelijk maakt een agent als oorzaak van wat voor gevolg ook te identificeren, nog los van de vraag of de *agent* als instrument of subject wordt gekwalificeerd.

In dat kader is het nuttig om een zijstap te maken naar de idee van *moral agency*. Vanwege de eis van verwijtbaarheid lijkt *moral agency* een mogelijkheidsvoorwaarde te zijn voor rechtssubjectiviteit binnen het domein van het strafrecht, ook al vallen beide zeker niet samen. Rechtssubjectiviteit wordt toegekend door het positieve recht, het is geen van nature gegeven categorie maar een kunstmatige constructie, die het toekennen van rechten en plichten mogelijk maakt. Morele subjectiviteit is evenmin een natuurlijk gegeven, maar staat los van juridische attributie en heeft op zichzelf genomen geen rechtsgevolg. In zijn bespreking van kunstmatige *agents* stelt informatiefilosoof en –ethicus Floridi, in navolging van Aristoteles, de idee van een *moral agent* tegenover die van een *moral patient*.[37] Terwijl de *agent* de relatief interactieve, autonome en adaptieve entiteit is die actief ingrijpt en daarmee bijvoorbeeld nadeel (schade of letsel) veroorzaakt, is de *patient* de entititeit die het gevolg van die ingrepen ondergaat en aldus schade of letsel bekomt. Floridi abstraheert daarbij van de aanwezigheid van een innerlijk bewustzijn; zijn *agents* kunnen heel wel geestloze entiteiten zijn die desondanks het vermogen hebben om 'kwaad' te doen door het beschadigen van *patients*. Ook een *patient* is bij Floridi niet noodzakelijk een met gevoel uitgerust wezen; het is minstens een identificeerbare entiteit met een zekere complexiteit die in staat is te reageren op de ingrepen van de *agent*. Floridi wijst erop dat onder invloed van milieuprotagonisten de categorie van morele *patients* enorm is uitgebreid (van dieren en planten tot hele ecosystemen), terwijl de categorie van morele *agents* afhankelijk blijft van vrije wilsvorming en intenties. Tegelijkertijd is de invloed van kunstmatige systemen die zich als geestloze *agents* gedragen exponentieel toe aan het nemen, waarbij – geheel los van intenties of bewustzijn – het vermogen van deze *agents* om nadeel, schade, leed of letsel toe te brengen aan levende maar ook aan waardevolle niet-levende systemen evenredig toeneemt. Hij beargumenteert dat het erkennen van de morele relevantie van het gedrag van deze *agents* pertinent is, willen wij tot een redelijke en ook veilige omgang met kunstmatige agenten komen. Daarbij spreekt hij zelf van moreel gedrag, waar ik toch graag van moreel relevant gedrag zou blijven spreken, vasthoudend aan de idee dat de kwalificatie 'moreel' tenminste een

37. Zie Floridi en Sanders (2001, 2004), Hildebrandt (2011b, 2015a).

handelende *agent* eist die tot oordeelsvorming in staat is. Interessant is dat Floridi bepleit dat ook vernietiging van of schade aan een niet-levende entititeit door een niet-menselijke *agent* moreel relevant is en moet worden afgewezen en indien mogelijk voorkomen – voor zover mogelijk. Floridi lijkt te claimen dat ook wanneer het niet mogelijk was om zoiets te voorkomen toch sprake is van moreel kwaad, puur en alleen vanwege de vernietiging of beschadiging van een *patient*.

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

2.3 Daderschap, wederrechtelijkheid, causaliteit en schuld

De doctrine van het materiele strafrecht in Nederland gaat uit van de leer van het strafbare feit, die de voorwaarden voor strafbaarheid bevat. [38] Voor strafbaarheid is vereist: (1) een handeling, die kan bestaan uit een niet-handelen waar dat wel geboden was; die (2) valt onder de delictsomschrijving en dus gekwalificeerd kan worden als een strafbaar feit; die (3) wederrechtelijk is en waarvoor geen rechtvaardigingsgrond kan worden aangewezen; en die, tenslotte, (4) aan schuld te wijten is, bij gebreke van een schulduitsluitingsgrond. Wanneer in de delictsomschrijving het woord 'wederrechtelijk' of de zinsnede 'aan schuld te wijten' (of terminologie van gelijke strekking) is opgenomen moet dit worden bewezen, anders volgt uit het voldoen aan de delictsomschrijving in beginsel dat het handelen onrechtmatig en/of verwijtbaar is. Alleen wanneer een verweer wordt gevoerd (maar nu bevinden we ons in het formeel strafrecht, art. 350 WSv en verder), moet de rechter naar aanleiding daarvan zelfstandig vaststellen dat sprake is van wederrechtelijk en/of verwijtbaar handelen.

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

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

De eerste vraag is of het *gedrag* van een *agent* als *handeling* aan een rechtssubject kan worden toegerekend en of het onder een delictsomschrijving valt. Met andere woorden, is sprake van daderschap en kan de handeling worden gekwalificeerd als een strafbaar feit? Normaliter is dat deels een feitelijke en deels een rechtsvraag, nu het gaat om de constellatie van feiten en omstandigheden die mede bepalen of het ontwikkelen, verkopen of gebruiken van een gereedschap, apparaat of systeem in een specifiek geval heeft te gelden als hetgeen in de diverse bestanddelen van de delictsomschrijving wordt beschreven. Het zal dus afhangen van allerlei factoren, waarbij het strafrechtelijk analogieverbod en prudentie ten aanzien van extensieve interpretatie van belang zijn (het binnendringen van een computer door een *agent* is geen huisvredebreuk en kan door de rechter niet naar analogie als computervredebreuk worden gekwalificeerd; daarvoor is wetgeving nodig).[39] Interessant is dat het hier uiteindelijk gaat om de vraag of het gedrag van een *agent* mag gelden als onderdeel van het handelen van een rechtssubject. Kennelijk moet aan het gedrag van de agent betekenis worden verleend die het mogelijk maakt de verbinding te leggen met een handeling – en die betekenis wordt in laatste instantie niet door het rechtssubject verleend, maar door het recht en uiteindelijk door de spreekbuis van het recht, de rechter. Als *agents* rechtspersoonlijkheid zouden hebben, zou hun opdrachtgever als doen-pleger kunnen worden vervolgd, nu doen-plegen ziet op een strafrechtelijke figuur waarbij degene die de strafbare gedraging uitvoert zelf niet strafbaar is, bijvoorbeeld vanwege dwang, minderjarigheid of een strafuitsluitingsgrond. Indien de wetgever zou besluiten dat *agents* rechtssubject kunnen zijn en onder bepaalde voorwaarden ook strafbaar, zouden zij als medeplegers kunnen gelden, uitgelokt door een natuurlijk persoon of andere rechtspersoon of zelfs omgekeerd (de *agent* verleidt natuurlijke personen of rechtspersonen

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

door te wijzen op gedragingen die een gewenst gevolg hebben ook al zijn ze strafrechtelijk verboden). Positiefrechtelijk is dit vooralsnog onzin want de agent is geen rechtssubject, maar het gedachtenexperiment is juridisch wel relevant. Het zou goed zijn eens na te denken in hoeverre nieuwe deelnemingsvormen ontwikkeld kunnen worden die rechtssubjecten als dader kwalificeren op basis van de specifieke relatie met een *agent* wiens gedrag de bestanddelen van een delictsomschrijving vervult (afgezien van eventuele wederrechtelijkheid en schuld). Een ander belangrijk punt betreft de specifieke voorwaarden van doleuze dan wel culpoze delicten. Wanneer kan het kleurloos opzet van een *agent* aan de dader worden toegerekend,[40] hoe ver mag het leerstuk van voorwaardelijk opzet worden opgerekt bij opzet op de wederrechtelijkheid en hoe verhoudt het bestanddeel 'aan schuld te wijten' zich tot het gedrag van de *agent* en de kennis van de dader? Kleurloos opzet en onbewuste schuld lijken hier op het lijf geschreven van de geestloze *agents*. Het doet er niet toe wat de bedoeling was en of de *agent* zich ergens van bewust was, het gedrag heeft in het maatschappelijk verkeer als opzet dan wel schuld te gelden. Althans, ten aanzien van de dader. Dat de *agent* geen bedoelingen had en geen schuldbewustzijn is dan niet relevant; het gaat erom dat ook in het reguliere commune strafrecht sprake kan zijn van kleurloos opzet en onbewuste schuld die tot strafbaarheid leiden.[41]

De tweede vraag was of het strafrechtelijk relevante gevolg aan het gedrag van een *agent* kan worden toegerekend. Hier gaat het om de causaliteit in geval van een materieel omschreven delict. Uitgaande van het feit dat het gedrag van de *agent* aan de dader kan worden toegerekend is de vraag of hier sprake is van causaal verband tussen het handelen van de dader en het ingetreden strafbare gevolg. Causaliteit wordt in beginsel toegerekend op basis van conditio sine qua non, maar in geval van dubbele causaliteit (meerdere handelingen kunnen ieder voor zich als oorzaak van het strafbare gevolg worden aangewezen), alternatieve causaliteit (een van meerdere handelingen heeft als oorzaak te gelden, maar onduidelijk is welke), of eigen schuld (het gevolg was niet ingetreden als het slachtoffer niet causaal had bijgedragen), wordt ook naar andere factoren gekeken. Daar komt bij dat de conditio sine qua non een te groot net over de werkelijkheid gooit nu bijvoorbeeld ook de geboorte van het slachtoffer als

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

conditio sine qua non kan worden aangemerkt. Dit wordt enigszins ondervangen door de leer van de causa proximus, die de aandacht richt op de – in tijd en ruimte – meest nabije oorzaak. Zo kennen we ook nog de nova causa interveniens (niet toe te rekenen aan de dader) die de causale keten doorbreekt (hoewel het strafbare gevolg mogelijk had kunnen optreden zonder deze interventie moet worden aangenomen dat de interventie de meest voor de hand liggende oorzaak is, die de eerdere als het ware uitwist). Tenslotte kan het zijn dat een handeling moet worden aangemerkt als conditio sine qua non, terwijl het gevolg voor de veroorzaker niet of nauwelijks voorzienbaar was. Hoewel de voorzienbaarheid pas aan de orde komt bij de vraag naar de verwijtbaarheid, kan die desondanks meespelen bij de causaliteitsvraag, met name bij culpose gevolgsdelicten (bijvoorbeeld dood door schuld). Wanneer *agents* worden ingezet met het doel een delict te plegen, zal wanneer het strafbare gevolg intreedt toerekening van causaal verband meestal geen probleem zijn (hooguit een bewijsprobleem dat wordt veroorzaakt door de hierboven genoemde onzichtbaarheid van cybercriminaliteit en door de snelheid waarmee sporen kunnen worden uitgewist). Wanneer *agent*gedrag zonder opzet leidt tot strafbare gevolgen ligt dat anders, met name in geval van culpoze delicten. Hier worden we geconfronteerd met het feit dat ML gebaseerd is op probabilistische aannamen, die werken met foutmarges en – in geval van distributieve profielen – met profielen die wellicht helemaal niet van toepassing zijn op het voorliggende geval.[42] Meestal is er een trade-off tussen de foutmarges voor fout-positieven en fout-negatieven. Het instellen van de drempel waaronder de *agent* moet blijven lijkt een relevante eis die al bij de causaliteitsvraag getoetst moet worden: welk voorzienbaar risico nam de dader, gezien de inzet van de *agent*? Gezien de potentieel desastreuze gevolgen van op elkaar inwerkende *agents* en de complexe keten van oorzaken die daarmee – ingevolge het netwerkeffect – gegeven is, lijkt de vaststelling van causaliteit zowel ex ante (door de ontwikkelaar, verkoper of gebruiker van de *agent*s) als ex post (door de rechter) een Herculeaanse opdracht.

De derde vraag was welke rol het gedrag van *agents* speelt bij het vaststellen van de wederrechtelijkheid (als bestanddeel van een delictsomschrijving) en de onrechtmatigheid (als element van het strafbare feit), met bijzondere aandacht voor het beroep op noodweer of noodtoestand. Wanneer de wederrechtelijkheid is opgenomen in de delictsomschrijving gaat het meestal om handelen zonder toestemming of andere juridische grondslag. Zo valt het gebruik van penetratiesoftware waarmee de security

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

van een systeem kan worden getest in beginsel onder art. 138ab WvSr (hacking), ware het niet dat de eis van wederrechtelijkheid deel uitmaakt van de delictsomschrijving. In gelijke zin zal een wettelijke bevoegdheid voor het op afstand binnendringen van computersystemen voor politieagenten de wederrechtelijkheid wegnemen. Ten aanzien van *agents* is dan bijvoorbeeld de vraag van belang wanneer het gebruik van bepaalde *agents* toestemming impliceert om bepaalde formeel omschreven delicten te plegen. Als ik applicaties gebruik die mijn computer binnendringen om daar gegevens te kopiëren op basis van toestemming zal het niet eenvoudig zijn om tot veroordeling wegens hacking te komen. Het zou overigens interessant kunnen zijn om eens een proefproces te voeren wanneer duidelijk is dat de gegevens voor een ander – niet verenigbaar – doel worden gebruikt, waarvoor dan ook geen toestemming is gegeven. In dat geval kan – lijkt mij – wel degelijk sprake zijn van schending van art. 138ab lid 1 Sv.[43]

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

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

voorhand willen uitsluiten. Vergelijk de virtuele verkrachting,[44] die juridisch interessante vragen oproept inzake wat hier nog onder noodweer zou kunnen vallen (gebruik van software die het systeem van de provider plat legt als enige effectieve mogelijkheid om de aanranding te voorkomen?).

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

Gless en Weigend (2014:565-6, 590-1) suggereren dat we misschien moeten accepteren dat de voordelen van het op grote schaal gebruiken van dit soort technologie opwegen tegen het feit dat we in veel gevallen geen

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

strafbare handeling aan een rechtssubject kunnen toerekenen, dan wel in de knoop komen bij de causaliteit, de wederrechtelijkheid/onrechtmatigheid of de schuld. Dit zou dan met name opgaan voor zelflerende systemen, die zowel onvoorspelbaar als – juist daarom – bijzonder nuttig kunnen zijn. Zij stellen voor de zorgplicht in te perken vanwege het ontwikkelingsrisico en/of een rechtvaardigingsgrond in te voeren onder de noemer van 'sociaal-adequate inzet' van *agents* (idem:591). De vergelijking met verkeersstrafrecht dringt zich op. Ook daar accepteren we schade en letsel vanwege het veronderstelde maatschappelijke nut van de auto, en beperken de strafbaarheid van de eindgebruiker (de automobilist) tot hetgeen voorzienbaar en vermijdbaar was, terwijl vage normen zoals die van art. 5 WVW de weggebruiker aanmanen om zowel soepel als vlot en veilig te anticiperen op andere weggebruikers.[45] Het zou kunnen dat de zelfrijdende auto veel van die problemen oplost en tegelijkertijd een heel nieuw type problemen met zich meebrengt. Misschien een nieuw artikel invoeren in het commune strafrecht:[46]

> Met hechtenis van maximaal x maanden of een boete van de y^{e} categorie wordt gestraft een ieder die zich bedient van *agents* die zich zodanig gedragen dat gevaar voor personen, goederen of diensten wordt veroorzaakt of kan worden veroorzaakt of die zich zodanig gedragen dat het maatschappelijk verkeer wordt gehinderd of kan worden gehinderd.

2.4 Data-gestuurde toerekening

De inzet van data-gestuurde intelligentie aan de zijde van politie en justitie komt uiteraard aan de orde onder het kopje formeel strafrecht, bij de bespreking van *police intelligence*.[47] Het vermogen om correlatieve

45. Art. 5 WVW: 'Het is een ieder verboden zich zodanig te gedragen dat gevaar op de weg wordt veroorzaakt of kan worden veroorzaakt of dat het verkeer op de weg wordt gehinderd of kan worden gehinderd.' Overtreding is strafbaar gesteld in art. 177 WVW. Het gaat om een overtreding, niet om een misdrijf (art. 178 WVW). Uiteraard kan het veroorzaken van dood of ernstig letsel door schuld in het verkeer op basis van het commune delict worden vervolgd (art. 307, 308 Sr).
46. Ik ga ervan uit dat de lezer voldoende ironisch is onderlegd om in te schatten dat de problemen hiermee niet zijn opgelost. Interessant is desondanks het feit dat art. 179 lid 2 WVW de mogelijkheid opent een bijkomende straf op te leggen: ontzegging van de rijbevoegdheid. Het zou niet verkeerd zijn natuurlijke personen of juist rechtspersonen naar aanleiding van overtreding de bevoegdheid te ontzeggen nog langer gebruik te maken van *agents*.
47. Nederlandse vertaling met 'politie intelligentie' is niet gebruikelijk, het kan bovendien worden uitgelegd als een inschatting van de gemiddelde intelligentie van politieagenten. Vertaling met 'inlichtingen' of de 'vergaring' daarvan stamt uit een vorig tijdperk en zag ook toen over het hoofd dat het gaat om het detecteren van relevante verbanden. Over smart policing, police intelligence enzomeer Bob Hoogenboom (2009).

patronen te detecteren die biometrische, locatie, surf en vooral ook sociale media datapunten verbinden met gewelddadig gedrag, pedofilie, of fraude in de sociale zekerheid en belastingen roept echter ook vragen op omtrent strafrechtelijke aansprakelijkheid. Het is van cruciaal belang om de uitbreiding van strafbaarheid in het vizier te krijgen waartoe predictieve data analyse kan uitlokken. Het gaat dan met name om de rol van profielen die worden verkregen bij smart policing, fenomeenonderzoek, grootschalig onderzoek van informatiesystemen, en bij de koppeling van allerlei gegevensbestanden uit de publieke en private sector.

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

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

48. *La Defense Sociale* was een stroming binnen de strafrechtswetenschappen rond het begin van de 20e eeuw, die de functie van de straf terugbracht tot 'sociaal verweer' tegen sociaal onwenselijk gedrag en ertoe neigde het strafrecht om te vormen tot een sociale wetenschap, cf. de grondleggers Ancel (1981), Van Hamel (1907); zie de analyse in Foqué en 't Hart (1990: hoofdstuk 7).
49. Of, 'positivistische' narratieven, cf. Wendt (2015).
50. Van Delft (2003), De Geest (2004), zie verder het uitstekende vakblad *Law and Method*, <http://www.bjutijdschriften.nl/tijdschrift/lawandmethod/detail>.

homo behavioralis die kan worden aangestuurd dank zij kennis van haar neiging tot irrationeel gedrag. *Der Methodenstreit revisited*.[51]

De rechtswetenschap moet weer een normatieve wetenschap durven zijn en zich bezinnen op de betekenis van die normativiteit. Normatief kan immers niet betekenen dat de jurist zich als moraalridder gaat gedragen. Het verschil tussen recht en moraal zetelt onder meer in de positiviteit van het recht,[52] die het mogelijk maakt om op juridische gronden knopen door te hakken waar dat op grond van de moraal niet kan (nu we het over die moraal meestal niet eens zijn). De jurist in functie is dus gebonden aan het recht, zij mag haar persoonlijke morele inzichten niet opleggen aan anderen.[53] Dat betekent echter niet dat het recht geen normatieve kaders schept die onderhouden moeten worden. De jurist moet haar rug recht houden als het gaat om het recht als systeem van checks en balances dat ongelijkheid compenseert om rechtsgenoten de mogelijkheid – zo men wil capability – te bieden zich zelfstandig tot anderen te verhouden en zichzelf daarbij steeds opnieuw uit te vinden. Dat speelt bij de uitleg van geldend recht,[54] maar uiteraard ook bij het adviseren van de wetgever. De vrijheid waar het om gaat mag dan weer niet in naïef voluntaristische zin als een natuurverschijnsel worden begrepen, maar speelt in die zin dat het recht de institutionele architectuur meebepaalt waarbinnen persoonlijke vrijheid en verantwoordelijkheid vorm kunnen krijgen. Vrijheid kan niet verondersteld worden, het moet worden bevochten – als het ware tegen de tweede wet van de thermodynamica in.[55]

51. De methodestrijd tussen de natuurwetenschappen en de geesteswetenschappen barstte los in de 19e eeuw, waarbij de geesteswetenschappen een eigen positie en methode claimden. De idee was dat natuurwetenschappen streven naar verklaringen (causaliteit), terwijl de geesteswetenschappen gericht zijn op begrip (betekenis), cf. Leezenberg en De Vries (2012). In de 20e eeuw deed zich een hernieuwde strijd voor, nu met name binnen de sociale wetenschappen die bang waren de status van wetenschap te verliezen als zij de methoden en technieken van de natuurwetenschappen niet overnamen, cf. Schuyt (1986). Over de relativering van de tegenstelling de reeds aangehaalde Geertz (2001) en bijvoorbeeld ook Prigogine en Stengers (1984), die op basis van de transformaties van de natuurwetenschappen zelf het positivistische beeld van de natuurwetenschappen als achterhaald dogmatisme afwijzen. Over de 'science wars' tussen de postmodernisten en laat 20e eeuwse positivisten Stengers (2010), Latour (1998). Met het oog op het recht Loth en Gaakeer (2005), Hildebrandt (2004).
52. Niet te verwarren met rechtspositivisme, dat de positiviteit verabsoluteert ten koste van de instrumentaliteit en de rechtvaardigheid. Zie Radbruch (1950:173), Hildebrandt (2015b:52-54).
53. De rechter moet geldend recht dat zij onrechtvaardig acht in beginsel desondanks toepassen, tenzij de betreffende normen niet meer kunnen worden begrepen als *gericht op* rechtvaardigheid, aldus Radbruch (1950, 1945). In dat geval is eigenlijk geen sprake meer van recht, maar van bestuur.
54. Overigens niet alleen bij het strafrecht. Zie over de doorwerking van grondrechten in het privaatrecht Sieburgh (2015).
55. Over de relatie tussen entropie, onzekerheid en vrijheid, vanuit een informatietheoretisch perspectief Leydesdorff (2010); relevantie voor het recht Hildebrandt (2016a).

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

Ook als uitbreiding van strafbaarheid niet aan de orde is, kunnen police intelligence en profiling desondanks leiden tot uitbreiding van de inzet van *maatregelen*,[56] op te leggen naar aanleiding van het begaan van een strafbaar feit. Stel dat uit inzage van historische gedragsgegevens (bijvoorbeeld metadata van telecommunicatie, postings op sociale media, energieverbruiksgegevens) blijkt dat datapunten van de verdachte correleren met recidive of juist met 'vatbaarheid voor' of 'geneigdheid tot' geheel andere strafbare feiten of zelfs met andere vormen van ongewenst gedrag. Mag dit aanleiding zijn om maatregelen op te leggen die – losgekoppeld van de ernst van het feit en de mate van schuld – veel ingrijpender zijn dan hun punitieve tegenhangers? In juridische zin is dit niet zonder meer verboden.[57] Wat nu als politie of andere *agents* correlaties ontdekken tussen een reductie van agressie in gevangenissen en de inname van voedingssupplementen? Kunnen we ons voorstellen dat een maatregel wordt opgelegd die eist dat de veroordeelde haar bloed laat controleren ten einde vast te stellen dat zij haar supplementen heeft ingenomen, bijvoorbeeld in het kader van een voorwaardelijke straf? Als zij haar pillen niet braaf

56. Maatregelen zijn niet punitief van aard en dus ook niet gebonden aan de evenredigheidseis ten aanzien van de ernst van het feit of de mate van schuld. Zie Titel IIa WvSr. Het gaat om onttrekking aan het verkeer, ontneming van wederrechtelijk verkregen voordeel, schadevergoeding, plaatsing in een psychiatrisch ziekenhuis of in een inrichting voor stelselmatige daders (ISD), ofwel oplegging van een vrijheidsbeperkende maatregel. Over grondslag en normering Kooijmans (2002). In het kader van pre-emptieve maatregelen zie Struijk (2015) over de ISD.
57. Zie bijvoorbeeld art. 36e WSr waar een ontnemingsmaatregel mogelijk wordt gemaakt voor voordeel behaald door 'andere strafbare feiten, waaromtrent voldoende aanwijzingen bestaan dat zij door de veroordeelde zijn begaan', wanneer 'aannemelijk is dat of dat misdrijf of andere strafbare feiten op enigerlei wijze ertoe hebben geleid dat de veroordeelde wederrechtelijk voordeel heeft verkregen' en bij de vaststelling van het voordeel mag worden uitgegaan van een aantal vermoedens (art. 36e lid 3 onder a en b WvSr). Bij plaatsing in een psychiatrische inrichting, ter beschikkingstelling, dwangverpleging en plaatsing in een ISD wordt vooral gelet op het gevaar dat de verdachte zou kunnen veroorzaken (art. 37, 37a, 37b, 38m WvSr); ook bij de vrijheidsbeperkende maatregel staat beveiliging van de samenleving en het voorkomen van strafbare feiten voorop (art. 38v WvSr). Het mag duidelijk zijn dat de strafrechtelijke maatregel voortkomt uit de idee van het sociaal verweer, zie hierboven noot 48.

inneemt wordt de straf alsnog ten uitvoer gelegd. Dit is geen science fiction, ook al bestaat die maatregel nog niet.[58]

De vraag is of het strafrecht zich daartoe moet lenen. Of is het wellicht zo dat juist het strafrecht vanuit een scherp gevoel voor de constitutieve samenhang van instrumentaliteit en rechtsbescherming weerstand kan bieden aan weer een nieuwe versie van wat Foqué en 't Hart (1990) begin jaren '90 'beheersingsdenken' noemden. Zij benoemden daarmee wat inmiddels het reguleringsparadigma mag heten, dat wil zeggen de behoefte om het recht te reduceren tot een instrument om mensen te beïnvloeden, in plaats van een instrument dat mensen aanspreekt. Voor zover de strafrechter – eerder dan het OM of het bestuur – weerstand weet te bieden aan zulk beheersingsdenken, zou dat ervoor kunnen pleiten om maatregelen naar aanleiding van een strafbaar feit zoveel mogelijk binnen het strafrecht te houden en dus bij de strafrechter te laten. De inzet van politie-*agents*[59] om beslissingen te genereren die pre-emptief ingrijpen ter voorkoming van nog te plegen misdrijven of overtredingen mag intussen niet gelijk worden gesteld met het beheersingsdenken van eind 20ste, begin 21ste eeuw. Dat was gebaseerd op een hiërarchisch soort systeemdenken waarbij de overheid een centrale rol had. Het nieuwe beheersingsdenken is niet meer systeemgerelateerd maar 'denkt' in termen van netwerken; het richt zich niet meer op *government* maar op *governance*, wijst *command and control* af en verschuilt zich achter de objectieve feiten die zouden blijken uit 'harde' data analyse.

Bovendien is niet ondenkbaar dat de straffende overheid haar controletaken steeds meer moet delen met politie-*agents* die zij niet volledig in de hand heeft, terwijl zij er wel steeds meer van afhankelijk wordt.

Dat laatste zal de grootste verandering worden; data analytics en daaruit afgeleide voorspellingen zijn van een andere orde dan machinaal lerende systemen die ingrijpen in de maatschappelijke orde. De ambtenaren die de uitvoerende macht handen en voeten geven, zullen mogelijk deels worden vervangen door *agents* en de ambtenaar van de toekomst zal in dat geval worden gerekruteerd op haar vermogen om daarmee samen te werken. Dat is niet slecht of fout, maar het maakt wel degelijk uit. *Agents* die hun eigen programmatuur bijstellen met het oog op het verwezenlijken van de doelen

58. Op dit moment loopt een experiment met dergelijke supplementen naar aanleiding van positieve resultaten bij een eerder experiment, zie de Visser (2015). Daarbij is vooralsnog geen sprake van een verplichting, maar het laat zich denken dat op zeker moment weigering gevolgen kan krijgen.
59. A*gents* die door de politie (onder gezag van het OM) worden ingezet duid ik hieronder aan als politie-*agents*, wanneer dat het leesgemak en de herkenbaarheid bevordert.

van strafrechtelijk beleid, kunnen op de loop gaan met de methodologie – en daarmee ook met de doelstellingen – van hun opdrachtgevers.[60]

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

De schuld ligt dan bijvoorbeeld in afwijzing van hulp bij het bevechten van zulke neigingen. De idee dat mensen strafrechtelijk aansprakelijk zouden worden gesteld voor het feit dat hun gedrag correleert met een neiging tot geweldpleging, tot pedofilie, tot fraude met belastingen of sociale zekerheid of tot fundamentalistisch radicalisme lijkt – misschien – absurd. Tegelijkertijd worden systemen ontwikkeld waarmee dergelijke neigingen kunnen worden berekend. Het is verstandig, zo niet pertinent, om al in dit stadium te bedenken hoe wij de architectuur van de onlife wereld zo in kunnen richten dat dit soort machinale toerekening kan worden voorkomen. Voorkomen is hier zeker beter dan genezen; de kans dat dergelijke informatie gebruikt gaat worden tegen degenen die ermee 'getarget' kunnen worden is niet onaanzienlijk.[61]

3. Formeel strafrecht: verdachte en handhaver als homo digitalis

3.1 Introductie: het doel van de strafvordering

In de MvT van de Wet BOB sprak de Minister van – toen nog slechts – Justitie de onsterfelijke woorden:[62]

60. De ervaring leert dat wie de middelen beheert daarmee deels ook de doelen in de hand heeft. Wijsgerig heeft met name Dewey (1967) het constitutieve verband tussen middel en doel verder uitgewerkt.
61. Inmiddels is in de VS software ontwikkeld die de kans op recidive berekent met de bedoeling die ter beschikking te stellen aan rechters, ten einde een meer objectieve maatstaf te bieden bij het vaststellen van de straf, zie Tokmetzis (2015) en Barry-Jester, Casselman en Goldstein (2015). Algoritmische straftoemeting is overigens beslist niet objectief, zie voor een interessante analyse Aas (2005).
62. Handelingen Tweede Kamer 1996-97, 25 403, nr. 3, Memorie van Toelichting Wetsvoorstel tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), p. 3.

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

Ik vrees dat de behoefte om de eigen informatiepositie te verbeteren niet alleen in het verleden maar ook in heden en toekomst doorslaggevend zal zijn.[63] Het woordje 'positie' doet vermoeden dat het vooral ook gaat om informatieoverwicht ten opzichte van anderen, zoals bijvoorbeeld verdachten of mogelijke verdachten. Zo'n informatieoverwicht leidt echter gemakkelijk tot informatieover*ge*wicht, hetgeen om een veelheid van redenen niet wenselijk is. De behoefte om de beschikking te hebben over heel veel informatie, en liefst ook heel veel 'big en open data', hangt samen met de verzelfstandiging van het vooronderzoek ten opzichte van het hoofdonderzoek ter terechtzitting. Het doel van de strafvordering was enerzijds, ingevolge het procesbeginsel, de voorbereiding van het onderzoek ter terechtzitting ten einde in een openbaar proces bij een onpartijdige en onafhankelijke rechter op tegenspraak vast te stellen of de verdachte het tenlastegelegde strafbare feit heeft gepleegd, en anderzijds, in het verlengde daarvan de voorbereiding van het straffen zelf ingeval de verdachte wordt veroordeeld. De voortgaande relativering van het procesbeginsel betekent dat in de meeste gevallen de straf niet door de strafrechter wordt opgelegd, maar door het Openbaar Ministerie wordt opgelegd of overeengekomen (in de vorm van een strafbeschikking of transactie).[64] Daarmee blijft echter overeind dat de strafvordering de *voorbereiding* is van een straf die alleen mag worden opgelegd op voorwaarde van een aantal processuele waarborgen. Een daarvan is toegang tot de rechter. De voorbereiding mag niet worden verward met de straf zelf; de strafvordering zelf heeft geen punitief karakter.

63. Het 'discours' over de informatiepositie van overheden wordt vaak gevoerd onder de noemer van 'surveillance'. Na afronding van de eerste versie van dit preadvies zag ik dat ik het woord 'surveillance' helemaal niet gebruik. De term is inmiddels beladen met een keten van associaties die mijns inziens in de weg kunnen staan aan een open discussie over (1) de bevoegdheden die overactieve overheden wel en niet nodig hebben, (2) de precieze waarborgen die deze bevoegdheden inperken en legitimeren en (3) de manier waarop we kunnen voorkomen dat overheden voortdurend de grenzen opzoeken van hun bevoegdheden.
64. Materieel gezien is een transactie een straf in de zin van art. 6 EVRM. Ook de bestuurlijke sancties met een punitief karakter, zoals bijvoorbeeld de bestuurlijke boete, zijn materieel gezien straffen en bevestigen dat de meeste straffen niet door de strafrechter worden opgelegd. Zie ook Crijns (2014). Over het procesbeginsel Hildebrandt (2002).

Intussen heeft het Ministerie van Veiligheid & Justitie ingezet op een integrale 'Modernisering van het Wetboek van Strafvordering',[65] waarbij de nadruk van de strafvordering nog verder verschuift naar het voorbereidend onderzoek. Het gevolg hiervan is minstens dat allerhande vormen van monitoring en ander onderzoek, al dan niet gebaseerd op data-gestuurde risicoanalyses, de rechter niet zullen bereiken en dus door anderen getoetst moeten worden.[66] Juist bij toenemende inzet van politie-*agents* moet in een rechtsstaat de aanvechtbaarheid worden gekoesterd en veilig gesteld van de beslissingen die – grotendeels onder de radar – door (of op basis van) dergelijke systemen worden genomen.

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

65. Contourennota Modernisering Wetboek van Strafvordering, aangeboden aan de Tweede Kamer op 3 februari 2015, <http://www.rijksoverheid.nl/documenten-en-publicaties/brieven/2015/02/03/brief-concept-contourennota-modernisering-wetboek-van-strafvordering.html>, hierna aangehaald als Contourennota 2015. Vergelijk ook het preadvies van Knigge (1994), en de bespreking van de in 2014 door het Ministerie van Veiligheid en Justitie voorgestelde discussienota door Keulen (2014). Zie inmiddels het advies van de Raad voor de Rechtspraak (2015), onder meer verwijzend naar het rapport van de PG bij de Hoge Raad inzake de naleving van het recht bij strafbeschikkingen (Fokkens 2014).
66. Daaraan kleven grote risico's, zie bijvoorbeeld, over de omgang met bijzondere persoonsgegevens in het kader van de strafvordering: zie CBP (2015).

methodieken voorzag,[67] de Wetten Computercriminaliteit I (1993) en II (2006), en III (ligt nu voor),[68] en de Wet ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven (2007).[69] De voorgenomen modernisering van het wetboek moet worden toegejuicht voor zover het gaat om hernieuwde inzichtelijkheid, toegankelijkheid en systematische integratie van de eisen van effectiviteit en rechtsstatelijkheid.[70] Modernisering lijkt inmiddels een wat ouderwetse term.[71] 'Upgrade' zou meer bij deze tijd passen en expliciteren dat het gaat om een reconfiguratie die inspeelt op de veranderende omgeving en de eigen functionaliteit verbetert (en dus meer is dan een 'update'). Bovendien gaat het niet om een upgrade van de software maar van de 'firmware', dat wil zeggen van het meest stabiele onderdeel van het 'operating system' van het strafrecht, dat nauw verbonden is met de 'hardware' (de institutionele ondergrond, inclusief de Grondwet, en de organieke wetgeving inzake rechterlijke

67. De Wet BOB van 2000. Het ging met name om de invoering van de volgende bevoegdheden: observatie, infiltratie, pseudokoop, pseudodienst-verlening, stelselmatige informatie-inwinning, het betreden van een besloten plaats en het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel; de wettelijke regeling van de informant, de burgerinfiltrant en de burgerpseudokoop- of dienstverlening; een aangepaste regeling van de bevoegdheid tot het opnemen van telecommunicatie en het vorderen van inlichtingen; een nieuwe grondslag voor de toepassing van specifieke opsporingsbevoegdheden, te weten 'aanwijzingen' dat in georganiseerd verband ernstige misdrijven worden 'beraamd' of gepleegd en de regeling van het verkennend onderzoek. Wat betreft dat laatste is nieuw dat onder de opsporing worden gebracht: (1) bevoegdheden waarvoor geen redelijke verdenking wordt vereist en (2) bevoegdheden inzake strafbare feiten die nog niet gepleegd zijn en waar geen sprake is van een poging of voorbereidingshandeling.
68. Computercriminaliteit III beoogt te regelen: heimelijk onderzoek op afstand in een computer systeem (hacken), aanpassing regeling ontoegankelijk maken gegevens, decryptiebevel aan verdachte bij verdenking enkele zeer ernstige delicten (in de definitieve versie geschrapt), strafbaarstelling wederrechtelijk overnemen en 'helen' van gegevens. Het wetsvoorstel is op 22 december 2015 ingediend bij de Tweede Kamer, het is beschikbaar via < https://www.rijksoverheid.nl/actueel/nieuws/2015/12/22/wetsvoorstel-computercriminaliteit-bij-tweede-kamer-ingediend>.
69. In zijn Contourennota (2015:3) noemt de Minister ook nog de aanpassingen die zijn ingevoerd naar aanleiding van de resultaten van het Onderzoeksproject Strafvordering 2001, onder leiding van Knigge en Groenhuijzen: Wet OM-afdoening (Stb. 2006, 330), de regeling van de versterking van de positie van het slachtoffer (Stb. 2010, 1) en die van de deskundige (Stb. 2009, 33), Wet herziening regels betreffende de processtukken in strafzaken (Stb. 2011, 601) en de Wet versterking positie rechter-commissaris (Stb. 2011, 600).
70. Contourennota 2015. Voor commentaar op het eerder rondgestuurde discussiestuk zie bijvoorbeeld Keulen (2014) en het advies van de Raad voor de Rechtspraak (2015).
71. Het begrip modernisering kan verwijzen naar de transformaties die plaatsvonden na de industriële revolutie, en hangt dan samen met een bepaald soort vooruitgangsgeloof. In dat kader zou Beck's (1986) reflexieve modernisering ook hier van nut kunnen zijn. Beck richtte zich op het besef dat technologische vooruitgang inmiddels niet alleen problemen oplost maar ook nieuwe schept, waarbij catastrofale gevolgen niet zijn uitgesloten.

macht, advocatuur) en daarmee feitelijk de mogelijkheden bepaalt van de te implementeren software (nadere regelgeving, beleidsregels en protocollen voor de uitvoering).[72] De functionaliteit van het Wetboek van Strafvordering is genesteld in de constitutieve samenhang tussen de instrumentaliteit en de rechtsbescherming van het strafrecht als rechtsstatelijk georiënteerde omgang met criminaliteit. Dat betekent bijvoorbeeld dat 'modernisering' niet kan betekenen dat de wirwar van bestaande bevoegdheden op toegankelijke wijze gerangschikt worden, liefst hier en daar uitgebreid,[73] en voorzien van wat algemene clausules die zouden moeten waarborgen dat de hele zaak 'Straatsburg en Luxemburg proof' is.[74] Met name het voorstel om de proportionaliteit en de subsidiariteit als een bijkans magische formule toe te voegen in de hoop dat de praktijk daar wel weg mee weet, is problematisch en onzorgvuldig.[75] Het lijkt op een achteraf toegevoegde 'add-on' (in termen van de onli*f*e wereld) en we weten dat een 'add-on' meestal niet goed werkt omdat die de werking van een systeem vertraagt. Wie rechtsbescherming als onderdeel van de functionaliteit van het strafrecht ziet (dus niet als een bijkomende gedachte) moet die inbouwen in de diepste lagen van het systeem, zodat het deel uitmaakt van ieder onderdeel. *The devil is in the details*, dat geldt ook voor het strafrecht.

Zo'n add-on is des te hachelijker wanneer in beleidskringen de neiging bestaat om punitieve aspecten van de rechtshandhaving op te nemen in strafvordering, door het benadrukken van de preventieve werking van *strafvorderlijke* bevoegdheden. Het lijkt er soms op neer te komen dat het

72. Ach, 'update', 'upgrade', 'software', 'hardware' en 'operating system' zijn hier 'maar' metaforen. Uiteindelijk denken wij echter onvermijdelijk en steeds in metaforen (zij het vaak zo versleten dat we het metaforisch karakter niet meer herkennen, zie Ricoeur (1975) die de zaken naar mijn mening scherper en fundamenteler formuleert dan Lakoff en Johnson (2003). Daarom is het verstandig wanneer het om de inrichting van de samenleving gaat ons permanent te bezinnen op de inzet van metaforen. Het gebruik van metaforen als 'upgrade', 'firmware' etc. is er niet op gericht de werking van de samenleving gelijk te stellen aan die van de digitale infrastructuur (het blijven metaforen); het is wel gericht op erkenning van de transformaties van de ICT-infrastructuur die het recht mede vormt (zie hieronder hoofdstuk 4).
73. Met name ten aanzien van de inzet van 'heimelijke bevoegdheden' (de term 'bijzondere opsporingsbevoegdheden' wordt geschrapt). Het gaat bijvoorbeeld om de regeling van 'de stelselmatige vastlegging van persoonsgegevens op het internet, de inzet van een 'stille sms' of IMSI-catcher ter plaatsbepaling, of een tijdslot voor de uitvoering van een bevel tot het opnemen van vertrouwelijke communicatie (Contourennota 2015: 56)'.
74. Zo keert de eis van proportionaliteit en subsidiariteit in de Contourennota op een wel heel hoog abstractieniveau steeds weer terug, als een soort van bezweringsformule, die het stroomlijnen van de voorwaarden voor de inzet van bevoegdheden van een mensenrechtelijk vernisje moet voorzien. Zie Contourennota (2015:27-28, 42-45), met name in verband met voorlopige hechtenis en wat de Minister verdenkingscriteria noemt. De idee is dat deze beginselen in het tweede Boek, dat betrekking heeft op het Voorbereidend Onderzoek, worden gecodificeerd.
75. Zie ook: Raad voor de Rechtspraak (2015:10).

afdoen van zaken ter terechtzitting een uitzondering zou moeten blijven, omdat het duur is en veel gedoe geeft; alles wat in het voorveld van de zitting meegenomen kan worden is winst en dat houdt ook in dat de meeste zaken nooit ter zitting verschijnen. Denk aan de strafbeschikking,[76] aan het verkennend onderzoek dat zich onderscheidt doordat het niet is gericht op strafvorderlijke beslissingen, en denk alvast aan de inzet van politie-*agents* die op geaggregeerd niveau voorspellend en zo mogelijk op individueel niveau ondervangend zullen functioneren. In de bespreking van de eerste ervaringen met de nieuwe strafvorderlijke bevoegdheden in geval van aanwijzingen van het beramen of plegen van terroristische misdrijven, lezen wij dat (De Poot e.a. 2008:6):

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

Hier wordt onomwonden gesproken van de preventieve werking van dwangmiddelen en andere onderzoeksbevoegdheden. Gesteld wordt dat de afschrikkende werking van de straf geen indruk maakt op terroristen en dat de ernst van terroristische misdrijven niet toelaat te wachten tot het misdrijf is voltooid. Het gaat dus niet om de gebruikelijke doelen van de straf zelf, maar om de preventieve werking van vroegtijdig onderzoeken, bewijs verzamelen en ingrijpen – voordat sprake is van veroordeling en strafoplegging. Daarmee worden aspecten van de punitieve rechtshandhaving naar voren geschoven. Wanneer dat samenvalt met de inzet van *agents* raakt de punitieve rechtshandhaving gemakkelijk ingebed in de logica van semi-actuariële risico-instrumenten die zich met het voortschrijden der techniek ontpoppen als geavanceerde predictie- en mogelijk ook als pre-emptiemachines.[77]

Het is belangrijk om die vlucht naar voren te duiden in samenhang met verschuivingen in het opsporingsbegrip en complexe aanvullingen daarop in de vorm van het verkennend onderzoek.[78] Uit de aanpassing van de

76. Zeer kritisch daarover Fokkens (2014). In de Contourennota (2015: 57) wordt nader onderzoek en aanpassing van de wettelijke regeling aangekondigd.
77. De Nederlandse vertaling zou luiden: voorspel- en ondervangingsmachines.
78. Zie ook, zeer genuanceerd, de oratie van Borgers (2007).

definitie van het opsporingsbegrip (in 2007) volgt dat de eis van een verdenking (redelijk vermoeden) ten aanzien van een bepaalde persoon of een bepaald strafbaar feit niet meer noodzakelijk is om van opsporing te spreken (art. 132a WSv):[79]

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

Ook de bevoegdheden die mogen worden uitgeoefend op basis van aanwijzingen vallen kennelijk onder opsporing, hoewel zij wettelijk geregeld zijn als verkennend onderzoek ter voorbereiding van de opsporing.[80] Het verkennend onderzoek was overigens van begin af aan (in 2000) al mogelijk op basis aanwijzingen voor het *beramen* van misdrijven in

79. Aangepast bij de invoering van de Wet ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven, in 2007. De oude definitie (ingevoerd bij de Wet BOB in 2000) luidde: 'Onder het opsporingsonderzoek wordt verstaan het onderzoek onder leiding van de officier van justitie naar aanleiding van een redelijk vermoeden dat een strafbaar feit is begaan of dat in georganiseerd verband misdrijven worden beraamd of gepleegd, als omschreven in artikel 67, eerste lid, die gezien hun aard of samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren, met als doel het nemen van strafvorderlijke beslissingen.'
80. In de Memorie van Toelichting bij het Wetsvoorstel Wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven (Tweede Kamer, 2004-2005, 30 164, nr. 3:17) meldt de Minister dat het onderscheid is gelegen in het feit dat het verkennend onderzoek nog niet is gericht op het nemen van strafvorderlijke beslissingen, maar op de voorbereiding daarvan. Cleiren (2015) noemt als reden voor de uitbreiding van het bereik van art. 132a WSv de destijds nieuwe bevoegdheid van het preventief fouilleren in veiligheidsrisicogebieden met het oog op terroristische aanslagen. Over de inmiddels hallucinante verhouding tussen opsporingsonderzoek, voorbereidend en verkennend onderzoek, ook in relatie tot de strafvordering (het legaliteitsbeginsel van art. 1 WSv) en de strafrechtelijke handhaving van de rechtsorde (art. 13 Pw) zie Blom (2015a). De wijze waarop Van der Meij (2015) art. 132a WSv bespreekt lijkt mij niet te sporen met de manier waarop Cleiren en Blom de verhouding tussen verkennend onderzoek en opsporingsonderzoek bezien, nu deze laatsten anders dan Van der Meij menen dat het verkennend onderzoek niet onder de opsporing valt (maar onder de voorbereiding van de opsporing en voorbehouden aan opsporingsambtenaren). We zien uit naar verheldering.

georganiseerd verband (art. 126gg WSv).[81] Wie zich mijn zorg over de strafbaarstelling van een neiging tot strafbaar – of zelfs ongewenst – gedrag herinnert uit het voorgaande hoofdstuk over materieel strafrecht, zal begrijpen dat ik hier een bevestiging zie van de neiging om de strafvordering te richten op het voorkomen van strafbare feiten. Niet door met een straf op een reeds gepleegd strafbaar feit te reageren, maar door bepaalde gedragingen zoveel mogelijk te ondervangen. Hierdoor worden niet alleen de rechter en alle waarborgen waar die voor staat in vergaande mate buiten spel gezet, maar wordt de straf zelf schijnbaar vermeden. Enerzijds wordt de straf in formele zin (opgelegd door de strafrechter na het geding ter terechtzitting) steeds meer een uitzondering, anderzijds duiken de punitieve aspecten van de straf in materiele zin op in het voorveld van de bestraffing met name waar het gaat om afschrikking (preventie). Nog ernstiger is de tendens om de straf te vervangen door de ondervanging van ongewenst gedrag, hetgeen impliceert dat de categorie van de verdachte wordt opgerekt tot zo ongeveer alle burgers. Daarmee wordt de categorie van strafbaar gedrag gerelativeerd zodat die zo ongeveer alle ongewenst gedrag gaat omvatten, terwijl tegelijkertijd de idee van een aanspreekbaar rechtssubject samen met de idee van de straf als gedateerde, illusoire instituties kunnen worden vergeten.

Het is intussen niet mijn bedoeling om af te dingen op de preventieve werking van het strafrecht. Ik kan mij bovendien vele situaties voorstellen waarbij het ondervangen van strafbaar of ook ongewenst gedrag een publiek belang is. Dat gaat op bij terroristische aanvallen, maar ook bij belastingontduiking, pesten op het werk en het veel te vroeg buiten zetten van afval (dat vervolgens door meeuwen over de hele straat wordt verspreid). Dat wil echter niet zeggen dat het strafrecht het meest geëigende systeem is om het betreffende publieke belang te beschermen. De preventieve werking van het strafrecht zetelt in een specifieke samenhang van norm en handeling. Ten eerste de handeling waarbij een normschending strafbaar wordt gesteld, vervolgens de handeling waarbij diezelfde norm

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

wordt geschonden, tenslotte de handeling waarbij die normschending wordt bestraft. Op het moment dat normschendingen die niet strafbaar zijn gesteld (zoals beraming van een strafbaar feit), of dermate vaag zijn dat zij geen duidelijkheid verschaffen over welk handelen een schending vormt, toch voorwerp van opsporing lijken te worden, wordt de samenhang tussen strafrechtelijk beschermde normen en de gerechtvaardigde verwachtingen van de burger doorbroken. Hetzelfde geldt wanneer de reactie op een vermeende normschending bestaat uit opsporingshandelingen die geen duidelijke publieke bestraffing naar aanleiding van een publiek strafproces vormen, maar al dan niet succesvolle pogingen om normschendingen in kaart te brengen, te ondervangen en eventueel via een besloten procedure te bestraffen (Crijns 2014).

De preventieve werking van dat samenspel heeft niet zoveel van doen met de preventieve doelen van het strafrecht; het is meer een poging tot disciplinering (*nudging* en *priming*) dan een strafrechtelijk appel. Of daarmee het publieke belang van het terugdringen van bepaald handelen gediend is kan niet gemakkelijk worden vastgesteld. Handelen wordt hier namelijk als gedrag bezien; het krijgt niet de aandacht maar wordt afgedaan.[82] Uiteindelijk zal dit niet effectief zijn en strategisch gedrag oproepen van de burger, die zich immers niet serieus aangesproken voelt door een automatisch afgeschreven boete.[83]

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

*3.2 **Agents** van voorspelling en ondervanging*

Het Wetsontwerp Computercriminaliteit III omvat onder meer een nieuwe bevoegdheid die het voor de politie mogelijk maakt om onder specifieke voorwaarden rechtmatig op afstand binnen te dringen in computersystemen.

82. In zijn Nijmeegse oratie wijst Buruma (1996) op het belang van de aandacht van de strafrechter, die niet mag worden gedwongen haar aandacht dusdanig te verdelen dat die wordt afgeleid van de hoofdtaak (vaststellen van de strafbaarheid en de oplegging van straf). Aandacht is iets waar we zuinig op moeten zijn; het is een schaars goed, ook in het strafrecht. In de onlife wereld is onze (machinaal leesbare) aandacht inmiddels een te verhandelen gedragsmodus, die tijdens online veilingen aan de hoogstbiedende adverteerder wordt doorverkocht. Hier dringt zich het onderscheid op tussen aandacht als meetbaar gedrag en aandacht als handeling.
83. Dat was de conclusie van mijn proefschrift (Hildebrandt 2002).

Dit heeft – onder meer – te maken met de toenemende versleuteling van communicatie, die ertoe kan leiden dat alleen toegang tot gegevens voor en na de versleuteling (op de 'randapparatuur' van de gebruiker) de inhoud van communicatie beschikbaar maakt.[84] Uiteraard heeft het ook te maken de noodzaak om botnets te ontmantelen, gegevens en programma's ontoegankelijk te maken ten einde algemeen gevaar voor personen, goederen, diensten en infrastructuur te weren. Bij de ontmanteling van het Bredolab botnet werd reeds geëxperimenteerd met dit type remote control.[85] Mede dankzij aanhoudende maatschappelijke bevraging van de rechtmatigheid hiervan ligt nu een regeling voor die de betreffende bevoegdheid in het leven roept en normeert (art. 126nba WSv). Vooralsnog geldt deze regeling 'alleen' in geval van art. 67 WSv delicten (waarbij voor terroristische misdrijven de eis van een ernstige verdenking vervalt), mits sprake is van een ernstige inbreuk op de rechtsorde (een eis die in het nieuwe WSv zou moeten vervallen). Doel is het bepalen van de aanwezigheid van gegevens of van de identiteit of locatie van het geautomatiseerde werk of de gebruiker; het overnemen van gegevens die in het geautomatiseerde werk of een daarmee in verbinding staande gegevensdrager zijn of worden verwerkt;[86] of ook de ontoegankelijkmaking van gegevens. De bevoegdheid vereist een bevel van de OvJ na machtiging van de RC (die in noodgevallen mondeling mogen worden gegeven, met schriftelijke vastlegging achteraf, binnen drie dagen). In het nu voorgestelde art. 126uba WSv wordt vervolgens bepaald dat binnen mag worden gedrongen 'bij een persoon ten aanzien van wie uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat hij betrokken is bij het in georganiseerd verband beramen of plegen van misdrijven'. Hier vervalt de eis van ernstige verdenking eveneens en is 'betrokkenheid bij' voldoende, waarbij het bovendien kan gaan om het – in georganiseerd verband – 'beramen' van misdrijven (zonder verdere inperking). Wat betekent 'betrokkenheid bij het beramen van misdrijven in georganiseerd verband' (stoute jongens die zich voornemen gezamenlijk een supermarkt te beroven)? Bij wege van het nu voorgestelde art. 126zpa WSv wordt bovendien 'in geval van aanwijzingen van een terroristisch misdrijf' onderzoek op afstand mogelijk 'in een geautomatiseerd werk dat in gebruik is bij een persoon' (die dus zelfs geen verdachte hoeft te zijn). Rekening houdend met de voorgestelde ruime definitie van 'geautomatiseerd

84. Zie hierover – in relatie tot de veiligheids- en inlichtingendiensten Jacobs (2015).
85. Zie Koning (2012) en Oerlemans (2011).
86. Wat betreft de MvT sluit deze formulering niet uit dat onderzoek zal worden gedaan in servers die zich de facto buiten Nederland bevinden. Deze heikele kwestie roept veel vragen op, onder meer betreffende het raakvlak tussen cybercriminaliteit en cyberoorlog, die ik – gezien de 'beperkte' omvang van dit preadvies – buiten beschouwing moet laten. Zie bijvoorbeeld B.-J. Koops en Goodwin (2014), Klip en Massa (2010), Hildebrandt en Koning (2012), Hildebrandt (2013c).

werk' in art. 80sexies WSr,[87] lijkt deze bevoegdheid minst genomen 'overinclusive' zoals de Engelsen het zo mooi zeggen. Dat politie en justitie deze bevoegdheid wensen is begrijpelijk en de regeling lijkt voorzien van keurige waarborgen. Mijn punt is echter vooral dat we de omvang van de implicaties van toepassing van 'remote hacking' door politie-*agents* pas kunnen beoordelen als we beseffen dat de 'opgehaalde' gegevens bij zullen dragen aan voortgaande data-gestuurde interventies, net als bij via interceptie verkregen gegevens. Daarbij ligt voor de hand dat op enig moment uitbreiding van de hackbevoegdheid zal worden bepleit voor misdrijven die met een zekere waarschijnlijkheid beraamd zullen worden. Dat laatste zou betekenen dat de functionaliteiten van politie-*agents* de toepassing van dit type bevoegdheden in vergaande mate zullen bepalen.[88]

De ontwikkeling van data-gestuurde systemen met het oog op de opsporing vindt – voor zover bekend – plaats in de context van het Internet Recherche & Onderzoek Netwerk (iRN),[89] een onderdeel van de Nationale Politie, waarin naast de politie onder meer ook de Belastingdienst, de Nationaal Coördinator Terrorisme Bestrijding en Veiligheid, de UVW, de Nederlandsche Bank, en diverse Nederlandse Gemeentes samenwerken met gespecialiseerde private IT bedrijven.[90] Het iRN functioneert als een beveiligde Internet Service Provider voor en van de overheid. Het biedt de mogelijkheid om platformen in te richten waarbinnen verschillende modules (deelprogramma's) kunnen worden ontwikkeld en uitgeprobeerd.

87. 'Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken.' Zie ook paragraaf 3.4.
88. Van Noort en Kist (2015) beschrijven predictieve politie technologie, die bijvoorbeeld volgens IBM aan de Nederlandse politie wordt verkocht. Het is precies dat type technologie dat aanwijzingen van het beramen van een terroristisch misdrijf kan opleveren, op basis van gegevens verkregen uit interceptie en binnendringen op afstand.
89. Uiteraard wordt ook en juist binnen de veiligheidsdiensten gewerkt aan data-gestuurde systemen, bijvoorbeeld ARGO II, zie bijvoorbeeld <https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/inhoud/inlichtingen-en-veiligheid/gegevens-verwerken-met-argo-ii>. Uitwisseling tussen de diensten enerzijds en politie en justitie anderzijds vindt plaats in het kader van een ambtsbericht (op basis van art. 36 en 38 Wiv 2002, en de *Handleiding informatieverstrekking van en door de AIVD en de MIVD*), zie Brinkhof (2014), en Vervaele (2005).
90. Over iRN bijvoorbeeld de websites van Committ (een private publieke samenwerking die naar eigen zeggen 'unites academic research and (non-)profit organizations in ICT. It is a use-inspired fundamental ICT-research in well-being and well-working, in public safety, in science, in information services and search, and with applications in culture, agriculture, and health care.'): <http://www.commit-nl.nl/universities/politie-gelderland-zuid> en Flusso (naar eigen zeggen: 'een maatwerk applicatieontwikkelaar en ICT dienstverlener die meedenkt en adviseert over de architectuur van applicaties.'): <http://www.flusso.nl/Werk/big_data-nationalepolitie/>. Tevens Roessingh (2013), Bert-Jaap Koops e.a. (2012).

Meer specifiek voor politie en justitie is binnen iRN het iColumbo platform gebouwd met als doel het analyseren van 'open en big data' ten einde inzicht te verkrijgen in specifieke criminaliteitspatronen (bijvoorbeeld witwassen, mensensmokkel, drugssmokkel, geweld, terrorisme)[91] dan wel het monitoren en profileren van een specifiek persoon of een specifieke groep personen, in verband met gepleegde of mogelijk te plegen strafbare feiten. Het mag duidelijk zijn dat steeds wanneer onderzoek plaats vindt dat een min of meer ernstige inbreuk impliceert op een of meer grondrechten, hiervoor min of meer specifieke, wettelijk bevoegdheden, voorzien van proportionele waarborgen noodzakelijk zijn. Ik kom daarop terug in paragraaf 3.3 en hoofstuk 4.

In het – oorspronkelijk kennelijk geheime – TNO rapport *Herkenning van digitale informatie* uit 2010 worden een aantal toepassingen beschreven voor het automatisch detecteren van specifieke informatie: (bijna)-identieke bestanden of delen daarvan; verborgen boodschappen; personen; verdacht gedrag; objecten, zoals logo's of auto's; tekst in beeld/video; opvallend internet-/netwerkverkeer; netwerken van personen (sociale netwerken); taaluitingen.[92] Het onderzoek was gericht op de beschikbaarheid en geschiktheid van bestaande en nieuw te ontwikkelen software modules die op basis van machinaal leren en andere vormen van data analyse relatief snel en relatief betrouwbaar relevante informatie afleiden uit grote gegevensbestanden (zowel tekst, geluid, als plaatjes, internetverkeer en sociale netwerken). De uitkomsten van het onderzoek zijn niet opzienbarend, de beschreven applicaties lijken trouwhartig de stand der techniek te volgen. De onderzoekers signaleren daarbij allerlei praktische incompatibiliteiten, bijvoorbeeld wijzend op het feit dat bestaande commerciële producten niet noodzakelijkerwijs aansluiten bij de onderzoeksbehoeften van de opsporende of inlichtingen verzamelende overheden.[93] Dat wil niet zeggen dat met dit type technieken geen verrassende voorspellingen kunnen worden gedaan en patronen kunnen worden blootgelegd. Het lijkt erop alsof de besproken toepassingen niet meer doen dan automatisch doorzoeken wat anders met de hand was doorzocht, maar dat is zeker niet het geval. Enerzijds omdat de mankracht om de voortdurend exponentieel toenemende datastromen te doorzoeken ontbreekt, hetgeen individuele datapunten – zelfs wanneer overheden ze verzamelen en opslaan – nog

91. Dit is mijn inschatting, ik heb geen expliciete informatie kunnen detecteren vanwege de overheid waarin uit de doeken wordt gedaan wat precies wordt onderzocht. Maar dat laat zich tot op zekere hoogte raden.
92. TNO (2010: 3), dit rapport werd kennelijk pas openbaar gemaakt op de website van de NCTB na een beroep op de Wob van Rejo Zengers, zie <https://rejo.zenger.nl/inzicht/herkenning-digitale-informatie-en-fingerprinting-episode-2/> en <https://www.nctv.nl/onderwerpen-a-z/herkenning-digitale-informatie-en-fingerprinting.aspx>.
93. TNO (2010:109-11) met een bijzonder nuttige samenvatting van wat de onderzochte technologieën nu wel en niet vermogen, en een serie aanbevelingen.

steeds redelijk onvindbaar maakt. Met dit soort software wordt die onvindbaarheid echter op zijn minst gerelativeerd. Het is belangrijk dat burgers zich daarvan bewust zijn. Anderzijds is het mogelijk om via machinaal leren nieuwe patronen te ontdekken; om als het ware nieuwe hypothesen te ontwikkelen over de samenhang tussen criminaliteit, gedrag, gebouwde omgeving, weersomstandigheden, bestedingscapaciteit, buurt, leeftijd, huwelijkse staat, genetisch profiel, energieverbruik, opleiding van de ouders, kinderziektes, reisgedrag en zo meer. Waar dit soort hypotheses vroeger door sociale wetenschappers werden bedacht, ontwikkeld en vervolgens getest aan de hand van een of meer steekproeven, is het nu mogelijk om toepassingen te bouwen die op basis van mathematische en statistische technieken zelfstandig verbanden leggen en aldus hypotheses genereren waar wij wellicht nooit op waren gekomen. Door de beschikbaarheid van schier eindeloze hoeveelheden gedragsdata (deels vrijwillig in de vorm van postings door gebruikers van sociale media vrijgegeven) is het nu bovendien mogelijk de betrouwbaarheid van die hypotheses te testen, en bijvoorbeeld irrelevante correlaties weg te filteren. We zijn hier terug bij Pentland's sociale fysica. Er is namelijk geen sprake van een theorie die verklaart waar deze correlaties op zijn gebaseerd; het gaat hier niet om oorzaken of redenen voor gedrag maar om statistische samenhang. Het gaat niet om handelen maar om gedrag, niet om *homo sapiens* maar om *homo behavioralis*. Dat is interessant, maar niet meer dan een beginpunt van nader onderzoek dat zich wel degelijk zou moeten bekommeren om de betekenis van het gedrag als handeling van een individueel persoon. Binnen het strafrecht is die persoon een rechtssubject en als zodanig ook aanspreekbaar; niet alleen maar een object van onderzoek dat gelaten moet afwachten welke correlaties haar status als verdachte of mogelijk verdachte, potentieel mogelijk verdachte of eventueel potentieel mogelijk verdachte zullen bepalen.[94] Naast dit type bezwaren roep ik in herinnering dat 'de wet van de grote aantallen' niet overal en altijd opgaat, en dat op eenzelfde dataset verschillende algoritmes getraind kunnen worden met heel verschillende uitkomsten.[95]

94. In zijn Contourennota (2015:41-2) wil de Minister de verdenkingscriteria terugbrengen van 10 naar 4. Hij verwart daarbij overigens de voorwaarden voor de toepassing van bepaalde dwangmiddelen (zoals dat sprake moet zijn van een verdenking van een strafbaar feit waarvoor voorlopige hechtenis is toegelaten of dat sprake moet zijn van een ernstige inbreuk op de rechtsorde) met de graad van verdenking (aanwijzingen, vermoeden, redelijk vermoeden, ernstige bezwaren). Het is opmerkelijk dat daarbij de voorwaarden en criteria vooral naar beneden worden bijgesteld. Zo wenst hij de eis dat sprake moet zijn van een ernstige inbreuk op de rechtsorde maar gewoon af te schaffen omdat hij die eis vaag acht.
95. Zie hierboven noot 9 en par. 5.

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

Uit de informatie die beschikbaar is over het iRN en iColumbo leid ik af dat het in kaart brengen van geaggregeerde en gepersonaliseerde patronen plaats vindt (of zal vinden) op basis van daarmee gelieerde metadata (locatie, telecommunicatie verkeersgegevens), openbaar beschikbare gegevens (gepost op sociale media of anderszins op internet gepubliceerd), in combinatie met gegevens uit andere bestanden (GBA, energieverbruik, sociale zekerheid, belastingaangifte, meldpunt witwassen en zo meer). In hoeverre de bevoegdheid bestaat om gegevensbestanden te koppelen hangt af van de vraag of daarvoor een wettelijke grondslag is,[96] en of is voldaan aan het doelbindingsbeginsel. Dat laatste is binnen het strafrecht bekend als het verbod van *detournement de pouvoir*, dat in beginsel uitsluit dat resultaten verkregen op basis van een specifieke bevoegdheid worden gebruikt voor een doel waarvoor die bevoegdheid niet was verleend. Ik kom daarop terug in paragraaf 3.4.

Het iRN is geen uitvinding van Google of DARPA, zoveel is duidelijk.[97] In het licht van hetgeen grote technologiebedrijven en financieel goed bedeelde onderzoeksinstituten van defensie in de VS intussen uitvinden en ontwikkelen moeten we aannemen dat de overgang van informatie systemen naar data-gestuurde beslissystemen ook binnen de Nederlandse opsporing tot initiatieven in die richting zal leiden. Ik breng in herinnering

96. Bijvoorbeeld in het kader van het verkennend onderzoek, waar art. 126hh WSv de bevoegdheid toekent om gegevensbestanden te vorderen van private of publieke partijen en deze te koppelen en bewerken, waarbij lid 2 eventuele beperkingen uit de WPg buiten toepassing verklaart, zie Blom (2015b). Hiervoor is dan wel een machtiging nodig van de rechter-commissaris.
97. DARPA staat voor Defense Advances Research Projects Agency (onderdeel van Defensie in de VS), die de voorganger van het internet (ARPA-net) uitvond, en in het kader van de 'robotics challenges' aan de wieg stond van de zelfrijdende auto, cf. Markoff (2015, 2015a). Zie <http://www.darpa.mil>. Google investeert in de high speed ontwikkeling van intuïtieve herkenning van objecten en concepten op basis van ongecontroleerd machinaal leren, met spectaculaire resultaten, zie Hern (2015) en <http://googleresearch.blogspot.co.uk/2015/06/inceptionism-going-deeper-into-neural.html>.

dat het mij in dit preadvies niet zozeer gaat om informatieverwerking maar om *agents*, dat wil zeggen systemen die hun omgeving niet alleen waarnemen maar daarin ook ingrijpen en in toenemende maat ook kunnen leren van de feedback. Dat is op dit moment – zo lijkt het althans[98] – nog niet aan de orde binnen de opsporing. Het punt is dat alles erop wijst dat het binnenkort wel aan de orde is en dat het in dit geval niet verstandig is om af te wachten en de put te dempen als het kalf verdronken is. Wanneer *agents* eenmaal ontworpen, getest en in omloop zijn gebracht zal het niet eenvoudig zijn om de specifieke combinatie van instrumentaliteit en rechtsbescherming in te bouwen die noodzakelijk is voor een verantwoorde strafvordering. Vandaar het belang van juridische bescherming by design, nader te bespreken in hoofdstuk 4.

3.3 Aantasting van grondrechten

3.3.1 Het vertekende beeld van de weegschaal

Het beeld van de weegschaal keert altijd weer terug in het recht. En te-recht. Over de misleidende retoriek van de weegschaal wordt intussen regelmatig de klok geluid.[99] Ook dat is terecht. In de strafvordering keert de noodzaak tot afweging voortdurend terug. Ten eerste een afweging van de belangen van derden tegen die van de verdachte en die van 'de maatschappij'; denk aan getuigen, maar ook aan eventueel potentieel verdachten of aan iedereen[100] die op enig moment kan worden gemonitord omdat politie-*agents* ergens een mogelijk verband ontwaren. Ten tweede een afweging van de belangen van de verdachte tegen die van 'de maatschappij'; denk aan vrijheidsbenemende maatregelen in het kader van de maatschappelijke veiligheid. Ten derde het belang van het strafrechtelijk onderzoek tegen de belangen van de verdachte; denk aan vluchtgevaar, of vernietiging van bewijsmateriaal. Ten vierde moeten vaak belangen worden afgewogen tegen een of meer fundamentele rechten; denk aan het belang van de opsporing tegen het belang van privacy, het belang van een redelijk zicht op in de toekomst te plegen strafbare feiten tegen belangen als privacy, non-discriminatie en vrijheid van informatie. Ten vijfde en ten laatste blijken onderscheiden fundamentele rechten in concrete situaties vaak met elkaar te botsen en dus alweer om afweging te vragen.

98. Justitie is niet geneigd inzicht te geven in de gebruikte technologie, zie Van Noort en Kist (2015).
99. Zie bijvoorbeeld de verzuchting van Leyten (1997) die het woord afweging niet meer wilde horen. En de meesterlijke wijze waarop Waldron (2003) de retorische kunstgrepen fileert waarmee de weegschaal allerhande onrecht rechtvaardigt.
100. Iedereen moet hier worden gelezen als het Engelse *anybody*, niet als *everybody*.

Hier wil ik kort vijf punten maken, om aan te geven dat een juridische afweging complex is en vooringenomenheid of ongerechtvaardigde ongelijkheid kan verhullen (Waldron 2003, Hildebrandt 2013d). Allereerst is de mogelijkheid om belangen af te wegen tegen rechten niet evident; zij kunnen niet zomaar vergeleken worden. Daarnaast wordt vaak gesuggereerd dat vrijheid een *individuee*l recht of belang zou zijn, terwijl veiligheid een *collectief* recht of *publiek* belang is; dit is evident een verkeerde manier om het debat over afwegingen te 'framen', nu beiden zowel individuele als collectieve, publieke dimensies hebben. In de derde plaats wordt de vrijheid van de ene groep vaak afgewogen tegen de veiligheid van andere groepen; de vrijheid van migranten wordt bijvoorbeeld ingeperkt opdat autochtonen zich veilig voelen. Ten vierde ziet de weegschaal op evenwicht, niet op een trade-off; een trade-off is alleen aan de orde als *noodzakelijkerwijs* vrijheid moet worden ingeleverd om veiligheid te bekomen. Tenslotte, wanneer een trade-off onvermijdelijk is moet de daarmee gemoeide schending van grondrechten worden gecompenseerd (de weegschaal!) door het toekennen van effectieve rechten aan degene wiens grondrecht wordt geschonden. Bij de mogelijke aantasting van of inbreuken op grondrechten speelt de proportionaliteit een prominente rol.[101] Het lijkt er wel eens op dat het invoegen van de spreuk 'rekening houdend met proportionaliteit en subsidiariteit' voldoende is om inbreuken en mogelijke inbreuken bij voorbaat en achteraf te bezweren als zijnde redelijk, zo niet onvermijdelijk. Bij de analyse van de impact van politie-*agents* op relevante grondrechten moeten deze vijf punten in het achterhoofd worden gehouden; het gaat zelden of nooit om een simpele afweging van het ene belang of recht tegen het andere.

3.3.2 De onschuldpresumptie

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

Een ander aspect van de onschuldpresumptie betreft de rechtsgevolgen die zijn verbonden met de status van 'verdachte'. Het gaat daarbij om de wijze waarop deze wel en niet bejegend mag worden. In het verlengde daarvan gaat het ook om de status van niet-verdachten die in het kader van

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

de strafvordering in zeer brede zin op het netvlies van politie en justitie verschijnen. Daarbij doet zich de vraag voor of het verstandig is daarbij uit te gaan van de stelling dat we weliswaar niet iedereen tegelijk kunnen verdenken maar ten minste bereid moeten zijn om in beginsel om het even wie te verdenken. De stelling zou kunnen verwijzen naar het beginsel dat bij de opsporing en vervolging van strafbare feiten geen sprake mag zijn van vooringenomenheid, ook en juist wanneer de verleiding daartoe groot is. De stelling kan ook anders worden gelezen, namelijk dat de inzet van politie-*agents* het mogelijk maakt om iedere burger in beginsel te bezien als een potentiele verdachte. In paragraaf 3.2 sprak ik van een status als verdachte of mogelijk verdachte, potentieel mogelijk verdachte of eventueel potentieel mogelijk verdachte. In juridische zin is dat een hachelijke zaak, want alleen de verdachte heeft een juridische status, nu de kwalificatie van 'verdachte' een aantal rechtsgevolgen heeft die haar vaak in een betere positie brengen dan bijvoorbeeld een getuige of zelfs een slachtoffer (bijvoorbeeld het zwijgrecht en andere rechten die voortvloeien uit het *nemo tenetur* beginsel, en de inzage in processtukken die samenhangt met de interne openbaarheid en de vereiste *equality of arms*). Dergelijke rechtsgevolgen zijn niet toegekend aan degene die op basis van data-analyse tot een risicogroep behoort die bijzondere aandacht krijgt, dat wil zeggen nadere observatie of verdergaand onderzoek naar reisgedrag, sociale media netwerk-analyse, energieverbruiksgedrag en zo meer. Het is wel zo dat op basis van de Wet politiegegevens (Wpg) een aantal rechten en plichten zijn verbonden aan het verwerken van de persoonsgegevens van zo'n mogelijk, potentieel mogelijk of eventueel potentieel mogelijk verdachte.[102] De Wpg onderscheidt volgens de *Aanwijzing Wet Politiegegevens en de rol van de Officier van Justitie* 'twee verschillende vormen van doorzoeken van politiegegevens: geautomatiseerd vergelijken (art. 8 lid 2, 11 lid 1, 11 lid 2 en 12 lid 4 Wpg) en in combinatie verwerken (art. 8 lid 3 en 11 lid 4)'.[103] Terwijl de Wpg niet uitlegt wat hieronder moet worden verstaan gaat de *Aanwijzing* uit van het volgende:[104]

> Geautomatiseerd vergelijken: het met een binaire zoeksleutel van (een)trefwoord(en) zoeken van bepaalde politiegegevens. Het resultaat van deze gerichte zoekslag is een uitkomst van hit / no hit. Gecombineerd verwerken: zonder binaire zoeksleutel binnen (een selectie van) beschikbare politiegegevens zoeken naar verbanden. Het resultaat van deze vrije zoekslag is een verzameling van gegevens die voldoen aan bepaalde gemeenschappelijke kenmerken. Deze gemeenschappelijke kenmerken kunnen een profiel van indicatoren of bepaalde kenmerken (trefwoorden) inhouden. Het zoeken met een com-

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

> plex en/of uitgebreid profiel met indicatoren of kenmerken dat is verkregen met een gecombineerde verwerking dient weer gezien te worden als een geautomatiseerde vergelijking. [H]et zoeken met gemeenschappelijke kenmerken [kan] een grote inbreuk op de privacy opleveren en deze verwerking [valt] daarmee snel onder de verwerkingsdoeleinden van art. 9 en 10 Wpg, [w]aaruit veelal nog grotere inbreuken op de privacy voortvloeien.

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

Ik zou hier dan ook wel van *agents* durven spreken, voor zover deze systemen zelfstandig beslissen welke personen in aanmerking komen voor stelselmatige gegevensverwerking (dan wel bepalende invloed hebben op een bijna-automatische beslissing hieromtrent van een opsporingsambtenaar). Dankzij dit soort machinaal leren kan iemand op basis van slimme algoritmes ingedeeld raken in een categorie van nader te monitoren personen. Hoewel het belang van het onderzoek zich wel zal verzetten tegen het verstrekken van profieltransparantie aan specifieke individuen is het toch zaak om inzicht te geven in de vraag of en zo ja, in welk opzicht *men* kan worden geprofileerd.

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

Hoe verhouden deze – merendeels heimelijke – operaties zich nu tot de onschuldpresumptie?[105] Om te beginnen is het goed om de verhouding tussen de onschuldpresumptie als *vermoeden van onschuld* en de verdenking als redelijk *vermoeden van schuld* te bezien.[106] De eerste betreft een regel die het handelen van overheidsdienaren normeert, de tweede betreft een voorwaarde voor het uitoefenen van een aantal bevoegdheden die mogelijk inbreuk maken op grondrechten. In die zin zijn beide niet met elkaar in strijd; het is eerder zo dat de onschuldpresumptie het complement of tegenwicht vormt van de verdenking. Omdat *een ieder* in strafrechtelijke zin voor onschuldig moet worden gehouden totdat de schuld aan een strafbaar feit in rechte is vastgesteld, zal een redelijk vermoeden de presumptie als het ware relevant maken en de gevolgen van dat vermoeden normeren. Dat hangt samen met het feit dat het redelijk vermoeden van schuld lange tijd de enige ingang was voor het toepassen van dwangmiddelen, die niet met punitieve interventies verward mogen worden. Precies vanwege de onschuldpresumptie mogen strafvorderlijke bevoegdheden uitsluitend worden uitgeoefend met het oog op de bewijsvergaring, de onttrekking aan het verkeer, het voorkomen van beïnvloeding van getuigen, vluchtgevaar, en het voorkomen van nog te plegen strafbare feiten. Dwangmiddelen dienen niet de specifieke of generale preventie die uitgaat van de afschrikkende werking van de straf, noch de vergelding of de genoegdoening die immers allemaal inherent zijn aan de punitieve werking van de straf.

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

105. Zie voor een overzicht van argumenten omtrent de inhoud en reikwijdte van de onschuldpresumptie in juridische en ethische zin Mackor en Geeraets (2013). Ik spits hier toe op de relevantie voor de toepassing van dwangmiddelen en de inzet van *agents* en laat de andere aspecten van de presumptie grotendeels buiten beschouwing (bijvoorbeeld de strafrechtelijke bewijslastverdeling en het verbod om publiekelijk uitspraken te doen over de schuld van een verdachte die ter zake (nog) niet is veroordeeld of is vrijgesproken (bijvoorbeeld wegens gebrek aan bewijs). Zie ook Vitkauskas (2012) voor de relevante jurisprudentie van het EHRM.
106. Vergelijk ook Packer (1968):161-162 en 167), die onderscheidt tussen *factual guilt* ('het gedaan hebben') en *legal guilt* ('aan alle voorwaarden voor strafbaarheid hebben voldaan, zoals vastgesteld door de rechter na een eerlijk proces'), cf. Hildebrandt (2002:341-342).

maken, evenals de vraag wat zo'n toepassing dan zou inhouden. Uit de jurisprudentie van het EHRM blijkt dat de onschuldpresumptie ook geldt voordat sprake is van een 'criminal charge',[107] ook al lijkt daarover geen overeenstemming te zijn binnen de doctrine.[108] Daarbij gaat het echter vaak om uitspraken inzake de schuld van een verdachte of vrijgesprokene,[109] en niet om de beslissing dat een bepaald persoon 'mogelijk betrokken' is bij een of meer reeds gepleegde, beraamde of nog te plegen strafbare feiten op basis van onderzoek van politiegegevens.

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

In dat verband is het goed kennis te nemen van de concept Richtlijn Onschuldpresumptie,[110] die onder 'Toepassingsgebied' stelt:

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

Zolang strafvorderlijke bevoegdheden zich beperken tot verdachten of personen ten aanzien van wie een vervolgingsbeslissing is genomen lijkt dit een zinnige inperking van de reikwijdte van de onschuldpresumptie. Wanneer echter op grote schaal risicoanalyses worden uitgevoerd op 'big

107. Het Hof hanteert daarbij een materieel verdenkingscriterium, cf. EHRM, 21 december 2000, nr. 34720/97 (Heaney and McGuinness v. Ireland), r.o. 41; EHRM, 27 november 2008, nr. 36391/02 (Salduz v Turkey) r.o. 50 en 52; EHRM, 14 oktober 2010, nr. 1466/07 (Brusco v. France) r.o. 47; het is niet doorslaggevend of justitie iemand formeel als verdachte kwalificeert, maar of zij de persoon de facto verdenkt.
108. Zie bijvoorbeeld Weigend (2013:196) over de traditionele betekenis van de onschuldpresumptie: 'a person charged with a crime is to be treated as if he had not committed that crime until the court has found him guilty.' In de Nederlandse context zou het betekenen dat de onschuldpresumptie pas relevant wordt vanaf het moment dat een vervolgingsbeslissing is genomen.
109. Bijvoorbeeld EHRM 25 maart 1983, nr. 8660/79 (Minelli v. Switzerland) r.o. 25-41; EHRM, 10 februari 1995, nr. 15175/89 (Allenet de Ribemont v. France) r.o. 39-41.
110. Brussel, 27.11.2013, COM(2013) 821 final, Voorstel voor een Richtlijn van het Europees Parlement en de Raad inzake de versterking van bepaalde aspecten van het vermoeden van onschuld en van het recht om in strafprocedures bij het proces aanwezig te zijn, p. 6 punt 15, (zie ook art. 2 van de concept Richtlijn).

en open data' om zicht te krijgen op criminaliteitspatronen die vervolgens worden toegepast op niet-verdachten, ten einde te beslissen wie in aanmerking komen voor stelselmatige gegevensverwerking,[111] lijkt het moment gekomen om de relevantie van de onschuldpresumptie voor alle burgers wier gegevens worden verwerkt te benadrukken. Dit roept de interessante vraag op of de onschuldpresumptie niet voor alle burgers geldt of hoort te gelden, zoals ik hierboven eigenlijk al formuleerde door te spreken van *een ieder*, geheel los van enigerlei onderzoek of verdenking.[112] In dat geval vallen a t/m d zonder meer binnen het bereik van de presumptie en gaat het er meer om wat deze in onderscheiden omstandigheden betekent. Of nog concreter, welke rechtsgevolgen de presumptie in ieder van de genoemde gevallen heeft. Ik breng in dat verband de articulatie van de strafrechtelijke bewijslastverdeling onder de aandacht, zoals in de concept Richtlijn Onschuldpresumptie geformuleerd als uitvloeisel van de presumptie (art. 5, inzake bewijslast en vereiste bewijsstandaard):[113]

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

111. Die beslissing wordt in de Contourennota (2015:56) aangemerkt als een nieuw in te voeren en te normeren strafvorderlijke bevoegdheid, naar analogie van de stelselmatige observatie, waarbij de Contourennota spreekt van 'stelselmatige vastlegging van persoonsgegevens op het internet' zonder aan te geven wat daaronder precies moet worden verstaan en hoe normering plaats vindt. Zie bijvoorbeeld Oerlemans en Koops (2012), die overigens van mening verschillen over de vraag of gegevens die zich achter een wachtwoord of registratie bevinden onder openbaar toegankelijke gegevens mogen worden begrepen.
112. Zie Duff (2013:171) over verschillende varianten van de presumptie: 'Some argue that the PoI [presumption of innocence, mh] operates only within the trial, as a rule that lays the burden of proof on the prosecution. Others argue that it applies more broadly: for instance that it incorporates all the demands of due process; that it applies to pre-trial detention as well as to the trial; that it is implicated if samples of DNA are retained even from those who have not been convicted; that it might have implications for the process of criminalization; that it is an aspect of a broad "principle of civility" that governs our civic dealings with each other.'
113. Sinds jaar en dag, maar zeker sinds Salabiaku (EHRM 7 oktober 1988, Serie A, no. 141-A) wordt een objectieve delictsomschrijving bij minder ernstige strafbare feiten geduld, mits de verdediging de kans heeft het daarmee gegeven schuldvermoeden te weerleggen.

3. De lidstaten zorgen ervoor dat, wanneer de procesrechter de schuld van een verdachte of beklaagde onderzoekt en er gegronde twijfel bestaat over de schuld van de betrokkene, deze wordt vrijgesproken.

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

Bijkomende vraag is of die grotere kans op schending van een strafrechtelijk beschermde norm in geval van *overtredingen* mag leiden tot een omkering van de bewijslast in de zin van art. 5 lid 2 van de concept Richtlijn ten aanzien van de oplegging van een boete? Of kan het zijn dat dit toch te ver gaat, maar dat op enig moment wel degelijk strafvorderlijke bevoegdheden kunnen worden uitgeoefend in het kader van een verder uitgebreid verkennend onderzoek – ook al is geen sprake van een reeds gepleegd, gepoogd, voorbereid of beraamd strafbaar feit? Absurd? Gezien de gestage verzelfstandiging van het voorbereidend onderzoek, de reeds bestaande mogelijkheid in te grijpen ingevolge aanwijzingen dat misdrijven worden beraamd

en de inzet van politie-*agents* lijkt me deze wending niet ondenkbaar. Maar wel evident in strijd met de onschuldpresumptie.

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

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

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

sowieso vaak sterk ingeperkt,[115] en wie heeft de tijd en de middelen om bij voortduring de gang naar de rechter te bewandelen voor allerlei lichte straffen.[116] Ook daarom is het zaak de onschuldpresumptie in herinnering te roepen en te erkennen dat met de voortgaande verzelfstandiging van het voorbereidend onderzoek de rechtsgevolgen van de toepassing van de onschuldpresumptie een belangrijk tegenwicht kunnen gaan vormen als het gaat om buitengerechtelijk onderzoek en buitengerechtelijke bestraffing. Cruciale vraag is dan wel wie de naleving van strafvorderlijke normen kan toetsen als de rechter hier niet aan te pas komt.

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

De rechten in data, bestanden en methoden bestaan uit de fundamentele rechten op gegevensbescherming, privacy, vrijheid van informatie, het auteursrecht (op software en op databanken), het sui generis recht op databanken en soms wellicht het patentenrecht (op software en hardware). Al deze rechten zijn in beginsel absolute rechten in die zin dat ze tegenover

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

een ieder kunnen worden gehandhaafd.[117] Dat betekent uiteraard niet dat deze rechten absoluut zijn in de zin van onbeperkt. Het feit dat het om absolute rechten gaat impliceert ook niet noodzakelijkerwijs dat het exclusieve rechten zijn in de zin dat de rechthebbende in beginsel het exclusieve recht heeft om het uitsluiting van alle anderen over de data, bestanden en methoden te beschikken. Dat is overigens wel het geval bij de IP-rechten, maar dat komt dus niet omdat het absolute rechten zijn in bovengenoemde zin: handhaafbaar tegenover een ieder. Wanneer de rechthebbende haar beschikkingsrecht door middel van een overeenkomst inperkt kan daar overigens een relatief recht uit voortvloeien, bijvoorbeeld een licentie om een ebook te downloaden of een licentie om persoonsgegevens voor een specifiek doel te gaan verwerken.[118]

Met name het recht op gegevensbescherming wordt ten onrechte vaak gekwalificeerd als een soort van eigendomsrecht, alsof het recht om gegevens te verwerken exclusief zou toekomen aan het data subject.[119] Dat is volkomen onzinnig. Het zou betekenen dat het verwerken van een gegeven zoals mijn naam een exclusief recht van mijzelf zou zijn, terwijl de naam nu juist een manier is om mij aan te spreken en aan te duiden binnen enigerlei vorm van gezelschap. Robinson Crusoë had geen naam (nodig) voordat Vrijdag arriveerde.

Het grondrecht op gegevensbescherming is een bundel rechten die onder meer de verhouding regelt tussen een data subject (de identificeerbare natuurlijke persoon naar wie een data verwijst) en een of meer data controller(s) (degene die het doel en de middelen van een verwerking bepaalt).[120] Binnen die verhouding *kan* het fundamentele recht op gegevensbescherming (van het data subject) ook beschikkingsrechten omvatten, namelijk daar waar het data subject het verwerken van haar gegevens kan toestaan (en dus ook kan weigeren) of een overeenkomst kan sluiten omtrent het gebruik van de gegevens (dataverwerkingslicentie), zolang die verwerking aan de overige eisen van het gegevensbeschermingrecht voldoet.[121]

---

117. Pitlo e.a. (1995). Het complement van absolute rechten zijn relatieve rechten, die niet tegenover een ieder maar alleen tegenover specifieke rechtssubjecten kunnen worden ingeroepen (bijvoorbeeld rechten uit overeenkomst of onrechtmatige daad).
118. Binnen het KP7 EU project USEMP hebben wij daartoe een zogenaamde data licensing agreement (DLA) ontwikkeld. Zie <http://www.usemp-project.eu>.
119. Novotny en Spiekermann (2013) pleiten op grond van gedragseconomische argumenten voor een soort eigendomsrecht in persoonsgegevens. Voor een gedegen analyse van de zin en onzin van eigendomsrechten op persoonsgegevens zie bijvoorbeeld Purtova (2012).
120. De Nederlandse vertaling van 'betrokkene' en 'verantwoordelijke' vind ik minder gelukkig dan de Engelse termen 'data subject' en 'data controller'. Betrokkene is mij te vaag en te bestuursrechtelijk en geeft minder direct aan dat het om het subject van een data gaat (de verwijzing naar het begrip persoonsgegeven gaat verloren bij gebruik van de term 'betrokkene'); verantwoordelijke verwijst niet expliciet naar degene die controle heeft over de data.
121. In ieder geval heeft het data subject een aantal transparantierechten – ook wanneer haar toestemming of contractuele instemming niet nodig zijn.

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

Het feit dat de betreffende telecomproviders, 'content' providers en andere dienstverleners beschikkingsrechten hebben in deze gegevens (verwerking voor een specifiek en tevoren geëxpliciteerd doel, art. 7 en 9 Wbp, op een van de juridische gronden uit art. 8 WBP) sluit niet uit dat politie en justitie ook beschikkingsrechten hebben in de data – onder bepaalde voorwaarden en met het oog op specifieke doelen, conform de Wpg. Die rechten en bevoegdheden sluiten bovendien niet uit dat ook het data subject rechten heeft in deze persoonsgegevens (met name transparantierechten, correctie- en verzetsrechten, art. 16-20 Kaderbesluit gegevensbescherming inzake politiële en justitiële samenwerking, art. 25-28 Wpg).[122]

Anders dan IP rechten is het dataverwerkingsrecht in beginsel dus geen exclusief recht. Terwijl het recht om te beslissen over publicatie, verspreiding en vermenigvuldiging van een werk uitsluitend toekomt aan de auteur, is de bundel van rechten die voortvloeien uit het gegevensbeschermingsrecht niet per se exclusief. Wanneer de overheid een wettelijke verwerkingsgrond heeft en binnen de bandbreedte van een geëxpliciteerd, specifiek en legitiem doel blijft, heeft diezelfde overheid

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

een specifiek beschikkingsrecht ten aanzien van de betreffende data. Datzelfde geldt in beginsel dus ook voor een bedrijf dat persoonsgegevens nodig heeft om aan haar contractuele verplichtingen te voldoen en zelfs voor een bedrijf dat de gegevens moet verwerken in het kader van haar legitieme belang (cf. art. 8 sub f Wbp). In dat laatste geval eist het recht echter dat daarmee de fundamentele rechten van het data subject niet overruled mogen worden; hier wordt een afweging vereist. De rechten die personen en rechtspersonen hebben in data, bestanden en methoden kunnen dus botsen, zelfs *binnen* het kader van het gegevensbeschermingsrecht.

De inzet van data-gestuurde *agents* in het kader van de strafvordering vormt al snel een aantasting van diverse grondrechten die verband houden met de verwerking van persoonsgegevens. Ten aanzien van het grondrecht op gegevensbescherming (art. 8 Handvest Grondrechten van de Europese Unie, dat deels doorwerkt in art. 8 EVRM)[123] heb ik hierboven al specifiek gekeken naar de wijze waarop de inzet van politie-*agents* in de Wpg wordt genormeerd. Het grondrecht op gegevensbescherming is vaak een instrument om andere grondrechten te beschermen, toegespitst op de specifieke implicaties van de verwerking van persoonsgegevens. Ik beperk mij hier dan ook tot een verwijzing naar de paragraaf over de onschuldpresumptie en de nog te bespreken grondrechten van non-discriminatie en vrijheid van informatie. Tenslotte zal ik er in de paragraaf over legaliteit en doelbinding nog eens op terugkomen. Het lijkt me bovendien verstandig om weerstand te bieden aan de wijdverbreide neiging om de problemen die door de inzet van *agents* worden gegenereerd zoveel mogelijk onder de noemer van privacy 'af te handelen'. Daarmee bedoel ik zeker niet te stellen dat privacy niet aan de orde is, maar ik ga de mij toegemeten ruimte niet besteden aan de reeds goed beschreven afweging tussen het fundamentele recht op privacy enerzijds en het belang van het opsporingsonderzoek, van de geschokte rechtsorde, van het voorkomen van gevaar en het veiligstellen van mogelijk bewijsmateriaal

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

anderzijds.[124] Ik merk daarbij op dat het mij hier vooral ook gaat om het verruimen van het blikveld door scherp te stellen op *agents* in plaats van gegevensbescherming *an sich*. Dat betekent vooral dat de eis van voorzienbaarheid opnieuw doordacht moet worden, nu met name *agents* die opereren op basis van ML geacht worden problemen op te lossen juist omdat zij enigszins onvoorspelbaar zijn.

Het grondrecht op non-discriminatie speelt in het strafrecht een grote rol, omdat het profileren van 'mogelijke betrokkenen' bij eventueel nog te plegen strafbare feiten gemakkelijk leidt tot het categoriseren van groepen van personen die zouden neigen tot strafbaar gedrag. Zoals bijvoorbeeld Zedner (2008) opmerkt zijn er belangrijke morele – en ik zou zeggen ook politieke[125] – gronden om het systematisch monitoren van specifieke groepen te verwerpen, enerzijds vanwege de stigmatiserende werking en anderzijds vanwege het effect van een self-fulfilling prophesy. Harcourt (2007) heeft intussen mooi aangetoond dat de statistiek die het voorspellen van crimineel gedrag onderbouwt geen goede raadgever is als het gaat om

124. Over de complexe interactie tussen beide Europese constitutionele hoven De Hert en Gutwirth (2009); over de relevante afwegingen vanuit het perspectief van de Nederlandse Grondwet Koops (2011). In EHRM, 29 juni 2006, nr. 54934/00 (Weber en Saravia/ Duitsland) heeft het EHRM de eisen samengevat die gesteld moeten worden aan interceptie van en toegang tot informatie die een inbreuk vormt op art. 8.1 EVRM. In r.o. 95 overweegt het Straatsburgse Hof dat de volgende waarborgen wettelijk geregeld moeten zijn: de aard van de strafbare feiten die aanleiding kunnen zijn voor interceptie; duidelijke afbakening van de categorieën personen wiens telefoon mag worden afgetapt; afbakening van de periode gedurende welke mag wordt afgetapt; de te volgen procedure bij analyse, gebruik en opslag van verkregen data; te nemen voorzorgsmaatregelen bij het doorgeven van de data aan andere partijen; en de voorwaarden waaronder opgeslagen informatie kan of moet worden vernietigd, eventueel inclusief de informatiedragers). Zie ook EHRM 1 juli 2008, 58243/00 (Liberty e.a./Verenigd Koninkrijk). Ten aanzien van de analyse van metadata is het nu interessanter te verwijzen naar de interpretatie van het HJEU, 8 april 2014, C-293/12 en C-594/12 (Digital Rights Ireland/ Ierland), dat – in lijn met de jurisprudentie van het EHRM – oordeelde over de Richtlijn Data Retentie (24/2006/EG) en deze wegens een gebrek aan noodzakelijke waarborgen nietig verklaarde (zie r.o. 62-68). Het Luxemburgse Hof baseert zich daarbij op de onderling verbonden maar niet met elkaar gelijk te stellen grondrechten op privacy en gegevensbescherming (art. 7 en 8 Handvest Fundamentele Rechten van de Europese Unie). Bij data-gestuurde opsporing is het probleem vooral (r.o. 27): 'Uit deze gegevens, in hun geheel beschouwd, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren'.
125. Het opdelen van de samenleving in allerlei data-gestuurde 'groepen' die meer of minder neigen tot crimineel gedrag leidt tot problematische fragmentering en gebrek aan nadruk op wat mensen bindt en zou moeten binden (het slaat de bodem weg onder het democratisch debat over wat ons zou moeten binden); vergelijk de argumenten die Sunstein (2001) aanvoert tegen het gepersonaliseerd filteren van online nieuws.

het verdelen van de aandacht van de politie.[126] Hij wijst erop dat de hoge verwachtingen van pre-emptief politie optreden gebaseerd zijn op de elasticiteit van de 'vraag naar' criminaliteit.[127] Zo'n elasticiteit zou betekenen dat criminaliteit meer en beter kan worden teruggedrongen wanneer politie en justitie zich bij de inzet van middelen concentreert op personen die voorspelbaar meer crimineel gedrag zullen vertonen. Die veronderstelling gaat volgens Harcourt niet op omdat de vraag niet noodzakelijk elastisch is. Ten eerste omdat zelfs wanneer de voorspellingen zouden kloppen dit niet betekent dat de motivatie om strafbare feiten te plegen afneemt door extra inzet (afschrikking werkt niet bij alle vormen van criminaliteit). Ten tweede omdat herverdeling van middelen op basis van statistiek zal leiden tot minder oog voor degenen die voorspelbaar minder strafbare feiten plegen. Volgens Harcourt mogen we echter niet veronderstellen dat dit *niet* zal leiden tot meer strafbaar handelen bij die specifieke groep. Dat laatste is ook problematisch omdat een eventuele toename minder zichtbaar zal zijn juist omdat er minder op wordt gelet. Ten derde is er het verschijnsel van 'overfitting' dat ertoe kan leiden dat politie-*agents* gaandeweg minder goed in staat zijn om 'outliers' waar te nemen die buiten het model vallen. Dit is een bekend probleem in ML en kan op allerlei manieren worden ondervangen, maar dat vraagt dan wel een waakzaam oog op de vooroordelen die zich in toepassingen van ML nestelen.[128]

Wanneer de opsporing in toenemende mate gebruik gaat maken van politie-*agents*, moet de rechter in staat zijn contra-expertise te beoordelen die de ML van deze *agents* kan aanvechten of evalueren.[129] Heikel punt blijft echter dat de meeste implicaties van de inzet van deze *agents* door de verzelfstandiging van het vooronderzoek buiten de aandacht van de rechter blijven. Cruciale vraag is dan ook wie de inzet van deze agents wel kan toetsen.

---

126. Over de inzet van crime mapping Coldren, Huntoon en Medaris (2013), en bijvoorbeeld Cope (2004). Zie ook Hoogenboom (2010) en Hildebrandt (2016b te verschijnen).
127. Elasticiteit is een begrip uit de micro economie en wordt gebruikt om de afstemming van vraag en aanbod via het prijsmechanisme te beschrijven. Normaliter neemt de vraag toe als de prijs daalt (dat heet prijselasticiteit). Er zijn echter allerlei omstandigheden waarin deze correlatie niet opgaat. Harcourt beargumenteert dat die elasticiteit bij het begaan van strafbare feiten vaak niet opgaat, omdat de motieven voor het plegen van bijvoorbeeld geweldsdelicten niet noodzakelijk samenhangen met angst voor straf (die hier als te betalen prijs wordt gezien).
128. Over machinaal leren Russell en Norvig (2009:693-859). Bias kan voortkomen uit overfitting (idem:705, 736), maar natuurlijk ook uit vooroordelen die verdisconteerd zijn in de input data. In dezelfde zin Mitchell (1997:42-45), die expliciteert dat machinaal leren bias veronderstelt om van nut te kunnen zijn, een inzicht dat de hermeneutici onder ons niet zal verbazen, cf. Gadamer (1990).
129. Over de catch-22 die hiermee gemoeid is Hildebrandt (2004).

De inzet van politie-*agents* zal steeds berusten op de verwerking van politiegegevens,[130] daarmee is ook enige bescherming tegen verboden discriminatie gegeven. Artikel 5 Wpg stipuleert dat verwerking van gegevens met betrekking tot iemands 'godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging, slechts plaats [vindt] in aanvulling op de verwerking van andere politiegegevens en voor zover dit voor het doel van de verwerking onvermijdelijk is.' De grote vraag is wat dat betekent voor geautomatiseerd zoeken en in combinatie zoeken, waarbij immers al gauw sprake is van aanvullende gegevens. Sterker nog, dankzij slimme *agents* kun je datapunten vinden die redelijk betrouwbaar correleren met genoemde gegevens, zodat je zonder deze gegevens direct te verwerken, toch in staat bent om indirect op ras, geloof of vakbondslidmaatschap te discrimineren. Naar analogie van de anti-discriminatie wetgeving zou indirecte discriminatie op basis van dit type gegevens eveneens onder het verzwaard regiem moeten komen.[131] Dat wil zeggen dat naast deze – of ermee correlerende – datapunten altijd aanvullende gegevens in de analyse moeten worden betrokken, en dat er altijd sprake moet zijn van een verzwaarde noodzakelijkheidseis (onvermijdelijkheid).

Om te achterhalen of bepaalde politie-*agents* tot indirecte discriminatie leiden, doordat zij selecteren op kenmerken die bij nader inzien correleren met art. 5 Wpg gegevens, kunnen daarvoor ontwikkelende technieken worden ingezet, zoals 'discrimination aware data mining' (Pedreshi, Ruggieri en Turini 2008). Ik kom dan ook tot een diametraal tegenovergestelde

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

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

positie dan die van de Moerel en Prins, die menen dat het speciaal regiem voor bijzondere persoonsgegevens beter afgeschaft kan worden.[132]

Het grondrecht op vrijheid van informatie verwijst in dit verband naar het grondrecht om overheidsinformatie op te vragen en te ontvangen.[133] In Nederland gaat het dan om de reeds besproken Wpg, de Wet Openbaarheid van Bestuur 1991 (Wob), en de Wet hergebruik van overheidsinformatie 2015 (Who).[134] We moeten daarbij onderscheid maken tussen drie situaties: (1) een persoon die verzoekt om inzage (of correctie) van op haarzelf betrekking hebbende persoonsgegevens; (2) een persoon of instantie die verzoekt om specifieke overheidsinformatie openbaar te maken, of (3) te mogen hergebruiken. In het tweede of derde geval zal het vaak niet om persoonsgegevens gaan, hoewel evident complicaties optreden als dat wel

132. Verboden discriminatie speelt immers niet alleen binnen het strafrecht, maar ook binnen de private sector. De niet-haalbaarheid van het speciale regiem is in de huidige situatie inderdaad evident. Dat moet echter niet leiden tot afschaffing, maar tot het inbouwen van adequate bescherming in de cyberfysieke infrastructuur, waarbij met name het doormeten van indirecte discriminatie van groot maatschappelijk belang zal zijn. Dat zal alleen gebeuren als de bescherming van deze gegevens onder de komende Avg daadwerkelijk gehandhaafd wordt. Gezien de boetebepalingen in de Avg (tot aan 4% van de wereldomzet) ben ik daarover optimistischer dan Moerel en Prins. Dat het speciaal regiem tot onnodige bescherming leidt lijkt mij gezien de uitzonderingen niet houdbaar, tenzij daarmee wordt bedoeld dat het onwenselijk is dat data controllers moeten onderzoeken of een uitzondering van toepassing is. Dat onderzoek zal echter terugkeren in het kader van de door Moerel en Prins voorgestane toets aan het 'gerechtvaardigd belang', maar nu als minder zichtbaar en nog casuistischer criterium voor de afweging.
133. Andere implicaties van de vrijheid van informatie zijn hier niet direct relevant, zoals de vrijheid van betoging en de vrijheid van meningsuiting, zie art. 7 Grondwet, art. 10 EHRM en art. 11 Hv (vrijheid van meningsuiting), dat naar vaste jurisprudentie ook het recht op het ontvangen van informatie omvat (als zodanig ook geformuleerd in 10 EVRM en 11 Hv). Dit gaat echter om het recht om kennis te nemen van informatie die door om het even welke partij wordt geuit; het betreft een verbod op overheidscensuur. In Nederland is het recht op openbaarheid van bestuur apart geregeld in art. 110 Grondwet. Een ander relevant aspect van de vrijheid van informatie betreft het 'chilling effect' dat uitgaat van het besef dat politie en justitie steeds meer toegang claimen tot telecommunicatie. Dit kan indirect leiden tot deuken in de vrijheid van meningsuiting.
134. De Who is in feite een rib uit het lijf van de Wob (hoofdstuk V-A wordt uit de Wob gelicht). De Wob betreft toegang tot overheidsinformatie, de Who gaat om hergebruik en stipuleert dat deze informatie zo mogelijk in elektronisch formaat wordt aangeleverd. De invoering is vooral het resultaat van de aanpassingen van de Richtlijn inzake hergebruik overheidsinformatie 2013/37/EU, die nu een verplichting bevat tot het ter beschikking stellen van alle overheidsinformatie, behoudens een aantal uitzonderingen.

het geval is.[135] Het opvragen van persoonsgegevens die door de politie worden verwerkt valt bij uitsluiting onder de Wpg, die – naast regels voor de verstrekking aan degene die het betreft – een eigen regiem kent voor de verstrekking van politiegegevens aan andere instanties.[136] Met betrekking tot de inzet van *agents* is het echter belangrijk om te kunnen voorzien welke type verbanden worden gezocht in welk type gegevensbestanden, en met welke technologie dit gebeurt. Het vrijgeven van het geheime TNO rapport over digitale herkenningstechnieken is een mooi voorbeeld van wat vrijheid van informatie kan betekenen als het gaat om politie-*agents*.[137] Dit rapport is echter evident achterhaald. Zowel het voorbeeld van CityPulse als een blik op de technologie die op de markt is voor politie, veiligheids- en inlichtingendiensten maken duidelijk dat ook wordt geëxperimenteerd met meer geavanceerde patroonherkenning.[138] In dat kader zou het interessant kunnen zijn om te zijner tijd een verzoek in te dienen op grond van de Who om onderzoek te mogen doen via Pentland's Safe Answers technologie, waarbij geen toegang wordt gegeven tot de politiegegevens zelf, maar wel inzicht kan worden verkregen omtrent, bijvoorbeeld, criminaliteitspatronen.[139] Dat is niet alleen interessant voor

135. Art. 10.1 sub d Wob sluit verstrekking van persoonsgegevens op basis van de Wob uit 'tenzij de verstrekking kennelijk geen inbreuk op de persoonlijke levenssfeer maakt.' Dit is interessant omdat het aansluit bij het recht op privacy dat met de ontsluiting van persoonsgegevens gemoeid kan zijn. Het enkele feit dat het om een persoonsgegeven gaat is dus niet doorslaggevend. Zie ook art. 2.1 sub g Who, die hergebruik uitsluit van 'informatie die betrekking heeft op openbare persoonsgegevens waarvan hergebruik onverenigbaar is met de doeleinden waarvoor ze zijn verkregen'. Hier wordt aangesloten bij het doelbindingsbeginsel uit het gegevensbeschermingsrecht, met name voor openbare persoonsgegevens (bijvoorbeeld informatie die gebruikers zelf op openbaar beschikbare delen van het web zetten).
136. Zie paragraaf 3 van de Wpg inzake verstrekking aan anderen dan politie en marechaussee. De regeling van de Wpg sluit toepasselijkheid van de Wob uit, zie Afdeling Bestuursrechtspraak Raad van State, 4 februari 2015, 201309828/1/A3, r.o. 3.1.
137. Zie hierboven noot 92. Vergelijk ook het onderzoek naar audits inzake uitvoering van de Wpg (Bits of Freedom 2012), dat beschikbaar kwam na vele Wob verzoeken om de resultaten van de audits boven water te krijgen.
138. Zie Van Noort en Kist (2015) die wijzen op marktleider IBM die zelf aangeeft zaken te doen met Nederlandse politiekorpsen. Zie verder hoofdstuk 4 inzake het 'Living Labs' experiment in Eindhoven, met predictieve policing technologie van ATOS.
139. De aangepaste Richtlijn hergebruik overheidsinformatie, specificeert in art. 1.4: 'Deze richtlijn laat het niveau van de bescherming van individuen met betrekking tot het verwerken van persoonsgegevens krachtens de bepalingen van het Gemeenschapsrecht en de nationale wetgeving intact en heeft daar geen enkele invloed op, en houdt met name geen wijziging in van de verplichtingen en rechten in Richtlijn 95/46/EG.' Dit is van groot belang omdat de in 2013 aangepaste richtlijn een *verplichting* bevat tot het verstrekken van overheidsinformatie voor hergebruik. Persoonsgegevens vormen daarop ingevolge art. 1.4 een uitzondering (zie ook Art. 29 Werkgroep in haar advies 06/2013 over open gegevens en hergebruik van overheidsinformatie). Het verstrekken van de mogelijkheid om zonder toegang tot de data onderzoek te doen naar relevante verbanden kan niet op grond van Richtlijn 95/46/EG worden uitgesloten. Interessant is dan ook de relatie tussen Wpg en de Who: sluit het eigen verstrekkingsregiem ook de toepasselijkheid van de Who uit?

hen die overwegen strafbare feiten te plegen maar ook voor wetenschappelijk onderzoekers, security bedrijven, en voor potentieel verdachte burgers. De politie zal zich hier uiteraard tegen verzetten, onder het mom van: 'Dat zou te veel prijsgeven over onze tactiek bij politiewerk. Dat zou door kwaadwillenden verkeerd gebruikt kunnen'.[140]

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

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

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

3.4 Legaliteit en legalisme: detournement de pouvoir

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

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

term discretie dus niet naar willekeur maar naar een genormeerde vrije ruimte die enerzijds mogelijkheden biedt om taken naar beste inzicht en toegesneden op concrete omstandigheden uit te voeren en anderzijds wel degelijk eisen stelt aan de rechtmatigheid van die uitvoering.[141] Een van die eisen vinden we terug in het doelbindingsbeginsel: bevoegdheden mogen alleen worden gebruikt voor het legitieme doel waarvoor zij zijn toegekend. Discretionaire bevoegdheden worden aldus genormeerd door het doel waarvoor zij zijn gegeven; op die manier dient het doel zowel de instrumentaliteit (het maakt overheidsoptreden mogelijk) als de rechtsbescherming (het begrenst datzelfde optreden).

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

Gezien de grote economische belangen die gemoeid zijn met gegevensbescherming in de private sector en de mogelijke inbreuken op grondrechten is het doelbindingsbeginsel van meet af aan richtinggevend geweest voor de juridische normering van de verwerking van persoonsgegevens. Zo is het legitieme belang van de data controller sinds jaar en dag een rechtmatige *grond* van verwerking (art. 8 Wbp), maar wordt daarnaast bij iedere grond de *voorwaarde* gesteld dat het betreffende data subject weet voor welk doel haar gegevens wel en niet gebruikt worden (art. 7 en 9 Wbp). Door naast een juridische bevoegdheidsgrondslag (toestemming, contract, vitaal belang van het data subject, publieke taak of het legitieme belang van de data controller) steeds te eisen dat de controller duidelijk maakt met welk doel of welke doelen de verwerking plaatsvindt, wordt voorkomen dat de grondslag een *carte blanche* wordt voor om het even welke verwerking. In het verlengde hiervan is het verwerken van persoonsgegevens voor een ander doel dan waarvoor ze zijn verkregen onrechtmatig voor zover het nieuwe doel onverenigbaar is met het oorspronkelijke doel. Deze benadering sluit aan bij Nissenbaum's nadruk op contextuele integriteit, die rechtstreeks samenhangt met de redelijke verwachting van degene

141. In gelijke zin Muller, Dubelaar en Cleiren (2007: 596-8) over 'beleidsvrijheid' en de normering die uitgaat van 'algemene beginselen van behoorlijke politiezorg). Ik zie dan ook niets in de idee dat creatieve omgang met bevoegdheden onder het 'stoere' kopje van 'het opzoeken van de grenzen van wet- en regelgeving' illegaal overheidshandelen met zich meebrengt, zie bijvoorbeeld Halderen en Lasthuizen (2013:17), die dat benoemen als 'noble cause corruption' (ibid). Vergelijk bijvoorbeeld Schuyt (2009) die in geval van burgerlijke ongehoorzaamheid veronderstelt dat men bereid is de consequenties van het negeren van democratisch gelegitimeerde normen te aanvaarden, waaronder met name ook strafbaarheid. Juist in geval van ambtelijke ongehoorzaamheid moet helder zijn dat onrechtmatige experimenten tot strafvervolging van de betreffende ambtenaar en diens leidinggevende kunnen leiden.

wiens gegevens worden verwerkt.[142] Nadeel van 'context' is dat niet duidelijk is wie op welk moment bepaalt welke context aan de orde is. Dit wringt met name omdat gegevensverwerking in de onli*f*e wereld vaak plaatsvindt in een veelvoud van contexten, waarbij de economische context bijna altijd een voorname rol speelt. Voordeel van doelbinding is de attributie van verantwoordelijkheid en aansprakelijkheid die ermee gegeven is (Hildebrandt 2014, 2015a). De data controller moet een legitiem doel specificeren en expliciteren, ten laatste op het moment dat de gegevens worden verwerkt en is daar vervolgens aan gebonden.

In het preadvies van Moerel en Prins wordt voorgesteld om binnen de private sector, waar horizontale verhoudingen de boventoon voeren, doelbinding als een achterhaald en ineffectief beginsel af te schaffen. Zij stellen voor in plaats daarvan de bescherming van het gerechtvaardigde belang van het data subject als ijkpunt en toetssteen te nemen. Een verfrissend voorstel dat het aandurft de zaken op een radicaal andere wijze te bekijken, ongehinderd door blinde navolging van de huidige systematiek van de gegevensbescherming. Het voorstel lijkt – in termen van het gegevensbeschermingsrecht – gronden en voorwaarden te verwarren. Van verwarring is bij de preadviseurs echter geen sprake, integendeel, zij constateren dat doelbinding in het tijdperk van big data en IoT vaak een wassen neus is, omdat de data controller daarmee zelf bepaalt waartoe zij is gehouden en zich bij het vaststellen van het doel weinig of niets aantrekt van het gerechtvaardigde belang van het data subject. Precies om die reden stellen zij vervolgens voorop dat gegevensverwerking altijd legitiem moet zijn in het licht van de fundamentele rechten en vrijheden van het data subject. Dit sluit aan bij de huidige juridische grondslag van art. 8.f Wbp die een afweging eist van het legitieme belang van de data controller tegen de rechten en belangen van het data subject. Hoewel verfrissend, is het voorstel wat mij betreft niet overtuigend. Het is mij bijvoorbeeld niet duidelijk waarom het weglaten van de eis van doelbinding bedrijven ertoe zou verleiden zich nu ineens wel iets aan te trekken van de rechten en belangen van het data subject, nu zij daartoe ook op dit moment verplicht zijn. Het criterium van het gerechtvaardigde belang heeft overigens dezelfde nadelen als dat van contextuele integriteit, wanneer het toetssteen en ijkpunt van legitieme gegevensverwerking wordt. Anders dan bij doelbinding is mij vooralsnog onduidelijk wie de inhoud en reikwijdte ervan bepaalt, op welk moment, en hoe dit kenbaar moet worden gemaakt aan data subjecten. Door het perspectief te verhuizen naar dat van het data subject, maar de data controller verantwoordelijk te houden ontstaat voor

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

de data controller bovendien grote onzekerheid, want de betekenis van de fundamentele rechten en belangen zal per persoon, context en applicatie verschillen. Zo keert de complexiteit die met de voorgestelde vereenvoudiging moet worden teruggedrongen langs de achterdeur terug.[143] Dat heeft ook van doen met het feit dat de keuze voor het gerechtvaardigde belang – anders dan doelbinding – hecht verbonden is met een belangenafweging, die allerlei vragen oproept rond de vergelijkbaarheid van de belangen, de distributie van kosten en baten en de kwalificatie van belangen als individueel dan wel publiek belang.[144] Moerel en Prins wijzen er overigens terecht op dat onder omstandigheden het uitblijven van een belangenafweging tot minder bescherming leidt. Dat pleit ervoor om die belangenafweging *ook* verplicht te stellen in geval van toestemming. Mijn punt is dat ook in dat geval doelbinding een voorwaarde is om tot een juiste afweging te komen, namelijk een afweging binnen de bandbreedte van het verenigbare, legitieme doel.

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

De op mededingingsrecht geïnspireerde boete van maximaal 4% van de wereldomzet voor schending van de bepalingen van de komende Algemene Verordening Gegevensbescherming (Avg) zal een 'game changer' zijn, die het speelveld voor alle partijen opnieuw zal structureren.[145] Door doelbinding daadwerkelijk te handhaven wordt de data controller terecht gedwongen zich de vraag te stellen waartoe hij de gegevens nodig heeft en dat in heldere taal mee te delen aan degene wiens data worden verwerkt. Dat levert een vorm van rechtzekerheid op die bij het legitiem belang als enig criterium niet eenvoudig te realiseren is. De gebruiker kan immers niet voorzien welke gegevensverwerking het toekomstige economische belang van de controller kan rechtvaardigen.

Moerel en Prins menen intussen dat ook 'informed consent' een zinloze voorwaarde is, die in de praktijk hooguit leidt tot het afvinken van allerlei vakjes om maar zo snel mogelijk toegang te krijgen tot de gewenste

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

applicatie. Dat is op dit moment zeker het geval en ik ben het eens met de idee dat *voordat* sprake kan zijn van 'informed consent' een 'level playing field' moet worden geschapen zodat de gebruiker default instellingen kan kiezen die het leven gemakkelijk maken en tegelijk bescherming bieden. Een mooi voorbeeld van het creëren van zo'n level playing field was art. 7 lid 4 van de concept Avg, zoals vastgesteld door het Europees Parlement:

> The execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of data that is *not necessary for the execution of the contract or the provision of the service* pursuant to Article 6(1), point (b) (mijn nadruk).[146]

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

Is dit relevant voor de strafvordering? Gezien de gestage uitbreiding van publiek-private samenwerking, met name in de context van het bestrijden van (internationale) cybercriminaliteit moeten we ervan uitgaan dat alle gegevens die op enig moment worden verzameld door private partijen, niet alleen in theorie maar ook in de praktijk beschikbaar kunnen komen voor politie en justitie (de inlichtingen- en veiligheidsdiensten laat ik er dan nog buiten). Zeker wanneer de voorgestelde definitie van computers ('geautomatiseerde werken') als onderdeel van het wetsvoorstel Computercriminaliteit III kracht van wet krijgt: 'Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken' (art. 80sexies WSr). De komst van het

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

Internet van de Dingen leidt ertoe dat zo ongeveer alle 'dingen' die online verbonden zijn ofwel op afstand uitgelezen kunnen worden onder het bereik van de term 'geautomatiseerd werk' komen te vallen.[147] Dat alles betekent dat alle burgers bij het delen van – vaak onbewust vergeven – gedragsgegevens zouden moeten beseffen dat zij als eventueel mogelijk potentieel verdachte in beeld komen. Ook wanneer hun gegevens worden verwerkt in de private context. Dat is nu al het geval, op basis van art. 125i en verder (doorzoeking ter vastlegging van gegevens), art. 126l (plaatsing technisch hulpmiddel om vertrouwelijke informatie op te nemen), art. 126m en verder (interceptie telecommunicatie), art. 126nc Sv en verder (vordering gegevens), art. 126q lid 1 sub b (het overnemen van gegevens van computers) en zo voort en zo verder, maar het besef van de gevolgen van het opvragen en uitlezen van metadata, inhoud en profielen bij private partijen lijkt nauwelijks aanwezig.

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

In de strafvordering zelf geldt – net als in het bestuursrecht – het constitutionele beginsel van *detournement de pouvoir* (ddp), dat stipuleert dat overheden, en zeker de straffende overheid, een bevoegdheid alleen mag gebruiken voor het doel waarvoor die bevoegdheid is gegeven. Het gaat hier dus niet om *doelbinding als zelfbinding*. Dat is wel het geval als private partijen, zonder daartoe verplicht te zijn, diensten aanbieden waarbij het noodzakelijk is om persoonsgegevens te verwerken. Zij zijn dan gehouden een voldoende specifiek legitiem doel te communiceren en zichzelf daardoor te binden. Die noodzaak kan heel praktisch zijn, zo zal bijvoorbeeld een adres nodig zijn om goederen af te kunnen leveren. Het kan ook om een economische noodzaak gaan, wanneer het verdienmodel gratis dienstverlening combineert met gepersonaliseerde advertentie-inkomsten. Doelbinding is echter niet altijd een kwestie van zelfbinding; ook private partijen zijn vaak verplicht persoonsgegevens te verwerken in het kader van een publieke taak, ten behoeve van het vitale belang van het data subject of op grond van een wettelijke verplichting (belastingwetgeving). Daarmee is het doel van de verwerking meestal ook gegeven. Bij de straf-

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

vordering bepaalt de wetgever per definitie het doel. Het gaat dan bovendien om bijzonder ingrijpende bevoegdheden, niet voor niets dwangmiddelen genoemd, en nog los daarvan gaat het vaak om heimelijke bevoegdheden. Het ingrijpende karakter eist dat burgers een goed beeld hebben van de gevallen waarin zij onderworpen mogen worden aan dwangmiddelen, juist ook wanneer de toepassing voor hen verborgen wordt. Daar hoort niet bij dat dwangmiddelen die met het oog op een specifiek doel wettelijk zijn toegestaan worden gebruikt voor een ander doel, waartoe de wettelijke bevoegdheid in het voorliggende geval ontbreekt. Dat heet misbruik van bevoegdheid en – in het Frans – machtsmisbruik.[148] Het feit dat de strafvordering vaak heimelijke interventies vereist, maakt de doelbepaling in het kader van de rechtszekerheid en het vertrouwensbeginsel nog pregnanter. Het doel is immers zowel constitutief als limitatief voor de toe te passen bevoegdheid (Cleiren 1992:15, Hildebrandt 2014:26). Dat komt verder tot uiting in het feit dat schending van ddp kan leiden tot bewijsuitsluiting (art. 359a WSv). Doelbinding vloeit dan ook voort uit het rechtsstatelijk legaliteitsbeginsel, niet te verwarren met het legalisme van de 19e eeuw.

Legaliteit betekent hier dat overheidsorganen gehouden zijn te handelen in overeenstemming met hun wettelijke opdracht, binnen de grenzen van het recht, terwijl hun handelen gericht moet zijn op het algemeen belang en de bescherming van individuen. Daarmee normeert de legaliteit ook onderhandelende en netwerkende overheden en stelt grenzen aan wat een legitieme overheid wel en niet vermag. Het loslaten van ddp in het strafrecht in het kader van het accorderen van 'creatieve omgang' met bevoegdheden door de opsporing klinkt sommigen misschien als muziek in de oren (veelbelovend, adaptief, onvermijdelijk),[149] het is een teken aan de wand en moet naar mijn mening in ronde bewoordingen af worden gewezen.

---

148. We kunnen natuurlijk neuzelen over de vraag of *abus de pouvoir* en *detournement de pouvoir* niet heel verschillende zaken benoemen. Ook misbruik van bevoegdheid door bevoegdheden weliswaar voor het juiste doel maar disproportioneel in te zetten is in de strafvordering onrechtmatig, maar dat valt niet onder het inzetten voor een ander doel. Het gaat mij hier dus uitsluitend om het gebruik van een strafvorderlijke bevoegdheid voor een ander doel dan waarvoor die is gegeven. Verdere categorisering is altijd mogelijk, zie Halderen en Lasthuizen (2013: 22), die onderscheiden tussen niet inzetten, misbruik, oneigenlijk gebruik en selectief inzetten van bevoegdheden.
149. Onderzoek van Halderen en Lasthuizen (2013) laat zien hoe groot de verleiding is om 'creatief' om te gaan met bevoegdheden en hoe belangrijk het is om juist dan binnen de grenzen van ddp te blijven. Zie idem p. 26 over het informeel delen van informatie over een bewoner met een woningcorporatie die uitzetting overweegt. Creatieve omgang is echter niet per definitie in strijd met de legaliteit. Ik zou, in tegendeel, willen beargumenteren dat de discretionaire ruimte voor politie en justitie cruciaal zijn bij het vervullen van de hen toegemeten taken. Zie hierboven noot 141 en Hildebrandt (2016b te verschijnen).

Dat ddp zonder daar veel woorden aan vuil te maken als een ouderwetse hinderpaal terzijde wordt gesteld – dus ook in het strafrecht – mag worden opgemaakt uit een arrest van het Hof in Den Bosch van 5 oktober 2010.[150] Hoewel hierbij geen politie-*agents* zijn ingezet raakt het arrest aan de kern van de problematiek die met *agents* aan de orde is. Kort gezegd werd door de politie in Limburg een verkeerscontrole georganiseerd op de A2, waarbij het eigenlijke doel een drugscontrole was, gericht op het 'vangen' van drugskoeriers. Dit alles onder de noemer van het Project Waakzaam 2,[151] dat – zo lezen wij in het vonnis van rechtbank Maastricht – is gericht op 'verhoging van de veiligheid in de regio Limburg-Zuid – in het bijzonder door het bestrijden van de overlast die wordt veroorzaakt door uit Frankrijk afkomstige zogenaamde drugkoeriers'. Het verhogen van de veiligheid vindt plaats door (opnieuw volgens de rechtbank) 'controleacties (…) op en rond de verkeersstromen in het gebied Limburg-Zuid.' In plaats van het aanhouden van alle weggebruikers in hoop om daarbij toestemming te bekomen de auto te mogen doorzoeken, maakte de politie gebruik van slimme camera's met automatische nummerplaatherkenning (ANPR: Automatic Number Plate Recognition). De rechtbank vervolgt: 'Hierbij werden kentekens van passerende personenauto's gescand en vervolgens telkens vergeleken met een vergelijkingsbestand waarin kentekens zijn verzameld die bij de politie bekend zijn wegens eerdere betrokkenheid bij druggerelateerde criminaliteit. Indien een gescand kenteken overeenkwam met een kenteken in het vergelijkingsbestand, een zogenaamde 'hit', werd deze personenauto door de politie naar een controleplaats geleid, alwaar een controle plaatsvond.' Het voertuig in kwestie werd na selectie via genoemde ANPR-apparatuur 'na een volgteken te hebben gekregen, door een motoragent naar de controleplaats te Gronsveld geleid. De selectie uit de verkeersstroom, het geven van aanwijzingen om te volgen en het feitelijk tot stilstand doen brengen van het voertuig op de controleplaats levert een stopteken op als bedoeld in artikel 160 van de Wegenverkeerswet 1994. Nadat [het voertuig, mh] op de controleplaats stopte, vorderde verbalisant [verbalisant] het rijbewijs van medeverdachte [medeverdachte], die de auto bestuurde. Nadat [medeverdachte] hem de autopapieren had overhandigd vroeg verbalisant [verbalisant] in de Franse taal aan [medeverdachte] of hij drugs in zijn bezit had, wat door [medeverdachte] werd ontkend. Vervolgens vroeg verbalisant [verbalisant] in de Franse taal aan [medeverdachte] of hij het voertuig mocht onderzoeken op de aanwezigheid van drugs. Met toestemming van [medeverdachte] werd het voertuig onderzocht. In het voertuig werd in de kofferbakruimte 633,5 gram heroïne en 4,8 gram cocaïne aangetroffen.' De rechtbank spreekt de

150. Hof 's-Hertogenbosch, 5 oktober 2010, ECLI:NL:GHSHE:2010:BN9352, waarin opgenomen het vonnis van Rechtbank Maastricht, 17 februari 2010.
151. Interessante vraag is of wij ooit hadden vernomen over dit boeiende voorbeeld van 'smart policing' als hierover geen uitspraak was gedaan.

verdachte vrij wegens schending van ddp, waarna Hof Den Bosch de verdachte veroordeelt omdat er geen sprake is van ddp. De verdachte is immers gevraagd naar zijn papieren hetgeen duidelijk maakt dat het wel degelijk ging om uitoefening van een bevoegdheid op basis van de WVW (aldus het hof), en het bewijsmateriaal is gevonden dankzij toestemming, zodat geen bevoegdheid nodig was (aldus het hof).[152] Hof Den Bosch maakt er niet veel woorden aan vuil. Ook de Hoge Raad spreekt zich uit, maar tegen die tijd gaat het alleen nog maar om een foutje in de betekening. Ybo Buruma merkte in de NRC op:[153]

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

Volgens Buruma, toen nog hoogleraar Strafrecht aan de Radboud Universiteit, staat die nieuwe methode op gespannen voet met de onschuldpresumptie en had het Hof zich er om die reden niet zomaar vanaf mogen maken. Weliswaar is het inmiddels vaste rechtspraak dat geen sprake is van misbruik van de controlebevoegdheid van de WVW als het stopteken mede wordt gebruikt ter controle van kenteken en/of rijbewijs,[154] hier is overduidelijk sprake van geautomatiseerd voorsorteren van personen ten aanzien waarvan geen sprake is van een *redelijk vermoeden van* of zelfs maar *aanwijzingen voor* schuld aan een strafbaar feit. Het is niet ondenkbaar dat sommigen uit deze rechtspraak afleiden dat ook in het strafrecht doelbinding een wassen neus is geworden. Dat is niet onaannemelijk,[155]

152. Cruciale vraag is of een opsporingsambtenaar om toestemming mag vragen om datgene te verrichten waarvoor zij geen wettelijke bevoegdheid heeft. Mij dunkt dat gezien de ingrijpende gevolgen van strafvorderlijke interventies die toestemming op gespannen voet kan staan met de ratio van *nemo tenetur*.
153. Het gaat om een commentaar dat Buruma op uitnodiging schreef bij een artikel van Jensma, Buruma en De Swart (2010).
154. Hoge Raad, 21 november 2006, ECLI:NL:PHR:2006:AY9670. De problematiek van het inzetten van bevoegdheden uit de ene context (verkeersveiligheid) in een andere context (drugscriminaliteit) houdt ook verband met de vraag naar de rechtmatigheid van de voortgezette toepassing van bevoegdheden die speelt in de verhouding tussen bijzonder en commuun strafrecht. Zie Cleiren (2015).
155. Zie immers ook HR 12 november 2002, ECLI:NL:HR:2002:AE9028, r.o. 4.2 en 4.3. Hier ging het overigens om de vraag of het is toegestaan een verdachte op grond van art. 52 WSv staande te houden door een stopteken te geven dat kan worden opgevat als een stopteken in de zin van art. 160 WVW. Het Hof schrijft, met instemming van de HR: 'Uit de vaststelling dat artikel 52 van het Wetboek van Strafvordering de staandehouding legitimeert, en het hof de wijze waarop die bevoegdheid is gehanteerd niet onrechtmatig oordeelt, volgt bovendien, dat zich hier niet het geval voordoet waarbij de opsporing uitsluitend mogelijk is gemaakt door het oneigenlijk gebruik van een aan de Wegenverkeerswet 1994 te ontlenen bevoegdheid tot controle.' Het woordje 'uitsluitend' doet vermoeden dat het er niet toe doet of wie dan ook het stopteken – mede – baseerde op de WVW, zolang maar sprake is van een verdenking die staande houden rechtvaardigt.

maar dat is geen argument dat pleit tegen ddp. Integendeel, het verfrommelen van de onschuldpresumptie en het verkwanselen van ddp door de strafrechter zijn niet onbegrijpelijk maar wel hachelijk en onaanvaardbaar in het licht van de inzet van *agents*. Niet onbegrijpelijk voor zover ook de rechter een steentje bij wil dragen aan de slagvaardigheid van de strafvordering; hachelijk en onaanvaardbaar omdat deze verfrommeling en verkwanseling in flagrante strijd zijn met de voorzienbaarheid van het *ius puniendi* en van de daartoe noodzakelijke strafvorderlijke bevoegdheden.

4. Naar een veilig strafrecht in een data-gestuurde samenleving

4.1 Reflexieve modernisering van het Wetboek van Strafvordering?

In de Contourennota (2015:4) voor een nieuw Wetboek van Strafvordering wordt als een van de doelstellingen van de modernisering van het Wetboek de 'facilitering van de digitalisering' genoemd. Dat is de omgekeerde wereld. Digitalisering zou bij moeten dragen aan een legitieme en effectieve strafvordering, niet omgekeerd. Als gezegd, gaat het bij deze modernisering om een 'upgrade' van de 'firmware', dat wil zeggen van het meest stabiele onderdeel van het 'operating system' van het strafrecht, dat nauw verbonden is met de 'hardware' (de institutionele ondergrond, inclusief de Grondwet, en de organieke wetgeving inzake rechterlijke macht, advocatuur). Deze 'firmware' bepaalt feitelijk de mogelijkheden van de te implementeren software (nadere regelgeving, beleidsregels en protocollen voor de uitvoering).[156]

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

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

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

156. Zie hierboven paragraaf 3.1.

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

Als Roessingh (2013) in Trouw schrijft 'iColumbo kan meer dan hij mag', duidt hij een van de grootste uitdagingen van de stuwende kracht van technologie in de onli*f*e wereld. Politie-*agents* kunnen vrijwel altijd meer dan is toegestaan. Dat vraagt een dubbele bezinning. Ten eerste moet bij de introductie van data-gestuurde technologie steeds onder ogen worden gezien of, en zo ja in hoeverre het onvermijdelijk is dat de investering in nieuwe systemen leidt tot *agents* die meer kunnen dan zij mogen.[157] Hier geldt dat voorkomen beter is dan genezen; door de aanmaak, het opslaan, uitlezen of koppelen van gegevens technisch lastig te maken is de kans dat bevoegdheden op grote schaal worden overtreden kleiner, evenals de kans dat criminelen zich toegang verschaffen tot opgeslagen gegevens. Daarbij moet worden bedacht dat de aanzwellende data-obesitas in de private sector niet alleen zal leiden tot het dichtslibben van allerhande informatiesystemen en tot lekkage en diefstal van persoonsgegevens, maar dat het politie en justitie kan verleiden hun heil te zoeken in verdere ondergraving van de onschuldpresumptie door zich toegang te verschaffen tot steeds meer gegevens over steeds grotere groepen personen.[158] Ten tweede is het zaak om – voor zover systemen inderdaad meer kunnen dan mag – technisch controleerbaar te maken of, hoe en door wie bevoegdheden worden overschreden. Met name wanneer het gaat om *agents* die eraan bijdragen dat personen heimelijk in een categorie worden geplaatst van wie stelselmatig persoonsgegevens zullen worden verwerkt is die controle cruciaal. We kunnen er juist dan niet van uitgaan dat de strafrechter er

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

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

überhaupt aan te pas zal komen en zullen dus van meet af aan 'auditability' en 'accountability' in moeten bouwen.

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

4.2 Legaliteit en grondrechtenbescherming 'by design'

Voortbouwend op inzichten uit de techniekfilosofie en de studie van de inbedding van waarden en normen in apparaten, technische systemen, architectuur en infrastructuur (Verbeek 2011, Flanagan, Howe en Nissenbaum 2007), wordt inmiddels in verschillende contexten gewerkt aan het vertalen van juridische bescherming naar technische specificaties, standaarden en protocollen. Denk aan de nieuwe verplichting tot gegevensbescherming by design in de komende Avg (art. 23), de in Duitsland ontwikkelde methode KORA (*Konkretisierung rechtlicher Anforderungen*), en het idee van Ambient Law dat technische bescherming zou moeten bieden in een omgeving geënt op Ambient Intelligence.[159]

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

We kunnen dus wel een regel opschrijven en uitvaardigen die stipuleert dat we een recht hebben om voor onschuldig gehouden te worden tot onze schuld in rechte is vastgesteld, maar daarmee zijn we er nog niet. Als we tegelijkertijd systemen ontwerpen die het gemakkelijk maken om mensen op afstand te volgen en hun gedrag te voorspellen en te ondervangen, wordt het zaak de inzet van die systemen door politie en justitie aan banden te leggen. De

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

Pavlov reflex is om daartoe weer regeltjes op te schrijven en uit te vaardigen en zo voort en zo verder. Daar gaan we de oorlog niet mee winnen. Juridische bescherming by design gaat er daarom van uit dat rechtsstatelijk waarborgen moeten worden gearticuleerd in de technische systemen die we gebruiken.

Net zoals de paradox van de rechtsstaat erin bestaat dat we ons tegen de staat (de wetgever, het bestuur) kunnen verzetten dankzij diezelfde staat (de rechter), moeten we leren de technische systemen waaraan we onze veiligheid en ons welzijn danken te gebruiken om ons tegen diezelfde systemen te beschermen. Die bescherming moet dus zo diep mogelijk in de architectuur, het ontwerp, de technische inrichting en de default instellingen worden ingebouwd. Door te spreken van juridische bescherming by design, in plaats van techno-regulering, wil ik in de tweede plaats benadrukken dat het *niet* gaat om het afdwingen van de naleving van bestuurlijke normen met technische middelen (Hildebrandt 2010). Dat zou een kwestie zijn van nudging of van technoregulering, waarbij burgers en bedrijven met technische middelen in plaats van juridische normen tot zogenaamd 'compliant' gedrag worden verleid of gedwongen.[160] Techno-regulering gaat uit van een bestuurskundig reguleringsparadigma, waar recht een beleidsinstrument is, bedoeld om gedrag te beïnvloeden.[161] De idee van technoregulering is gebaseerd is op een sociaal-wetenschappelijk, extern perspectief op het recht. Dat leidt gemakkelijk tot het afwegen van de instrumentaliteit tegen de rechtsbescherming, in plaats van beiden als wederzijds constitutief samen te denken.[162] Bescherming en effectiviteit moeten in een rechtsstaat twee kanten van dezelfde medaille zijn; ze moeten als het ware afhankelijk zijn van elkaar en dus niet tegen elkaar worden uitgespeeld.

160. Zie bijvoorbeeld Berkhout en Engers (2012: 827) over informatiegestuurd fiscaal toezicht op basis van de *homo behavioralis*: 'een theorie over de mechanismen die aan fiscaal non-compliant gedrag ten grondslag liggen'.
161. Probleem van het sociaal-wetenschappelijk perspectief dat ten grondslag ligt aan het reguleringsparadigma is een onhoudbaar methodologisch individualisme dat geen inzicht kan geven in de constitutieve samenhang van instrumentaliteit en rechtsbescherming, en zich noodzakelijkerwijs moet beperken tot speltheoretisch, gedragseconomisch en kwantitatief georiënteerd empirisch onderzoek. In dat verband is het nuttig te wijzen op de nuttelоosheid van theorieloos kwantiatief onderzoek, waarvan onduidelijk is welke theorie nu eigenlijk gefalsificeerd kan worden. Misschien is dat probleem nog dringender dan het feit dat veel onderzoek niet gerepliceerd kan worden (bv Open Science Collaboration 2015), zie ook hierboven voetnoot 51.
162. Zie hierover de discussie tussen Leenes (2011) en Hildebrandt (2011c). Over de gevaren van technoregulering en de onmogelijkheid om juridische normen restloos te vertalen in technische specificaties Leenes (2010, 1998). Sceptisch over de vertaling van rechtsnormen in technische systemen (juist omdat hij geen onderscheid maakt tussen technoregularing en juridische bescherming by design) Koops (2013).

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

Kort gezegd gaat het bij juridische bescherming by design om de *noodzaak* om in specifieke gevallen het geschreven en ongeschreven recht tevens in de cyberfysieke infrastructuur te articuleren. Juist bij het gebruik van *agents* in de opsporing, die uiteindelijk zien op de toepassing van het geweldmonopolie en het ius puniendi is de verankering van bescherming in technische systemen pertinent. Het gaat er eigenlijk om de normatieve neutraliteit van het recht te bewaken door compenserende juridische normering door te voeren, steeds wanneer technologische ontwikkelingen de effectieve bescherming van grondrechten frustreert (Hildebrandt 2010, Hildebrandt en Tielemans 2013). Een analyse van de gevolgen van de inzet van specifieke politie-*agents* voor het beschermde rechtsgoed van bestaande grondrechten zou inspiratie kunnen vinden in Nissenbaums' (2010) beslissingsheuristiek inzake contextuele integriteit, die toestaat om volgens een stappenplan zulke gevolgen in kaart te brengen en daarmee een proportionaliteitstoets voor te bereiden.[163] Meer specifiek valt te denken aan de nieuwe juridische verplichting om bij de inzet van technologie die het risico op schending van gegevensbescherming verhoogt een 'data protection impact assessment' (DPIA) uit te voeren (art. 33 Avg).

Voor het strafrecht zou als opmaat naar juridische bescherming by design een 'presumption of innocence-assessment' (POIA) aangewezen kunnen zijn, die zich richt op de risico's voor de effectieve bescherming van de onschuldpresumptie, het verbod van niet-gerechtvaardigde discriminatie, de privacy en de gegevensbescherming, en het recht op vrijheid van informatie. Daarbij gaat het dan niet alleen om schending van de rechten van de verdachte, maar ook van degene ten aanzien van wie aanwijzingen bestaan van betrokkenheid bij het beramen van strafbare feiten en ook

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

van de burger die op basis van risicoprofielen in aanmerking komt voor stelselmatige observatie, waarbij dan ook weer diens sociale netwerk in beeld zal komen. De hierboven gesignaleerde tendens om het zwaartepunt van de strafvordering nog verder te verschuiven naar het vooronderzoek, naar het verkennend onderzoek en meer in het algemeen richting predictive policing leidt zoals aangegeven tot een steeds groter aandeel van heimelijke observaties die niet door de strafrechter worden getoetst, en in dat opzicht vergelijkbaar zijn met heimelijke operaties van de inlichtingen- en veiligheidsdiensten. Daarmee wordt relevant om kennis te nemen van de reactie van de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD) op het concept Wetsvoorstel Wet Inlichtingen- en Veiligheidsdiensten 20xx, met name waar de CTIVD aandacht besteedt aan toezicht op heimelijke bevoegdheden die niet aan de rechter worden voorgelegd, en het belang van organisatorische en technische functionele scheiding van systemen die grote databestanden beschikbaar maken voor data-analyse.[164] De CTIVD (2015:36) adviseert:

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

De toezichthouder spreekt ook van geautomatiseerd toezicht.[165] Hoewel dit niet wordt gedefinieerd vermeldt het rapport wel een viertal randvoorwaarden die onder meer verwijzen naar functiescheiding, compartimentering en transparant gegevensbeheer, automatische rapportage en digitale ontsluiting van gegevensbestanden. In de komende Avg worden naast de voorgeschreven DPIA nog andere verplichtingen opgelegd die functionele scheiding van gegevensverwerkingssystemen en automatisch toezicht aantrekkelijk kunnen maken, met name in art. 28 (documentatie van type dataverwerking, doel, doorgifte aan derde partijen en zo meer, welke documentatie op verzoek beschikbaar moet worden gemaakt voor de autoriteit gegevensbescherming).

Zeer relevant is art. 14.1a(h) van de komende Avg die stipuleert dat ten aanzien van profiling drie zaken moeten worden gecommuniceerd aan het betreffende data subject: (1) het feit dat sprake is van profiling, (2) begrijpelijke informatie over de onderliggende logica en (3) de voorziene gevolgen.[166] Ook al is de concept Avg niet van toepassing op gegevensverwer-

164. CTIVD (2015: 35-37). Zie ook het onderzoek van Loof e.a. (2015) naar het mensenrechtelijk kader voor toezicht op de diensten.
165. CTIVD (2015), die op p. 21 opmerkt 'Naar de mogelijkheden van deze vormen van toezicht verricht de CTIVD momenteel onderzoek'.
166. Art. 14 lid 1a sub h: 'the existence of automated decision making including profiling referred to in Article 20(1) and (3) and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.'

king door politie-*agents*, dit type profieltransparantie zou op geaggregeerd niveau beschikbaar moeten komen voor alle burgers ten einde voorzienbaar te maken welk type gedrag tot stelselmatige observatie kan leiden – zodat de burger haar gedrag aan kan passen. Niet om dan heimelijk strafbare feiten te plegen, buiten het zicht van justitie (ook al zal dat zeker ook een gevolg zijn), maar om ervoor te kiezen geen strafbare feiten te plegen dan wel het risico te nemen dat men tegen de lamp loopt.[167]

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

Zowel op het niveau van de wetgever als op dat van het bestuur en de rechter zullen afwegingen moeten worden gemaakt tussen het algemene belang van profieltransparantie en het algemene belang van criminaliteitsbestrijding.[168] Dit is op zichzelf niets nieuws. In een onlife wereld kan die afweging echter niet beperkt blijven tot het geschreven of ongeschreven recht. Daar zal, ook bij het ontwerp van de architectuur van de communicatie en informatie infrastructuur, moeten worden onderzocht hoe de schending van grondrechten die in de architectuur zit ingebakken (bijvoorbeeld: backdoors die justitie toegang moeten geven tot communicatie via internet) kan worden voorkomen of gecompenseerd (bijvoorbeeld door eventuele interceptie zo lastig te maken dat die technisch alleen per geval kan worden geeffectueerd).

167. De komende Richtlijn gegevensbescherming opsporing en vervolging, justitiële samenwerking, opsporings- doeleinden stipuleert in art. 9: 'Article 9 Measures based on profiling and automated processing. (1) Member States shall provide that measures which produce an adverse legal effect for the data subject or significantly affect them and which are based solely on automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall be prohibited unless authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.' In de Richtlijn is echter, anders dan in de Avg, geen transparantierecht opgenomen ten aanzien van profielen. Hoe begrijpelijk ook, in een rechtsstaat kan het niet zo zijn dat we geen idee hebben hoe we door justitie en politie kunnen worden getarget. Hier is slimme wetgeving nodig, die niet alleen beschermt tegen criminaliteit maar ook tegen 'overijverige' overheden.
    2. Automated processing of personal data intended to evaluate certain personal aspects relating to the data subject shall not be based solely on special categories of personal data referred to in Article 8.
168. Met in achtneming van de caveats uit sectie 3.3.1.

Het is bovendien zaak dat de proportionaliteit die moet worden ingebouwd in de technische systemen door een onafhankelijke toezichthouder wordt getoetst, juist omdat de rechter in te veel gevallen buiten spel staat (ten eerste vanwege buitengerechtelijke afdoening en bestraffing, ten tweede vanwege de inzet van heimelijke bevoegdheden die niet tot strafzaken leiden, en ten derde vanwege de inzet van heimelijke bevoegdheden die niet bijdragen aan het bewijs en om die reden buiten het geding ter terechtzitting blijven).

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

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

Een volledig data-gestuurde samenleving kan eigenlijk niet veilig zijn, voor zover daarin alle vormen van sturing afhankelijk zijn geworden van machinaal lerende systemen. We zijn dan de macht over het stuur kwijtgeraakt. Interessant is dat juist uit de hoek van de 'voormannen' van de kunstmatige intelligentie waarschuwingen klinken tegen de toenemende afhankelijkheid van *agents*, vanwege hun toenemend vermogen om zelfstandig in te grijpen en zich daarbij ook steeds zelfstandiger te ontwikkelen.[169] Die waarschuwingen betreffen vooral de snelheid waarmee wij ons over lijken te geven aan systemen die we steeds minder in de hand hebben. Die snelheid ontneemt ons de kans om sturend te blijven bij het ontwerp van de architectuur die bepalend zal zijn voor de speelruimte van de *homo digitalis*. Tegelijk gaan stemmen op om de werkelijkheid onder ogen te zien en de onli*f*e wereld met open vizier te betreden in het besef dat die wereld deels bevolkt wordt door entiteiten die 'handelend' optreden, allerlei 'intenties' bemiddelen en zowel de dingen als de mensen in hun omgeving voortdurend statistisch 'uitlezen'.[170] In mijn recente boek (Hildebrandt 2015) bepleit ik zo'n open vizier, inclusief het besef dat data-gestuurde *agents* weliswaar hun omgeving waarnemen, erop ingrijpen en ons gedrag proberen te ondervangen maar vooralsnog geen bewustzijn, geen zelfbewustzijn en geen gevoel ontwikkelen. Data, data-modellen en 'data lakes' (ongestructureerde datasets) moeten niet verward worden met datgene waarnaar ze verwijzen of waarvan ze de sporen of inferenties vastleggen. Zo is het ook met *agents* die aardig lijken, intelligent, zelfs humorvol. Zij kunnen uitstekend simuleren en dat kan niet alleen heel nuttig maar ook heel prettig zijn. Ze hebben echter niets te verliezen.

169. Gibbs (2015).
170. Markoff (2015b), Kool en van Est (2015).

Voor het strafrecht betekent dit dat we de opbrengst van de inzet van politie-*agents* niet moeten overschatten en de kosten niet mogen onderschatten. Data-gestuurde intelligentie is veelbelovend maar geen panacee, en er zijn kosten verbonden aan de uitholling van de onschuldpresumptie, aan de kans dat verfijnde onzichtbare discriminatie de regel wordt in plaats van de uitzondering en aan de permanente invasie van ons privéleven. Die invasie vindt weliswaar plaats door middel van *agents* en in eerste instantie dus niet door personen, maar die *agents* zullen de afgeleide kennis op enig moment delen met wie daartoe bevoegd zijn. Bovendien, als we de betreffende *agents* niet slim ontwerpen, delen ze die informatie ook en voortdurend met wie daartoe niet bevoegd zijn.

We kunnen niet iedereen tegelijk verdenken, maar zouden wel om het even wie moeten kunnen verdenken. Deze stelling kan op twee manier gelezen worden. Ten eerste vanuit een eenzijdig beveiligingsperspectief. Dan gaat het erom in tijden van hyperconnectiviteit, remote control, en geautomatiseerde aanvallen te waarborgen dat iedereen voortdurend in de gaten wordt gehouden ten einde om het even wie onder verdenking te kunnen plaatsen – liefst nog voor zij zelfs maar een strafbaar feit heeft beraamd. Ten tweede vanuit het driedubbelperspectief van beveiliging, democratisch samenleven en individuele vrijheid. Dan gaat het erom te *voorkomen* dat politie-*agents* iedereen voortdurend in de gaten houden, en personen voorsorteren op basis van (voor hen zelf) onleesbare patronen, die uitmaken wie in aanmerking komen voor straffen en/of maatregelen. De bereidheid om 'om het even wie' te verdenken, *als feiten en omstandigheden daar aanleiding toe geven*, sluit in deze interpretatie juist uit dat we worden opgesloten in de gedragsprofielen van de *homo behaviouralis*. Dat zal alleen lukken als juristen zich niet alleen bezighouden met de vraag of de toedeling en de uitoefening van bevoegdheden in overeenstemming is met het strafvorderlijk legaliteitsbeginsel en de mensenrechten, maar zich ook actief gaan bezighouden met de vraag of politie-*agents* zo zijn ontworpen dat zij alleen mogelijk maken wat *niet* mag als dit *strikt noodzakelijk* is, en zichtbaar en controleerbaar maken wanneer welke bevoegdheden door wie worden overschreden. Voorwaar, geen sinecure.

5. Literatuur

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

———. 2010. “Juridische bescherming ‘by design’?” *Rechtsfilosofie & Rechtstheorie* (2): 101–6.

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

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

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

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

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

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

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

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

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

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

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

———. 2016a. "Law as information in the era of data-driven agency (Chorley Lecture)". *The Modern Law Review*, *The Modern Law Review* 79 (1), 1–30.

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

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

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

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

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

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

———. 2009. *Bringing the police back in. Notes on the lost & found character of the police in police*

Studies. Oratie VU, Stichting Maatschappij, Veiligheid en Politie (SMVP). <http://www.maatschappijenveiligheid.nl/kennisbank/hoogenboom_english/>.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

TNO. 2010. "Herkenning van digitale informatie". Delft.

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

van Delft, D. 2003. "'Geléérd zijn jullie wel'". *NRC Handelsblad*, 12 april.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Privaatrecht voor de homo digitalis: eigendom, gebruik en handhaving

Eric Tjong Tjin Tai

1. Inleiding

1.1 Het probleem

> "I have heard you say that it is difficult for a man to have any object in daily use without leaving the impress of his individuality upon it in such a way that a trained observer might read it. Now, I have here a watch which has recently come into my possession. Would you have the kindness to let me have an opinion upon the character or habits of the late owner?" (…)
>
> "He was a man of untidy habits,--very untidy and careless. He was left with good prospects, but he threw away his chances, lived for some time in poverty with occasional short intervals of prosperity, and finally, taking to drink, he died. That is all I can gather."
>
> _____
>
> Sir Arthur Conan Doyle, (1890), Chapter I: The Science of Deduction.

Niet eens zo lang geleden waren anonimiteit en onbekendheid vanzelfsprekend. Identificatie was het probleem, en scherpzinnige technieken werden ontwikkeld om daders en slachtoffers te achterhalen aan de hand van allerlei onopvallende kenmerken.[1] Vingerafdrukken, bloedsporen, stof en allerlei andere onbeduidende sporen worden dan ook routinematig verzameld bij politieonderzoek. Maar in de populaire literatuur of lectuur wordt ook de persoon met superieure redeneervermogens gepresenteerd om uit die aanwijzingen gevolgtrekkingen te maken die feilloos een persoon kunnen identificeren. Anonimiteit was het probleem, niet het doel. Uit het bovenstaand citaat blijkt echter ook de keerzijde: sommige gegevens of kenmerken liggen persoonlijk gevoelig. Tegelijk laat het een complicatie zien. Een horloge is geen persoonsgegeven. Sherlock Holmes leidt er niettemin wel de gehele persoonsgeschiedenis uit af.

Tegenwoordig laten we overal digitale sporen achter waar met nieuwe technieken vérgaande gevolgtrekkingen aan zijn te verbinden: dit is onderdeel van de belofte van *big data*.[2] Met genoeg gegevens zijn verbanden te leggen die buiten het deductievermogen van gewone mensen liggen. Ieder bedrijf is nu in potentie een Sherlock Holmes. Maar daarmee heeft niet ieder bedrijf noodzakelijk respect voor persoonlijke gevoeligheden.

1. Zie Ginzburg (1979) en (1980) over de intellectuele historie van deze denkrichting.
2. Mayer-Schönberger & Cukier (2013), Kool, Timmer & Van Est (2015).

Weliswaar is niet gezegd dat al die data[3] perfect ieder individu beschrijft en voorspelt: het gaat om globale verbanden die in concrete gevallen niet hoeven op te gaan. Dit roept onbehagen op.

De Wet bescherming persoonsgegevens[4] richt zich voor de bescherming van privacy primair op wat wordt genoemd 'persoonsgegevens',[5] zoals naam, adres, medische gegevens. Deze moeten zorgvuldig worden verwerkt: zij mogen in beginsel niet zonder toestemming aan derden worden doorgegeven en alleen worden gebruikt ('verwerkt') voorzover de toestemming reikt.[6] De 'verantwoordelijke' (art. 1 sub d Wbp) is hier verantwoordelijk voor:[7] civielrechtelijk zouden we geneigd zijn te spreken over de 'bezitter', degene die de facto en de jure controle heeft over de databank waarin de persoonsgegevens zijn opgenomen.

Een voor de hand liggende reactie op ontwikkelingen als *big data* zou zijn om ieder kenmerk of gegeven dat potentieel tot identificatie kan leiden als persoonsgegeven aan te merken.[8] Het voorbeeld van Sherlock Holmes suggereert dat dit een heilloze weg is. Uiteindelijk kan *ieder* gegeven bijdragen tot identificatie, zodat alle gegevens als persoonsgegevens zouden moeten worden aangemerkt. Dan vallen 'persoonsgegevens' samen met het algemene begrip 'gegevens' en verliest dit onderscheidend vermogen.[9] Gevolg zou zijn dat voor ieder gegeven toestemming moet worden gevraagd voor alle mogelijk betrokken personen, wat vooral tot een enorme administratieve last leidt en niet tot daadwerkelijke bescherming van privacy, aangezien individuen dan voortdurend toestemming moeten en zullen geven voor verwerking van huns inziens onschuldige gegevens. Dit is in essentie wat we gezien hebben met het toestemmingsvereiste voor

3. Ik gebruik 'data' veelal in enkelvoud, in navolging van het vigerende gebruik in de IT-branche en in het Engels (https://onzetaal.nl/taaladvies/advies/de-data-is-zijn-onderzocht). Deze keuze is mede ingegeven doordat ik mij richt op het belang van data in de zin van in plaats van 'gegevens'. De lezer moet dus afstand nemen van de oorspronkelijke betekenis in het Latijn, die inmiddels in het maatschappelijk verkeer nauwelijks meer wordt gevolgd. Evenzo hoeven we niet te aarzelen om 'digitalis' te gebruiken als adjectief voor zekere IT-ontwikkelingen ofschoon dit voor anderen zou doen denken aan vingerhoedskruid of het Latijnse .
4. Ik schets het systeem van de Wbp slechts kort nu dit systeem als zodanig hier niet onderwerp van discussie is. Geïnteresseerden worden verwezen naar de overige preadviezen alsmede Berkvens & Prins (2014).
5. "elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon" (art. 1 sub a Wbp).
6. Art. 8 sub a Wbp.
7. Andere partijen zoals de 'bewerker' (art 1 sub e Wbp) vallen onder zijn verantwoordelijkheid.
8. Dit is nochtans de weg die vooralsnog lijkt te worden ingeslagen, zie verwijzingen bij Zwenne (2013) en Cuijpers & Marcelis (2012).
9. Zie verder de uitvoerige kritiek van Zwenne (2013) en Cuijpers & Marcelis (2012).

cookies, dat eerst te scherp leek te worden aangezet en daarna is versoepeld omdat het onwerkbaar was en onwenselijke gevolgen had.[10]

Dit alles wil niet zeggen dat bescherming van persoonsgegevens niet zinvol is, echter het lijkt beter dit te beperken tot concrete gegevens die vrij direct personen en hun kenmerken betreffen. De toenemende greep van bedrijven en buitenstaanders op onze privacy behoeft aanvullende benaderingen ter inperking.

Een alternatieve of aanvullende benadering zou zijn dat het privacyrecht zich sterker richt op het reguleren van het *gebruik* ('verwerking' zegt de Wbp) van data ook na of los van toestemming. De preadviezen van Corien Prins en Lokke Moerel respectievelijk Mireille Hildebrandt richten zich dan ook mede op nadere controle en regels over de fase na het verzamelen van data.

Deze twee benaderingen, geënt op regulering van wat we zouden kunnen aanduiden[11] als 'bezit' dan wel 'gebruik' van persoonsgegevens, zijn belangrijke bouwstenen om privacybescherming van burgers te verwezenlijken. Zij zijn echter niet toereikend om alle belangen van individuen in de digitale samenleving afdoende te beschermen. Twee casus laten iets zien van de problematiek.

> Een vrouw wordt erop gewezen dat op Facebook een filmpje is gezet waar zij met haar toenmalige vriend seks heeft. Destijds is dat met haar toestemming gemaakt door haar vriend, maar met de bedoeling dat dit privé zou blijven. Het is onbekend wie het filmpje op Facebook heeft gezet. De vrouw wil de dader aanspreken, maar Facebook weigert medewerking. Zij maakt een kort geding aanhangig teneinde de persoonsgegevens van de dader te verkrijgen. Bij de zitting stelt Facebook dat zij niet langer over de gegevens beschikt nu deze zijn gewist. De Voorzieningenrechter gelooft dit niet en beveelt onder meer dat Facebook medewerking moet verlenen aan een deskundigenonderzoek van de Facebook-servers om te bepalen of deze gegevens toch nog te achterhalen zijn.
> (Rb Amsterdam 25 juni 2015, ECLI:NL:RBAMS:2015:3984)

> Een man heeft zijn verzameling digitale foto's bij een sociale netwerksite opgeslagen, zodat ook anderen de foto's kunnen zien. Hij bewaart geen backup. Na een serverupgrade kan hij niet langer bij zijn foto's; als zijn account weer hersteld is blijkt deze leeg te zijn. Uiteindelijk blijkt dat bij de upgrade zijn account tijdelijk onzichtbaar was. Toen de helpdeksmedewerker een nieuwe account met dezelfde naam creeërde werd de oude account overschreven. De foto's zijn definitief verdwenen, zegt de netwerksite.

10. Zie de latere wetswijziging (wetsvoorstel 33902, inmiddels aangenomen en in werking getreden), als beschreven in Computerrecht 2014/87 en 2015/60.
11. Ik wijk hier bewust van het begrippenkader van de Wbp af, om het mogelijk te maken een verbinding te leggen met de privaatrechtelijke benadering van digitale ontwikkelingen.

Beide casus laten zien dat het in het digitale tijdperk niet louter gaat om bescherming tegen het bekend worden van persoonsgegevens. Een filmpje of foto is eigenlijk niet zozeer een gewoon persoonsgegeven maar vooral een *databestand*.[12] Bovendien wilde de vrouw nu juist persoonsgegevens van de dader achterhalen en was het probleem dat Facebook deze weigerde af te geven en uiteindelijk heeft gewist. Privacybescherming lijkt hier veeleer het obstakel te zijn, nu de weigering van Facebook mogelijk is ingegeven door privacybezwaren tegen het prijsgeven van de persoonsgegevens van de dader. In het tweede voorbeeld is de bedoeling juist dat de foto's voor anderen zichtbaar zijn en is het probleem dat de foto's zijn verdwenen. In beide gevallen speelt een verlies aan *controle*.[13]

Daarnaast blijkt in beide casus dat het publiekrechtelijke deel van het privacyrecht geen rol van betekenis speelt. In de eerste casus zou weliswaar theoretisch het Cbp[14] actie kunnen ondernemen, echter in de praktijk zal het Cbp niet snel zijn beperkte capaciteit inzetten om op verzoek van een particulier tegen een incidentele overtreding van een andere particulier op te treden. Bovendien kan het Cbp geen schadevergoeding voor het slachtoffer verkrijgen. Als individuen bescherming wensen zullen zij zelf een privaatrechtelijke actie moeten starten: het is van belang dat het privaatrecht hen daartoe de mogelijkheden biedt.[15]

1.2 Lijn van het betoog

In dit preadvies zal ik betogen dat het privaatrecht kan bijdragen aan de gewenste controle, als men digitale fenomenen vanuit een ander perspectief benadert. Het draait erom dat zowel *bezit* als *gebruik* van data, en wat ik noem (par. 3.3) digitale objecten, verdergaande privaatrechtelijke erkenning behoeft. Dit combineert in essentie de twee privacyrechtelijke benaderingen en werkt dit uit met privaatrechtelijke remedies. Daarnaast is institutionele ondersteuning nodig opdat deze remedies daadwerkelijk effectief worden (par. 4). Het privaatrecht beweegt zich al in de hier geschetste richting, zoals blijkt uit allerlei verspreide ontwikkelingen. Ik

12. Het is waarschijnlijk wel een persoonsgegeven in de zin van de Wbp, maar die kwalificatie is vermoedelijk alleen voor Wbp-specialisten interessant. Persoonsgegevens kunnen ook onschuldige gegevens zijn als de hobby van een individu (HvJ 6 november 2003, zaak C-101/01 (Lindqvist)), zodat die kwalificatie weinig zegt over de ernst van de inbreuk op de privacy (in de zin van art. 8 EVRM).
13. T.a.v. controle over persoonsgegevens bij de overheid: Schoenmakers, Sloots & Wendt (2014).
14. Het Cbp wordt sinds 1 januari 2016 (Wet 4 juni 2015, Stb. 2015/230, iwtr. Stb. 2015/281) 'in het maatschappelijk verkeer' aangeduid als 'Autoriteit Persoonsgegevens', zie art. 51 lid 4 Wbp. Dit preadvies lijkt mij niet te vallen onder het maatschappelijk verkeer in deze zin.
15. Art. 8 EVRM verplicht hier wat betreft privacy ook toe, gelet op de noodzaak van een 'effective remedy'.

betoog hier dat deze ontwikkelingen het beste verklaard kunnen worden door een erkenning van de waarde en het belang van digitale objecten. Centraal in de argumentatie is dat gedigitaliseerde informatie of *data*[16] gecontroleerd kan worden en dat enige controle ook wenselijk is. Let wel: ik spreek over *digitale* informatie (data), wat iets anders is dan informatie zonder meer (zie par 2.4).[17] Nodig is niet alleen bescherming *tegen* gebruik van persoonsgegevens, maar ook en zelfs veeleer controle *over* digitale gegevens, data. Dat hoeft niet alleen via een eigendomsconcept van gegevens;[18] controle kan ook ontstaan door de mogelijkheid je te verzetten tegen bepaalde gevolgen of vormen van gebruik. De voornaamste instrumenten van het privaatrecht – eigendom, contract, en onrechtmatige daad – behoeven aanpassing voor gebruik in het digitale tijdperk.

Om misverstanden te voorkomen: ik verdedig *niet* dat er eigendom op informatie of gegevens nodig is, dat bestrijd ik integendeel. In lijn hiermee bestrijd ik eveneens dat eigendom op persoonsgegevens nodig of wenselijk is. Veeleer betoog ik dat een eigendomsrechtelijke *benadering*, in termen van bevoegdheden en rechten, van *gedigitaliseerde* informatie (dus niet informatie sec) nodig is. Een dergelijke benadering noopt wellicht tot aanpassing van het traditionele eigendomsbegrip. Dit blijkt in het bijzonder uit de veelvoorkomende misvatting dat een eigendomsrechtelijke benadering exclusiviteit vereist. De lezer zij dus gewaarschuwd: men kan de hedendaagse digitale wereld niet goed begrijpen als men blijft denken dat data moet lijken op zaken om er privaatrechtelijke bescherming aan te geven.

Ik zal beginnen met een beschrijving van de ontwikkeling van een primair fysieke wereld naar een digitale wereld waarin data centraal staat (par. 2). Dit is de wereld van de *homo digitalis*. Vervolgens zal ik beargumenteren dat controle op digitale activa het beste kan aansluiten bij de goederenrechtelijke benadering van zaken, terwijl privaatrechtelijke bescherming van privacy kan worden bereikt met reeds bestaande remedies, waarbij rechterlijke controle op contractsvoorwaarden noodzakelijk is ter voorkoming van een te vergaand wegcontracteren van bevoegdheden en rechten op digitale activa en privacy (par. 3). Tot slot zal ik in een korte schets aangeven dat het in par. 3 beschreven juridisch kader verdergaande aanpassingen in de juridische en digitale infrastructuur behoeft om daadwerkelijk effectief te zijn (par. 4).

Mijn argumentatie is, zoals past bij een privaatrechtelijk betoog, niet beperkt tot principes maar vooral ook gericht op daadwerkelijke toepas-

16. In het Engels is deze term dubbelzinnig aangezien het ook ‘gegevens’ kan betekenen, niettemin wordt het in de literatuur vaak ook of juist gebruikt om de gegevensbestanden aan te duiden. Die dubbelzinnigheid is wezenlijk voor de discussie, vandaar dat ik niet zal proberen een kunstmatige alternatieve eenduidige term te introduceren.
17. Bedrijven als Google en Facebook kunnen daarom betogen dat informatie vrij moet zijn, terwijl zij hun data krampachtig geheim houden.
18. Marwick & boyd (2014) bestrijden bijvoorbeeld een dergelijke benadering.

singsvragen. Een louter principieel betoog loopt al snel het risico losgezongen te raken van effectieve implementatie. Remedies zonder principes zijn blind, maar principes zonder remedies zijn leeg.[19] Omdat dit echter een preadvies is, waarvan de omvang beperkt moest blijven, kan ik slechts in beperkte mate op details ingaan: verdere uitwerking behoeft nader onderzoek. Om dezelfde reden verwijs ik niet uitputtend naar de relevante literatuur, en zal ik niet alle digitale fenomenen die ik noem nader toelichten; ik veronderstel deze bekend en verwijs de lezer zonodig naar zoekmachines als Duckduckgo of Startpage.com, of als men minder aan privacy hecht, Google.

2. Van het fysieke naar het digitale

2.1 Privaatrecht en de fysieke wereld

Het privaatrecht is gevormd door de gestolde ervaring van eeuwen, waardoor principiële doch onwerkbare ideeën grotendeels zijn verdwenen en voornamelijk werkbare regels zijn overgebleven. Rechten die niet zijn te handhaven moeten niet worden toegekend, omgekeerd moeten rechten wel remedies krijgen om geeffectueerd te kunnen worden. *Ubi ius, ibi remedium*. Privaatrecht is meer pragmatisch dan principieel. Daarom streeft het privaatrecht ernaar niet te zeer uit de pas te lopen met de feitelijke werkelijkheid. Als de feiten te lang afwijken van de juridische toestand en het recht daardoor niet langer te handhaven is, moet het recht uiteindelijk wijken voor de feitelijke toestand.[20]

De handhaafbaarheid van het privaatrecht gaat evenwel uit van enige aannames die zo vanzelfsprekend zijn dat zij tot op heden nauwelijks aandacht ontvingen. Handhaving veronderstelt beheersbaarheid van fysieke zaken en personen. Het instrumentarium van verhaal, beslag, exploit, executie, gijzeling veronderstelt de mogelijkheid om met de sterke arm der wet in de fysieke wereld in te grijpen. Niet-tastbare objecten of rechten worden vooral aan de hand van registers[21] juridisch hanteerbaar. In de fysieke wereld is handhaving mogelijk doordat inbreuken meestal gemakkelijk zichtbaar zijn en merkbaar sporen achterlaten. Bescherming van individuele vrijheid en privacy geschiedt primair door fysieke begrenzing als sloten en gordijnen, versterkt met juridische instrumenten als het huisrecht. Die bescherming is echter ook begrensd: de fysieke barrière kan ongedaan worden gemaakt door de werkelijke rechthebbende die zich

19. Vrij naar Kant (begrippen zonder waarneming zijn leeg, waarnemingen zonder begrippen zijn blind).
20. Art. 3:105 BW.
21. Zoals het kadaster (grondeigendom is niet per se tastbaar of zichtbaar), octrooiregister, merkenregister.

toegang kan verschaffen en op die wijze zijn rechten geldend maken, zoals de erfgenaam of deurwaarder ingeval van inventarisatie van de boedel.

Deze nadruk op het fysieke is tevens de grens van de zwaardmacht: het intellectuele domein, de wereld van de geest, blijft grotendeels onttrokken aan juridische regulering. De gedachten zijn vrij (Heine).

2.2 De wereld van de homo digitalis

De status quo begint te schuiven door de opkomst van de digitale wereld. Deze is het gevolg van drie interacterende fenomenen: het toenemend gebruik van digitale data, de toegenomen mogelijkheden voor automatische dataverwerking, en de opkomst van Internet. Het digitale is niet langer een loutere afspiegeling van de fysieke wereld doch heeft een zelfstandig belang. We hebben de sprong naar cyberspace gemaakt. De traditionele middelen en regels behoeven daarom aanpassing aangezien de digitale wereld niet aan dezelfde wetten gehoorzaamt als het fysieke.

Heel kort gekenschetst gaat het om het volgende.[22]

1. *Data*, gedigitaliseerde informatie, wordt tegenwoordig op zeer grote schaal verzameld en verwerkt. De beschikbaarheid van grootschalige dataopslag tegen zeer lage kosten, alsmede het wijdverbreide gebruik van computers (van enorme mainframes en serverparken tot minuscule smartwatches en sensoren) stimuleert het verzamelen van data. Veel informatie die vroeger alleen in de hoofden van mensen of op papier of in andere vorm beschikbaar was is tegenwoordig digitaal beschikbaar als *data*.[23] Inmiddels worden daarnaast zeer veel gegevens automatisch verzameld met behulp van goedkope sensoren, cameras e.d.[24] Die datacollectie is weer mogelijk door de goedkope opslag, naast het feit dat data wezenlijk gemakkelijk te kopiëren is.
2. *Computers* zijn in de laatste decennia voortdurend sneller en kleiner geworden en goedkoper, waardoor particulieren daadwerkelijk de rekenkracht van vroegere mainframes in hun zak hebben in de vorm van een smartphone. Deze snelheid heeft inmiddels geleid tot kwalitatief nieuwe vorem van computergebruik: real-time simulatie, ook 'slimme' analyse met expertsystemen (big data, ook digitaal leren). Computers kunnen daardoor conclusies trekken en activiteiten verrichten op een niveau dat vergelijkbaar is met dat van mensen. (1) en (2) samen duidt men ook wel aan als *datafication*.
3. *Internet* maakt snelle en goedkope communicatie mogelijk over de gehele wereld. Dit maakt mogelijk dat samengewerkt wordt over de

22. Het navolgende is geenszins origineel; ik som het alleen op ter opfrissing. Zie bijv. ook Kleve (2004: hfdst. 3).
23. Dit is bewust bevorderd door projecten als Google Books en Google Maps, elektronische archivering door overheden.
24. Mayer-Schönberger & Cukier (2013).

> gehele wereld met nagenoeg onmiddellijke communicatie, waardoor de fysieke locatie irrelevant wordt.[25]

De combinatie van deze drie ontwikkelingen leidt tot het ontstaan van een digitale wereld die grotendeels zelfstandige waarde en betekenis heeft. In die digitale wereld zijn er geen fysieke locaties of identiteiten meer, slechts weblocaties en digitale personae. We wisselen informatie en digitale objecten uit, linken, appen, en twitteren dat het een lust is. Er is daardoor minder behoefte aan fysieke objecten en bezigheden als papieren boeken of sport, nu we evengoed onze informatiebehoefte of spelbehoefte digitaal kunnen bevredigen. We kopen digitale goederen als ebooks en muziek, en slaan deze op in de *cloud* (digitale kluizen als DropBox). We maken online vriendschappen met andere mensen zonder hun fysieke plaats of nationaliteit te kennen. We werken samen met talloze onbekenden om een project te financieren via *crowdfunding.* Overigens heeft dit alles ook een schaduwzijde: het oprukken van cybercrime.[26]

Dit alles is alleen mogelijk met elektronische gegevensbestanden, data. Data werkt anders dan fysieke objecten. Data is fluïde, niet solide. Tegelijk is data reëel. Enerzijds is data zeer vluchtig – immers kan gemakkelijk restloos verdwijnen, terwijl fysieke objecten vaak nog enigszins hersteld kunnen worden –, anderzijds zeer persistent doordat overal kopieen kunnen zijn bewaard (waardoor onwelgevallige data moeilijk te verwijderen is). Tezamen met de grote hoeveelheid gegevens die beschikbaar zijn over individuen leidt dit tot vrees voor verlies van privacy en controle. Ook is bewijs en verhaal hierdoor lastiger dan in de fysieke wereld. Het vluchtige van data strekt zich uit tot de gehele digitale wereld: alles is afhankelijk van een digitale infrastructuur: servers, dienstverleners, omgevingen. Als die verdwijnen, vervliegen eveneens de objecten daarin. Het vluchtige van data is tegelijk een kracht: het is gemakkelijk om iets in het virtuele domein te construeren. Daarmee is het echter ook mogelijk voor kwaadwillenden om onjuiste indrukken te wekken. Vertrouwen is ook in de digitale wereld een probleem.

Verder leidt de vrijwel gratis communicatie tot verlagen van transactiekosten, en daarmee tot het omzeilen van de traditionele tussenpersonen en tussenschakels. Inmiddels beginnen we te zien dat een groot deel van de economie bestaat uit tussenpersonen, blijkend uit het succes van zogenaamde *disruptive* businessmodellen als Uber en Airbnb die deze schakels overslaan.

De digitale ontwikkelingen leiden dus tot nieuwe mogelijkheden naast nieuwe problemen. Een voorbeeld van een daadwerkelijk nieuw fenomeen is de *blockchain*. Dit is in essentie een digitaal register van transacties van

25. Shirky (2008).
26. Koops (2014), Van der Meulen & Lodder (2014), Tjong Tjin Tai e.a. (2015).

Bitcoin, dat essentieel is voor Bitcoin.[27] Hiermee wordt openbaar bijgehouden dat een zekere bitcoin via geldige transacties bij een zekere eigenaar is terechtgekomen. De blockchain bevindt zich niet op een centrale plaats: bij iedere bitcoin miner staat een kopie op de computer. De *bitcoin miners* helpen om de gecommuniceerde transacties te verifieren en in hun eigen kopie van de blockchain te bewaren. In ruil ontvangen zij weer (een kans op) bitcoins terugkrijgen. Een dergelijk publiek, gedistribueerd, automatisch functionerend register was vroeger onmogelijk.[28] Data, *computing power* en Internet tezamen maken dit werkelijkheid.

2.3 Van klassieke kwalificatie naar erkenning van zelfstandigheid van digitale fenomenen

Hoe heeft het privaatrecht op deze ontwikkelingen gereageerd? Reeds vanaf de introductie van computers is er discussie geweest over de juridische erkenning en kwalificatie van diverse digitale verschijnselen. De Internetrevolutie heeft dit proces versneld. Achteraf kunnen we vaststellen dat de specifieke geïntroduceerde regels op zichzelf weinig hebben toegevoegd aan wat reeds zou gelden op basis van het commune, pre-digitale recht. Ons privaatrecht is *grosso modo* voldoende open en flexibel om nieuwe verschijnselen betrekkelijk moeiteloos of zelfs geruisloos te incorporeren.[29] Waar twijfel rees, zijn nieuwe wettelijke regels aangenomen.

Digitaal bewijs kon op basis van ons open stelsel van bewijsrecht zonder enige aanpassing worden erkend.[30] Elektronische handtekeningen[31] zijn voornamelijk expliciet geregeld omdat de Europese wetgever vreesde dat uiteenlopende regels een belemmering voor het handelsverkeer zou vormen.[32] Elektronische overeenkomsten[33] en de elektronische akte zijn geregeld wegens onduidelijkheid in hoeverre het schriftelijkheidsvereiste en de daaraan verbonden belangen in de weg stonden aan elektronische aktes.[34]

Enige frictie kan niettemin bestaan, in het bijzonder waar vereisten zijn geënt op de fysieke wereld, en niet evident is dat deze vereisten kunnen

27. Spaas & Van Roey (2015), Tjong Tjin Tai (2015a) met verwijzingen.
28. Overigens is er onzekerheid over de lange-termijn levensvatbaarheid van Bitcoin, zie Mike Hearn, 'The resolution of the Bitcoin experiment', https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.8mkwcxqr3 gepubliceerd 15 januari 2016. Dit geeft aan dat ook dergelijke systemen zwaktes hebben.
29. Vgl. Hendrikse (2014) voor het handelsrecht. Zie bijv. voor de notariële zorgplicht Blokland (2015).
30. Uitvoerig Van Stekelenburg (2009). Een uitzondering was de elektronische akte (zie hierna).
31. Art. 3:15a BW, ter implementatie van Richtlijn 1999/93/EG.
32. Considerans 4 Richtlijn 1999/93/EG.
33. Art. 6:227a-c BW.
34. Thans art. 156a Rv, hierover bijv. Martius (2007a, 2007b en 2008), Van Es (2008), Van Drunen & Snijder-Kuipers (2014).

worden losgelaten in het digitale domein. Dan is het nodig om expliciet de regels aan te passen; dit kan ook nodig zijn als signaal dat bepaalde vereisten inderdaad niet meer nodig zijn.[35] Voorbeelden zijn de notariële executieverkoop,[36] de bescherming van de koper te goeder trouw bij koop in een winkel ('daartoe bestemde bedrijfsruimte', art. 3:86 lid 3 BW),[37] de publicatie op Internet van de verlening van handlichting.[38] Ook het digitale exploot (art. 45 lid 2 Rv) kan men hieronder scharen.[39]

Het juridische handwerk om deze verschijnselen te kwalificeren en aan te geven hoe zij behandeld moeten worden is nuttig, maar wijkt niet intrinsiek af van wat er bij talloze andere nieuwe verschijnselen gebeurt.[40] Het komt grotendeels neer op het toespitsen en bijstellen van de open normen van het privaatrecht, op basis van een goed ontwikkeld gevoel voor rechtvaardigheid en praktijk, aansluitend op het systeem van het recht.

Inmiddels heeft er zich echter een fundamentelere verschuiving voltrokken. Dit kan geïllustreerd worden aan de hand van het arrest HR 27 april 2012, NJ 2012/293 (Beeldbrigade). De hier aan de orde zijnde vraag was of titel 7.1 van het BW inzake de koopovereenkomst ook van toepassing was op verkrijging van een digitale kopie van software.[41] Technisch-juridisch bestaat deze transactie uit het sluiten van een overeenkomst waarbij tegen betaling een gebruikslicentie voor zekere software wordt verleend, en het feitelijk verschaffen van een digitale kopie van die software (meestal door een download, wat in essentie communicatie van data is van de server naar de computer van de gebruiker). Het lijkt op zichzelf niet vreemd om aan te sluiten bij de koopregeling:[42] er wordt iets welomschrevens verkregen tegen betaling. De Hoge Raad weigert aan te geven hoe software gekwalificeerd moet worden (r.o. 3.4). Maar zijn redenering om in r.o. 3.5 te komen tot rechtstreekse toepasselijkheid van de kooptitel verdient nadere bestudering.

Als eerste wordt aangegeven dat de kooptitel van toepassing is op alle goederen, de wetgever wenste derhalve een ruim bereik eraan te geven. Vervolgens overweegt de Hoge Raad dat "een overeenkomst tot het

35. Aangezien anders partijen het niet zouden aandurven van de vormvereisten af te wijken.
36. Vonck (2014) met verwijzingen.
37. Koops en Verheul (2014), Salomons (2000), Fikkers (2000).
38. Rb. Midden-Nederland 10 april 2015, ECLI:NL:RBMNE:2015:2404.
39. Flach (2014: 82-83). Zie nader par. 4.2 over digitale identiteit.
40. Vgl. Van der Ven (2014).
41. De wetgever heeft dit standpunt overgenomen voor de koop van alle digitale inhoud, waarbij een uitzondering is gemaakt voor streaming overeenkomsten (waarbij immers geen feitelijke macht is uit te oefenen over de beschikbaar gestelde inhoud). Zie TK 2014-15, 34071, nr. 2 en 3 (p. 2-3) over het voorgestelde nieuwe art. 7:5 BW, en eerder Neppelenbroek (2013) en Loos (2013). Overigens is het met technische kunstgrepen wél mogelijk om streaming inhoud tegen de bedoeling van de leverancier in op te slaan. Omdat daar dan de toestemming voor ontbreekt zal dit niet vallen onder het 'feitelijke macht' kunnen uitoefenen.
42. Loos (2011).

aanschaffen van standaardcomputerprogrammatuur – op een gegevensdrager of via een download – voor een niet in tijdsduur beperkt gebruik tegen betaling van een bepaald bedrag ertoe strekt de verkrijger *iets te verschaffen dat geïndividualiseerd is en waarover hij feitelijke macht kan uitoefenen* [cursivering TTT]." Dit pleit, zegt de Hoge Raad voor toepasselijkheid van de kooptitel.

Tot nog toe bestond de neiging (zie par 2.4) om data als iets accidenteels te beschouwen: de aandacht ging uit naar de licentieovereenkomst, het IE-recht, de know-how. Data werd gezien als vluchtig, ongrijpbaar. Nu echter erkent de Hoge Raad uitdrukkelijk dat een softwarebestand (en daarmee data) *geïndividualiseerd* is en dat daar *feitelijke macht* over kan worden uitgeoefend. Dit ligt zeer dicht aan tegen de kenmerken die gewoonlijk aan stoffelijke objecten, zaken worden toegekend:[43] zaken zijn voor *menselijke beheersing* vatbare stoffelijke objecten.

De erkenning van *onstoffelijke doch beheersbare* objecten kan een basis vormen voor verdergaande erkenning van de zelfstandigheid van de digitale wereld.[44] Het arrest Beeldbrigade vormt zodoende een scharnierpunt tussen een conservatieve benadering, uitgaande van het geldend recht en de daarin besloten liggen uitgangspunten, en een vernieuwende visie waarin de bekende steunpunten verlaten worden en een nieuw evenwicht bereikt moet worden tussen klassieke beginselen en hedendaagse behoeften.

2.4 Data: digitale informatie

Om misverstanden te vermijden is het nodig om scherp te krijgen wat onder data moet verstaan, en vooral: niet verstaan. Data is in essentie de digitale belichaming van informatie, dat wil zeggen, de belichaming in (gegevens)bestanden.[45] Het is daarmee onderscheiden van de informatie zelf,[46] op dezelfde wijze als pagina 110 van een gedichtenbundel in mijn boekenkast onderscheiden is van het gedicht 'Herinnering aan Holland' dat daarop is afgedrukt. Het is de data *zelf* die van belang is. Zo draait de centrale overweging in het Beeldbrigade-arrest ook niet om de softwarelicentie (die alleen een *recht* op gebruik geeft, niet de feitelijke mogelijkheid daartoe) maar om de feitelijke levering van een *bestand* (dat het feitelijke gebruik van de software mogelijk maakt).

43. Evenzo Spath (2015a), p. 45 en (2015b), verwijzend naar Drion (2013). Verstijlen (2014) betoogt dat software als vermogensrecht moet worden beschouwd.
44. Een alternatieve benadering is die van Neppelenbroek (2006a, 2013a), die betoogt dat data(bestanden) als moeten worden beschouwd. Dit leidt tot enigszins vergelijkbare resultaten; een verschil is bijvoorbeeld dat data in zijn opvatting wordt nagetrokken door de drager.
45. De concept-richtlijn digitale inhoud COM(2015)634 geldt voor digitale inhoud, waarmee gedoeld wordt op data (art. 2(1)).
46. Zie de scherpzinnige en grondige discussie in Kleve 2004, p. 105-113 en 139-146, Neppelenbroek (2006a en 2013a).

Dit laat tevens zien waarom het hier niet gaat om een quasi-IE-recht. IE-rechten, in het bijzonder het auteursrecht, hebben het zogenaamde *corpus mysticum* als object.[47] Een afdruk van een gedicht is niet het object van auteursrecht; als alle afdrukken waren vernietigd zou het gedicht nog steeds bestaan. Iemand die het uit zijn hoofd heeft geleerd kan het dan weer opschrijven. De omvangrijke databestanden waar het tegenwoordig om gaat bestaan daarentegen alleen in digitale vorm: zij kunnen onmogelijk worden onthouden en weer gereconstrueerd uit het geheugen. Denk aan digitale foto's, een bestand met meetgegevens van een fabriek; als alle kopieën van zulke databestanden zijn verdwenen is de data zelf weg. Mensen kunnen weliswaar veel informatie onthouden, maar niet de digitale bestanden waar het hier om gaat: de meeste data bestaat uit bits/bytes die voor mensen geen betekenis hebben en daarom niet te onthouden zijn.[48]

Hiermee is een deel van de vroegere discussies irrelevant: deze betroffen juist de informatie of gegevens.[49] In het verleden was informatie vooral van belang in de vorm van *kennis* in de hoofden van mensen, aangezien informatie alleen door mensen kon worden verwerkt. Tegenwoordig kan informatie ook door computers worden verwerkt, mits het in digitale vorm beschikbaar is: als *data*. Die vertaalslag is noodzakelijk en opent, eenmaal verricht, een wereld van mogelijkheden. Een simpel voorbeeld is het digitaliseringsproject van Google Books. Qua informatie heeft dit in eerste instantie niets opgeleverd: alle informatie was al in boeken beschikbaar, en Google claimt ook geen rechten op die informatie (kan dat bovendien niet). Echter de beschikbaarheid van deze informatie als *data* is nuttig en waardevol en biedt tal van nieuwe mogelijkheden.[50] Grootschalige verzamelingen data laten analyses toe op nooit vertoonde schaal. *Streamen* van geripte muziek of van video *on demand* is een alledaags verschijnsel, evenals het online delen van fotobestanden op *social media*. Steeds meer informatie of objecten worden gedigitaliseerd, of zijn zelfs van meet af aan en zelfs uitsluitend beschikbaar in het digitale domein. We delen informatie *via* data. Data is het nieuwe medium. De data zelf moet dan ook als object van recht worden erkend.[51]

Dit doet de oude discussies kantelen. De digitale belichaming van informatie is namelijk, anders dan informatie op zichzelf, wel voor menselijke beheersing vatbaar, en heeft bovendien een duidelijke gebruikswaarde

47. Spoor, Verkade & Visser (2005), p. 60.
48. Dit zal alleen anders zijn voor een klein tekst-bestandje in platte-tekstformaat (.TXT).
49. Bijv. Verkade (1988), Prins (2005).
50. Denk ook aan het (apocriefe?) geval van waarbij de geautomatiseerde administratie van een bedrijf opzettelijk alleen op papier afgedrukt werd overhandigd.
51. Ten aanzien van software en digitale content heb ik dit reeds betoogd in Tjong Tjin Tai (2003), aansluitend bij Amerikaanse doctrine en rechtspraak, welke lijn thans ook in Europa lijkt te zijn ingezet. Zie HvJ 3 juli 2012, C-128/11 (UsedSoft), waar het bestand van software eenzelfde juridische behandeling krijgt als gekochte fysieke objecten. Zie ook Neppelenbroek (2013a), p. 174 e.v.

voor particulieren en bedrijven. Tegelijk brengen deze mogelijkheden ook extra risico's met zich op het vlak van privacy-aantasting.

De waarde van data vindt tot op heden onvoldoende erkenning in het privaatrecht. Ofschoon er op veel punten wel enige bescherming mogelijk is via contractenrecht en onrechtmatige daad zijn er nog steeds ernstige lacunes. Het is daarom zinvol bij wijze van perspectiefwijziging uit te gaan van de zelfstandige belangen gemoeid met data.

Het gaat hierbij om twee belangen:

a. De waarde van data voor de 'eigenaar'. Degene die feitelijk en/of juridisch kan beschikken over de data heeft daar baat bij. Dit kan bestaan uit een gebruikswaarde voor hem persoonlijk (zoals het genoegen van terugkijken van privé-foto's), maar ook economische waarde en/of marktwaarde. De waarde vereist niet per se exclusiviteit van de data, al is dat bij marktwaarde meestal wel het geval, aangezien 'verkoop' van data meestal enige mate van exclusiviteit veronderstelt.
b. Het vermogen van data om derden te benadelen. Dit kan privacy betreffen, maar ook schade als gevolg van gebrekkige data. Schending van IE-rechten blijft hier grotendeels buiten beschouwing, nu dat in de bestaande literatuur reeds uitputtend wordt behandeld. Strikt genomen is privacy een onderwerp dat los van data kan worden behandeld, echter de opkomst van de digitale samenleving, met de mogelijkheden voor grootschalige automatische verwerking (en openbaarmaking) van privacy-gevoelige informatie, heeft dit belang klemmender gemaakt.

We beheersen data, en data beheerst ons. In hoeverre helpt het privaatrecht om de controle terug te krijgen? In de digitale wereld verwachten we dat we over 'onze' databestanden controle kunnen uitoefenen, terwijl we eveneens verwachten dat data ons niet overvleugelt. Dit kan worden gerealiseerd door regulering die zich richt op bezit en gebruik van data.

3. Privaatrecht voor het digitale domein

3.1 Inleiding

In deze paragraaf zal ik betogen dat voor wat ik zal noemen 'digitale activa' (data en digitale objecten) een goederenrechtelijke benadering zinvol is, nu daarmee diverse lacunes in het privaatrecht worden blootgelegd. Het positieve recht ontwikkelt zich ook in deze richting. Een complete regeling vereist daarnaast regulering van het gebruik van data, waaronder ook privacybelangen vallen.

3.2 Data en eigendomsbevoegdheden

Het gebruik van het criterum van 'feitelijk hanteerbaar' (par. 2.3) maakt het mogelijk om meer greep te krijgen op digitale fenomenen die voordien een tamelijk mistig bestaan leidden in het juridische denken. Hiervoor is het meest aansprekend het perspectief van *eigendom*. Dit behoeft enige toelichting. Het Nederlandse privaatrecht zou alleen toestaan te spreken over data als vermogensrecht (aangezien eigendom als begrip alleen mag worden toegepast op zaken, art. 5:1 lid 1 BW). Ik zal hier niettemin spreken van 'eigendom', nu ik dit als analytisch begrip wil hanteren dat ruimer is dan het Nederlands positieve recht, en daarmee eventueel voor wijziging van het wettelijke systeem zou willen pleiten.[52] Dit ruimere gebruik sluit bovendien beter aan bij het Engelse gebruik van 'property'. Het is dan wel van belang te expliciteren waar ik op doel met een benadering vanuit 'eigendom'.

In het common law perspectief doelt men met 'eigendom' veelal op een bundel van bevoegdheden en/of rechten.[53] Het gaat dan met name om[54]

a. gebruik (nut), wat bij data mogelijk wordt gemaakt door toegang (*access*) tot de data,
b. beschikkingsbevoegdheid (controle), wat bij data mogelijk wordt gemaakt door verbodsrechten, controle op toegang (feitelijk dan wel juridisch),
c. vertrouwelijkheid, te weten exclusieve toegang. Dit is bij zaken in beginsel vanzelfsprekend:[55] de eigenaar hoeft geen inbreuken te dulden, mede omdat gebruik van de zaak snel wordt gehinderd door inbreuken door derden. Bij data ligt dat echter anders: data is niet vanzelf exclusief.[56]

Bij data hoeven niet steeds al deze bevoegdheden of belangen aan de orde te zijn. Er zijn diverse gevallen waar in essentie toegang tot data (of zelfs alleen informatie) volstaat als die aanwezig is, zonder dat controle of exclusiviteit nodig is. In die oudere procedures bewandelde eiser dan de

52. Zie ook Tjong Tjin Tai (2015b), vgl. Neppelenbroek (2012).
53. Alexander & Peñalver (2012:2), Purtova (2011). Het is daardoor gemakkelijker om data als aan te merken. Kleve (2004, p. 188) wijst op wisselende jurisprudentie.
54. Asser/Bartels & Van Mierlo 3-IV 2013/38 noemen alleen de eerste twee. Snijders & Rank-Berenschot (2012), nr. 174-178 noemen deze drie (in andere bewoordingen) en daarnaast het recht op vruchten ('generatievermogen'), en zie ook nr. 65-68. Er zijn daarnaast meer bevoegdheden die vooral voor juristen interessant zijn, zoals het en het separatist zijn.
55. Asser/Bartels & Van Mierlo 3-IV 2013/38 noemt exclusiviteit daarom niet als bevoegdheid.
56. Vgl. Fairfield (2005: 1049), die onderscheidt tussen 'rivalrous' (feitelijk uitsluitend) en 'exclusivity' (exclusiviteit, die gevolg kan zijn van 'rivalrous' maar ook van een juridische regeling). Ook Gleason & Fairfield (2004: 317), die lijken te suggereren dat in cyberspace exclusiviteit geen vereiste voor eigendom behoeft te zijn.

weg van afdwingen van daden of handelingen, omdat er geen eenvoudig gereedliggende data aanwezig was.[57] De mogelijkheid om kopieën van data te verkrijgen[58] is een efficiënt alternatief voor het belastende inbeslagnemen van administratie.[59]

Daarentegen zijn er ook gevallen waar juist de exclusiviteit of vertrouwelijkheid van belang is. Traditioneel zien we dit bij geheimhoudingsplichten van beroepsbeoefenaren, vertrouwelijkheidsbedingen (confidentiality/non-disclosure), en het leerstuk van bescherming van know-how.[60] Het gaat hier primair om contractuele aangelegenheden: het is op zichzelf niet onrechtmatig om van vertrouwelijke gegevens kennis te nemen, al is er een tendens om dergelijke gegevens verdere bescherming te verlenen.[61] Exclusiviteit kan overigens ook aan de orde zijn bij data waar wél een verbodsrecht aanwezig is, zoals bij data over privé-aangelegenheden. Daar kan een individu ervoor kiezen de vertrouwelijkheid selectief op te heffen, al dan niet uit commerciële motieven.[62] De grondslag voor bescherming is dan gelegen in *erga omnes* uitsluitende rechten als het recht op privacy (besloten in art. 8 EVRM) of het portretrecht (art. 25 Aw).

Het ongehinderde, eventueel exclusieve, gebruik van data wordt versterkt door diverse strafrechtelijke bepalingen die aantasting van de vertrouwelijkheid en het genot van data strafbaar verklaren: computervredebreuk inclusief overnemen van data in de computer (art. 138ab lid 1 en 2 Sr),[63] toegang belemmeren tot een computer o.a. door DDoS-aanval (art. 138b Sr), aftappen of opnemen van data die voor anderen is bestemd (art. 139c Sr) en het bezit van dergelijke afgetapte data (art. 139e Sr), bekendmaking van door een misdrijf verkregen vertrouwelijke gegevens van een onderneming (art. 273 lid 1 sub 2 Sr), schending van de vertrouwelijkheid van digitale communicatie (art. 273d Sr), opzettelijke en culpose vernie-

57. Bijv. AIDS-test (HR 18 juni 1993, NJ 1994/347, vgl. HR 12 december 2003, NJ 2004/17), ook afdwingen van vaderschapsonderzoek.
58. Thans mogelijk met het bewijsbeslag (zie par. 4.4) en algemener de exhibitieplicht (art. 843a Rv).
59. Zoals in strafrechtelijke zaken of bij faillissement mogelijk is. Indien achteraf de inbeslagname onterecht was, heeft de onderneming schade geleden doordat de administratie enige tijd niet toegankelijk was, zoals bv. in HR 19 december 2003, NJ 2004/348 aan de orde.
60. Gielen (1999), Van der Korst (2007: 54-63), Huydecoper (2008), Pors (2013).
61. Zie de ontwerp-Richtlijn bedrijfsgeheimen, COM(2013)813 final. Daarbij is een element van 'bedrijfsgeheim' dat de informatie handelswaarde bezit omdat zij geheim is (art. 2 lid 1 sub a).
62. HR 19 januari 1979, NJ 1979/383 ('t Schaep met de 5 pooten), HR 14 juni 2013, NJ 2015/112 (Cruijff). Vgl. House of Lords 2 mei 2007, Douglas v Hello! [2007] UKHL 21.
63. Het voorgestelde art. 138c Sr (Voorstel Wet Computercriminaliteit III, ingediend 22 december 2015) maakt ook het enkele kopiëren van niet-openbare data strafbaar (dus zonder eigen computervredebreuk).

ling van computergegevens (art. 350a en 350b Sr).[64] Dit allegaartje aan bepalingen geeft in grote trekken bescherming van data tegen illegaal kopiëren en vernieling/hinder. Ingevolge art. 6:162 BW is inbreuk op wettelijke verboden ook civielrechtelijk onrechtmatig; aan het relativiteitsvereiste zal bij schending jegens de eigenaar evident zijn voldaan.

De feitelijke macht over data (die het gebruik daarvan mogelijk maakt), in combinatie met de hierboven geschetste mogelijkheden van contractenrecht en onrechtmatige-daadsrecht voor het behoud van vertrouwelijkheid en afweren van stoornis kan een 'bezitter' van data nagenoeg in dezelfde positie brengen als die van een bezitter van een goed.[65]

Van de genoemde bevoegdheden blijft dan slechts over de controle of beschikkingsbevoegdheid. Dit bestaat enerzijds uit de mogelijkheid dat de 'eigenaar' ook anderen toegang tot de data kan geven, wat (tezamen met afdwingbare vertrouwelijkheid) juridisch en feitelijk licentiëring toelaat. Anderzijds valt hieronder de daadwerkelijke mogelijkheid van overdracht. Bij know-how was dit in het verleden problematisch. De desbetreffende kennis en informatie was vroeger deels op schrift beschikbaar, in dossiers en dergelijke, en in zoverre overdraagbaar,[66] maar voor een groot deel ook aanwezig in de hoofden van betrokkenen en daardoor alleen te delen, niet over te dragen.[67] Voor data ligt dat evenwel anders: veel data is zo omvangrijk dat zij alleen in digitale vorm aanwezig is. Data kan in die vorm ook eenvoudig feitelijk worden overgedragen.[68] Eventuele exclusiviteit kan grotendeels op verbintenisrechtelijke wijze worden afgedwongen (par. 3.8).

Deze analyse laat zien dat feitelijk en rechtens de 'bezitter' van data nu al vrijwel in een met eigendom vergelijkbare positie verkeert, mits hij correcte contractuele regelingen treft.[69] Vrijwel, maar niet geheel. In de volgende paragrafen zal ik aangeven waar deze positie nog niet gelijk staat, en waar dit wel wenselijk zou zijn. Los van de vraag of data nu wel of niet past in ons goederenrechtelijke systeem[70] blijft dan nog de vraag over of een eigendomsrechtelijke benadering van data wenselijk of passend is.

64. Vgl. voor bepaalde werken art. 161sexies en 161septies Sr.
65. Tjong Tjin Tai (2015b).
66. Vgl. de discussie over het retentierecht op het dossier: HR 15 april 1994, NJ 1995/640 en verwijzingen in Asser/Tjong Tjin Tai 7-IV 2014/117.
67. Huydecoper (2008: 159).
68. Door eenvoudige kopie of transmissie van de data zelf, of als het om zeer grote hoeveelheden data gaat, door feitelijke overdracht van de fysieke dragers.
69. Vgl. Tjong Tjin Tai (2015b).
70. Ik laat derhalve open of ons BW aanpassing behoeft op dit punt, of dat het systeem reeds thans erkenning van data als goed toelaat. Kleve (2004, hfdst. 5 en 6) en Neppelenbroek (2006a, 2013a) verdedigen dat data(bestanden) stoffelijk en daarom goederen zijn. Vgl. Verstijlen (2014) over de inpassing van software in het goederenrecht, en Snijders (2005), die een rekkelijke opvatting over het goederenrechtelijk systeem verdedigt. Zie ook de analyse van Degenkamp (1997).

Daar zal ik nu op ingaan.

Waarom zouden we data als object van 'eigendom' willen behandelen? Twee verwante redenen dienen zich aan: data heeft materiële en immateriële waarde,[71] en data is verkregen door werk en investeringen. Deze laatste rechtvaardiging blijkt overtuigend bij de Europese wetgever: de introductie van het databankrecht en het voorstel voor bescherming van bedrijfsgeheimen zijn daarop gebaseerd.[72] Bij zakelijke data is er vaak aanzienlijke vermogenswaarde opgebouwd, die echter in het privaatrecht nog slechts beperkt wordt erkend (par. 3.9). Maar ook privé-personen doen aanzienlijke investeringen in data: immense foto-bestanden, *social media* accounts, digitale muziekverzamelingen. De inspanningen waarmee deze dataverzamelingen zijn gecreëerd verlangen bescherming. De bescherming van belangen schiet evenwel nog steeds tekort, onder meer doordat – wat ik hierboven als conditie aanstipte – privé-personen zich meestal niet in de positie bevinden om een adequate contractuele regeling van hun positie te onderhandelen met dienstverleners die hun data beheren.[73] Door data niet als 'eigendom' te regelen blijven er lacunes bestaan; als die weggenomen zouden worden zou het inderdaad niet nodig zijn om data als 'eigendom' op te vatten. In zoverre gaat het hier om een hypothese die helpt om wenselijk recht vorm te geven. Daarnaast is er het expressieve argument dat erkenning van eigendom van data beter aansluit bij de in het maatschappelijk verkeer levende verwachtingen. Niet-juristen spreken inmiddels vanzelf over 'bezit' van data,[74] kennelijk om de partij aan te duiden die de controle over de data heeft.

Tegelijk zijn er ook tegenargumenten. Een bekend argument is een beroep op de vrijheid van informatie.[75] Hierboven heb ik echter al aangegeven dat de bescherming van data geen aanspraak op de informatie inhoudt. Wel is hier een mogelijke botsing als het gaat om wederrechtelijk verkregen data die wordt gebruikt om misstanden aan de kaak te stellen. Dit valt echter op te lossen door hiervoor een exceptie op te nemen,[76] zoals ook in bredere zin voor klokkeluiders is voorgesteld.[77] Bovendien impliceert bescherming van data niet noodzakelijk exclusiviteit; een deel van de beoogde bescherming staat hier los van.

Een praktisch doch lastig probleem is verder dat data, hoewel beheersbaar, minder welomschreven is dan stoffelijke objecten. Tegenwoordig wordt data veelvuldig tijdelijk of langdurig gekopieerd, al dan niet in

71. Degenkamp (1997).
72. Considerans nr. 7 Databankenrichtlijn 96/9/EG, considerans nr. 1 concept-Richtlijn bedrijfsgeheimen COM(2013)813.
73. Zie de opmerkingen in par. 4.6 over dataportabiliteit.
74. Bijv. Kool, Timmer & Van Est (2015: 13, 28, 53).
75. Verkade (1988, nr. 12), zie hiertegen het betoog van Kleve (2004: 128-136).
76. Vgl. art. 273 lid 2 Sr.
77. Vgl. considerans nr. 12 en art. 4 lid 2 concept-Richtlijn bedrijfsgeheimen COM(2013)813.

gedeelten. Bedrijven en individuen maken regelmatig backups die zij weer vergeten, zij bewaren data wellicht bij derden zoals in de *cloud*, zij verzenden wellicht delen van de data aan derden. Tegelijk claimt een bezitter op zeker moment weer zijn rechten en verlangt dat kopieën na afloop van de contractuele relatie worden verwijderd. Data is zo bezien meer als rubber of kauwgum: het dijt uit en krimpt naar believen, en kan gewild of ongewild resten achterlaten.[78] Data heeft geen vaste kern of locatie: als ik een bestand van mijn computer thuis naar mijn werkcomputer stuur en vervolgens thuis verwijder, is het bestand alleen nog bij de mailserver op werk aanwezig, ook al is dat het bestand waar ik rechten op claim. Bovendien is er niet noodzakelijk een duidelijke *feitelijke* locatie van data.[79] Hoewel we spreken van één bestand is mogelijk dat het bestand technisch-feitelijk is versnipperd over diverse andere bestanden, harde schijven of servers, zoals bij gebruik van RAID-technologie. Toch heeft in al die verschillende hoedanigheden een databestand tegenwoordig voldoende welomschreven identiteit om dit als object van recht te erkennen.[80] Ook gewone zaken kunnen transformaties ondergaan – zoals natrekking en scheiding van zaken, verspreiding in minieme delen als in het geval van bijenspat en asbest,[81] vermenging en zaaksvorming – die er niet aan in de weg staan om over zaken met welomschreven identiteit te spreken. Wel blijkt data niet zomaar in het klassieke eigendomsbegrip te passen. We zullen dit bijvoorbeeld hierna zien bij de splitsing tussen revindicatie en exclusiviteit.

3.3 Digitale objecten

Naast data zijn er andere digitale fenomenen die vaak mede worden belichaamd door data, maar daar niet mee samenvallen en afzonderlijke aandacht verdienen. Dit gaat primair om objecten die uit hun aard exclusief zijn. Voorbeelden zijn domeinnamen, virtuele objecten in spelomgevin-

78. Dit is geen argument tegen een goederenrechtelijke benadering. Vloeibare goederen als olie of gesmolten aluminium kunnen eveneens worden gesplitst tot meerdere goederen die afzonderlijk kunnen worden overgedragen; daarnaast kunnen zij ook weer worden vermengd.
79. Dit is de voornaamste reden waarom ik afwijk van de positie van Kleve (2004) en Neppelenbroek (2006a), die (als ik hen goed begrijp) data als stoffelijk beschouwen wegens de belichaming in een concrete configuratie van deeltjes op een gegevensdrager. Een databestand staat in mijn benadering los van de fysieke wijze van opslag. Dit sluit beter aan bij hoe tegenwoordig in het maatschappelijk verkeer over databestanden wordt gesproken.
80. De benadering van het HvJ EU in de UsedSoft-uitspraak tendeert in deze richting. Zie bijv. ook Senftleben en Scholten (2014: 131), die betogen dat de auteursrechtelijke exceptie voor privé-kopieën ook moet gelden voor kopieën in de ‘cloud’.
81. Vgl. HR 18 september 1998, NJ 1999/69 respectievelijk HR 7 november 2003, NJ 2004/292.

gen, pseudoniemen voor blogs, Twitter e.d.[82] Hoewel deze in data tot uiting komen, worden zij mede gevormd door contractuele en feitelijke verhoudingen. Dergelijke *digitale objecten* (zoals ik ze hierna zal noemen) kunnen waarde hebben: anderen zouden deze graag overnemen en zijn onder omstandigheden bereid daarvoor te betalen. De waarde van digitale objecten kan gelegen zijn in de investering die daarin is gedaan (tijd of geld om het te verwerven of creëren, of om bijbehorende reputatie te verwerven), of eenvoudigweg in de locatie die het inneemt (zoals met een interessante domeinnaam). Ook dat laatste komt voor in de fysieke wereld: particuliere woningen ontlenen een groot deel van hun waarde puur aan de locatie waar de woning zich bevindt. Virtueel geld, in het bijzonder *bitcoin* valt hier ook onder. Bitcoin wordt verkregen door inspanning (het 'minen') die door het systeem is opgelegd, en om exclusiviteit te verzekeren is een ingenieus mechanisme ontworpen.

In dergelijke gevallen kan men veelal het object overdragen binnen de omgeving waar het zich in bevindt; er is geen noodzaak tot juridische afdwingbaarheid van exclusiviteit aangezien beschikkingsbevoegdheid vanzelf exclusiviteit met zich brengt. Ik merk hierbij op dat digitale objecten zijn gebaseerd op een infrastructuur die door een derde[83] wordt beheerd: deze derde zal veelal bij de overdracht betrokken worden, althans de mogelijkheid voor overdracht hebben opgenomen in de omgeving. Zie nader par. 4.6.

Men kan lang debatteren over de kwalificatie van digitale objecten en de mogelijkheid van overdracht. In essentie gaat het naar geldend recht om contractuele afspraken, en deze zijn in beginsel te cederen. Dit is in elk geval hoe het voor domeinnamen bij SIDN uitwerkt.[84] Voor het beschikken over dergelijke objecten is dus geen afzonderlijke regeling nodig.

Toch is het te verdedigen dat, gelet op de belangen die met digitale objecten gemoeid zijn, een analyse naar analogie met eigendom van zaken wenselijk is. In het bijzonder spelen hierbij dezelfde kwesties van bescherming van de waarde van dergelijke objecten, beslag en verhaal, en eventueel overgang van rechten onder algemene titel. Daar wordt inmiddels enige aandacht aan besteed; een principiële erkenning van digitale objecten lijkt wenselijk om de vele in de praktijk levende vragen op dit gebied adequaat te kunnen beantwoorden.

82. Zie o.a. Neppelenbroek (2006b), Lodder (2006 en 2008). Principieel tegen erkenning: Nelson (2010). Zijn betoog berust niet op juridische bezwaren als wel op zijns inziens onwenselijke gevolgen, o.a. voor het escapisme in virtuele werelden.
83. Overigens kunnen dat ook vele derden zijn, zoals bij bitcoin: daar is de bitcoin gemeenschap in wezen de beherende derde (via de blockchain).
84. Biemans (2009), Meijboom (2007).

3.4 Gevolgen van erkenning van digitale activa (algemeen)

We zien dus twee objecten ten aanzien waarvan een eigendomsrechtelijke benadering zinvol lijkt: data, en digitale objecten. Naar geldend recht is het lastig om deze objecten in het vermogensrecht te plaatsen door de tweedeling in art. 3:1 BW tussen zaken en vermogensrechten. Het betreft evident geen zaken, terwijl het daarnaast ook geen *rechten* zijn maar objecten die een digitale werkelijkheid hebben (al kan men daar bij virtuele objecten nog enigszins aan twijfelen, deze hebben ook een 'rechten'-kant). Ik zal hierna spreken over *digitale activa*, naar analogie van de term 'digital assets' die in Amerika in zwang is geraakt.[85] De term wordt gebruikt in regelgeving die beoogt het probleem op te lossen dat beheer en beschikken over digitale 'eigendommen' van overledenen (en bij fiduciaire verhoudingen) slecht geregeld is.[86] Het bezwaar van deze regeling is dat zij slechts op een deelprobleem ziet, terwijl het grotere probleem daarin is gelegen dat dergelijke digitale activa beter in alle gevallen kan worden benaderd op een wijze analoog aan eigendom van zaken. Ik zal hier het grotere vraagstuk behandelen.[87] Het voordeel van de term 'digitale activa' is dat men deze kan hanteren zonder te hoeven aanvaarden dat dergelijke objecten vatbaar voor eigendom zijn.

Hoewel een goederenrechtelijke erkenning strikt genomen niet nodig is voor *overdracht* (par. 3.2, 3.3 en 3.5), is mijns inziens zodanige erkenning wél zinvol aangezien dit in één keer een verzameling problemen oplost. Het bij analogie toepassen van de gewone regeling voor zaken[88] laat zien waar aanpassingen wenselijk zijn. In het vervolg van dit preadvies zal ik op deze aanpassingen ingaan. Het gaat, kort gezegd, om het volgende.

Als eerste is er een reeks goederenrechtelijke consequenties die nader moeten worden doordacht. Concepten als originaire verkrijging, zekerheid, beslag, verhaal, vereisen aanpassing om bij digitale activa te kunnen werken. Daarnaast is de positie van rechtsverkrijgenden onder algemene titel en tot executie bevoegden (zoals de curator of de executeur) nog onduidelijk. Ook kan men denken aan aanpassing van aanverwante leerstukken als kwalitatieve rechten en verplichtingen, zaaksvervanging e.d.

85. Vgl. Van der Geld (2014), sprekend over 'digitale bezittingen' naar analogie met het Amerikaanse-Engelse 'digital assets'.
86. Zie de Fiduciary Access to Digital Assets Act (revised 2015) op http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20(2015). Wetsvoorstellen voor invoering van deze wet is inmiddels in vele Amerikaanse staten geïntroduceerd (zie overzicht op http://www.uniformlaws.org/Legislation.aspx).
87. Overigens heeft de Uniform Fiduciary Access to Digital Assets Act (UFADAA) het voordeel dat het expliciet ingaat op problemen rond privacy by fiduciary access op digitale activa (zoals bij e-mails etcetera). Dergelijke problemen behandel ik niet.
88. Vgl. Spath (2015) die pleit voor een art. 3:2a BW in deze zin.

Als tweede is er de vraag naar de remedies. Ik zal hier slechts ingaan op drie die voor digitale activa specifieke aanpassing behoeven: revindicatie (par. 3.7), exclusiviteit (par. 3.8) en schadevergoeding (par. 3.9).

Als derde is er de vraag naar beperkingen of aanspraken op de eigenaar. Dit gaat enerzijds om aansprakelijkheid voor digitale activa (par. 3.12). Anderzijds gaat het hier om de handhaving van privacy (par. 3.10). Een relevante vraag hierbij is of er niet teveel kan worden weggecontracteerd (par. 3.11).

3.5 Rechthebbende van digitale activa

3.5.1 Algemeen

Als we eenmaal aannemen dat digitale activa bij analogie als object van eigendom moeten worden behandeld, wordt het van belang een geschikte regeling te hebben om te bepalen wie de rechthebbende is. Voor digitale objecten als bedoeld in par. 3.3 volgt dit uit de contractuele verhouding. Voor data is dit minder eenvoudig te beantwoorden. Als men uitgaat van de belangen die de 'bezitter' van data doorgaans heeft (de waarde, alsmede de gedane investeringen om de data te verkrijgen) ligt het voor de hand bij deze aspecten aansluiting te zoeken.

Er is echter een complicatie die aandacht verdient. Veel data heeft betrekking op personen. Intuïtief hebben de personen die onderwerp van deze data zijn enig belang bij deze data (par. 3.9). Er wordt daarom wel verdedigd dat zulke data 'eigendom' dienen te zijn van de persoon die object van deze data is.[89] Het meest voor de hand liggend is evenwel te werken volgens de principes van het goederenrecht. Privacy-aspecten[90] zouden dan vooral 'lasten', 'beperkingen' zijn op de eigendom, zoals burenrecht het zakenrecht beperkt. De spanning tussen deze perspectieven is in de praktijk wellicht minder groot dan het lijkt. Ook bij IE-rechten bestaat een spanning tussen de eigendom van de fysieke kopie en de rechthebbende op het IE-recht zelf. Maar het IE-recht wordt veelal (bv. bij het maken van een schilderij) verkregen bij het maken van de eerste fysieke kopie, en omgekeerd raakt het IE-recht uitgeput bij het toestemming geven voor fysieke kopieën. Evenzo wordt veel privacygevoelige data primair door de betreffende persoon zelf gegenereerd,[91] zodat maker van data en object van data samenvallen. De eigendom wordt vervolgens overgedragen door toestemming, maar dat is een gebruikelijke privaatrechtelijke rechtshandeling. Hoewel toestemming minder goed werkt voor adequate

89. Zie over deze discussie Purtova (2011).
90. Zoals de eisen die de Wbp stelt.
91. Of direct met medeweten en in opdracht van deze persoon, zoals het dossier dat een arts bijhoudt van zijn patiënt.

regulering van privacy (par. 3.10 en 3.12), is het niettemin de voornaamste wijze waarop over data kan worden beschikt.

Er zijn ook gevallen waar de maker van de data een ander is dan het onderwerp daarvan. Als een bekende zanger een verkeersregelaar slaat is hij de originator van dat feit, maar dit wordt door een omstander vastgelegd in een videofilmpje. Voor dergelijke gevallen lijkt het niet passend dat de persoon die onderwerp van de data is ook de eerste rechthebbende is. In zoverre lijkt mij derhalve het perspectief van eigendom van 'persoonlijke' data niet geschikt om het vraagstuk van verkrijging van data in het algemeen te benaderen.

Dit alles impliceert dat bij data niet altijd een eenduidig en volledig eigendom aanwezig is:[92] veeleer gaat het om een mengeling van primaire 'eigendom' naast bevoegdheden van derden (zoals gebruikslicentie) en gemeenschappelijke bevoegdheden. Dit is niet uniek voor data: zoals we zagen is in het IE-recht een dergelijke mengeling niet ongebruikelijk.

Wel bijzonder is dat data kan worden gesplitst: een voldoende ruime, niet-exclusieve licentie op data verschaft de licentienemer dezelfde bevoegdheden over zijn kopie van de data als de oorspronkelijke rechthebbende over het oorspronkelijke bestand. Men zal derhalve moeten beseffen dat licenties op data een verdergaande strekking kunnen hebben dan andere soorten licenties: zij leiden tot een eigendom van de kopie! Splitsing kan ook bij zaken, zoals bij het opdelen van een vracht olie.

Los van deze complicaties is van belang vast te stellen wie de eerste 'eigenaar' is. Eigendom kan men in het algemeen op drie manieren verkrijgen.

a. originaire verkrijging.
b. overdracht.
c. verkrijging onder algemene titel.

3.5.2 Originaire verkrijging[93]

Er zijn verschillende partijen die doorgaans rechten op data claimen. Het 'eigendomsrecht' heeft prioriteit voorzover er geen andere rechten zijn, zodat er enig belang is bij wie de eigenaar is, tenzij men prima facie deelrechten toekent aan zekere partijen in hun hoedanigheid, zoals de opdrachtgever, de feitelijke maker, de bepaler, het individu over wie de data gaat. Dit kan leiden tot lastige vragen en afwegingen. Echter ook als men geen 'eigendom' op digitale activa erkent zullen deze afwegingen zich voordoen, alleen worden zij dan verhuld door het ontbreken van een wettelijke regeling, zodat men is aangewezen op de tekortschietende algemene regels en contractsvoorwaarden die door de machtigste partij worden opgelegd (par. 3.12). Dat is allerminst een bevredigend alternatief.

92. Vgl. Schoenmakers, Sloots & Wendt (2014: 62).
93. Vgl. Hoeren (2013).

Als eerste benadering lijkt passend dat degene die de data daadwerkelijk vastlegt (dan wel degene in wiens opdracht dit gebeurt) de rechthebbende, de verkrijger is. Hiervoor zijn verschillende omstandigheden mogelijk relevant: degene die de vastlegging instigeert, degene die juridisch gezien opdracht geeft (opdrachtgever of werkgever), degene op wiens hardware de data wordt vastgelegd, degene in wiens infrastructuur de data wordt vastgelegd. Daarnaast is 'vastlegging' niet eenduidig. Wat ingeval een auto data verzamelt doordat de fabrikant hier apparatuur voor heeft geïnstalleerd, en deze data direct naar de fabrikant wordt doorgezonden zonder in de auto te worden bewaard? Is de data dan in de auto vastgelegd, of pas bij de fabrikant? En wie is überhaupt de verkrijger: is het fair dat dit de eigenaar van de auto is of de fabrikant?

Men kan deels aansluiting zoeken bij het databankrecht, dat – indachtig de ratio van het databankrecht – zich richt op de partij die de benodigde investeringen heeft gedaan. Dit zou kunnen wijzen op de fabrikant die de meetapparatuur in de auto heeft ontwikkeld. Echter als het gaat om een computer is evident dat de fabrikant niet de verkrijger wordt van de digitale documenten die op de computer zijn geschreven door de gebruiker; de gebruiker heeft integendeel de computer gekocht om die documenten te kunnen genereren. De auto-eigenaar heeft de auto gekocht en daarmee een investering gedaan. Investeringen in de benodigde infrastructuur zijn derhalve niet eenduidig.

Ook een aanknopingspunt is de daadwerkelijke inspanning voor vastlegging. Bij Whatsapp en Facebook maken de individuen de concrete data, maar het bedrijf verzamelt alles en brengt het in kaart. *Is* de data dan van de klanten of van het bedrijf? Dit is een hoogst omstreden kwestie,[94] die verder gecompliceerd wordt doordat een bedrijf kan volstaan met het verkrijgen van een vérstrekkende gebruikslicentie die in feite eigenaarsbevoegdheden aan het bedrijf geeft van kopieën van de data.[95] In de regel lijkt de eigendom in strikte zin bij de gebruiker te blijven: de *posts* op een online forum of de *tweets* van een *user* in Twitter blijven van de gebruiker. De algemene voorwaarden die bedrijven hanteren kennen daarnaast evenwel doorgaans significante gebruiksrechten toe aan het bedrijf.

Dit alles geeft aan dat reeds voor deze detailvraag nader onderzoek gewenst is. Dit is geen bezwaar voor de eigendomsrechtelijke benadering; zonder die benadering blijven dezelfde vragen van rechtvaardigheid bestaan maar moeten deze worden beantwoord aan de nog onduidelijker open normen inzake de toelaatbaarheid van contractuele voorwaarden en de aanvullende werking van redelijkheid en billijkheid (ingeval geen regeling is afgesproken).

94. Zie ter illustratie zoekresultaten op 'ownership', 'data' en Facebook of andere sociale website.
95. Zie par. 3.5.1, slot.

3.5.3 Overdracht

Zoals hierboven aangegeven (par. 3.2) is overdracht ook thans al feitelijk en juridisch mogelijk – al dan niet in de vorm van 'toestemming'. Dit is doorgaans toereikend. Een toereikende juridische regeling zou het beste inhouden dat levering door een daartoe strekkende akte geschiedt (vgl. art. 3:95 BW); een akte is sowieso uit bewijsrechtelijk oogpunt verstandig.

Bij data die persoonsgegevens in de zin van de Wbp bevat is dit lastiger, aangezien in principe toestemming voor overdracht is vereist van de persoon die onderwerp is van de gegevens.[96] Privaatrechtelijk zou dit (in afwijking van de bedoeling van de Wbp) kunnen worden opgelost met voorwaardelijke of impliciete toestemming of overdracht.[97] De primaire toestemming is gegeven met een bepaald gebruiksdoel in het hoofd. Andere vormen van gebruik kunnen worden getoetst aan de hand van het criterium van uitleg van de overeenkomst, dan wel in hoeverre een verbod op dat gebruik afstuit op misbruik van bevoegdheid door het individu. Omgekeerd kunnen te ver strekkende vormen van gebruik worden verboden doordat eventuele toestemming alsdan aan een wilsgebrek onderhevig zou zijn, dan wel door middel van zorgplichten gemoduleerd kan worden door nadere informatieverschaffing te vereisen.

Het privaatrecht biedt in zoverre, mits men wil afwijken van het gangbare publiekrechtelijke privacykader, een genuanceerd instrumentarium. Dit leidt noodzakelijk ertoe dat de gebruiker niet geheel zeker is van wat nu wel en niet is toegestaan, maar het is verdedigbaar dat dit precies de meerwaarde vomt van een dergelijk systeem: de gebruiker zal zelf moeten nadenken welk gebruik riskant is en daarvoor zonodig de individuen moeten benaderen, zonder dat de overheid als toezichthouder steeds moet nagaan of iets wel of niet mag en daar dan tegen moet optreden.

3.5.4 Opvolging onder algemene titel

Ingeval van overlijden, of fusie of overname van ondernemingen, is op dit moment ongeregeld in hoeverre de opvolger een recht heeft op digitale activa van de oorspronkelijke 'eigenaar'.[98] Erkenning van eigendom van

96. Die overdracht leidt immers in de regel tot een andere verwerking dan oorspronkelijk bedoeld; zo niet is overdracht niet zonder meer in strijd met de Wbp. Vgl. Rb. Amsterdam 22 oktober 2015, ECLI:NL:RBAMS:2015:7501: executoriale verkoop van namenbestand toegestaan, aangezien individuen na overdracht bezwaar konden maken bij de verkrijger van het bestand.
97. Kritisch over impliciete toestemming: Gisclard (2014).
98. Ten aanzien van het bewijs van de opvolging zie par. 4.2.

data zou de positie van opvolgende rechthebbenden versterken. Dit geldt in het bijzonder bij data die in beheer of bewaring is bij andere partijen.[99] Zonder een goederenrechtelijke claim is men thans volledig afhankelijk van de contractuele voorwaarden en het gehanteerde beleid,[100] dan wel het kennen van inlognaam en wachtwoord.[101] Op basis van een quasi-revindicatoire claim zou de rechthebbende de bewaarder kunnen aanspreken tot overgave van de data.

Een bezwaar hiertegen is dat het de bedoeling kan zijn geweest dat de data vertrouwelijk bleef en juist niet in handen van de erven zou komen.[102] Ook in het verleden kwam dit voor: brieven die de notaris pas mocht openen na vervuld zijn van zekere voorwaarden, documenten die moesten worden vernietigd na overlijden, medische dossiers van overledenen. Een recht op data heeft het nadeel dat dergelijke gevallen uitdrukkelijk geregeld moeten worden. Dit lijkt echter onvermijdelijk: zonder regeling hangt alles af van toevalligheden in de concrete omstandigheden. Het gaat hierbij veelal om gevallen waar de eigenaar ook een eigen privacy-belang heeft, echter het kan ook gaan om gevallen waar de eigenaar de privacy van een ander wil beschermen.[103] Een mogelijkheid zou zijn dat dan een juridische beperking op de data wordt erkend, uit oogpunt van privacy dan wel een last die aanvangt na overlijden, en die met zich brengt dat de erven hun recht op de data geblokkeerd zien: hetzij de data wordt beschouwd als geen onderdeel van de boedel uitmakend, hetzij het valt in de boedel maar met een last die de erven verhindert daar kennis van te nemen. Voor een uitgewerkte regeling is nader onderzoek vereist naar het recht op data na overlijden.[104] Zie verder de Amerikaanse regeling over *digital assets* (par. 3.4).

3.5.5 Conclusie

Deze paragraaf lost weinig problemen op. Het betoog is vooral erop gericht te laten zien dat deze problemen zich sowieso voordoen, en waar. Het is beter deze vanuit een coherent algemeen perspectief op te lossen dan per casus aan de hand van toepasselijke algemene voorwaarden.

99. Asser/Van Schaik 7-VIII* 2012/3 betoogt dat de bepalingen inzake bewaarneming bij analogie kunnen worden toegepast op bijv. cloud computing, en wijst op art. IV.C-5:101 DCFR dat wel bewaarneming van data toelaat.
100. Visser (2007).
101. Immers dan kan men gewoon op naam van de oorspronkelijke eigenaar inloggen.
102. Vgl. Blok (2003) over privacy na de dood.
103. Bijvoorbeeld omdat documenten een geheim van een vriend bevatten.
104. Dit speelt immers nu ook al bij het recht op inzage in medische dossiers van de overledene.

3.6 Zekerheid en verhaal op digitale activa

Als digitale activa eenmaal worden erkend impliceert dit ook de mogelijkheid van het geven van zekerheid op die activa, en de verhaalsmogelijkheden die bij goederen horen. Dit is een argument ten gunste van erkenning van digitale activa. Inmiddels zijn er ondernemingen waarvan de voornaamste vermogensbestanddelen bestaan uit data. Het is onwenselijk als dergelijke ondernemingen niet in staat zijn financiering te verkrijgen omdat zij niet beschikken over voldoende objecten van zekerheid, terwijl het evenmin wenselijk is dat de voornaamste activa van die ondernemingen geen object van verhaal van schuldeisers (al dan niet vertegenwoordigd door de faillissementscurator) kunnen vormen. De waarde van data is te groot om buiten het privaatrecht te houden. Het betreft een cluster aan onderwerpen: zekerheid, beslag, verhaal en executie (al dan niet in faillissement). Opnieuw is dit een onderwerp dat veeleer een dissertatie dan een preadvies vergt. Ik geef hier slechts een schets van mogelijkheden.

3.6.1 Zekerheid

Zekerheid op digitale activa, in het bijzonder op data, is gecompliceerd door de vluchtigheid en fluïditeit van data. Het ligt het meest voor de hand aansluiting te zoeken bij de regeling van het pandrecht en/of zekerheid op vermogensrechten. Voor vorderingen is (als derdenwerking wordt vereist) uiteindelijk mededeling aan de schuldenaar nodig. Probleem is dat bij data geen schuldenaar aanwezig is. In zoverre lijkt digitale eigendom meer op een immaterieel goed als een IE-recht. Zekerheid daarop verkrijgt men bij akte,[105] die soms ten behoeve van derdenwerking moet worden ingeschreven in het betreffende IE-register.[106] Als er geen register is, is het onzeker of er geen andere conflicterende zekerheidsrechten zijn. Die onzekerheid is echter niet een noodlottig beletsel: dit is ook aanwezig bij stil pandrecht. Verder is er bij digitale activa regelmatig ook een derde betrokken waar de activa feitelijk in beheer zijn (par. 4.6). In dergelijke gevallen is zekerheid eenvoudiger te regelen nu dit door de derde kan worden geëffectueerd. Dan zou een vorm van pandrecht met derdenwerking zinvol zijn, waarbij de pandgever het pandrecht ook aan derden mededeelt, en de pandnemer het recht verkrijgt om toekomstige derden van dit pandrecht mededeling te doen.

Een bijzonderheid van data is de mogelijkheid van kopieën. Daardoor is een variant van vuistpand mogelijk: de pandnemer zou een kopie van de data kunnen verkrijgen (of desnoods bij een derde in bewaring geven:

105. Vgl. art. 3:98 en 3:236 lid 2 BW: zekerheidsverschaffing geschiedt op dezelfde wijze als levering.
106. Zie nader de relevante passages in Gielen (2014).

escrow) om te verzekeren dat hij daadwerkelijk de macht over de data kan verkrijgen ten behoeve van executie. Het voordeel is dat zodanige regeling de pandgever niet het gebruik belet.

Overigens zal verpanding van data waarschijnlijk ook impliceren dat de pandgever de data exclusief moet houden teneinde de waarde van het pand niet aan te tasten. Een expliciet beding van die strekking zou zinvol zijn.

3.6.2 Beslag

Een regeling inzake beslag kan worden afgeleid van een regeling inzake zekerheid. Als het gaat om digitale activa die bij een derde is ondergebracht kan de regeling inzake derdenbeslag van toepassing zijn, mits de rechtsverhouding met die derde kan worden geconstrueerd als inhoudende een vordering op de derde. In de praktijk is voor het beslag op domeinnamen een contractuele regeling tot stand gekomen die sterke gelijkenis vertoont met derdenbeslag.[107] Dit wijst erop dat een regeling in deze zin de voorkeur verdient; bij gebreke van een wettelijke regeling kan de derde met contractsvoorwaarden een vergelijkbaar resultaat bewerkstelligen.

Voor data die niet bij een derde is ondergebracht ontbreekt momenteel een regeling. Dit is een lacune waarvan twijfelachtig is of deze door rechtersrecht kan worden opgevuld.[108] Verhaalsbeslag op data kan niet dan met een zeer extensieve interpretatie onder de categorieën in Rv worden gebracht. Voor beslag op IE-rechten zijn er specifieke wettelijke bepalingen, wat suggereert dat er een toereikende wettelijke grondslag nodig is voor beslag. Dat lijkt ook gerechtvaardigd gelet op de inbreuk op rechten die dit met zich brengt: het lijkt mij zeer wel mogelijk dat data als een eigendomsrecht in de zin van art. 1 Eerste Protocol bij het EVRM moet worden aangemerkt. Het bewijsbeslag[109] omvat weliswaar beslag op data, doch dat is geen beslag tot verhaal.

Een toereikende regeling zou verder mogelijk een beperking moeten bevatten voor beslag op hoogstpersoonlijke digitale objecten.[110] Wellicht zou ook een uitsluiting nodig zijn voor digitale activa die nodig zijn om inkomen te verwerven, denk aan de zelf verzamelde notities en aantekeningen, maar ook software.[111]

Ook voor beslag zou escrow mogelijk zijn zodat de beslagene de digitale objecten nog kan blijven gebruiken. Een praktisch bezwaar is dat de

107. Biemans (2009), Meijboom (2007).
108. In Rb. Amsterdam 22 oktober 2015, ECLI:NL:RBAMS:2015:7501 is executoriaal beslag op data wel toegelaten.
109. HR 13 september 2013, NJ 2014/455 (bewijsbeslag).
110. Dit kan volgen uit het privacyrecht, of bij analogie naar het in het auteursrecht, zie art. 2 lid 4 Aw.
111. Vgl. art. 447 sub 2 en 448 lid 1 Rv voor boeken nodig voor het beroep, werktuigen en gereedschappen.

beslagene vooralsnog niet verplicht is tot exclusiviteit zoals bij zekerheid gewenst (par. 3.6.1). Ook hiervoor zou een wettelijke regeling wenselijk zijn.

3.6.3 Verhaal en executie

Bij verhaal en executie ontstaan er enige praktische problemen. Digitale activa zullen als regel moeten worden verkocht om verhaal te bieden. Indien het gaat om activa die in de infrastructuur van een derde zijn ondergebracht, zal de executant moeten aantonen dat hij beschikkingsbevoegd is en zal de derde moeten meewerken of de geëxecuteerde tot medewerking moeten bewegen. De geëxecuteerde zal bijvoorbeeld met zijn avatar moeten inloggen en het virtuele zwaard laten 'droppen' opdat de koper het zwaard kan oppakken. Als de geëxecuteerde weigert mee te werken kunnen soms dwangmiddelen worden ingezet, die echter niet altijd ter beschikking staan of effectief zijn. Alternatief zou zijn dat de executant de inloggegevens verkrijgt (maar hoe?) en zelf de feitelijke levering voltrekt. Echter de executant, althans de deurwaarder, zal op dit moment waarschijnlijk veelal niet over de vereiste kennis bezitten om dit te kunnen doen. Algemeen zal derhalve voor digitale executie een terdege op de hoogte zijnde deurwaarder nodig zijn. Dit zou een zinvol specialisme kunnen worden. Juridisch bezien zullen diverse aanvullende regels of uitzonderingen nodig zijn om de deurwaarder in staat te stellen zijn taak te vervullen zonder schending van privacyregels[112] en gebruiksvoorwaarden. De rechtspraak tendeert reeds in deze richting, door verplichtingen aan te nemen om sleutels en wachtwoorden ter beschikking te stellen.[113]

Ingeval van soorten digitale activa waar exclusiviteit wel vereist is doch niet inherent is aan de activa zal een effectieve executie vereisen dat de geëxecuteerde die exclusiviteit respecteert. Hij mag bijvoorbeeld niet langer een backup of andere kopie van de data gebruiken. Dit is een feitelijk probleem voor executie. Bij software kan de leverancier vaak dubbel gebruik van licentiecodes detecteren, zodat de koper het risico loopt op problemen met de leverancier, wat de waarde van bij executie verkochte software kan drukken.

3.6.4 Executie door faillissementscurator en executeur

Een erkenning van digitale activa als goed leidt vanzelf tot het gevolg dat digitale activa ook in het vermogen vallen, en dus ex art. 20 Fw voor exe-

112. Vgl. Rb. Amsterdam 22 oktober 2015, ECLI:NL:RBAMS:2015:7501: betrokken personen kunnen na executoriale verkoop toestemming voor hun persoonsgegevens weigeren.
113. HR 13 september 2013, NJ 2014/455 (bewijsbeslag), Rb Rotterdam 4 september 2015, ECLI:NL:RBROT:2015:7101.

cutie in faillissement vatbaar zijn. Omgekeerd is dit opnieuw een argument voor toekenning van rechten op digitale activa. Als men geen aanpassing van het goederenrecht wenst zou het ten minste aanbeveling verdienen art. 20 Fw aan te passen om digitale activa onder de bevoegheid van de curator te brengen. Dit lijkt mij een dringende noodzaak nu onvermijdelijk is dat de komende jaren significante activa in de vorm van data zullen worden aangetroffen in de boedel. Tevens is verdedigbaar dat aan het begrip 'vermogen' in art. 20 Fw een ruime uitleg wordt gegeven indien de wetgever hier niet in actie komt. Een dergelijke ruime uitleg past bij het uitgangspunt dat een schuldenaar met zijn gehele vermogen voor zijn schulden in staat. Hij wordt geacht zich in te spannen om zijn schulden te voldoen, en daarbij behoort ook dat hij zonodig activa als data te gelde zou maken. Indien hij dit nalaat, dient de curator dit in zijn naam te kunnen doen.

Wel kan een beperking worden aangenomen voor bepaalde soorten digitale activa. Het zal hierbij gaan om hoogstpersoonlijke objecten dan wel private gegevens. Als een filmster failliet gaat mag de curator niet diens persoonlijk dagboek verkopen. Deels kan aansluiting worden gezocht bij de reeds bestaande uitsluitingen in art. 21 Fw.[114]

Verder is een complicatie dat bij data niet direct duidelijk is of het zonder meer in de boedel valt, dan wel dat de data slechts tijdelijk gebruikt mag worden of in bewaring is o.i.d. Problematisch is dan mede dat aanspraken op data naar geldend recht mede gestalte krijgen door contractuele afspraken: verbintenisrechtelijke afspraken binden evenwel de faillissementscurator slechts in beperkte mate. De rechtspraak hierover is lastig te interpreteren en geeft aanleiding tot veel discussie.[115] Een meer goederenrechtelijke benadering van data zou wellicht richting kunnen geven voor redelijke oplossingen. Zoals de analyse in par. 3.6.1-3.6.3 laat zien blijven evenwel enkele complicaties bestaan die uit de bijzondere aard van data voortvloeien.

Als digitale activa in de boedel vallen zal de curator hier ook onderzoek naar moeten doen. De failliet zal hem hierbij behulpzaam moeten zijn, maar het is niet uitgesloten dat deze onwillig blijkt. Digitale activa zijn gemakkelijker te verbergen dan stoffelijke objecten, al is dit geen nieuw probleem: buitenlandse bankrekeningen konden ook in het verleden al worden verborgen voor de curator. Een theoretische oplossing zou zijn dat er een eenvoudiger mechanisme zou worden ontworpen en aanvaard waarmee dergelijke onderzoek kon worden verricht. Men zou kunnen denken aan een op derdenbeslag lijkende figuur, waarmee bij een centraal meldpunt alle grote relevante dienstverleners zouden kunnen worden aangesproken aan de hand van bepaalde kenmerken van de failliet of erflater, en deze dienstverleners vervolgens een opgave zouden moeten doen van

114. Deels verwijzend naar de uitsluitingen bij beslag, waarover par. 3.6.2.
115. In het bijzonder HR 3 november 2006, NJ 2007/155 (Nebula) en HR 11 juli 2014, NJ 2014/407 (ABN AMRO/Berzona). De literatuur hierover is overvloedig, ik zie kortheidshalve af van een overzicht.

relevante accounts bij hen. Dit heeft het praktische bezwaar dat de curator hiervoor waarschijnlijk reeds de accounts moet kennen, althans de loginnaam of het ter login gebruikte e-mailadres. Dan kan hij bijna net zo goed zelf de relevante dienstverleners aflopen (met als enige voordeel dat hij geen wachtwoorden hoeft te achterhalen). Hier valt nog winst te behalen met een praktische regeling.

Een verwante kwestie is de mogelijkheid van opeising van goederen door de curator.[116] Dit zou mogelijk moeten zijn: ook als de rekening niet langer wordt betaald zou de curator de data van de failliet uit de cloud mogen terughalen.

Tot slot zal de curator bij contacten met derden mogelijk bewijs moeten leveren van zijn bevoegdheid (zie par. 4.2).

Voor de executeur van een nalatenschap valt evenzeer aan te nemen dat deze ook de digitale boedel in de nalatenschap moet beschrijven (vgl. art. 4:146 BW) en te gelde maken.[117] Hij zal andere beperkingen ontmoeten dan een faillissementscurator: enerzijds heeft hij geen tegenwerkende failliet, anderzijds kan de erflater hem niet van inlichtingen voorzien. Verder zullen er wellicht minder goederen buiten zijn executiebevoegheid vallen nu ook persoonlijke zaken hieronder vallen. Wel zal hij mogelijk moeten letten op privacy-gevoelig materiaal dat niet aan de erven moet worden overgedragen.

3.7 Remedies (1): revindicatie

De belangrijkste bijkomende bevoegdheid uit een eigendomsachtige benadering van data is (quasi)-revindicatie: het recht op verkrijging van (een kopie van) de data indien deze is ontstolen,[118] althans in de macht van een ander (zoals een bewaarder) die weigert deze af te staan (d.w.z. een kopie te verschaffen). Indien data als goed wordt erkend, volgt uit art. 5:2 BW een recht op revindicatie voor de rechthebbende.[119] Naar geldend recht lijkt in veel gevallen al een recht aanwezig om data terug te ontvangen: hetzij contractueel (volgens de regels van bewaarneming) als nakoming van een verplichting, hetzij op basis van onrechtmatige daad in de vorm van schadevergoeding in natura, kan een vordering tot afgifte van een kopie worden toegewezen. Immers meestal zal de houder in een contractuele relatie staan met de 'eigenaar' of zal de houder de data door onrechtmatig handelen hebben verkregen. Complicaties zijn er vooral ingeval de

116. Waarover Wessels (2015), zij het dat hij zich richt op het informationele aspect en niet de executiewaarde.
117. Van der Geld (2014), mede verwijzend naar L. van der Geld, 'De digitale nalatenschap', Kwartaalbericht Estate Planning 2013/35.
118. D.w.z. een ander heeft voor zichzelf een kopie van de data gemaakt en de oorspronkelijke kopie verwijderd.
119. Vgl. art. 3:125 BW voor de bezitter.

'houder' van de data deze toevallig in bezit heeft: dat is het voordeel van de erga omnes werking van revindicatie. Derhalve zou een wettelijke regeling duidelijke voordelen bieden.

Overigens lijkt dit tevens te impliceren een verplichting van de eerdere 'houder' om de data te verwijderen.[120] Exclusiviteit is echter niet altijd nodig, en moet daarom bij data als een afzonderlijke remedie worden beschouwd. Zie nader par. 3.8.

Voor digitale objecten is normaal gesproken geen regeling nodig aangezien deze bij derden in beheer zijn, zodat deze derden op contractuele basis kunnen worden aangesproken om de status quo te herstellen.

Wat revindicatie van digitale activa na rechtsovergang betreft is er nog wel een probleem: hoe weet de bewaarder/houder wie daadwerkelijk recht heeft op toegang van de data? Dit geldt voor gevallen waar de oorspronkelijke eigenaar slechts onder pseudononiem bekend was, maar ook indien de erven hun claim moeten bewijzen tegenover een bewaarder in een afgelegen land. Ook kan het zich voordoen dat de eigenaar zelf zijn gegevens is kwijtgeraakt en alsnog bij zijn data wil kunnen. De vraag is of in de digitale wereld intussen behoefte bestaat om te werken met een breder erkende digitale identiteit (par. 4.2).

3.8 Remedies (2): exclusiviteit

Een wenselijke nieuwe remedie is het afdwingen van exclusiviteit. Voor data kan het nodig zijn dat exclusiviteit moet worden afgedwongen om revindicatie te voltooiien, aangezien dit lijkt te veronderstellen dat de oorspronkelijke stand van zaken (waarbij de rechthebbende de data exclusief bezat) moet worden hersteld. Dit zou neerkomen op een gebod om kopieën te verwijderen en verbod om kopieën te hebben van de data.

Een dergelijke afdwingbare exclusiviteit lijkt bij velen op bezwaren te stuiten aangezien dit lijkt op een *erga omnes* afdwingbaar recht, terwijl fundamentele bezwaren gelden tegen een 'eigendom' van informatie. Men gaat er dan echter aan voorbij dat reeds naar geldend recht of komend recht al een nagenoeg complete afdwingbare exclusiviteit bestaat ten aanzien van data, zonder dat daarmee enige pretentie bestaat ten aanzien van de in die data neergelegde informatie.

Als het gaat om 'gestolen' data, dat wil zeggen door computervredebreuk verkregen kopieën van data, kan jegens de dief verwijdering van kopieën worden gevorderd als schadevergoeding in natura (art. 6:103 BW) op grond van onrechtmatige daad, bestaande uit schending van art. 138ab lid 2 Sr en 139e Sr (vgl. par. 3.2). Jegens een verkrijger anders dan de 'dief' zijn deze bepalingen niet van toepassing. Echter voorzover niet

120. Hierbij dient men echter wel te bedenken dat het wenselijk kan zijn dat de houder enige tijd een backup behoudt, voor het geval bij de feitelijke overdracht iets mis gaat!

precies is voldaan aan de eisen van vorenstaande strafrechtelijke bepalingen artikelen zal vermoedelijk veelal wel een schending van ongeschreven recht worden aangenomen, in het bijzonder jegens een 'heler'.[121] Tegen een 'onschuldige' verkrijger kan mogelijk op grond van ongerechtvaardigde verrijking worden geageerd.

Bij contractuele relaties zal veelal in de relatie geïmpliceerd zijn dat de data waartoe toegang werd verschaft niet mag worden gekopieerd of behouden na beëindiging van de contractuele relatie.[122] Daarnaast kunnen in vele relaties expliciete geheimhoudingsbedingen zijn overeengekomen. Ook dan zal het behoud van kopieën grond bieden voor een actie tot wissen van kopieën als schadevergoeding in natura voor deze wanprestatie.

Indien de concept-richtlijn bedrijfsgeheimen COM (2013)813def. wordt aangenomen krijgen bedrijfsgeheimen bescherming. Dit betreft informatie die niet algemeen bekend is, handelswaarde heeft omdat zij geheim is, en geheim wordt gehouden met redelijke maatregelen (art. 2(1) concept-Richtlijn). Het zonder toestemming kopiëren van de data is dan onrechtmatig.[123] In veel gevallen zal zodanig kopiëren reeds thans als onrechtmatig worden aangemerkt.[124]

Als op de data ook een IE-recht rust van een ander (zoals bij ebooks, muziekbestanden) zal ook de 'eigenaar' van de data een belang erbij hebben dat deze bestanden niet illegaal worden verspreid. De data kan immers een digitaal watermerk bevatten waarmee de bestanden naar hem getraceerd kunnen worden en hij kan worden aangesproken door de rechthebbende.[125] Kopieën van die data zijn dan tevens onrechtmatig jegens de eigenaar van de bestanden die een licentie heeft van de IE-rechthebbende. Waar geen watermerk aanwezig is, zal de 'eigenaar' van het bronbestand op zichzelf geen belang hebben om achter illegale kopieën aan te gaan: dat ligt dan op de weg van de IE-rechthebbende.

Als het om particuliere data gaat waarin persoonsgegevens in de zin van de Wbp zijn vervat, zijn kopieën zonder (impliciete) toestemming in beginsel onrechtmatig op grond van schending van de Wbp.[126]

121. De Minister heeft aangegeven 'heling' van gegevens strafbaar te willen stellen (TK 2014-2015, Aanhangsel Handelingen, nr. 933, p. 3). Zie het voorgestelde art. 139g Sr (Voorstel Wet Computercriminaliteit III, ingediend 22 december 2015).
122. Voor de overeenkomst van opdracht blijkt dit impliciet uit art. 7:412 BW ten aanzien van schriftelijke stukken. Men kan deze bepaling extensief uitleggen zodat ook data hieronder valt.
123. Onrechtmatigheid volgt ook uit het voorgestelde art. 138c Sr (Voorstel Wet Computercriminaliteit III, ingediend 22 december 2015).
124. Gielen (2014, nr. 760), mede verwijzend naar art. 39 TRIPS en uitvoerige Nederlandse rechtspraak.
125. Gellaerts (2015).
126. Art. 6 en 8 sub a en b Wbp, met uitzonderingen in art. 8 sub c-f Wbp. Art. 8 sub b Wbp gaat om gevallen waar in feite de toestemming geïmpliceerd is in de overeenkomst of de onderhandeling.

Daarnaast rust op vele particuliere databestanden een eigen IE-recht van de particuliere maker. Een voorbeeld zijn foto's waarop snel een auteursrecht rust. Bij triviale foto's (de zoveelste foto van de Eiffeltoren, zonder dat er herkenbare personen op staan afgebeeld) kan dat overigens anders zijn.

Als data in géén van deze categorieën valt, zal het gaan om particuliere data zonder enig privacy-belang of IE-recht, dan wel om zakelijke data zonder bedrijfsmatige betekenis of waarde. In dergelijke gevallen kan thans geen exclusiviteit worden afgedwongen. Maar dat is ook geen probleem: er is dan immers geen belang bij exclusiviteit. Dergelijke data wordt meestal ook vrijelijk gedeeld: het kan dan gaan om kleine brokstukjes informatie of meetgegevens, een eenvoudige routebeschrijving.

Exclusiviteit van data, voorzover wenselijk, is derhalve grotendeels in overeenstemming met geldend recht![127] Toegegeven zij dat handhaving lastig kan zijn. Het is niet altijd bekend dát er een illegale kopie bij een ander is. Dat is op zichzelf niet erg, aangezien een kopie vooral problematisch is als deze op enige wijze gebruikt wordt, en daar zal de 'eigenaar' veelal gevolgen van ondervinden zodat op die manier de kopie van worden gedetecteerd. Verder is het moeilijk zeker te stellen dat er nergens een kopie rondzwerft (al dan niet per ongeluk op een backup). In de praktijk zal men niet verder komen dan een verbod versterkt met (hoge) dwangsom, waardoor de hoop is dat een inbreukmaker zal worden 'gepakt' als hij op enig moment later toch blijkt een kopie te hebben behouden. Voor handhaving is men dan feitelijk weer afhankelijk van detectie van het bezit van die data, wat waarschijnlijk alleen zal blijken door het daadwerkelijk gebruiken van deze gegevens. Overigens moet men ook niet te moeilijk doen over toevallige, niet gebruikte, kopieën. In veel gevallen is het wenselijk dat er nog geruime tijd reservekopieën aanwezig zijn, bijvoorbeeld juist om revindicatie door de 'eigenaar' mogelijk te maken.[128]

3.9 Remedies (3): schadevergoeding voor de rechthebbende

Volledige erkenning van digitale activa vergt ook dat de waarde hiervan wordt erkend. Dit lijkt voor de hand liggend, maar is het niet. In het privaatrecht wordt waarde primair erkend door compensatie, te weten vergoeding van de vermindering in vermogenswaarde. Naar Nederlands recht wordt schadevergoeding toegelaten voor alle soorten schade. Echter zaakschade en letselschade worden doorgaans aangemerkt als bevoorrecht, doordat bijvoorbeeld toerekening sneller wordt aangenomen dan bij zui-

127. Voorzover de data onrechtmatig verkregen is. Als de data door eigen inspanning van de ander is verworven (bijv. eigen waarnemingen) kan de verwijdering hiervan niet worden bewerkstelligd met beroep op exclusiviteit: het gaat dus duidelijk niet om een recht erga omnes zoals het octrooirecht.

128. Vgl. ook het recht op behoud van een kopie-dossier (HR 25 mei 2012, NJ 2012/566).

vere vermogensschade.[129] In andere rechtsstelsels geldt in nog sterkere mate terughoudendheid bij vergoeding van zuivere vermogensschade: bijvoorbeeld in de U.S.A. wordt dergelijke schade bij *negligence* als regel niet vergoed.[130] Daarnaast wordt in veel contracten en algemene voorwaarden schadevergoeding voor zuiver vermogensschade verregaand geëxonereerd, en dergelijke exoneraties houden merendeels stand.

Dergelijke beperkingen waren vroeger wellicht begrijpelijk, echter tegenwoordig vormt dit een moeilijk te rechtvaardigen algemene achterstelling van het digitale domein. In het bijzonder waar het gaat om contractuele verhoudingen die primair betrekking hebben op het digitale lijkt het vreemd dat de meest relevante en voorzienbare vorm van schade niet voor vergoeding in aanmerking zou komen. Toegegeven zij dat men kan aarzelen of een algehele gelijkschakeling wenselijk is; dit behoeft nadere discussie die tot op heden ontbreekt in de literatuur. Het zou derhalve nodig zijn dat beschadiging of verlies van data eenzelfde bescherming zou verkrijgen als zaakschade.

Een praktisch probleem hierbij kan zijn dat het niet altijd eenvoudig is om het waardeverlies bij beschadiging of kopieën van data te begroten. Een duidelijke markt voor data ontbreekt op dit moment nog. Het lijkt echter slechts een kwestie van tijd voordat hier duidelijker richtlijnen ontstaan.[131]

Een alternatieve sanctie zou zijn te werken met forfaitaire schadevergoeding. Bij verlies van persoonlijke data zonder vermogenswaarde zou een vordering wegens immateriële schade het beste in het wettelijk systeem passen. Hiervoor zou mogelijk een wetswijziging nodig zijn; het is niet zeker dat dit onder art. 6:106 BW valt te brengen.

3.10 Privaatrechtelijke handhaving van privacy-belangen

Naast economische waarde voor de 'bezitter' kan data ook een potentiële aantasting van de privacy van derden met zich brengen. Voor een privaatrechtelijke analyse is het relevant welke belangen aan de orde zijn: doorgaans is concrete, werkelijke benadeling vereist. Gering ongemak of ongenoegen is ontoereikend.[132] Vrees voor potentiële benadeling kan wel

129. Asser/Hartkamp & Sieburgh 6-II 2013/66.
130. Tjong Tjin Tai e.a. (2015: 86-87) met verwijzingen.
131. Indien herstel mogelijk is wordt de schade veelal op herstelkosten begroot: Hof Den Haag 27 december 2011, ECLI:NL:GHSGR:2011:BV1678 (Scope/KPN), Rb Midden-Nederland 16 januari 2013, ECLI:NL:RBMNE:2013:BY7960. In een geval van verlies van SMS-historie werd de schadevergoeding begroot op de gederfde schadeloosstelling (wegens ongewenste SMSjes): Hof Den Haag 1 september 2015, ECLI:NL:GHDHA:2015:2332.
132. Vgl. ten aanzien van hinder HR 15 februari 1991, NJ 1992/639 (De Staat/OVB) en HR 21 oktober 2005, NJ 2006/418 (Ludlage/Van Paradijs) en ten aanzien van ergernis wegens gemist gebruik HR 5 december 2008, NJ 2010/579 (Pollen/Linssen), r.o. 3.7.

een gebod of verbod rechtvaardigen,[133] doch vormt op zichzelf geen schade.[134]

Bij privacy zijn deze belangen echter niet zeer concreet.[135] Intuïtief voelen velen wel enig onbehagen bij de grootschalige dataverzameling die tegenwoordig plaatsvindt, echter het is lastig om het geschonden belang precies onder woorden te brengen behalve door weer te verwijzen naar het abstracte belang van privacy. Voor privacy tegenover de overheid kan nog aansluiting worden gezocht bij de onschuldspresumptie en het recht gevrijwaard te worden van inbreuken op het privé-leven, echter bij dataverwerking door bedrijven op basis van contractsvoorwaarden schieten dergelijke invalshoeken tekort. De concept-Verordening gegevensbescherming COM(2012)11def. noemt vier belangen:

a. het fundamentele recht van controle over persoonsgegevens,[136]
b. vermogensschade door identiteitsdiefstal,[137]
c. immateriële en vermogensschade door mogelijk risico van misbruik van data en onjuiste of onrechtmatige conclusies op basis van zodanige data,[138]
d. het algemene verlies aan autonomie door de aanwezigheid van ongecontroleerde persoonsgegevens.[139]

Deze belangen leveren op zichzelf geen grond voor privaatrechtelijke actie zolang geen concrete schade is geleden.[140] Concrete schade zou bij (b) of (c) aanwezig kunnen zijn, ook in de vorm van kosten van voorzorgsmaatregelen na de inbreuk.

Een alternatieve invalshoek is dat privacy, evenals eigendom in het algemeen, te maken heeft met wat filosofisch wordt aangeduid als vrijheid in de vorm van zelf-verwezenlijking of actualisatie.[141] Het selectief blootgeven en gebruiken van persoonlijke informatie is de manier waarop mensen controle hebben over hun publieke en private imago, en dit daarmee vormgeven, zoals mensen ook zichzelf vormgeven door hun identiteit te belichamen in eigendom. Dit belang wordt van oudsher erkend in de

133. HR 28 juni 1974, NJ 1974/400 (Kamsteeg/Chevron).
134. HR 23 mei 1980, NJ 1980/466 (Oranje Nassau Mijnen/Van den Broeck) is geen uitzondering: daar leidde de voorzienbare toekomstige feitelijke schade tot daling van de actuele marktwaarde en dus tot actuele schade (waardevermindering).
135. Zie nader Purtova 2011, p. 43-50.
136. Cons. 1-2, 6, 129, 133 Concept-verordening.
137. Cons. 67, 116 e.v. Concept-verordening.
138. Cons. 16 e.v., met name 38, ook 121-126 Concept-verordening.
139. Geïmpliceerd in cons. 55 en 70 Concept-verordening.
140. Behalve mogelijk een actie op grond van art. 6:106 lid 1 sub b BW wegens inbreuk op het recht op privacy, indien dit als aantasting van de persoon kan worden gekwalificeerd. Een argument hiervoor kan worden gevonden in het effectiviteitsbeginsel.
141. Dit is in essentie een Hegeliaans perspectief, al is Hegel voorzover mij bekend slechts één maal in verband gebracht met privacyrecht (De Boni & Prigmore 2004).

bescherming van eer en goede naam.[142] Tegenwoordig wordt ook erkend dat bepaalde rechten, zoals het portretrecht en privacy, zowel het immateriële belang dienen van bescherming van de privacy[143] als het daaraan verbonden belang van commercialisering van de eigen persoon.[144] In zoverre gaat het hierbij om meer dan alleen de onderwerpen die doorgaans in het privacyrecht worden behandeld.

De verbreding van loutere informationele privacy naar de publieke en private persona laat zien dat het niet puur gaat om geheimhouding: het gaat juist om selectieve openbaarmaking, wat gerelateerd is aan het publiek, de wederpartij van de eigen identiteit.[145] Het draait derhalve om *erkenning*. De reden om dit punt te benadrukken is dat daardoor duidelijker wordt waar het meestal werkelijk om draait: niet de concrete informatie als zodanig, maar om het gehele beeld zoals dat bij anderen leeft. Men streeft naar een bepaalde erkenning van een ander, wat mede met zich brengt een zekere behandeling door een ander.

Voor de bescherming van deze belangen zijn er verschillende benaderingen voorgesteld. Erkenning van een persoonlijk recht of 'eigendom' op persoonsgegevens is op zichzelf onvoldoende als in de praktijk die rechten in de regel integraal worden weggegeven door onontkoombare toestemming op websites.[146] Dit is ook een beperking van het systeem van de Wbp: inperking van de verwerkingsmogelijkheden vooraf heeft weinig zin of effect, mede doordat niet goed kan worden voorspeld welke gebruikswijzen in de toekomst wenselijk zijn of niet.[147] Wel zinvol is controle op onredelijk bezwarende contractsvoorwaarden (par. 3.12) of toekenning van onvervreembare bevoegdheden, zoals het (publiekrechtelijke) recht om verwijdering van eigen persoonsgegevens te vorderen indien deze in strijd met de toepasselijke regels worden verwerkt (art. 36 lid 1 Wbp).

142. Het oudere begrip had concrete gevolgen voor juridische status: Flannery (2007), Telecha (2007).
143. Vgl. HR 1 juli 1988, NJ 1988/1000 (Vondelpark).
144. HR 19 januari 1979, NJ 1979/383 ('t Schaep met de vijf pooten), HR 14 juni 2013, NJ 2015/112 (Cruijff). Zie algemeen over een recht op persona: Pinckaers (1996), vgl. Purtova (2011).
145. Vgl. Van der Sloot (2015) over art. 8 EVRM als bescherming van persoonlijke ontwikkeling.
146. Vergelijkbare ontwikkelingen zag en ziet men bij de verzamelpandakte (waarmee periodiek alle activa aan de bank worden verpand) en de nagenoeg volledige overdracht van auteursrecht aan beheersorganisaties.
147. Kool, Timmer & Van Est (2015: 33). Zie de vergelijkbare discussie rond licentiëring: vroeger vroegen uitgevers een te beperkte licentie, waardoor Internetpublicatie erbuiten viel, tegenwoordig zijn de licenties zo ruim dat alles wat ooit mogelijk is eronder valt maar dan het risico aanwezig is dat de rechthebbende teveel weggeeft zonder daar toereikende vergoeding voor te ontvangen.

Voor andere vormen van privaatrechtelijke handhaving is alleen grond bij concrete aantasting van belangen.[148] De aandacht verschuift dan vanzelf van de verzameling van gegevens naar het gebruik: wat gebeurt er concreet met de data, en in hoeverre is dit ongewenst? Opdat handhaving mogelijk is, dient eerder gegeven toestemming niet allesbepalend te zijn.[149] Voorzover een eerder verleende toestemming dit zou belemmeren zou die wellicht kunnen worden aangetast als zijnde een onredelijk bezwarende algemene voorwaarde.[150] Ook zou misbruik van bevoegdheid (art. 3:13 BW) in extreme gevallen uitkomst bieden. Dan zou, zonder dat de toestemming de casus bepaalt, een casuïstische afweging van belangen kunnen worden gebruikt binnen de bestaande rechtsfiguren om individuen de controle over privacy te geven die zij behoeven. Privaatrechtelijke actie heeft daarbij grote voordelen: het herstelt de autonomie nu individuen zelf kunnen ageren wanneer zij daartoe aanleiding zien, het wordt alleen ingeroepen en toegekend wanneer dat in concreto nodig is, en het kan rekening houden met nieuwe ontwikkelingen doordat steeds in de concrete situatie een beoordeling kan worden gegeven.

Deze abstracte argumentatie zal ik illustreren aan drie voorbeelden van concrete belangen die zouden nopen tot restricties bij het gebruik van privacy-gevoelige data.

1. Ten eerste is er het belang dat een consument op faire wijze wordt behandeld door bedrijven.[151] Met behulp van persoonsgegevens kan een bedrijf een consument (bijvoorbeeld op een webshop) informatie en aanbiedingen op maat aanleveren, wat op zichzelf wenselijk kan zijn. Fysieke winkels kennen ook het fenomeen dat vaste klanten door de eigenaar persoonlijker worden benaderd, en dit wordt veelal positief gewaardeerd. Voor webshops is dit echter misschien minder wenselijk, nu die individuele behandeling niet menselijk maar automatisch gegenereerd wordt, en er ook niet voor die behandeling is gekozen. Een consument kan bijvoorbeeld ook doelbewust naar een warenhuis gaan omdat hij als anonieme klant wil worden behandeld. Bovendien is de behandeling gebaseerd op aannames en afleidingen over grote groepen klanten, wat in in individuele gevallen onjuist of storend kan werken. Wie een filosofisch boek als cadeau voor een vriend koopt wil mogelijk niet lastig gevallen worden met meer aanbiedingen in dit genre: een winkelier kan dit weten omdat dit hem verteld wordt bij het afrekenen, maar een webshop kan dit soort onderscheiden niet maken. Die pro-

148. Dit is een beperking van het privaatrecht; voor niet-concrete mogelijke aantasting is publiekrechtelijke handhaving van groot belang.
149. Kool, Timmer & Van Est (2015: 33-36). Gisclard (2014) verdedigt daarom een 'right of withdrawal'. Morey, Forbath & Schoop (2015) adviseren bedrijven eveneens om consumenten betere controlemogelijkheden te bieden na eerdere toestemming.
150. Par 3.12, ook Kuczerawy & Coudert (2011).
151. Zie ook een te verwachten artikel van Neppelenbroek.

filering leidt gemakkelijk tot miskenning van de eigen identiteit en is daarom voor consumenten ergernis- en zorgwekkend. Op zichzelf zijn hier echter geen privaatrechtelijke instrumenten tegen. Dit valt privaatrechtelijk te rechtvaardigen door de mogelijkheid van consumenten om desgewenst een andere webshop te kiezen: men stemt met de voeten.[152] Desgewenst zou de (Europese) wetgever regels kunnen opleggen die bedrijven verplichten om consumenten meer invloed te geven op de wijze van profilering e.d.

Daarnaast kunnen persoonsgegevens gebruikt worden om een consument te sturen op basis van zijn beslissingsstrategie, een vorm van 'nudging'.[153] Daarmee wordt het keuzeproces van het individu bewust gemanipuleerd, wat vanuit privaatrechtelijk perspectief in commerciële verhoudingen verdacht is. Privaatrechtelijk kennen we hier evenwel al een correctie voor: de wilsgebreken. De rechtshandeling is verricht onder invloed van mededelingen van de wederpartij terwijl deze moest weten dat zonder deze mededelingen niet deze handeling of niet onder deze voorwaarden zou zijn verricht. Preciezer gelezen is nog niet evident dat de bestaande wilsgebreken ook op deze situatie zien. De rechtsfiguur van dwaling (art. 6:228 BW) vereist naast dergelijke invloed van mededelingen ook de daadwerkelijke aanwezigheid van feitelijke dwaling (een valse voorstelling van zaken), en het is niet evident dat er bij nudging zodanige valse voorstelling aanwezig is. Misbruik van omstandigheden (art. 3:44 lid 4 BW) vereist dat iemand bewogen wordt tot een zekere rechtshandeling door 'bijzondere omstandigheden' als afhankelijkheid of lichtzinnigheid: *nudging* van gewone consumenten valt niet evident hieronder. Een aanknopingspunt is mogelijk te vinden in de regeling inzake oneerlijke handelspraktijken. Art. 6:193c BW luidt: "Een handelspraktijk is misleidend indien informatie wordt verstrekt die feitelijk onjuist is of die de gemiddelde consument misleidt of kan misleiden, al dan niet door de algemene presentatie van de informatie, zoals (…), waardoor de gemiddelde consument een besluit over een overeenkomst neemt of kan nemen, dat hij anders niet had genomen." Alhoewel de expliciet genoemde voorbeelden van informatie vooral betrekking hebben op concrete gegevens omtrent de overeenkomst en voorwaarden, kan in een voldoende ruime lezing (met name gelet op het 'de algemene presentatie') ook *undisclosed nudging* hieronder worden gebracht. Wel geldt dat uiteindelijk het Hof van Justitie zal hebben te oordelen of een dergelijke uitleg van art. 6:193c BW is toegelaten, nu deze bepaling een implementatie is van art. 6 Richtlijn 2005/29/EG.

152. Of anders gezegd: er is een exit-optie.
153. Verwant hieraan is prijs-discriminatie, waarover Zuiderveen Borgesius (2015).

2. Een tweede concreet belang is de aloude eer en goede naam, oftewel reputatie. De bescherming hiervan wordt reeds met bekende juridische middelen bewerkstelligd, los van het systeem van de Wbp.[154] De wraakporno-zaak tegen Facebook (par. 1.1) is hier een voorbeeld van. Tegenwoordig ligt dit evenwel gecompliceerder als gevolg van de toegenomen mogelijkheden om anoniem informatie breed te verspreiden, terwijl de betrokken tussenpersonen veelal een beroep kunnen doen op de immuniteit voor ISP's. Dit vereist wijzigingen om handhaving effectief te maken (par. 4).
   Een ander nieuw probleem is dat handhaving vroeger doorgaans beperkt bleef en kon blijven tot de directe geografische omgeving. Tegenwoordig is informatie veelal wereldwijd beschikbaar en kan een actie tot bescherming van reputatie dus mogelijk ook overal worden ingesteld. De lokale normen kunnen evenwel verschillen. Bescherming van slechts het laagste niveau lijkt onjuist, maar omgekeerd lijkt het evenmin wenselijk dat het strengste niveau steeds kan worden toegepast.[155] Een oplossing voor deze tegenstelling valt slechts te bereiken via harmonisatie. Wel valt hierbij op te merken dat harmonisatie misschien ook thans reeds via culturele weg buiten het recht om plaatsvindt. Een uiting in een Nederlands tijdschrift komt nu snel ter kennis van de amerikaanse popster Rihanna en leidt door buitenjuridische druk tot excuses en ontslag van de hoofdredacteur.[156]
3. Een derde belang kan zijn de erkenning als individu door derden. Niet alleen in contractuele context, maar ook daarbuiten, zoals bij het gebruik van zoekmachines of presentatie van advertenties, neemt personalisatie toe. Dit kan vanuit het perspectief van erkenning worden bekritiseerd: iemand die alleen een wereld ziet die op zijn maat is gemaakt, wordt kennis van de werkelijkheid onthouden.[157] Opnieuw valt hier te betogen dat personalisatie in veel gevallen zinvol of wenselijk kan zijn; het punt is vooral dat iemand zich hier ook tegen zou moeten kunnen verzetten. Privaatrechtelijk lijkt hier geen gereedstaand juridisch instrument voor. Echter in de praktijk wordt dit technisch opgelost doordat men ervoor kan kiezen een andere zoekmachine te gebruiken of een adblocker te installeren: de keuze om geen perso-

154. Bijv. HR 1 juli 1988, NJ 1988/1000 (Vondelpark).
155. Zie de thans lopende discussie over de reikwijdte van het recht op vergetelheid jegens Google: werkt dit alleen nationaal of ook internationaal? <http://www.cnil.fr/english/news-and-events/news/article/right-to-delisting-google-informal-appeal-rejected/> Een te strenge norm kan ertoe leiden dat landen met strikte beperkingen aan vrijheid van meningsuiting indirect Internet in andere landen kunnen censureren. Een te lakse norm leidt ertoe dat materiaal dat wij onwenselijk achten (oproepen tot terrorisme, kinderporno) niet goed geweerd kan worden.
156. http://nos.nl/artikel/323809-hoofdredacteur-stapt-op-om-niggabitch-in-tijdschrift-jackie.html
157. Dit is in essentie de Hegeliaanse meester-slaaf dialectiek.

> nalisatie te wensen kan dus door een privé-persoon worden kenbaar gemaakt en geëffectueerd door dergelijke handelingen. Wie dit nalaat, kan worden aangerekend zelf te hebben gekozen voor een niet-objectieve benadering.[158]

Deze snelle analyse suggereert dat er al grotendeels geschikte privaatrechtelijke remedies bestaan voor drie concrete belangen die onder privacy vallen. Enkele aanpassingen zijn zinvol, maar een radicale omwenteling lijkt niet nodig. Dit adstrueert dat een privaatrechtelijke benadering van privacy daadwerkelijk effectief kan zijn, mits toestemming geen absoluut beletsel is.

Om misverstanden te vermijden: de bestaande regels voor privacyrecht inclusief de bijbehorende publiekrechtelijke handhavingsbevoegdheden zijn ook zinvol naast en in aanvulling op de hier beschreven privaatrechtelijke beschermingsmogelijkheden. Bijvoorbeeld het bewaren van bepaalde zeer privacygevoelige informatie kan duiden op een voorbereiding om onrechtmatig te handelen en kan beter en gemakkelijker publiekrechtelijk worden aangepakt.[159]

Op één punt is het privaatrecht nog weinig effectief: de schadevergoeding is meestal gering (par. 3.11).[160] Echter de hierboven besproken remedies bieden andere mogelijkheden en kunnen effectief zijn doordat zij sommige voordelen van privacyschending wegnemen. Als consumenten gebruik kunnen maken van wilsgebreken bij niet medegedeelde *nudging*, is dit een sterke prikkel tegen verborgen gebruik van hun persoonsgegevens. Een dergelijke actie is bovendien efficiënt aangezien zij alleen zal worden ingesteld door consumenten bij wie dit gebruik daadwerkelijk onwenselijk is; een consument die tevreden is, zal geen reden hebben om vernietiging te verlangen.

3.11 Aansprakelijkheid voor digitale activa

Bij de erkenning van digitale activa hoort ook aansprakelijkheid voor schade die door digitale activa is ontstaan. Dit kan hier slechts schetsmatig worden besproken. In het algemeen zullen de open normen voor contactuele en delictuele aansprakelijkheid een toereikende grondslag vormen voor de ontwikkeling van dit leerstuk. Mogelijk kan bij analogie aansluiting worden gezocht bij aansprakelijkheid van de bezitter voor roerende zaken of dieren voorzover het gaat om activa die kunnen handelen (zoals

158. De mogelijkheid van een technische benadering verdient meer aandacht. Bijvoorbeeld eisen veel op smartphones allerlei overbodige bevoegdheden die tot privacyschending kunnen leiden. Pas sinds kort beginnen besturingssystemen van smartphones genuanceerdere controlemogelijkheden te bieden.
159. Naast eventuele collectieve actie.
160. Ook Peters (2014) voor Amerikaans recht.

'bots'[161]), of bij productenaansprakelijkheid.[162] Het is mogelijk dat sommige wettelijke regels aanpassing behoeven: in het bijzonder productenaansprakelijkheid voor digitale activa (inclusief data en software) zou wetswijziging behoeven,[163] waarbij rekening dient te worden gehouden met de eigen aard van dergelijke objecten.

Aansprakelijkheid kan verder bestaan voor de kwaliteit van of gebreken in digitale activa. Oudere literatuur biedt hiervoor een eerste aanknopingspunt, al zal een hernieuwde doordenking nodig zijn.[164] De kwaliteit van data zal veelal afhangen van de kwaliteit van de informatie besloten in deze data en dus de regels inzake aansprakelijkheid voor informatie volgen.[165] Niettemin kan het ook om andere gevallen gaan: een voorbeeld is een muziekbestand dat niet de gewenste kwaliteit bezit (bijv. 16 bit/44.1 kHz resolutie inplaats van 24 bit/96 kHz). Het gaat dan (bij koop) om non-conformiteit[166] die door levering van een correct bestand kan worden verholpen.[167] Het is mogelijk dat data ook tot gevolgschade leidt:[168] denk aan kwalitatief mindere data die tot onjuiste beslissingen leidt. Onjuiste medische data zou zelfs tot letselschade kunnen leiden. In lijn met het betoogde in par. 3.2-3.3 zal erkenning van digitale activa ook dienen te leiden tot het serieuzer nemen van schade in het digitale domein.

Voor schade uit privacyschending geldt dat dit lastig te begroten is. Vermogensschade zal veelal niet aanwezig zijn,[169] behalve bij schending van reputatie of identiteitsdiefstal. Privacy valt echter tevens onder het fundamentele recht op family life (art. 8 EVRM): schending van een dergelijk fundamenteel recht is een andere aantasting van de persoon als bedoeld in art. 6:106 lid 1 sub b BW, en geeft recht op smartengeld. Schadevergoeding voor privacyschending kan soms substantieel zijn maar ook gering:[170] bij schending buiten gevallen van perspublicatie is onzeker of een substantiële vergoeding zal worden verkregen. Het is verdedigbaar

161. Vgl. hierover Schreuder (2014).
162. Bijv. Westerdijk (1995) en Rinzema (2012) ten aanzien van software, ook de Amerikaanse discussie als weergegeven in Tjong Tjin Tai e.a. (2015: 84-85 en 167-168).
163. Bijvoorbeeld van art. 6:187 lid 1 BW, dat dit leerstuk beperkt tot roerende zaken.
164. Bijv. Loos (2011) ten aanzien van koop van digitale inhoud.
165. Waarover (met name ten aanzien van de overheid) Barendrecht e.a. (2002) en HR 25 mei 2012, NJ 2012/340.
166. Vgl. art. 6 van de concept-richtlijn digitale inhoud COM(2015)634.
167. Hoewel hier complicaties kunnen optreden (Op Heij 2015).
168. Art. 14 van de concept-richtlijn digitale inhoud COM(2015)634 geeft een recht op vergoeding van economische schade.
169. Vgl. Peters (2014) die voor Amerikaans recht vaststelt dat er nauwelijks recht op schadevergoeding is, nu het vooral gaat om .
170. Lindenbergh (1998: 162-165) en GS Schadevergoeding (Lindenbergh), art. 106, aant. 2.8.6. De rechtspraak lijkt vooral te zien op perspublicaties. Van Dam (2015: nr. 405, 410, 411) is kritisch over de mogelijke eis dat sprake is van aantasting, en ziet in HR 4 oktober 2013, NJ 2013/479 een wenselijke kentering.

dat de effectieve bescherming van dit op Europese regelgeving gebaseerde recht op privacy een substantiëlere schadevergoeding vergt.[171] Handhaving via massaclaims zou daarnaast een effectief instrument kunnen zijn.

3.12 Onredelijk bezwarende voorwaarden omtrent digitale activa

De schets in de voorgaande paragrafen zou neerkomen op diverse wijzigingen in regelend recht. Voor een effectieve rechtsbescherming is dit echter ontoereikend aangezien IT-dienstverleners (praktisch) altijd algemene voorwaarden hanteren die veelal nauwkeurig aangeven welke rechten en bevoegdheden bij de dienstverlener liggen en welke voor de consument overblijven.[172] Dit leidt tot exoneratie van alle vergoeding voor schade behalve (irrelevante) zaakschade en letselschade, verlening aan de dienstverlener van zo ver mogelijk strekkende gebruiks- en beschikkingsbevoegdheden over de data, afstand van remedies, beperking aan overdracht van rechten aan derden. Dit leidt veelal ertoe dat benadeelden in feite geen betekenisvolle bescherming genieten.

Op zichzelf kunnen onereuze contractsvoorwaarden worden bestreden op basis van het algemene leerstuk van onredelijke bezwarende algemene voorwaarden (art. 6:231 e.v. BW).[173] De desbetreffende regeling en relevante jurisprudentie is evenwel vooral geënt op reeds bekende soorten oneerlijke bedingen, zoals exoneraties. Voor onredelijke bedingen ten aanzien van bijvoorbeeld licenties op data of afstand van een recht op teruggave van data bieden deze regelingen geen duidelijkheid: weliswaar kan de open norm van art. 6:233 BW ook dergelijke bedingen toetsen, maar het is onzeker hoe dit zal uitpakken.

In de praktijk vindt regulering op dit moment vooral plaats buiten de rechtszaal. Wanneer bedrijven als Facebook of Instagram hun voorwaarden wijzigen in voor de consument onwenselijke vorm wordt dit door oplettende gebruikers waargenomen en bekend gemaakt: dit leidt regelmatig tot correctie van te ver strekkende voorwaarden.[174] Gebruikers die op dergelijke berichten letten blijven op de hoogte van onwenselijke wijzigingen: ze kunnen uiteindelijk ervoor kiezen afstand te nemen van een dienst die te ver gaat. Als ze dat niet doen, kan dit worden uitgelegd als dat de ruil als eerlijk wordt ervaren.

171. Vgl. HvJ 10 april 1984, zaak 14/83, Jur. 1984, p. 1892 (Von Colson/Nordrhein-Westfalen) ten aanzien van discriminatie op sekse.
172. Bijv. over cloud computing Daniëls & Kits (2015).
173. Zie bij. Loos & Luziak (2015), die o.a. wijzen op beëindiging, eenzijdige wijziging van voorwaarden, exoneraties, rechts- en forumkeuze, en over privacy Kuczerawy & Coudert (2011).
174. Bijv. Instagram in december 2012 (https://en.wikipedia.org/wiki/Instagram#Terms_of_use), ook Kuczerawy & Coudert(2011).

Daarnaast hebben gebruikers technische mogelijkheden om ongebreidelde datacollectie tegen te gaan: het gebruik van ad-blockers[175] neemt toe vanwege de zorgen over dataverzameling. De roep om genuanceerdere mechanismen heeft geleid tot aanpassingen van Android bij het geven van toestemming (*permissions*) aan *apps*.[176]

Er vindt derhalve al een significante mate van regulering plaats die helpt om vorm te geven aan wat redelijke voorwaarden zijn. Tegelijk vindt er ook juridische regulering plaats, in het bijzonder door interventies van privacy-toezichthouders.[177]

Al deze ontwikkelingen kunnen worden geïnterpreteerd als een collectief leerproces waarin we proberen vast te stellen wat redelijke voorwaarden zijn en wat een redelijke contractuele *deal* is. De toekomst zal leren wat de uitkomst is. Dat neemt niet weg dat deze ontwikkeling mede gevoed wordt door adviezen van juristen over concrete stappen. Het is daarom zinvol om na te denken over wat redelijke voorwaarden en praktijken zijn. Men zou aansluiting kunnen zoeken bij de toetsing van overdracht en licentiëring van auteursrecht: daar stellen art. 2 lid 2 Aw en het auteurscontractenrecht[178] grenzen aan het wegcontracteren van latere, onbekende gebruikswijzen.[179] Verder bevat art. 25f Aw een speciale toets voor onredelijke bedingen. Zoals aangegeven in par. 3.5 bevinden particulieren zich ten aanzien van data regelmatig in eenzelfde positie als de maker/auteur ten aanzien van een auteursrechtelijk beschermd werk.

3.13 Conclusie

Naar geldend recht beschikt de 'eigenaar' van data of virtuele objecten reeds grotendeels over typische eigenaarsbevoegdheden, met name als hij toereikende contractuele regelingen treft. Dit is ook in overeenstemming met de belangen die gemoeid zijn met data en virtuele objecten in de tegenwoordige samenleving. Niettemin ontbreken op diverse punten bevoegdheden en bescherming: in het bijzonder voor revindicatie, beslag, en schadevergoeding zouden wijzigingen nodig zijn, terwijl bijvoorbeeld voor exclusiviteit en faillissement nadere regelingen rechtszekerheid zouden verschaffen. Voor bescherming van privacy kan het privaatrecht een belangrijke aanvullende bescherming bieden voor precies die gevallen

175. Die namelijk niet alleen het tonen van advertenties maar ook het volgen van internetgebruik blokkeren.
176. In Android 6.0 (Marshmallow).
177. Bijv. in 2015 de Belgische privacycommissie (https://www.privacycommission.be/en/news/judgment-facebook-case) en de Ierse Data Protection Commissioner (http://www.pcworld.com/article/2995418/privacy/irish-privacy-watchdog-to-investigate-facebook-over-spying-allegations.html) tegen Facebook.
178. Stb. 2015/257, iwtr. 1 juli 2015, Stb. 2015/258.
179. In het bijzonder art. 25c lid 6 en art. 25d Aw; krachtens art. 25h Aw is de regeling van dwingend recht.

waar privacyschending daadwerkelijk concrete belangen benadeelt: dit vergt toepassing van klassieke privaatrechtelijke leerstukken op nieuwe fenomenen.

Tegelijk geldt voor dit alles dat het contractenrecht ook een belemmering kan zijn: in veel gevallen worden wenselijke regelingen geblokkeerd door te ruime of juist te beperkende voorwaarden. De regeling inzake onredelijk bezwarende bedingen biedt te weinig zekerheid om hier de benodigde controle te bieden; nadere Europese regelgeving zou ook op deze punten het privaatrecht verder helpen door onwenselijke bedingen nietig te verklaren.

Deze wijzigingen zouden versterkt kunnen worden door verdergaande institutionele wijzigingen. Deze komen in de volgende paragraaf aan de orde.

4 Ondersteunende kwesties

4.1 Inleiding

De schets in par. 3 beschrijft vooral het materiële recht. Op Internet is dit echter nauwelijks effectief, deels doordat bedrijven en effecten grensoverstijgend zijn en daardoor lastig nationaal aan te pakken, deels door de eigenschappen van digitale activa en Internet. Een voorbeeld is de Facebook-zaak over wraakporno (par. 1). Facebook lijkt te hebben nagelaten de relevante gegevens over de uploader te bewaren, ofschoon zij wist van de lopende rechtszaak, en heeft daarme het achterhalen van de dader effectief onmogelijk gemaakt. Daardoor staat het slachtoffer mogelijk met lege handen. In deze paragraaf schets ik enkele ondersteunende maatregelen die wenselijk zijn om de beoogde bescherming van digitale activa en privacy effectiever te maken.

4.2 Digitale identiteit

Veel digitale rechten, objecten en gedragingen zijn verbonden aan digitale identiteiten.[180] Dit leidt tot twee problemen:

1. er is geen vanzelfsprekende of gemakkelijke koppeling tussen de digitale identiteit en de fysieke identiteit. Dit bemoeilijkt rechtshandhaving, die zich immers richt op de fysieke identiteit.
2. het is lastig aan te tonen dat men rechthebbende of beschikkingsbevoegde is. Dit bemoeilijkt de positie van erfgenamen of de faillissementscurator. Strikt juridisch bezien is elke digitale identiteit ver-

180. Niet alle: de domeinnaam wordt met gewone juridische contracten verbonden aan een rechtssubject.

bonden aan een echt rechtssubject, aangezien dat het account door een individu is aangemaakt.[181] Echter een dergelijk account is eenvoudig puur virtueel te maken waarbij men geen correcte privé-gegevens hoeft door te geven. Denk aan gratis accounts via Hotmail, Yahoo. Men kan bijvoorbeeld via een dergelijke digitale identiteit een account bij Dropbox aanmaken en daar aanzienlijke hoeveelheden data opslaan, die geld waard zijn, men kan een account bij een discussieforum aanmaken en daar lasterlijke beschuldigingen uiten. Weliswaar is het met veel inspanning vaak mogelijk uiteindelijk de fysieke persoon te achterhalen, maar dit is niet altijd mogelijk en kan kostbaar zijn.

Inmiddels zijn er daarom verschillende inspanningen om de online identiteit te verstevigen. Facebook[182] en LinkedIn[183] vereisen bijvoorbeeld dat je onder je echte naam bekend staat en weigeren pseudoniemen. Diverse websites trachten twijfelachtige identiteiten strenger te verifiëren met officiële documenten.[184] Dit kan worden omzeild en is niet waterdicht, toch kan men dit interpreteren als een poging om een gegarandeerde, betrouwbare verbinding aan te brengen tussen online en offline identiteit. Men ziet ook dat de Facebook-login kan of soms zelfs moet worden gebruikt als 'inlogmethode' of identificatie bij andere websites. Dit zou problemen met anonieme uitingen oplossen. Tegelijk zou dit de vrijheid van meningsuiting belemmeren: de anonimiteit op Internet wordt ook als een groot goed gezien.

Het gaat hier dus om een zekere mate van identificatie met tussenkomst van een autoriteit. De EU is deze weg ingeslagen met de Verordening elektronische identificatie en vertrouwensdiensten (eIDAS) 910/2014.[185] Deze ondersteunt *trust services* (vertrouwensdiensten) die (onder meer) de fysieke identiteit van iemand bevestigen in het digitale domein.[186] Een

181. Echter: het is ook mogelijk dat een account aanmaken en daaruit handelen. Weliswaar is de bot dan weer de verantwoordelijkheid van een rechtssubject, maar het aanmaken van de account is dan mogelijk automatisch geschied.
182. Facebook gaat echter pseudoniemen in beperkte mate toelaten: zie http://www.scribd.com/doc/287927116/Letter-from-Facebook-s-Alex-Schultz (november 2015).
183. art. 8.1 User Agreement https://www.linkedin.com/legal/user-agreement.
184. Bv. Airbnb met Verified ID (http://blog.airbnb.com/introducing-airbnb-verified-id/, https://www.airbnb.nl/support/article/269) die daartoe vraagt om koppeling met een Facebook, LinkedIn of Google+ account, telefoonnummer, toezending van kopie van paspoort, dan wel een video profile. Hierover kritisch bv. http://blogs.law.harvard.edu/doc/2013/05/28/lets-help-airbnb-rebuild-the-bridge-it-just-burned/ vanwege de privacy-consequenties van koppeling met Facebook/LinkedIn.
185. Over het voorstel COM (2012)238 zie Voulon (2013 en 2014: 354), Wefers Bettink & Theeven (2013).
186. Vgl. de notariële legalisatieverklaring, waarvan ook de vraag is of deze in het digitale tijdperk op andere wijze kan worden geverifieerd: Waaijer (2015).

voorbeeld hiervan is het in ontwikkeling zijnde Nederlandse eID Stelsel.[187] Estland biedt 'e-residency' aan voor niet-ingezetenen.[188]

Men kan zich echter afvragen of we digitale identiteiten niet zouden moeten benaderen vanuit hun eigen digitale domein en vermogen, aangezien dat executie en verhaal aanzienlijk vereenvoudigt (par. 4.5). Digitale identiteiten hebben zelf een digitale reputatie, en soms zelfs een digitaal vermogen of waarde. Discussiefora staan bijvoorbeeld gebruikers pas rechten (zoals het plakken van plaatjes) toe na een groot aantal posts, waardoor incidenteel misbruik wordt voorkomen doordat een gebruiker eerst zijn goede trouw heeft bevestigd door de inspanning om een waardevol lid van het forum te zijn. Het posten van een filmpje op Facebook zou bijvoorbeeld aan een dergelijke drempel kunnen worden onderworpen. Evenzo worden recensies en ratings van bekende en langdurige gebruikers serieuzer genomen dan van onbekende, incidentele gebruikers. Een andere maatstaf kan zijn of de account gelinkt is aan een aantal andere, betrouwbare, accounts.

Misbruik van de digitale identiteit wordt ontmoedigd aangezien dat op die digitale identiteit afstraalt. Daarnaast zou verhaal op die identiteit mogelijk kunnen worden (par. 4.5). Een voordeel is dat men misbruik en onrechtmatig handelen kan ontmoedigen zonder anonimiteit geheel op te geven. In de praktijk ziet men dit mechanisme werken via reputatie en rating van handelaren op bv. eBay:[189] de terugkoppeling houdt handelaren bij de les, handelaren met kortere historie zijn minder betrouwbaar. In het fysieke domein kennen we dit ook al bij het werk van het Bureau Kredietregistratie (BKR). Hiermee zouden we een digitale vertaling krijgen van de offline zekerheid in identiteit. Dat iemand serieus is, blijkt uit de investering die hij heeft gedaan in zijn identiteit. Dit is overigens geen absolute garantie. Het komt ook voor dat mensen welbewust een valse identiteit opbouwen met langdurige tijdsinvestering.[190]

Een digitale identiteit is geen oplossing voor het vraagstuk van opvolging onder algemene titel. Hiervoor zouden *trust services* in de zin van eIDAS Verordening 910/2014 kunnen dienen: deze zouden moeten worden uitgebreid om ook te bevestigen dat een digitale identiteit is overgenomen door een andere beschikkingsbevoegde partij zoals de erven of een faillissementscurator. Hiervoor zou een regeling moeten komen die de trust services verbinden aan overheidsinstanties[191] of ambtenaren die met

187. http://www.eid-stelsel.nl
188. https://e-estonia.com/e-residents/about/
189. Of bij Airbnb: aantal vrienden bij Facebook, aantal recensies over appartement.
190. Naar verluidt bieden Chinese organisaties diensten aan om gunstige recensies te schrijven: medewerkers worden dan betaald om op grote schaal fictieve recensies te schrijven.
191. De draft-UFADAA regeling voor *fiduciary access to digital assets* vereist een *court order* (art. 5).

voldoende betrouwbaarheid in internationaal verband kunnen waarborgen dat de opvolging in orde is volgens de toepasselijke officiële instanties.[192]

4.3 Online en digitaal procederen

De problemen met het bewijzen van identiteit en effectiviteit van handhaving worden deels veroorzaakt doordat de primaire veroorzaker lastig te achterhalen en aan te pakken is. In veel gevallen zijn echter ook derden betrokken, verantwoordelijk voor de infrastructuur (par. 4.6), die zouden kunnen helpen met handhaving en daar soms op zichzelf ook wel toe bereid zijn. Problematisch blijft dan evenwel dat een goedkope, effectieve rechtsgang regelmatig ontbreekt: procederen leidt tot gecompliceerde IPR-vragen en kan nopen tot procedures in andere landen aangezien Nederlandse uitspraken niet noodzakelijk zonder meer zullen worden nageleefd door buitenlandse ondernemingen. De praktijk lijkt zich daarom op een andere manier te helpen:[193] door informele vormen van online geschilbeslechting (Online Dispute Resolution, ODR),[194] die, alhoewel zij het dwingende en bindende karakter van overheidsrechtspraak ontberen, een effectievere vorm van geschilbeslechting opleveren dan de officiële weg. Let wel: ik doel hierbij niet op ODR in de zin van online varianten van overheidsrechtspraak.

Een voorbeeld is de arbitrage in internationale domeinnaamzaken (de Uniform Dispute Resolution Procedure of UDRP).[195] Kenmerken hiervan zijn:

– de grondslag is een overeenkomst,
– de procedure vindt geheel online plaats,
– partijen, inclusief betrokken derden, verbinden zich om de uitkomst na te leven,
– er is de mogelijkheid om na de uitspraak alsnog voor overheidsrechtspraak te kiezen.

Dit doet denken aan de kort-gedingprocedure naar Nederlands recht, die niet definitief bindend is (immers geen gezag van gewijsde heeft, art. 257 Rv) maar in de praktijk veelal toch definitief blijkt doordat partijen zich bij de uitkomst neerleggen.

Dergelijke vormen van geschilbeslechting zien we op meer plaatsen. Belangrijk is de regeling bij intermediairs als creditcardbedrijven, eBay en PayPal ingeval van klachten van de afnemer/betaler, waarbij een enigszins onderbouwde klacht doorgaans leidt tot terugbetaling en de schuldeiser maar anderszins verhaal moet halen.

192. Hier ligt een rol van het notariaat voor de hand (Lekkerkerker & Van Ee 2015).
193. Zie de voorbeelden in Busch & Reinhold (2015), Fokker (2009: 162-168).
194. Abdel Wahab, Katsh & Rainey 2012, Santing-Wubs (2014), Bonthuis-Krijger (2001).
195. Zie Fokker (2009: 152-156), De Weerd & Van Kralingen (2001).

Het voordeel van dergelijke regelingen is dat hiermee op gemakkelijke en goedkope wijze een voorlopige maatregel kan worden verkregen die grotendeels in overeenstemming is met de rechtvaardigheid en daadwerkelijk geëffectueerd wordt, zonder dat de toegang tot de overheidsrechter wordt afgesneden. Zulke regelingen voegen daadwerkelijke rechtsbescherming toe bij on-line transacties. Dit pleit ervoor een dergelijke vorm van ODR aan te moedigen voor zoveel mogelijk online geschillen.[196] De Verordening ODR consumenten 524/2013 doet dit voor online consumententransacties. Een stap verder zou zijn een verplichting om gevolg te geven aan ODR op verzoek van consumenten, waarbij wel de mogelijkheid moet bestaan om de beslissing bij de overheidsrechter aan te vechten.[197] Dergelijke geschillen behoeven niet alleen tegen een onderneming gericht te zijn; zij kunnen ook bestaan tussen twee particulieren die een transactie op een platform als eBay of Airbnb hebben gesloten.

Een principieel bezwaar lijkt dat een arbitragebeding jegens consumenten in beginsel niet bindend is (art. 6:236 sub n BW). Dat bezwaar mist evenwel doel. Het gaat hier om een geschillenregeling die alleen een voorlopige uitkomst geeft in afwezigheid van een dwingende rechterlijke uitspraak. Het is dus geen beding dat iemand van de rechter afhoudt, alleen een regeling die de status quo verschuift zonder te prejudiciëren of te binden. Het geeft partijen en de derde enige indicatie en kan in veel gevallen het eindpunt zijn, aangezien het voor partijen te lastig is om de procedure bij de overheidsrechter te voeren. Nochtans hebben zij dan tenminste enige vorm van geschilbeslechting verkregen.

Het voordeel van een meer verplichtende vorm of een door de overheid ondersteunde vorm (zoals in de ODR-Verordening) zou kunnen zijn dat dit de online handelsgebruiken[198] kunnen verwoorden en uitwerken, en op deze wijze tevens richtinggevend worden voor de overheidsrechter. Als zulke uitspraken gepubliceerd worden zou dit uiteindelijk leiden tot een vorm van online (precedenten)recht: langs deze weg zou harmonisering van privaatrecht kunnen plaatsvinden!

4.4 Online executie en verhaal

Het sluitstuk van de gelijkwaardige behandeling van de digitale wereld is de effectuering van uitspraken, hetzij uit ODR hetzij door de overheidsrechter. Een algemeen erkende vorm van ODR zou grote voordelen kunnen hebben. Als er eenmaal een goed functionerend netwerk van afspraken is waardoor tussenpersonen en beheerders zich verplichten om uitkomsten van ODR na te leven, kan executie en verhaal in veel gevallen worden

196. Busch & Reinhold (2015) bepleiten aanvullende standaardisatie.
197. Dit is vereist ingevolge art. 6 EVRM, en zie ook HvJ EU 18 maart 2010, NJ 2010/382 (Alassini) waarover Santing-Wubs (2014: 94-96).
198. Vgl. Polanski (2007).

vereenvoudigd. Noodzakelijk daarvoor is dat hetzij verboden of geboden worden nageleefd of afgedwongen, hetzij financieel verhaal is te nemen. Hiervoor zal in het digitale domein uiteindelijk cruciaal zijn de medewerking van beheerders van digitale infrastructuren (par. 4.6). Er zal een variant van derdenbeslag nodig zijn, op digitale goederen of bevoegdheden (zoals toegang tot een twitter-account) van de schuldenaar. Enerzijds kan dit als pressiemiddel dienen om de schuldenaar te prikkelen de uitspraak na te leven. Anderzijds biedt dit de mogelijkheid voor de schuldeiser om schadevergoeding te verkrijgen. Digitale activa zouden verkocht kunnen worden; ook zou via intermediairs als PayPal een soort 'bankgarantie' kunnen worden verstrekt.

De figuur van bankgarantie is in feite reeds aanwezig bij organisaties als Kickstarter, waar de sponsor van een project een betaling toezegt als de *goals* zijn gehaald.[199] Een vergelijkbare vorm zou kunnen zijn dat ISP's zouden vereisen dat gebruikers voor bepaalde mogelijk schadelijke acties een 'bankgarantie' stellen. Dit geeft benadeelde derden een begin van verhaal, geeft een mogelijkheid om de daadwerkelijke persoon achter de digitale identiteit te achterhalen via de betaling (als de betaling niet via bitcoin is gedaan), en bevestigt dat de handeling welgemeend is.

Voor de verwezenlijking van digitale executie is op dit moment eigenlijk alleen een daarop toegesneden praktijk nodig met bijbehorende afspraken tussen internetdienstverleners. Juridisch zal dit meestal derdenbeslag zijn, wat verlof van de overheidsrechter vereist. Theoretisch is denkbaar dat een buitenjuridische 'deurwaarder' wordt verbonden aan een algemeen erkende vorm van ODR die online conservatoir beslag zou kunnen leggen, zonder dat de overheidsrechter nodig is.

Als laatste is denkbaar dat in het digitale domein bepaalde vormen van executie (zoals van dwangsommen) automatisch zouden verlopen doordat bots kunnen nagaan of bepaalde voorwaarden worden nageleefd en automatisch overdracht van vorderingen of activa zouden kunnen bewerkstelligen. Verificatie zou kunnen geschieden via mechanismen als de blockchain.[200] Een nadeel hiervan blijft dat, zoals ook de rechtspraak over de bankgarantie laat zien, enige menselijke interpretatie dan wel toepassing van redelijkheid en billijkheid nodig blijft.[201] Dit is een algemeen punt: geautomatiseerde processen hebben tot op heden moeite met wat mensen redelijkheid en billijkheid noemen.

Als erkenning van ODR in deze vorm gemeengoed is, zou ook executie van overheidsrechtspraak vergemakkelijkt kunnen worden. Een mogelijk-

199. Dat wil zeggen, een drempel van financiering is bereikt.
200. http://www.nrc.nl/handelsblad/2015/11/17/wie-wordt-de-uber-van-de-bankensector-1557263, http://www.nrc.nl/handelsblad/2015/05/22/digitale-valuta-banken-willen-geen-bitcoins-maar-1499793, ook par. 2.2.
201. Tjong Tjin Tai (2015a).

heid zou zijn een online exequatur van een uitspraak van de overheidsrechter, om internetdienstverleners in andere jurisdicties ertoe te brengen gevolg te geven aan een rechterlijke uitspraak. Overigens zou dat slechts een voorlopige maatregel zijn waar de wederpartij zich in een nationale procedure tegen zou kunnen verzetten.

4.5 Betrouwbaarheid en bewijs in het digitale domein

Een probleem is verder de vluchtigheid van de digitale wereld. Data kan gemakkelijk verloren raken als dit niet goed bewaard wordt: archivering en back-ups zijn daarom van belang. Daarnaast wordt bewijslevering bemoeilijkt door de mogelijkheid van wijzigingen zonder sporen achter te laten. In de Facebook-casus uit par. 1 is min of meer bewust nagelaten gegevens te bewaren, zonder dat dit tot duidelijke sancties leidt.[202] Dit roept de vraag op naar een kader waarin duidelijk is wie welke plichten heeft ten aanzien van behoud en bewijs van data, en welke sancties er staan op schending van deze plichten. Meer algemeen is de vraag of er andere methoden zijn om de digitale vluchtigheid tegen te gaan.

Het algemene probleem bij data is garantie van authenticiteit en behoud van leesbaarheid.[203] Dit brengt voor archivering strengere eisen. Zij zouden ook een reflexwerking kunnen hebben voor bewijs van data: als een 'bezitter' of 'bewaarder' van data niet langer over relevante data beschikt doordat hij de archiveringsnormen niet heeft nageleefd, zou dat hem kunnen worden tegengeworpen op voet van art. 21 en 22 Rv.[204] Juist omdat data zo vluchtig is, zouden strengere normen nodig zijn om het behoud en de betrouwbaarheid van data te bevorderen.

Daarnaast is van belang vast te stellen wie data moet bewaren. Bewaren van back-ups is belangrijk om schade wegens verlies van data te vermijden. Het is echter vaak onduidelijk op wie deze verplichting rust.[205] Hier kan het 'eigendomsperspectief' helpen: primair dient de eigenaar hiervoor te zorgen, behalve als hij die verantwoordelijkheid contractueel bij een bewaarder heeft kunnen neerleggen. Het verlenen van een gebruikslicentie

202. In HR 14 november 2014, NJ 2015/193 (Shoppingspel III) overwoog de Hoge Raad dat vernietiging van administratie die nodig was om gemaakte winst vast te stellen kon leiden tot maken van gevolgtrekkingen die de rechter geraden acht, ex art. 21 en 22 Rv. Dat geldt echter voor de vordering op de wederpartij. In de Facebook-casus is de eigenlijke vordering gericht op een derde die kennelijk niet meer aan te spreken is.
203. Zie bijv. Boudrez (2006) en publicaties op http://www.edavid.be/publicaties.php; voor het notariaat Van der Woude & Sleeking (2015).
204. Vgl. HR 14 november 2014, NJ 2015/193 (Shoppingspel III).
205. Bijv. Rb Midden-Nederland 16 januari 2013, ECLI:NL:RBMNE:2013:BY7960, Hof Den Haag 27 december 2011, ECLI:NL:GHSGR:2011:BV1678 (Scope/KPN).

aan een hosting provider impliceert niet vanzelfsprekend een back-upverplichting bij die provider (zie casus 2 in par 1.1).[206] Omgekeerd hoeft een eigenaar niet noodzakelijk verplicht te zijn een backup te bewaren van data op wie hij een ander een gebruikslicentie geeft: mogelijk is dat hij zelf de databank inmiddels heeft gewijzigd of zelfs vernietigd. Bij gebreke van duidelijke regels is een mogelijkheid om in bepaalde gevallen te vereisen dat de gebruiker uitdrukkelijk wordt gewezen op de noodzaak zelf backups bij te houden: dit zou kunnen bij dienstverlening die enige vorm van opslag inhoudt.

Interessant is daarnaast de mogelijkheid betrouwbaarheid te verbeteren met ondersteunende institutionele maatregelen. Internationale betrouwbaarheid van feiten (zowel offline als online) kan worden bevorderd met betrouwbaarheidsdiensten (trust services).[207] Voor online-verificatie biedt de Verordening elektronische identificatie en vertrouwensdiensten 910/2014 in art. 25-37 enige aanknopingspunten voor met regels voor elektronische zegels, tijdstempels, aangetekende bezorging en authenticatie van websites. Voor offline verificatie zou een netwerk van lokale, betrouwbare deskundigen voor opname van feiten e.d. een rol kunnen spelen: deskundigen zouden bijvoorbeeld digitale foto's zouden kunnen maken ten behoeve van de ondersteuning van bewijsgaring.[208] Dit zou *peer-to-peer* georganiseerd kunnen worden.[209]

Een andere oplossing is distributie en samenwerking. Als data op meer plaatsen bewaard wordt is de kans dat data geheel verloren raakt kleiner. Intersubjectieve controle kan de betrouwbaarheid daarnaast vergroten. Een voorbeeld is de wijze waarop bitcoin werkt: transacties worden geverifieerd door de bitcoin gemeenschap en zijn daardoor nauwelijks vatbaar voor vervalsing.[210]

Tot slot moeten online-dienstverleners (onder passende waarborgen) medewerking verlenen aan online-bewijsverzoeken. Dit is in essentie het probleem van de Facebook-casus. Hierbij dient wel rekening gehouden te worden met andere belangen zoals privacy.[211] Hier is een passende regeling voor nodig, die onderdeel dient te zijn van een algehele herijking van de positie van ISP's.

206. Zie bijv. ook art. 3.2 LinkedIn user agreement https://www.linkedin.com/legal/user-agreement.
207. Bijv. door het notariaat, zie Lekkerkerker & Van Ee (2015).
208. Vgl. de mogelijkheid van Airbnb dat een professionele fotograaf bevestigt dat hij de te verhuren ruimte heeft bezocht en daar foto's heeft gemaakt, https://www.airbnb.nl/info/photography.
209. Een voorbeeld is Roamler, dat per app individuen tegen geringe betaling opdrachten laat uitvoeren zoals verificatie dat bepaalde producten in een supermarkt aanwezig zijn.
210. Behalve als meer dan 50% van de bitcoin clients in handen van één partij komt.
211. Vgl. HR 13 september 2013, NJ 2014/455 (Bewijsbeslag), r.o. 3.9.2. Ook Dijkstra (2013) en Dijkstra & Riehl (2012).

4.6 Zorgplichten voor tussenpersonen

Het sluitstuk van de benodigde infrastructuur is een actievere rol van online dienstverleners, ook wel genoemd Internet Service Providers (ISP's). Dit is een bijzonder omstreden kwestie. De neutrale rol van de ISP's wordt beschouwd als belangrijk of zelfs essentieel voor het functioneren van Internet, hetgeen onder meer tot uitdrukking komt in het zogenaamde beginsel van netneutraliteit en de aansprakelijkheidvrijwaring voor passieve ISP's (art. 6:169c BW).[212] Neutraliteit maakt anonimiteit op Internet mogelijk, wat wordt beschouwd als belangrijke waarborg van de uitingsvrijheid. Mijns inziens betreft dit evenwel een achterhaald standpunt.

Een teken aan de wand is de Delfi-uitspraak van de Grote Kamer van het EHRM.[213] Het EHRM zet in deze uitspraak expliciet het belang van de bescherming van het individu tegenover vrijheid van meningsuiting. De privacy van een individu kan worden geschonden door onrechtmatige uitingen van een anonieme Internetgebruiker. Een ISP die dergelijke uitingen faciliteert en onvoldoende maatregelen treft dergelijke uitingen tegen te gaan dan wel om de anonieme gebruiker te achterhalen kan aansprakelijk zijn zonder dat dit in strijd komt met art. 10 EVRM. In de Delfi-zaak leidde dit ertoe dat de ISP een kleine boete moest betalen voor de daad van een anonieme Internetgebruiker.[214] Het EHRM lijkt met name belang te hechten aan het feit dat de benadeelde met lege handen zou staan als de ISP kon volstaan met het na melding verwijderen van onrechtmatige uitingen. Dit is, zo is hierboven betoogd, een argument met bredere strekking. Veel wenselijke acties en gevolgen zijn niet te realiseren zonder de medewerking van ISPs. Het lijkt daarom niet langer houdbaar dat ISPs volledig passief mogen blijven; integendeel is het tijd om over te gaan naar erkenning van zorgplichten voor ISPs.[215] De vraag is dan vooral hoever zulke zorgplichten moeten strekken. Het is inmiddels onontkoombaar dat ISPs actiever worden; het is juist in het belang van ISPs dat de discussie hierover uitdrukkelijk wordt gevoerd omdat anders niet duidelijk is wat zij

212. Een implementatie van art. 12-15 E-commerce Richtlijn 2000/31/EG.
213. EHRM 16 juni 2015, no. 64569/09 (Delfi v. Estonia).
214. Het EHRM laat uitdrukkelijk buiten beschouwing de vrijwaring voor passieve ISP's omdat de nationale rechter had vastgesteld dat de ISP in casu niet passief was, een oordeel dat overigens op gespannen voet lijkt te staan met de rechtspraak van het HvJ EU (zoals HvJ 23 maart 2010, C-236/08 t/m C-238/08 (Google Adwords), HvJ 12 juli 2011, C-324/09 (L'Oréal/eBay), HvJ 24 november 2011, C-70/10 (Scarlet Extended/SABAM), HvJ 16 februari 2012, C-360/10 (SABAM/Netlog)).
215. Van Eijk (2010), Tjong Tjin Tai e.a. (2015). Ook Prins (2007 en 2013).

wel of niet moeten doen.[216] De hierboven beschreven institutionele punten als digitale identiteit, betrouwbaarheid en ODR kunnen ISPs in de praktijk helpen om correct en zonder vrees voor aansprakelijkheid te handelen.

Men moet beseffen dat de oude vrijwaring uit de E-commercerichtlijn was opgesteld teneinde het Internetverkeer te stimuleren. Onzekerheid over mogelijke aansprakelijkheid zou een onwenselijke rem zetten op de ontwikkeling van Internet. Echter nu inmiddels vele Internetondernemingen tot de grootste bedrijven ter wereld behoren lijkt die ratio op zijn zachtst gezegd achterhaald. Men kan anders denken over kleine ondernemingen of particulieren; het EHRM beperkt de Delfi-uitspraak dan ook uitdrukkelijk tot grote commerciële ISPs.

Dogmatisch gezien vallen verdergaande zorgplichten te rechtvaardigen door het maatschappelijke en institutionele belang dat inmiddels gemoeid is met ISPs. Gelet op de grote maatschappelijke belangen die met hun functioneren zijn gemoeid vallen zij tegenwoordig in dezelfde categorie als banken en beroepsbeoefenaren.[217] Dat zij in veel gevallen neutraal moeten zijn staat hier niet aan in de weg, integendeel: bijvoorbeeld notarissen moeten zich neutraal opstellen maar moeten daarbij tevens letten op belangen van partijen en betrokken derden. Dit kan ertoe leiden dat zij hun dienst moeten weigeren.[218] Het gaat om een *actieve* neutraliteit, niet een passieve. Dit compliceert inderdaad hun rol, maar dat is niet anders dan bij andere grote ondernemingen zoals banken.[219] Dat dit daadwerkelijk realiseerbaar is blijkt bijvoorbeeld met het *right to be forgotten* dat na HvJ 13 mei 2014, C-131/12 (Google/Spanje) zonder grote problemen is geëffectueerd.[220] Inmiddels blijkt dat grote ISPs als Facebook en Twitter daadwerkelijk beginnen met maatregelen te nemen om ongewenste uitingen tegen te gaan.[221]

Zorgplichten voor ISPs zouden naar Nederlands recht ook impliceren dat zij een grotere mate van zorgvuldigheid jegens hun klanten tonen, dat zij zich de belangen van hun klanten in sterkere mate aantrekken. Onder omstandigheden zou er een recht op continuïteit van dienstverlening kun-

216. Vgl. Van der Sloot (2014), Den Dekker & Van der Linden-Smith (2014), Ausloos (2014). Van Hoboken (2012) pleit ook voor duidelijkheid doch lijkt vooral vrijwaring ten behoeve van uitingsvrijheid te verdedigen; dit is te eenzijdig nu dit andere belangen (in het bijzonder privacy) onvoldoende in de beoordeling betrekt. Zie Kuczerawy (2015) over recente EU-ontwikkelingen.
217. Tjong Tjin Tai (2007, hfdst. 6).
218. Zie bijv. HR 3 april 2015, ECLI:NL:HR:2015:831, Heyman (2015) en Waaijer (2015), ook Tjong Tjin Tai (2007: 210-215).
219. Ten aanzien van banken bij dubieuze effectentransacties: HR 23 december 2005, NJ 2006/289 (Safe Haven) en HR 27 november 2015, ECLI:NL:HR:2015:3399.
220. Het zal voor Google significante uitvoeringskosten met zich brengen, maar die kosten zouden voor Google geen probleem moeten zijn.
221. Bijv. http://www.independent.co.uk/life-style/gadgets-and-tech/news/twitter-is-winning-war-on-trolls-and-extremists-says-its-europe-chief-a6786246.html, http://www.dw.com/de/facebook-will-schärfer-gegen-hassparolen-vorgehen/a-18918733.

nen zijn, of althans een recht om de infrastructuur voor eigen rekening voort te zetten.[222] De aanbieder heeft immers uitgelokt dat particulieren grote investeringen qua tijd hebben gedaan. Verdedigbaar is dat er ten minste een recht is op downloaden van de data bij beëindiging van de dienst.[223] Dit vindt erkenning in het door de Europese Commissie voorgestelde recht op dataportabiliteit.[224]

Een recht op dataportabiliteit vloeit logisch voort uit de in par. 3 verdedigde eigendomsrechtelijke benadering van digitale activa. Dit onderstreept het betoog van dit preadvies. Als we blijven denken vanuit het traditionele kader lopen we voortdurend achter de ontwikkelingen aan. De maatschappij heeft inmiddels de stap gemaakt naar een zelfstandige beschouwing en waardering van online fenomenen. Om te kunnen anticiperen op deze ontwikkelingen is het nodig om ook van perspectief te wisselen in het recht.

5. Conclusie

Een doordenking van het privaatrecht vanuit de belangen van de homo digitalis laat zien dat er op diverse punten wijzigingen wenselijk zijn. Deze kunnen niet alle door rechtspraak worden gerealiseerd; activiteit van de (Europese) wetgever is eveneens vereist. Dit betoog vindt steun in het gegeven dat diverse losse en zeer actuele ontwikkelingen (zoals bewijsbeslag, e-identificatie, bescherming van bedrijfsgeheimen, recht op dataportabiliteit, strafbaarstelling van 'heling' van data, zorgplichten van ISP's) alle in de geschetste richting passen. De weerstand tegen deze ontwikkelingen lijkt vanuit het hier verdedigde perspectief gebaseerd op posities die niet langer passend zijn bij de huidige stand van zaken, of op eenzijdige waardering van principes als privacy of uitingsvrijheid. Deze zorgen zijn relevant, maar niet per se doorslaggevend in de nieuwe werkelijkheid van de *homo digitalis*. Hopelijk kan dit preadvies bijdragen aan de realisering van een rechtssysteem dat op die werkelijkheid is toegesneden.

222. Bijv. bij spelomgevingen die worden opgedoekt: zouden fans dan de omgeving mogen voortzetten, zoals het toegestaan is een uitverkocht en niet langer in herdruk zijnd boek geheel te kopiëren (art. 16b lid 2 sub a Aw)? Dit is verwant aan, maar niet gelijk, aan de discussie over *abandonware*.
223. Hyves bood hiervoor de mogelijkheid bij opheffing van dit platform, http://www.nu.nl/tech/3629575/hyves-laat-gebruikers-profiel-downloaden.html. Voor digitale objecten (par. 3.3) biedt dit geen soelaas nu deze afhankelijk zijn van de infrastructuur.
224. Par. 4.1, Digital Single Market Strategy d.d. 6 mei 2015, COM(2015) 192 final, zie nader Graef (2014).

6. Literatuur

Asser/Bartels & Van Mierlo 3-IV 2013. S.E. Bartels & A.I. van Mierlo, *Mr. C. Asser's handleiding tot de beoefening van het Nederlands burgerlijk recht, deel 3-IV*, Deventer: Kluwer.

Asser/Hartkamp & Sieburgh 6-II 2013. A.S. Hartkamp & C.H. Sieburgh, *Mr. C. Asser's handleiding tot de beoefening van het Nederlands burgerlijk recht, deel 6-II*, 14e dr., Deventer: Kluwer.

Asser/Tjong Tjin Tai 7-IV 2014. *Mr. C. Asser's handleiding tot de beoefening van het Nederlands burgerlijk recht, deel 7-IV*, 2e dr., Deventer: Kluwer.

Mohamed S. Abdel Wahab, Ethan Katsh and Daniel Rainey (eds.). 2012. *Online Dispute Resolution: Theory and Practice*. The Hague: Eleven International Publishing.

G.S. Alexander en E.M. Peñalver. 2012. *An Introduction to Property Theory,* Cambridge: Cambridge University Press.

J. Ausloos. 2014. "Zoekmachines in Europa – gevangen tussen twee vuren?", *Computerrecht* 2014/179.

J.M. Barendrecht, I. Giesen, M.H.M. Schellekens, M.W. Scheltema. 2002. *Overheidsaansprakelijkheid voor informatieverstrekking*, Den Haag: BJu 2002.

J.M.A. Berkvens & J.E.J. Prins. 2014. 'De bescherming van persoonsgegevens', in: Van der Hof, Lodder & Zwenne (2014: 179-212).

J.W.A. Biemans. 2009. "Domeinnamen en 'overdracht', 'verpanding' en 'beslag' – het is niet wat het lijkt", *NTBR* 2009/2.

P.H. Blok. 2003. "Is er privé-leven na de dood?", *NJB* 2003/278.

P. Blokland 2015. "De zorg- en informatieplicht van de notaris in het digitale tijdperk", *WPNR* 7073.

M. De Boni & M. Prigmore. 2004. "A Hegelian Basis for Privacy as an Economic Right", *Contemporary Political Theory* vol. 3: 168–187.

M. Bonthuis-Krijger. 2001. "ODR.NL: Grensoverschrijdende online alternatieve geschillenbeslechting", *Computerrecht* 2001: 245-246.

d. boyd & A. Marwick. 2011, "Social Privacy in Networked Publics: Teens" Attitudes, Practices, and Strategies", paper op http://ssrn.com/abstract=1925128.

F. Boudrez. 2006. "Digitale handtekeningen en archiefdocumenten", *Computerrecht* 2006/40.

C. Busch & S. Reinhold. 2015. "Standardisation of Online Dispute Resolution Services: Towards a More Technological Approach", *EuCML* 1-2 (4), p. 50-58.

C.M.K.C. Cuijpers. 2004. *Privacyrecht of privaatrecht?*, diss. Tilburg, Nijmegen: Wolf Legal Publishers.

C. Cuijpers & P. Marcelis. 2012. 'Oprekking van het concept persoonsgegevens beperking van privacybescherming?', Computerrecht 2012/182.

C.C. van Dam. 2015. *Aansprakelijkheidsrecht, deel 1*, 2e dr., Den Haag: BJu.

K. Daniëls & P. Kits. 2015. "Contracteren in de cloud – ken uw risico's", *Contracteren* 2015/1: 2-16.

J.Th. Degenkamp. 1997. "Waarom mogen gegevens geen goederen zijn; en, waarom mag men geen eigenaar van gegevens zijn?", in: A.L. Mohr, F.H.J. Mijnssen en R.H. Stutterheim (red.), *J.L.P. Cahen-bundel*, Deventer: Gouda Quint.

D.F.P. den Dekker & M. van der Linden-Smith. 2014. "De positie van tussenpersonen in Internetcommunicatie", in: Van der Hof e.a. 2014: 261-284.

J. Dijkstra. 2013. "Seizing Electronic Evidence from Cloud Computing Environments", in: K. Ruan, *Cybercrime and Cloud Forensics: Applications for Investigation Processes*, Hershey: IGI 2013: 156-185, op http://www.csee.umbc.edu/~dykstra/Seizing-Electronic-Evidence-from-Cloud-Computing-Environments.pdf.

J. Dijkstra & D. Riehl. 2012. "Forensic Collection of Electronic Evidence from Infrastructure-As-a-Service Cloud Computing", *Richmond Journal of Law & Technology*, vol. XIX/1, op http://jolt.richmond.edu/v19i1/article1.pdf.

C. Drion, 2013. "Wat is 'iets'?", NJB 2013/383: 465.

M.M.G.B. van Drunen en B. Snijder-Kuipers, "De digitale notariële akte", in: Koops e.a., p. 53-68.

N.A.M. van Eijk e.a. 2010. *Op weg naar evenwicht: een onderzoek naar zorgplichten op het internet*, WODC, op http://wodc.nl/onderzoeksdatabase/zorgplicht-internet-service-providers-isps.aspx?cp=44&cs=6796.

P.C. van Es. 2008. "De elektronische onderhandse akte", *WPNR* 6764.

J.A.T. Fairfield. 2005. "Virtual Property", Boston University Law Review 85: 1047-1102.

H.A.G. Fikkers. 2000. "E-commerce en de derdenbescherming van art. 3:86 lid 3 sub a BW", *WPNR* 6406.

R.J.C. Flach. 2014. "Enkele opmerkingen over digitalisering, schaalvergroting en de hanteerbaarheid van het burgerlijk procesrecht", in: Koops e.a. 2014: 71-86.

J.P. Fokker. 2009. *E-arbitrage*, diss. Leiden, Deventer: Kluwer.

M.C. Flannery. 2007. "Brunhilde on Trial: Fama and Lydgatean Poetics", *The Chaucer Review* 42/2: 139-160.

L.A.G.M. van der Geld. 2014. "De executeur in een nalatenschap met bitcoins en andere "digitale bezittingen", Tijdschrift Erfrecht 6: 16–20.

S. Gellaerts. 2015. *Watermerken als juridisch bewijsmiddel*, diss. Tilburg.

Ch. Gielen. 1999. *Bescherming van bedrijfsgeheimen*, Preadvies van de Vereeniging "Handelsrecht", Rotterdam: W.E.J. Tjeenk Willink.

Ch. Gielen (red.). 2014. *Kort begrip van het intellectuele eigendomsrecht*, 11e dr., Deventer: Kluwer.

C. Ginzburg. 1979. "Clues: Roots of a Scientific Paradigm", *Theory and Society* 7/3: 273-288.

C. Ginzburg. 1980. "Morelli, Freud and Sherlock Holmes: Clues and Scientific Method", *History Workshop* 9: 5-36.

T. Gisclard. 2014. "Consent in Licenses of Personality Rights", *ERPL* 14/3: 345-370.

D.H. Gleason & L. Friedman. 2004. "Toward an Accessible Conception of Cyberspace", *Vermont Law Review* 28: 299-320.

I. Graef. 2014. "Misbruikverbod op Internet, onlineplatforms als poortwachters persoonsgegevens", *Computerrecht* 2014/38.

M.L. Hendrikse. 2014. "Elektronisch handelsrecht: daadwerkelijk nieuwe ontwikkeling of "oude wijn in nieuwe zakken"?", *NTHR* 2014-2: 46-60.

H.W. Heyman. 2015. "Notariële dienstverlening bij botsende rechten na HR 3 april 2015 (De Novitaris)", *WPNR* 7067.

J.V.J. van Hoboken. 2012. *Search engine freedom*, diss. Amsterdam (UvA).

Th. Hoeren. 2013. "Dateneigentum. Versuch einer Anwendung von § 303a StGB im Zivilrecht", *MMR* 2013/8: 486-491.

S. van der Hof, A.R. Lodder en G.J. Zwenne (red.). 2014. *Recht en computer*, 6e dr., Deventer: Kluwer.

J.L.R.A. Huydecoper. 2008. "Knowhow en het vermogensrecht", MvV 2008/7-8: 158-162.

P. Kleve. 2004. *Juridische iconen in het informatietijdperk*, diss. Rotterdam, Deventer: Kluwer.

L. Kool, J. Timmer & R. van Est. 2015. *De datagedreven samenleving*, Den Haag: Rathenau Instituut.

B.J. Koops. 2014. "Cybercriminaliteit", in: Van der Hof e.a. 2014: 213-241.

E. Koops, H.B. Krans, E.D.C. Neppelenbroek & A.J. Verheij (red.). 2014. *Digitaal Privaatrecht*, Den Haag: BJu.

E. Koops en E.F. Verheul. 2014. "Webwinkels en derdenbescherming", in: Koops e.a. 2014: 31-52.

P.J. van der Korst. 2007. *Bedrijfsgeheimen en transparantieplichten*, Deventer: Kluwer.

A. Kuczerawy. 2015. "Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative", Computer Law & Security Review 31: 46-56.

A. Kuczerawy & F. Coudert. 2011. "Privacy Settings in Social Networking Sites: Is It Fair?", in: S. Fischer-Hübner e.a. (eds.), *Privacy and Identity Management for Life*, 6th IFIP AICT 352: 231-243, download at <http://ssrn.com/abstract=2605050>.

S. Kulk, B. van Loenen, H.D. Ploeger. 2012. *Open data and beyond. Exploring existing open data projects to prepare a successful open data strategy*, Deelrapport Aansprakelijkheid. Beschikbaar op http://www.gdmc.nl/oosterom/NGI_aansprakelijkheid_2012.pdf

G.J.C. Lekkerkerker & J.W. van Ee. 2015. "De notaris in een digitale wereld, twee invalshoeken", *WPNR* 7070.

S.D. Lindenbergh. 1998. *Smartengeld*, diss. Leiden, Deventer: Kluwer.

A.R. Lodder (red.). 2006. *Recht in een virtuele wereld: Juridische aspecten van Massive Multi- player Online Role Playing Games (MMORPG)*, Den Haag: Elsevier.

A.R. Lodder. 2008. "Virtuele werelden: toepassing externe regulering na afweging in het licht van de magische cirkel", Ars Aequi 2008: 513-521.

M.B.M. Loos: 2011. "Overeenkomsten tot levering van digitale inhoud", *NTBR* 2011/81.

M.B.M. Loos. 2013. "Onvolkomenheden bij de implementatie van de richtlijn consumentenrecht", *NJB* 2013/2255: 2684-2685.

M.B.M. Loos & J. Luziak. 2015. "Wanted: a Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers", Journal on Consumer Policy, doi: 10.1007/s10603-015-9303-7.

H.P.A.J. Martius. 2007a. *Elektronisch handelsrecht*, diss. OU. Zutphen: Paris.

H.P.A.J. Martius. 2007b. "Hoe schriftelijk is elektronisch? Over post, e-post en e-akte", WPNR 6710: 452-459.

H.P.A.J. Martius. 2008. "Enige opmerkingen over het wetsvoorstel met betrekking tot de elektronische akte, de elektronische polis, elektronische algemene voorwaarden en elektronische mededelingen", *NTHR* 2008: 108-112.

A.E. Marwick & d. boyd. 2014. "Networked privacy: How teenagers negotiate context in social media", *new media & society*: 1-17.

V. Mayer-Schönberger & K. Cukier. 2013. *Big data*, London: Mariner Books.

A.P. Meijboom. 2007. "Ontwikkeling van domeinnaambescherming in Nederland", *Computerrecht* 2007/41.

N.S. van der Meulen & A.R. Lodder. 2014. "Cybersecurity", in: Van der Hof e.a. 2014: 301-318.

T. Morey, T. Forbath & A. Schoop. 2015. 'Customer data: designing for transparancy', Harvard Business Review, May 2015: 97-105.

J.W. Nelson. 2010. "The Virtual Property Problem", McGeorge Law Review 41: 281-309.

E.D.C. Neppelenbroek. 2006a. "Het drakenzwaard of: virtuele goederen als vorderingsrecht uit online-contracten", Ars Aequi 2006: 24-32.

E.D.C. Neppelenbroek. 2006b. "De verkrijging van de eigendom van elektronische bestanden over internet", *NJB* 2006/10: 560-566.

E.D.C. Neppelenbroek. 2012. "Digitalisering, auteursrecht en vier waarnemingen over de eigendom", *RM Themis* 2012/5: 211-222.

E.D.C. Neppelenbroek. 2013a. *Softwarebetrekkingen*, diss. Groningen, Den Haag: BJu.

E.D.C. Neppelenbroek. 2013b. "Stop het consumentenkooprecht voor digitale inhoud!", *NJB* 2013/413: 515-518.

D.J.B. Op Heij. 2015. "'Nakoming': een geschikte remedie voor overeenkomsten tot levering van digitale inhoud?", *TvC* 2015-2: 55-62.

Rachael M. Peters. 2014. "So You"ve Been Notified, Now What? The Problem With Current Data-Breach Notification Laws", *Arizona Law Review* 56/4: 1171-1202.

J.C.S. Pinckaers. 1996. *From Privacy Toward A New Intellectual Property Right in Persona*. Den Haag: Kluwer Law International.

P.P. Polanski. 2007. *Customary Law of the Internet*, Den Haag: T.M.C. Asser Press.

W. Pors. 2013. "Bescherming van bedrijfsgeheimen – De stand van zaken en de toekomst", BIE mei 2013: 126-134.

C. Prins. 2005. "Eigendom op informatie: economische realiteit maar juridische fictie?", *NJB* 2005: 623.

C. Prins. 2007. "Nalaten in Cyberspace", Nederlands Juristenblad 82/6: 321.

C. Prins. 2013. "Zorgplichten en Cybercrime", Nederlands Juristenblad 88/18: 1185.

N. Purtova. 2011. *Property Rights in Personal Data*, diss. Tilburg, Antwerpen: Maklu.

W.F.R. Rinzema. 2012. "Kwaliteit en software: een goede zaak", *Computerrecht* 2012/40.

J. Ronson. 2015. *So You"ve Been Publicly Shamed*. London: Pan Macmillan.

A.F. Salomons. 2000. "Inpassen of aanpassen? Vermogensrecht voor het digitale tijdperk", *WPNR* 6427: 901-907.

A.H. Santing-Wubs. 2014. "Digitale geschilbeslechting", in: Koops e.a. 2014: 87-103.

E.B.M. Schoenmakers, W.E.H. Sloots & J.A.I. Wendt. 2014. *Eigen gegevens, eigen regie?*, op <https://www.rijksoverheid.nl/documenten/rapporten/2014/10/01/eigen-gegevens-eigen-regie>

A.I. Schreuder. 2014. "Aansprakelijkheid voor 'zelfdenkende' apparatuur", *AV&S* 2014/20.

M. Schut. 2010. "Knowhow: aandachtspunten in de contractspraktijk en de rol van art. 39 TRIPS", *MvV* 2010/2: 15-20.

M.R.F. Senftleben & H.N. Scholtens. 2014. "Auteursrecht en cloud computing", in: Van der Hof e.a. 2014: 115-142.

C. Shirky. 2008. *Here comes everybody: the power of organizing without organizations*, New York: Penguin.

B. van der Sloot. 2014. "Welcome to the jungle: de aansprakelijkheid van internet- intermediairs voor privacyschendingen in Europa", *SEW* 2014/10: 420-431.

B. van der Sloot. 2015. "Privacy as Personality Right: Why the ECtHR"s Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"", Utrecht Journal of International and European Law 2015: 25-50.

H.J. Snijders & E.B. Rank-Berenschot. 2012. *Goederenrecht*, 5e dr., Deventer: Kluwer.

W. Snijders. 2005. "Ongeregeldheden in het vermogensrecht", *WPNR* 6607 en 6608.

T. Spaas & M. Van Roey. 2015. "Quo vadis Bitcoin?", *Computerrecht* 2015/84.

J.B. Spath. 2015a. "Breed burgerlijk recht", oratie Nijmegen. Nijmegen: Ars Aequi.

J.B. Spath. 2015b. "Digitale gegevensuitwisseling tegen betaling lijkt op koop, of niet?", *NTBR* 2015/15: 101-103.

J.H. Spoor, D.W.F. Verkade & D.J.G. Visser. 2005. *Auteursrecht*, Deventer: Kluwer.

M.C. Van Stekelenburg. 2009. *De betere byte in de strijd om het gelijk*, diss. Amsterdam (VU), Delft: Eburon.

J.A.S. Telecha. 2007. "*Fama publica*, infamy and defamation: judicial violence and social control of crimes against sexual morals in medieval Castile", *Journal of Medieval History* 33: 398-413.

T.F.E. Tjong Tjin Tai. 2003. "Exhaustion and Online Delivery of Digital Works", *EIPR* 25/5: 207-211.

T.F.E. Tjong Tjin Tai. 2007. *Zorgplichten en zorgethiek*, diss. Amsterdam (UvA) 2007, Deventer: Kluwer 2006.

T.F.E. Tjong Tjin Tai. 2015a. "De redelijke derde en de blockchain", *WPNR* 7072.

T.F.E. Tjong Tjin Tai. 2015b. "Data in het contractenrecht", *WPNR* 7085.

T.F.E. Tjong Tjin Tai, D.J.B. op Heij, K.K. e Silva, I. Skorvanek en B.J. Koops. 2015. *Duties of care and diligence against cybercrime*, rapport (te raadplegen via https://repository.uvt.nl).

F.W.J. van der Ven. "Digitaal privaatrecht, iets nieuws onder de zon?", in: Koops e.a. 2014, p. 173-191.

F.M.J. Verstijlen, 2014. "Goederenrecht 2.0?", in: Koops e.a. 2014, p. 135-150.

D.W.F. Verkade, "Gegevensbescherming en privaatrecht", NJV-preadvies 1988, Zwolle: W.E.J. Tjeenk Willink 1988, p. 35–91.

E.N.M. Visser, 2007. "Who owns your bits when you die?", Computerrecht 2007/113.

F.J. Vonck, "De executoriale verkoop van registergoederen via internet", in: Koops e.a. 2014, p. 105-122.

M.B. Voulon, *Automatisch contracteren*, diss. Leiden, Leiden University Press 2010.

M.B. Voulon, "Een Europese verordening voor identity management (IdM)", Computerrecht 2013/118.

M.B. Voulon, 2014. "Bewijs en bewaren", in: Van der Hof e.a., p. 347-359.

T.J.M. de Weerd & R. van Kralingen, 2001. "De WIPO Domeinnaam-arbitrage-procedure", Computerrecht 2001/5, p. 253-260.

H.W. Wefers Bettink & J. Theeven, "Een Gemeenschapsregime voor elektronische identificatie", NTER 2013, p. 1-6.

B. Wessels, "De curator en de cloud", NJB 2015/639, p. 818-821.

F. van der Woude & O.A. Sleeking, 2015. "Digitaal archiveren binnen het notariaat", WPNR 7073.

F.J. Zuiderveen Borgesius, 2015. "Online Price Discrimination and Data Protection Law", Amsterdam Law School Research Paper No. 2015-32, at at SSRN: http://ssrn.com/abstract=2652665.

G.-J. Zwenne. 2013. *De verwaterde privacywet*, inaugurele rede Leiden.

R. Zwitser, "Internetbankieren met PayPal". NJB 2000, p. 1479-1485.

Wordt de homo digitalis bestuursrechtelijk beschermd?

Gerrit-Jan Zwenne en Aernout Schmidt[1]

1. Universiteit Leiden (eLaw@Leiden).

DEEL I: INLEIDING

1 De Homo Digitalis en de overheid

1.1 Waarover gaat het?

In zijn rapport over iOverheid zet de Wetenschappelijk Raad voor het Regeringsbeleid uiteen hoe de overheid enthousiast informatietechnologie binnenhaalt voor haar complexe administratieve opdracht en de aanpak van urgente maatschappelijke uitdagingen, zoals daar zijn: terrorisme, veiligheid, mobiliteit en goede en betaalbare zorg.[2] In kamerstukken over de digitale overheid worden haar ambities vooral gearticuleerd in steekwoorden of slogans als 'de verbetering in kwaliteit van digitale overheidsinformatie en overheidsdienstverlening', 'administratieve lastenvermindering' en 'regeldrukreductie', het realiseren van 'efficiencywinsten' enz.[3] De terminologie suggereert dat digitalisering geen of slechts een beperkte impact heeft op de rechtspositie van burgers, consumenten, werknemers, studenten, belastingbetaler, cliënten, verzekerden, automobilisten, treinreizigers, patiënten, etc. Of, sterker nog, dat deze rechtspositie vooral zou worden versterkt doordat de hen toekomende rechten met minder moeite geëffectueerd kunnen worden. Uiteenlopende voorbeelden laten zien dat die suggestie niet altijd terecht is.

De digitalisering van de overheid verandert haar verhouding ten opzichte van burgers. Het is niet zo dat de positie van de burger in alle gevallen wordt verzwakt, maar we kunnen wel een paar gevallen noemen waar er tenminste de zorg is dat daarvan sprake kan zijn. DigiD biedt een voorbeeld. DigiD is de persoonlijke inlogcode waarmee burgers zich identificeren bij de digitale overheid en die wordt gebruikt voor het aanvragen van toeslagen als de kinderopvangtoeslagen, huur- en zorgtoeslagen. Door de zgn. Bulgarenfraude, die in april 2013 aan het licht werd gebracht, is duidelijk dat er daarbij nogal eens wat mis kan gaan.[4] Toch kunnen aanvragers van toeslagen die stellen slachtoffer te zijn van identiteitsfraude niet op veel begrip rekenen bij de bestuursrechter. Omdat de aanvraag voor de toeslag was ingediend op haar naam moest het volgens de bestuursrechter ervoor worden gehouden dat deze is gedaan met haar toestemming, dan wel dat zij haar persoonlijke en geheime DigID-code aan een ander heeft verstrekt. In de beide gevallen komt de onjuistheid van de aanvraag voor

2. WRR, iOverheid, rapport nr. 86, Den Haag / Amsterdam 2011, p. 11, 34 en 93.
3. Zie bijv. *Kamerstukken II* 2012/13, 26643, nr. 280, p. 1-2.
4. RTL Nieuws, 'Grootschalige fraude Bulgaren met toeslagen', 21 april 2013 www.rtlnieuws.nl/nieuws/binnenland/grootschalige-fraude-bulgaren-met-toeslagen en daaropvolgende niewsberichten.

haar rekening. En daaraan doet niet af dat de toeslagen waren uitbetaald op een rekeningnummer dat niet van de aanvrager was.[5]

Deze zaak staat niet op zichzelf. Het risico van misbruik van DigiD wordt doorgaans gelegd bij de burger, ook als die niet zo digivaardig is als door de overheid wordt verondersteld.

Een ander voorbeeld van veranderende burger-overheid verhoudingen vinden we in het omvangrijke, en diep in de persoonlijke levenssfeer ingrijpende, overheidsdigitaliseringsproject dat beoogt te komen tot een integraal optreden ten aanzien van – het is een hele mond vol – de voorkoming en bestrijding van onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen op het terrein van de sociale zekerheid en de inkomensafhankelijke regelingen, de voorkoming en bestrijding van belasting- en premiefraude en het niet naleven van arbeidswetten. Een recente grondslag daarvoor is te vinden in het zogeheten SyRI-besluit dat beoogt fraudeaanpak mogelijk te maken door gegevensuitwisseling en het effectief gebruik van de binnen de overheid bekend zijnde gegevens. In het kader daarvan wordt voorzien in een bevoegdheid tot risicoprofilering in het Systeem Risico Indicatie of SyRI (voorheen wel aangeduid als 'black-box')[6] dat lijkt te zijn bedoeld om *big data predictive analytics* mogelijk te maken.[7] Ook dat kan moeilijk worden gezien als versterking van de positie van de digitale burger, al was het maar in termen van bewijspositie of onschuldpresumptie: een burger met een verdacht profiel loopt het risico zich te moeten verweren tegen digitale verdachtmakingen of 'digitale predestinatie'.[8]

In dit preadvies verdiepen wij ons in de rechtspositie van de mens, *homo digitalis*, die zich moet zien te handhaven in een gedigitaliseerde wereld en die daarin een weg moet zien te vinden. Om te beginnen zetten we in dit eerste hoofdstuk uiteen wat we bedoelen met de notie van *homo digitalis* voor de bestuurder en de bestuurde. We ontlenen daarbij inzichten aan andere menstyperingen, zoals de *homo economicus*, de *homo ludens*, *homo universalis* etc. en lichten ze toe in Appendix 1. Vervolgens doen we in de hoofdstukken 2 tot en met 5 een poging aan de hand van voorbeeldsituaties te inventariseren, te categoriseren en te analyseren met welke risico's of bedreigingen de homo digitalis te maken kan krijgen als gevolg van digitalisering bij de overheid. Daaraan koppelen wij welke positiefrechtelijke

5. ABRvS 28 november 2012 ECLI:NL:RVS:2012:BY4444.
6. D. Stokmans, 'Sociale Zaken overtrad mogelijk de privacywetgeving', *NRC* 3 oktober 2014
7. Besluit van 1 september 2014 tot wijziging van het Besluit SUWI in verband met regels voor fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens met inzet van SyRI, *Stb*. 2014, 320.
8. De term is van de voorzitter van onze privacytoezichthouder, Jacob Kohnstamm, in zijn speech voor het ExpertForum van de Nationale DenkTank 2014 op 3 oktober 2014 (https://cbpweb.nl/sites/default/files/atoms/files/speech_big_data_nationale_denktank_versie_3_okt_2014_website.pdf, laatst geraadpleegd op 22 december 2015)

middelen het bestuursrecht te bieden heeft om deze het hoofd te bieden, en of er daaraan iets hapert. We vatten dit ruim op. We gaan het vervolgens in hoofdstuk 6 hebben over burgers en andere bestuurden (organisaties, ondernemingen etc.) die een andere positie krijgen c.q. innemen ten opzichte van de digitaliserende c.q. gedigitaliseerde overheid. Tenslotte komen we in hoofdstuk 7 tot een slotbeschouwing, waarin we één en ander samenbrengen, en met conclusies en aanbevelingen, met daarbij aandacht voor generaliseerbaarheid, en voor wat we wel en niet kunnen verwachten van het bestuursrecht als sturingsinstrument.

Het is ondenkbaar dat we in deze bijdrage volledig kunnen zijn. In het vervolg haken we aan bij de belangrijkste punten uit de 'visiebrief digitale overheid' van de minister van BZK uit 2013, een brief die ook rept over de gewenste toestand in 2017. Zo zorgen we ervoor dat onze bijdrage tenminste aansluit bij de dominante politieke denkkaders van het moment. We selecteren een viertal ambities zoals die door de minister worden onderkend. We zien elk van die ambities onder ogen, op zoek naar het antwoord op de vraag hoe de homo digitalis zich zal kunnen houden onder de verwachte wijzigingen die in het kader van genoemde ambities zullen optreden. We gaan daarbij enigszins anekdotisch te werk en beperken ons tot het geven van voorbeelden uit een praktijk die ons bekend is. Aan het eind van elk van deze verkennende en inventariserende hoofdstukken vatten we de geïdentificeerde risico's in enigszins gegeneraliseerde vorm samen, om in een later deel naar eventuele oplossingen te kunnen zoeken.

1.2 Welk beeld past bij het begrip homo digitalis?

Om eerlijk te zijn was het ons niet onmiddellijk helder wat met de term *homo digitalis* werd bedoeld toen ons werd gevraagd vanuit dat perspectief te redeneren.[9] We voelden weliswaar meteen aan waarom dat begrip toepasselijk is, maar zagen ons ermee geconfronteerd dat het begrip nog niet is ingeburgerd en in het recht geen standaardinterpretatie kent. Een verkennend literatuuronderzoekje wees uit dat antropologen het begrip vooral gebruiken om menselijk gedrag te typeren zoals dat zich op het moment in het westen openbaart. Vanuit een collectivistisch perspectief wordt het begrip gebruikt bij het duiden van de sociale behoeften en mogelijkheden van individuen, zoals bij het gebruik van sociale netwerken, bijv. bij revolutionaire bewegingen). En vanuit een individualistisch georiënteerd perspectief wordt het begrip ingezet om verwachtingen met betrekking tot kunstmatige intelligentie te duiden.

In dit pre-advies brengt onduidelijkheid over het begrip *homo digitalis* ons waarschijnlijk in de problemen. Als conceptueel anker moet het begrip onmiddellijk en zonder veel voorbereiding aanspreken. We hebben daar-

9. Een nadere onderbouwing voor deze paragraaf is opgenomen in Appendix 1.

om een werkdefinitie nodig. We hakken de knoop als volgt door en geven de definitie waarvan wij in deze bijdrage uitgaan:

> Een homo digitalis is een homo sapiens (mens) die zich in meer of mindere mate laat vertegenwoordigen of laat leiden door één of meer gedigitaliseerde processen, en die dus leeft en moet leven en overleven in een wereld of omgeving die dat mogelijk maakt.

We denken dat deze betekenis overeenkomt met wat intuïtief wordt begrepen door wie de term zonder nadere toelichting hoort.

Het is dan van belang dat ons begrip van *homo digitalis* een meerwaarde heeft in vergelijking met wat de verschillende andere, verwante deelbegrippen te bieden hebben voor de analyse van de menselijke natuur. We denken daarbij aan begrippen die zich inmiddels hebben gevestigd, zoals de *homo universalis* (drager van kennis, het ideaalbeeld uit de verlichting), *homo economicus* (met oog voor profijt en gezond eigenbelang), *homo ludens* (spelend van aard, innovator) en natuurlijk *homo sapiens* (het kunnen reflecteren, als biologische soort). Het is ook voor de rechtswetenschap nodig om aannamen te doen over de menselijke natuur die meebepaalt wat wel en wat niet juridisch kan zijn. Het recht gaat er van uit dat de mens als rechtssubject een vrije wil heeft, bewust keuzen kan maken en verantwoordelijkheid voor zijn handelen kan dragen, en dat de mens drager is van fundamentele rechten en vrijheden, zoals het recht op bescherming van zijn of haar persoonlijke levenssfeer.

Onze fascinatie met de *homo digitalis* wordt gevoed door het inzicht dat die mens ook juridisch moet zien te overleven in een wereld waarin de technologische mogelijkheden soms op verbijsterende wijze toenemen en veranderen. Wij houden in deze bijdrage als fundamenten van de rechtswetenschap vast aan uitgangspunten van vrije wil, bewust kiezen en verantwoordelijkheid dragen. De meerwaarde van het gebruiken van de definitie is dan, dat we daarmee duidelijk maken dat we er niet op uit zijn om naar een nieuw fundament voor het recht te zoeken waarin, bijvoorbeeld kunstmatig intelligente toepassingen ook verantwoordelijkheid dragen, maar naar mechanismen die het mogelijk maken voor respectievelijk overheden en burgers (d.w.z. bestuurders en bestuurden) om hun rol als dragers van verantwoordelijkheden te blijven spelen.

Met de *homo universalis, de homo sapiens, de homo ludens* en de *homo economicus* hebben we dus, zeker als die wordt aangevuld met de *homo digitalis*, de beschikking over een kleine familie van begrippen die bruikbaar zijn om bij het analyseren van situaties rekening te houden met essentieel geachte onderdelen van de menselijke natuur. Dat stelt ons in staat om nieuwe situaties die het recht uitdagen evenwichtig te behandelen. Zoals veel van de economische wetenschap rust op een mensbeeld van de redelijk handelende partijen vanuit goed begrepen eigenbelang, zo rust veel

van de rechtswetenschap op een mensbeeld van verantwoordelijkheid en vrije wil.[10]

In beleidsdocumenten en kamerstukken wordt de term 'digitalisering' vaak probleemloos zonder toelichting gebruikt.[11] Wij verstaan eronder het gebruik van moderne elektronische informatie- en communicatietechnologie om processen en procedures langs elektronische weg, en dus in digitale vorm, te laten verlopen. Het gaat bij digitalisering om de veranderingen die zich voltrekken in de maatschappij en de economie ten gevolge van deze technologie. We zien digitalisering als een groeiende kracht die de omgeving vormt voor menselijk handelen en die tegelijkertijd *zelf* het gevolg is van acties van rechtssubjecten.

Het gaat ons in deze bijdrage om verantwoorde besluitvorming, de legitimering daarvan en de rechtsbescherming in verband daarmee. In onze aanpak wordt derhalve met de term *homo digitalis* allereerst gerefereerd aan een verantwoordelijk individu, maar verder als dat zo uitkomt ook aan de individuen die deel uitmaken van instituties en instellingen, rechtspersonen, bestuursdiensten, ondernemingen en andere organisatievormen. In voorkomende gevallen zal dat met zich brengen dat we dergelijke organisatievormen in het taalgebruik in minder of meerdere mate vereenzelvigen met de desbetreffende individuen die alleen of met anderen invloed hebben op de wijze waarop deze in het maatschappelijk verkeer optreden. Een andere benadering, waarbij we het begrip rigide zouden opvatten, heeft het risico dat ons blikveld te beperkt wordt en dat we geen zicht hebben op belangrijke rechtspositionele implicaties die het gevolg zijn een toenemende verdichting van de digitale dienstverlening en van digital organisatievormen.

We gaan dus ervan uit dat de homo digitalis als autonoom individu voor zich handelt, en zijn ons ervan bewust dat zijn rol lijkt te verminderen en te veranderen wanneer hij optreedt als functionaris c.q. vertegenwoordiger van bijvoorbeeld een onderneming of overheidsdienst.

1.3 De homo digitalis getypeerd

Onze definitie staat uiteenlopende representanten van de 'soort' homo digitalis toe. Ertoe worden gerekend bestuurders en bestuurden of burgers, waarvan de laatstgenoemden afhankelijk van feitelijke en juridische

10. Wij kiezen ervoor, om de druk die wel vanuit de neurowetenschappen op deze aanname wordt uitgeoefend (bijvoorbeeld op basis van de 'Libet data') onder verwijzing naar en Dennett en Kinsbourne (1992) als irrelevant naast ons neer te leggen omdat het recht – ook als het, onder verwijzing naar Fuller (1930), mede berust op een fictie – een uiterst waardevol maatschappelijk spel oplevert waarvoor wij niet onmiddellijk een nieuw fundament zien. Met andere woorden: hoe verleidelijk misschien ook, we gaan niet op zoek naar een geheel nieuwe fundering voor de rechtswetenschap.
11. Zie bijv. *Kamerstukken II* 2014/15, 34 059, nr. 3.

omstandigheden allerlei hoedanigheden kunnen hebben, zoals die van consument, student, werknemer, werkgever, verzekerde, patiënt, automobilist, treinreiziger, zzp-er of andersoortig ondernemer, kiezer, et cetera.

Als gezegd gaat het in dit preadvies om de rechtspositie van de mens, *homo digitalis*, die zich moet zien te handhaven in een gedigitaliseerde wereld en daarin zijn weg moet vinden. We gebruiken vooral de begrippen 'bestuurder' en 'burger.' Onder de laatste verstaan we ook de 'ondernemer'[12] als iemand, die handelt in de uitoefening van een beroep of bedrijf. Voor deze ondernemers zal, in het kader van dat beroep of bedrijf, vooral betekenis toekomen aan aspecten als ondernemingsvrijheid, *level playing field* en, wie weet, ook innovatie.[13]

Het gaat ons vooral om de verhoudingen van burgers of ondernemers ten opzichte van bestuurders, en dus niet om die van burgers ten opzichte van ondernemers en omgekeerd. We beperken ons daarom tot de verhoudingen waarin de bestuurder een rol speelt. Om de typering in actie te bezien geven we een handvol soms hypothetische situaties waarbij het bijvoorbeeld gaat om de relaties tussen offline burgers en digitale bestuurders, en omgekeerd, van digitale burgers ten opzichte van offline bestuurders. De rapporten en onderzoeken van de Nationale ombudsman bieden daartoe voorbeelden. Zo is er het voorbeeld van iemand die zijn baan verliest en vervolgens niet de mogelijkheid heeft om zijn bijstandsuitkering langs digitale weg aan te vragen.[14] Een omgekeerde situatie, digitale burger tegenover offline bestuurder, betreft een Wob-verzoek dat in de gemeente Delft niet in digitale vorm kon worden gedaan.[15]

Een opmerkelijk slecht gedocumenteerd voorbeeld – de technische analyse van Fox-IT ervan is maar ten dele openbaargemaakt[16] – van de verhouding tussen digitale burgers of ondernemers tegenover offline of online bestuurders, is dat van de vermoedelijk Iraanse hackers die erin slaagden de digitale certificaten van Diginotar te vervalsen, en daarmee de bestuurders volledig verrasten.

12. Aldus sluiten we aan bij de gebruikelijk categorie-indelingen op belangrijke overheidswebsites, zoals overheid.nl en belastingdienst.nl, waar ook wordt uitgegaan van de categorieen «burgers of particulieren» en «ondernemers of bedrijven»; zie ook bijv. *Kamerstukken II* 2015/16, 26 643, nr. 373, p. 1.
13. Deze indeling sluit aan bij het onderscheid dat wordt gemaakt in het Dialogic onderzoek ter ondersteuning van de zgn. visiebrief digitale overheid 2017 van de minister van BZK 23 mei 2013, *Kamerstukken II* 2013/2013, 26 643, nr. 280. In dit onderzoek werd onderscheid gemaakt naar (1) digitaal niet-redzamen, (2) digitaal redzamen met ondersteuning, en (3) digitaal zelfredzamen. Zie Gillebaard en Vankan (2013). Zie ook Nationale ombudsman, De burger gaat digitaal, 2013/170, 9 december 2013, p. 13.
14. Nationale ombudsman, De burger gaat digitaal, 2013/170, 9 december 2013, p. 7.
15. No. Rapport 2014/113.
16. De Onderzoeksraad voor Veiligheid deed wel onderzoek, zie Onderzoeksraad voor Veiligheid (2012).

Een ander voor de verhoudingen van burgers en ondernemers tegenover digitale bestuurders interessant voorbeeld vinden we in het streven van de bewindspersoon verantwoordelijk voor veiligheid en justitie, om domeinoverschrijdende fraude in beeld te brengen en te bestrijden door te komen tot 'volledige uitwisseling van informatie,' en op grond van deze informatie analyses te maken die een 'integraal en effectief optreden' mogelijk moeten maken.[17]

1.4 Bestuursrechtelijke focus getypeerd

Traditioneel gaat het algemene bestuursrecht uit van het legaliteitsbeginsel, hetgeen zoveel wil zeggen dat het bestuur alleen bevoegd is om dat te doen waarvoor een wettelijke basis is gelegd. Eén van de vragen die we onder ogen zullen moeten zien is wat voor de verhouding van de digitale overheid ten opzichte van de digitale burger de betekenis kan zijn van het legaliteitsbeginsel en dan in hoeverre het voor digitale bestuurders een lege huls dreigt te worden, en wat we daartegen kunnen doen.

Een andere vraag die we onder ogen moeten zien is in hoeverre het bestuur zich kan, mag of moet overgeven aan samenwerkingsverbanden met experts uit het bedrijfsleven (en, wie weet, met experts uit de wetenschap) en op welke wijze de mandaterings- en verantwoordelijkheidsbetrekkingen transparant en effectief kunnen worden, of blijven. Het is voorts ons vermoeden dat, zoals de WRR aangaf, een inventarisatie van de digitale werkelijkheid aan het licht brengt dat daarmee aan steeds meer grote en complexe problemen het hoofd moet worden geboden, zoals daar zijn extremisme en terrorisme, veiligheid, mobiliteit of goede en betaalbare zorg – problemen die alleen nog maar voldoende lijken te kunnen worden begrepen door specialisten uit diverse disciplines te laten samenwerken.[18]

In het volgende deel gaan we verkennen. We bekijken de bestuursrechtelijke risico's, de rechtsmiddelen en de zwaktes daarin.

Deel II. VERKENNING

2. De gedigitaliseerde overheid

2.1 Inleiding

In wat met enig gevoel voor overdrijving wordt aangeduid als een 'visiebrief' geeft minister Plassterk een uiteenzetting van de pijlers of ambities

17. *Kamerstukken II* 2014/15, 32761, nr. 79.
18. WRR (2011) p. 11, 34 en 93.

waarop anno 2013 het kabinetsbeleid voor de digitalisering van de overheid steunt.[19] Deze pijlers bieden, ook al zijn ze misschien niet zo bedoeld, een goed vertrekpunt voor onze inventarisering van de rechtsposities van de homo digitalis, als burger en ondernemer en als bestuurder. Wij geven daaraan onze eigen draai en gebruiken deze pijlers om te komen tot een praktische indeling van aandachtsgebieden.[20] Aan de hand daarvan verkennen we dan op welke wijze digitalisering verschuivingen met zich brengt van de rechtsverhoudingen van de onderscheiden varianten van de homo digitalis ten opzichte van elkaar. Het gaat om de volgende aandachtsgebieden:

– de digitale beschikbaarheid van relevante overheidsinformatie en het bevorderen van de mogelijkheden tot digitale communicatie met de overheid (verkort aangeduid als 'beschikbaarheid en bereikbaarheid');
– het waarborgen van informatieveiligheid en in verband daarmee het realiseren van een betrouwbare identiteitsinfrastructuur ('informatieveiligheid en identiteitsinfrastructuur');
– het verbeteren van het gebruik van digitale gegevens binnen en door de overheid ('overheidsgegevensgebruik');
– het versterken van de informatiepositie van de burger en ondernemer ten opzichte van de versterkte informatiepositie van de digitale overheid ('evenwichtigheid van informatieverhoudingen').

Aan de eerste drie van de hierboven genoemde aandachtsgebieden wordt in de brief expliciet aandacht besteed. Aan het vierde aandachtsgebied wordt in de brief maar beperkte aandacht gegeven, maar het lijkt ons het belangrijkst omdat het oplossingen biedt voor de problemen die in de drie voorafgaande gebieden naar boven zijn gekomen. Wij behandelen het daarom afzonderlijk in het afsluitende deel van dit pre-advies.

Voor ieder aandachtsgebied bespreken we voorbeeldsituaties die inzichtelijk maken waar de homo digitalis tegenaan loopt en waarin hij met de middelen die het bestuursrecht biedt zijn weg moet zien te vinden. Voor elk aandachtsgebied wijden we ook een korte beschouwing aan de vraag

19. In de visiebrief (*Kamerstukken II* 2012/13, 26 643, nr. 280) worden deze pijlers op de volgende wijze aangeduid: (1) informatie moet online beschikbaar zijn; (2) burgers kunnen alle (aan)vragen aan de overheid digitaal versturen en alle berichten van de overheid digitaal ontvangen; (3) gebruiksvriendelijkheid en toegankelijkheid; (4) inzage- en correctierecht voor burgers; (5) informatieveiligheid en stelsel eID; (6) optimaal gebruik van digitale gegevens door de overheid; (7) samen verder bouwen aan een gezamenlijke infrastructuur; (8) huidige financieringswijze leidt tot inefficiënte eigen oplossingen.
20. We kiezen er mede gelet op de maatschappelijke urgentie van hoe de problematiek zich ontwikkelt in deze bijdrage uitdrukkelijk voor om aansluiting te zoeken bij het politiek-juridische discours zoals dat thans gaande is in plaats bij het voornamelijk positiefrechtelijke discours (waarmee onze bijdrage natuurlijk wel samenhang vertoont) zoals mede gevoerd door Barkhuysen et. al. (2014), Franken (1993), Groothuis (2011), Groothuis (2013), Overkleeft-Verburgh (1999), Overkleeft-Verburgh (2014),.

of de voorliggende transitie van onze samenleving, van offline naar digitaal, ook systeemrisico's (d.w.z. een risico dat aan het systeem als geheel en aan het complex van deelsystemen is verbonden) met zich meebrengt, en zo ja welke, en of daartegen vormen van rechtsbescherming in de beschouwing zouden moeten of kunnen worden betrokken.[21]

2.2 De gedigitaliseerde overheid en het sociaal contract

Het spreekt waarschijnlijk niet helemaal vanzelf hoe deze vier aandachtsgebieden samenhangen met een meer algemeen beeld van de krachten en beginselen die een rol hebben gespeeld (en nog spelen) bij de ontwikkeling van onze rechtssystemen, en de rollen (bevoegdheden, taken, plichten) die aan het bestuur worden toegekend. In het onderwijs van de Leidse rechtenfaculteit wordt bij het vak Encyclopedie de nadruk gelegd op enkele belangrijke ontwikkelingen in het rechtsdenken over het sociaal contract. Wat ons daarbij van belang voorkomt is dat in die ontwikkeling een aantal stappen kan worden herkend die laten zien dat er een aantal centrale concepten spelen: soevereiniteit, een geweldsmonopolie, de Rule of Law, de scheiding der machten en de algemene wil van een volk.[22]

In deze weg naar Westerse democratieën is de verhouding burger-soeverein weergegeven als een zich ontwikkelend concept. Die ontwikkeling verliep langs steeds betere manieren om het nodig geoordeelde geweldsmonopolie te brengen naar een bestuur dat steeds minder het risico in zich bergt van geweldsusurpatie. Ten eerste door de nadruk van bestuurstaken te leggen op het beschermen van vrijheid (vanaf Locke) in plaats van veiligheid. Ten tweede door grondrechten te formuleren (de Rule of Law) die grenzen stellen aan de wetgeving (doelbinding aan verwezenlijking van vrijheid). Ten derde door het bestuur in drie onafhankelijke instituties onder te brengen, en de wetgeving en de rechtspraak los te maken van het eigenlijke bestuur (machtenscheiding). Ten vierde, tenslotte, door de grondrechten als uiting te zien van de algemene wil van een volk, waaraan het bestuur zijn gezag ontleent.

In feite, en in grove lijnen, werden de Europese staten bijna allemaal tot ver in de negentiende eeuw bestuurd door nauwelijks door wetgeving ingetoomde absolute vorsten, of hun functionele equivalenten. De ideeën rond hoe regimes te verbeteren hebben in de loop der tijd vorm gekregen en zijn de daaropvolgende periodes ook verwezenlijkt, in het bijzonder

21. Hiermee wijkt onze benadering nogal af van het ons inziens overigens waardevolle Panteia onderzoek uit 2015 naar hoe de knelpunten bij de (digitale) overheid kunnen worden voorkomen en opgelost, omdat daar in "In overleg met de opdrachtgever is afgesproken dat de focus hierbij ligt op knelpunten bij de invoer van gegevens en gegevensverwerking, waar burgers het slachtoffer van worden." (p. 15). Ons perspectief is anders.
22. Die stappen zijn functioneel weergegeven in Appendix 2.

rond de Amerikaanse onafhankelijkheid, de Franse Revolutie, het Weense Congres van 1815 en de 'democratische lente' van 1848. In de geschetste ontwikkeling kan in grote lijnen een accentverschuiving worden waargenomen: van het primaat van de bescherming van individuele *veiligheid* naar het primaat van de bescherming van individuele *vrijheid*.

Eén en ander betekent dat de macht van het offline bestuur van de twintigste eeuw, voorafgaand aan de opkomst van de ICT,[23] werd beperkt door de wet (legaliteitsbeginsel), dat het bestuur een onafhankelijke institutie was naast de wetgever en de rechtspraak (machtenscheiding) en dat het bestuur als opdracht had om de grondrechten van individuele burgers te beschermen.[24]

We hebben deze beschouwing aan de ontwikkeling van onze bestuursrechtelijke arrangementen naar voren gebracht omdat we menen dat de ontwikkeling van onze samenleving van offline naar digitaal een misschien onverwachte wending neemt waar het gaat over hoe het gesteld is met onze individuele veiligheid en onze individuele vrijheid. We bezien of we de vier aandachtsgebieden die we in de brief van Plasterk herkenden kunnen plaatsen in dit spanningsveld:

– de digitale beschikbaarheid van relevante overheidsinformatie en het bevorderen van de mogelijkheden tot digitale communicatie met de overheid (verkort aangeduid als 'beschikbaarheid en bereikbaarheid') is essentieel voor de **individuele vrijheid** van de burger; vrijheid is immers nooit absoluut en kan door overheidsbesluiten en regelingen worden ingeperkt. Beschikbaarheid en bereikbaarheid van heldere informatie daarover maakt de overblijvende, vrije ruimte kenbaar.
– Het waarborgen van informatieveiligheid en in verband daarmee het realiseren van een betrouwbare identiteitsinfrastructuur ('informatieveiligheid en identiteitsinfrastructuur') is essentieel voor **individuele vrijheid** en **individuele veiligheid**); want de informatieveiligheid is nodig voor effectieve beschikbaarheid en de identiteitsinfrastructuur is nodig tegen de gevaren van identiteitsdiefstal - van de burger, maar ook van de overheid (DigID!).
– Het verbeteren van het gebruik van digitale gegevens binnen en door de overheid ('overheidsgegevensgebruik') wordt onder andere **gedaan om individuele veiligheid** zeker te stellen, maar doet vaak af aan **individuele vrijheid**); als argument voor de huidige datahonger van de overheid wordt vaak gewezen op de noodzaak om bescherming te bieden tegen ernstige misdrijven en terroristische dreigingen, maar diezelfde datahonger leidt er ook toe dat de beschikbare gegevens worden ingezet voor steeds meer (ook proactieve) vormen van handha-

23. Zie voor een analyse van de veranderende rol van de rechter in dit verband ook: Barkhuysen et al. (2014).
24. In deze geest ook al Overkleeft-Verburg (1999).

ving door de overheid; privacy is een belangrijke voorwaarde voor individuele vrijheid, en die verzwakt op deze wijze fundamenteel.
– Het versterken van de informatiepositie van de burger en ondernemer ten opzichte van de versterkte informatiepositie van de digitale overheid ('evenwichtigheid van informatieverhoudingen') beoogt bij te dragen aan **individuele vrijheid**; immers wanneer er een verschil van inzicht bestaat tussen een burger of bedrijf met de overheid over een overheidsbesluit of regeling (of de manier waarop die wordt gehandhaafd) is het resultaat mede afhankelijk van de mate waarin de informatieposities van beide partijen in evenwicht zijn. Een zekere mate van *equality of digital arms* is noodzakelijk voor het kunnen verdedigen, tegen de overheid, van de individuele vrijheden van homo digitalis.

En inderdaad, wanneer we naar de aandachtsgebieden kijken gaat het op het eerste gezicht steeds om de individuele vrijheid en veel minder vaak over individuele veiligheid van de burger. Met deze vaststelling komen we nu toe aan het verkennen en inventariseren van de risico's die we herkennen bij de drie expliciet behandelde aandachtgebieden uit de visiebrief.

3. Beschikbaarheid en bereikbaarheid

3.1 MijnOverheid.nl, MijnToeslagen.nl, MijnBelastingdienst.nl (etc.)

Onder wat wij hebben aangeduid als 'de digitale beschikbaarheid van relevante overheidsinformatie' wordt in de visiebrief[25] begrepen het streven dat alle als relevant gekwalificeerde overheidsinformatie digitaal beschikbaar wordt gesteld.[26] Erbij horen de uit de Angelsaksische wereld afkomstige initiatieven als 'open overheid' en 'open data'.[27] Het gaat niet alleen om het verbeteren van de publieke dienstverlening, maar ook om de kwaliteit van het openbaar bestuur en in dat verband het kunnen beïnvloeden van bestuurlijke besluitvorming, de controle daarop en de evaluatie ervan. Waar het de doelstellingen betreft die verband houden met open data initiatieven, gaat het ook om het mogelijk maken dat nieuwe informatieproducten, -diensten en -toepassingen door het bedrijfsleven worden ontwikkeld,

25. *Kamerstukken II* 2012/13, 26 643, nr. 280, p. 3.
26. Bij het schrijven van dit hoofdstuk is dankbaar gebruik gemaakt van S.R. Klaassen *Elektronisch verkeer met de overheid via de Berichtenbox. Een toekomstbestendig wettelijk kader?* 1 september 2015 (ongepubliceerd).
27. *Kamerstukken II* 2012/13, 26 643, nr. 280, p. 3; zie ook bijv. het Actieplan Open overheid, van het Ministerie BZK uit september 2013; of de website open-overheid.nl waar we al op de landingspagina een citaat van Barack Obama krijgen gepresenteerd (geraadpleegd 1 augustus 2015).

waarmee economische groei wordt gestimuleerd en maatschappelijk engagement wordt bevorderd.[28]

Verwant daaraan is de, ook in de visiebrief tot uitdrukking gebrachte ambitie dat de overheden zoveel mogelijk digitaal bereikbaar zijn en het streven dat er met deze overheden langs digitale weg kan worden gecommuniceerd.[29] Alle vragen en aanvragen moeten in digitale vorm naar de overheid kunnen worden verstuurd en omgekeerd moeten berichten van de overheid in dezelfde vorm kunnen worden ontvangen. Om dit te bereiken wordt, althans dat is de bedoeling,[30] in de Awb een regeling opgenomen die mogelijk moet maken dat Nederlanders, met inbegrip van Nederlanders in het buitenland en buitenlanders in Nederland, meer mogelijkheden krijgen om langs digitale weg met de overheid te communiceren. De regeling sluit wellicht aan bij de nog niet zo heel lang geleden in het Burgerlijk Wetboek opgenomen regelingen voor de totstandkoming van overeenkomsten langs elektronische weg[31] en elektronische besluitvorming in rechtspersonen.[32]

De ambities van de overheid met betrekking tot digitale beschikbaarheid en bereikbaarheid zijn niet bescheiden, maar lijken niet onhaalbaar. Het is nog niet eens zo heel lang geleden dat het enerzijds bijzonder moeilijk was geworden om een fysiek bankfiliaal te bezoeken (omdat die waren vervangen door geldautomaten, webpagina's en apps) terwijl anderzijds het telefoonmoeras van er-zijn-nog-17-wachtenden-voor-u opdoemde, vergezeld

28. Zie overw. 3 van Richtlijn 2013/37/EU van het Europees Parlement en de Raad van 26 juni 2013 tot wijziging van Richtlijn 2003/98/EG inzake het hergebruik van overheidsinformatie, *PbEU* 27.6.2013 L175/1: overwegende dat *"[b]eleid voor vrije gegevensverstrekking, dat brede beschikbaarheid en hergebruik van overheidsinformatie voor privé- of commerciële doeleinden met minimale of geen juridische, technische of financiële beperkingen aanmoedigt en het circuleren van informatie zowel voor marktdeelnemers als voor burgers bevordert, kan een belangrijke rol spelen in het op gang brengen van de ontwikkeling van nieuwe diensten die gebaseerd zijn op nieuwe manieren om dergelijke informatie te combineren en in te zetten, kan de economische groei stimuleren en maatschappelijk engagement bevorderen. […]*"; zie ook *Kamerstukken II* 2014/15, 34 123, nr. 3, p. 1-2.
29. *Kamerstukken II* 2012/13, 26 643, nr. 280, p. 3-4.
30. De Minister van EZ deed aanvankelijk de toezegging het wetsvoorstel nog in 2014 naar de Kamer te sturen (Kamerstukken II 2013/14, 32 637, nr. 88, p. 11) maar kwam daarop later terug omdat bij de voorbereiding van de internetconsultatie van het wetsvoorstel was gebleken dat er behoefte is aan harmonisatie van beleid op het terrein van de elektronische overheid. Om deze reden is ervoor gekozen het wetsvoorstel onderdeel te laten worden van een breder integraal wetgevingsprogramma (Kamerstukken II 2013/14, 32 637 nr. 131, p. 1). Inmiddels is de voorbereiding van het wetsvoorstel, waarvan de werktitel is geworden Wet GDI is, overgedragen aan de Minister van BZK, die in een kamerbrief van 4 december 2015 (Kamerstukken II 2015/16, 26 643, nr. 373, p. 1) heeft toegezegd het wetsvoorstel in 2016 naar de Kamer te sturen. Zie ook voetnoot 43 van dit pre-advies.
31. Art. 6:227a, eerste lid, BW.
32. Art. 2:217a e.v. BW.

van de aanbeveling een bepaalde website te bezoeken. Een jaar of twee geleden hebben belangrijke spelers in het bedrijfsleven een nieuwe koers ingeslagen die, tenminste voor wie beschikt over een internetverbinding en daarvan gebruik weet te maken, een ongekende verbetering inluidt. We hebben het over de inzet van direct chat-contact met een deskundige medewerker. Het voordeel van deze aanpak is dat de deskundige toegang heeft tot alle relevante bij zijn bedrijf geadministreerde gegevens over contract en dienstafnemer. En dat het gebruik van chat het toestaat om een deskundige medewerker in real time aan een informatietransactie of vijf tegelijkertijd te laten werken.

Dit beschikbaarheids- en bereikbaarheidsmodel is, voor zover wij overzien, begonnen bij telecomdienstverleners, maar het voorbeeld werd al snel gevolgd door banken en andere dienstaanbieders die zich daarmee wensen te onderscheiden van hun concurrenten. Vanzelfsprekend slaagt niet iedere aanbieder daarin, maar al-met-al lijkt het algemeen aanvaard dat deze vorm van digitalisering inderdaad kan bijdragen aan een betere bereikbaarheid en beschikbaarheid. Ook als we onderkennen dat er geen sprake is van echte concurrentie tussen bestuursdiensten ligt voor de hand dat overheden op een zelfde wijze het contact met de burger, homo digitalis, veel beter en gebruiksvriendelijker kunnen inrichten. Wat dit betreft zijn er, als gezegd, kansen voor de ambities van Plasterk. Er zijn echter ook bedreigingen en risico's.

Er zijn op alle niveaus talloze voorbeelden van overheden die zich zijn gaan inspannen om langs digitale weg relevante informatie beschikbaar te stellen aan burgers en ondernemers. In het verlengde daarvan zien we ook dat deze overheden ernaar streven om de communicatie met burgers en ondernemers langs dezelfde digitale weg mogelijk te maken. Dit kan immers vaak ook voor deze overheden voordelen hebben, al was het maar doordat er aanzienlijke besparingen op portokosten mogelijk zijn.[33]

In de visiebrief wordt verwezen naar de web portals die burgers en ondernemers in staat stellen kennis te nemen van, en zo nodig te communiceren over, de voor hun specifieke situatie relevante gegevens, met inbegrip van de op hen betrekking hebbende persoonsgegevens. Het gaat om de websites in het zgn. 'mijn-domein', waarop burgers of ondernemers inloggen om hun eigen overheidszaken te regelen. Denk aan MijnOverheid.nl, een portal die toegang biedt tot elektronische post van overheden en tot de door overheden vastgelegde persoonlijke gegevens, alsmede de stand van zaken van de bij deze overheden lopende zaken. Van MijnOverheid.nl

33. De RDW bijvoorbeeld was in 2014 goed voor iets minder dan 7 miljoen APK-keuringen (licht en zwaar) en stuurde in het kader daarvan zo een 6 miljoen geautomatiseerde brieven uit ter herinnering van het verlopen van de APK. Alleen al aan portokosten voor dit deel van de bedrijfsvoering van de dienst kunnen dus al snel enkele miljoenen worden bespaard. Zie het online-jaarverslag van de RDW: http://jaarverslag2014.rdw.nl/_layouts/Rdw.Jv2014.Portal/home.aspx (geraadpleegd 30 december 2015).

wordt gebruik gemaakt door de Belastingdienst, RDW, SVB, UWV, gemeenten en het Kadaster. Via de portal krijgt u, zo meldt startpagina, een herinnering als uw rijbewijs dreigt te verlopen. U kunt er controleren hoe u bij de gemeente geregistreerd staat of de status van een omgevingsvergunning volgen. En dat allemaal overzichtelijk, veilig en altijd beschikbaar. "*U logt gemakkelijk in met uw DigiD*." Andere voorbeelden van zulke overheidsportals zijn Werk.nl, MijnToeslagen.nl, MijnDUO.nl en de websites van gemeenten, zoals het Servicepunt Sociaal op DenHaag.nl.

Van dergelijke web portals kunnen worden onderscheiden de websites die bedoeld zijn voor de digitale beschikbaarstelling van algemene overheidsinformatie, dat wil zeggen: de overheidsinformatie die voor iedereen relevant kan zijn. Daarbij valt te denken aan de bekendmaking van wet- en regelgeving, kennisgevingen van vergunningen, besluiten en beleidsregels, bestemmingsplannen, reglementen, regelingen, aanvraagformulieren, beleidstukken, notulen van openbare vergaderingen, brochures, enzovoorts. Voorbeelden waarmee we als praktijkjuristen vertrouwd zijn geraakt betreffen natuurlijk Overheid.nl en Rechtspraak.nl, Belastingdienst.nl etc.

3.2 Digitaal, tenzij…

Er is recent enig onderzoek gedaan naar de digitale beschikbaarheid van overheidsinformatie en de bereikbaarheid van overheden. Voor ons is vooral het onderzoek van de Nationale ombudsman van belang. Dat onderzoek ging specifiek in op de belangen van de burgers die langs digitale weg in contact proberen te treden met de overheid. We ontlenen er een aantal zorgen aan over hoe de gedigitaliseerde overheid wordt vormgegeven en hoe het vanuit het perspectief van de digitale burger mis kan gaan.[34] Zo is een belangrijke bevinding dat voor een substantieel deel van de burgers met digitalisering het tegenovergestelde wordt bereikt van wat er wordt beoogd. Ongeveer twintig procent van de burgers heeft zoveel moeite met digitalisering dat het daardoor voor hen juist moeilijker wordt om met de overheid in contact te treden. Voor deze groep *offliners* is de digitalisering van de overheid problematisch, zeker als er geen mogelijkheid is om gebruik te maken van andere kanalen om de overheid te bereiken en als het voor hen lastig is om fouten in gedigitaliseerde systemen te herstellen.

Het rapport van de ombudsman wijst erop dat er sprake is van een 'opvallende verschuiving in de uitgangspunten van de overheid' over de voorwaarden die worden gesteld aan een goede gedigitaliseerde dienstverlening. In de daarvoor opgestelde gedragscode, de Burger Service Code, stond eerst de keuzevrijheid van de burger voorop. In latere beleidsstukken

34. Kanne en Van den Berg (2013).

verschoof het accent en staat dat persoonlijk contact mogelijk gemaakt wordt, als dat noodzakelijk of bevorderlijk is voor de kwaliteit van de dienstverlening. En dat wekt, aldus het rapport, de indruk dat het niet meer zozeer gaat om wat de burger wil maar om wat de overheid wenselijk acht. Een bevestiging daarvan zien we ook in het uitgangspunt van de verantwoordelijke minister dat wordt samengevat in de vuistregel '*digitaal, tenzij dat niet kan*'. De standaardsituatie of *default-setting* is digitalisering, andere kanalen zijn de uitzondering waarvan alleen gebruik wordt gemaakt als de noodzaak daarvan wordt aangetoond.

Er is niet veel fantasie nodig om te bedenken wat er dan kan misgaan. We willen wel geloven dat de groep van minder digitaalvaardige burgers, ondanks de vergrijzing,[35] inmiddels in omvang mogelijk is afgenomen en nog wel verder zal afnemen. Maar ook dan kan de gedigitaliseerde overheid het zich niet veroorloven dat zij een grote groep burgers niet goed kan bereiken en dat zij daardoor niet kan worden bereikt. Het is, zolang we het hebben over deze substantiële percentages, onontkoombaar dat de digitale overheid offline kanalen blijft aanbieden. We wagen ons niet aan percentages waarbij dergelijke kanalen niet meer nodig zouden zijn, maar kunnen wel zeggen dat op dit moment beschikbaarheid en bereikbaarheid niet daarzonder kunnen. In zoverre past scepsis bij de bezuinigingen die de overheid denkt te kunnen realiseren door digitalisering. Als we niet het risico willen lopen dat een grote groep offliners wordt uitgesloten, gaat digitalisering voorlopig waarschijnlijk vooral geld kosten. Daarbij is er natuurlijk de zorg dat besparingsambities er de facto toe gaan leiden dat een grote groep minder digivaardigen wordt uitgesloten van communicatie met de digitale overheid.

Risico I. Digitalisering met besparingsambities kan ertoe leiden dat een grote groep minder digivaardigen (offline burgers en ondernemers) *de facto* wordt uitgesloten.

3.3 Een recht op DigiD?

Verband houdend met het voorgaande (en met de in het volgende hoofdstuk nog te bespreken informatieveiligheid) is dat de bereikbaarheid en beschikbaarheid van de digitale overheid afhankelijk is van middelen die door diezelfde overheid ter beschikking worden gesteld. Om met de digitale overheid te communiceren is veelal een DigiD vereist. Er vanuit gaand dat iedere burger in staat moet zijn om met die overheid te communiceren zouden we verwachten dat iedereen daarop aanspraak maakt. De regeling van DigiD lijkt daarin echter niet zonder meer te voorzien. Wie gebruik wil maken van DigiD kan dat aanvragen en om het vervolgens toegekend te

35. Loos (2010).

krijgen. Tot voor kort werd daarvoor van hem of haar verlangd dat hij of zij akkoord ging met de Gebruiksvoorwaarden DigiD.[36]

Deze voorwaarden blonken niet uit in evenwichtigheid en bevatten maar weinig waarborgen voor de gebruiker, de digitale burger. Zo stond er dat Logius, als beheerder van DigiD de gebruiker kon uitsluiten van verder gebruik van DigiD "*[b]ij (het vermoeden van) misbruik of oneigenlijk gebruik van DigiD.*"[37] En ook dat Logius "*de toegang tot het gebruik van DigiD op elk gewenst moment [kan] (doen) beëindigen of blokkeren*". En "*[i]n geval van beëindiging of blokkering vervalt onmiddellijk het recht op het gebruik van DigiD*." Als het gebruik van DigiD werd beëindigd, onderbroken of geblokkeerd was het, zo bleek uit de voorwaarden, mogelijk dat "*de informatie die de Gebruiker via DigiD heeft opgeslagen niet meer achterhaald kan worden*." En dat was een risico dat de gebruiker maar heeft te accepteren. "*Gebruiker accepteert dit risico*."

Voorwaarden als deze zijn niet heel ongebruikelijk bij de besturingsprogrammatuur van onze smartphones of standaardsoftwarepakketten, maar misschien omdat we weten dat de afdwingbaarheid ervan beperkt wordt door het consumentenrecht kunnen we ermee leven. Anders kunnen we mogelijk met enige moeite migreren naar de een of andere alternatieve dienstverlener. Voor een overheid die uitgaat van digitale beschikbaarheid en bereikbaarheid (immers '*digitaal, tenzij…*') is wel duidelijk dat dit soort voorwaarden niet meer kan. Uit openbare bronnen hebben we niet kunnen achterhalen hoe vaak een DigiD wordt geweigerd of ingetrokken, maar naar verluidt zou dat enkele honderden keer per jaar gebeuren. Wat de overwegingen daarbij waren is ook onbekend. Over de rechtsmiddelen die ertegen zouden kunnen worden ingezet hebben we wel gedachten. Een probleem ontstaat natuurlijk als een DigiD nodig is om dat te doen …[38]

Een min-of-meer vergelijkbare situatie zagen we ook bij de gebruiksvoorwaarden van MijnOverheid.nl en andere mijn-domeinen van de digitale overheid. Ook daarvoor was de wettelijke grondslag voor de regeling ervan nogal zwak.[39] Voor MijnOverheid was deze geregeld in het Besluit

36. De Gebruiksvoorwaarden DigiD van 15 mei 2012 (versie 6.0) zijn nog steeds betrekkelijk eenvoudig te vinden met een internetzoekmachine en anders op https://www.digid.nl/fileadmin/digid/downloads/20120515_gebruiksvoorwaarden_digid_versie_6_0_def.pdf (geraadpleegd 30 december 2015).
37. Art. 2.15 van de Gebruiksvoorwaarden DigiD.
38. In de MvT bij het Wetsvoorstel Vereenvoudiging en digitalisering van het procesrecht wordt als authenticatiemiddel gedacht aan DigiD voor burger, aan eHerkenning voor rechtspersonen en aan de Advocatenpas voor advocaten. Aldus *Kamerstukken II* 2014/15, 34 059, nr. 3, p. 21, 35-36, 41-42 en 59.
39. Aldus ook Overkleeft-Verburg (2014) p. 321.

vaststelling aansluitvoorwaarden MijnOverheid.nl[40] en het Besluit beheer Persoonlijke Internetpagina.[41]

Inmiddels is één en ander geregeld in de Regeling voorzieningen GDI.[42] In deze regeling wordt niet meer uitgegaan van door de gebruikers expliciet te geven instemming met de betreffende gebruiksvoorwaarden. Dit is omdat het gebruik van MijnOverheid.nl met de door de Wet elektronisch berichtenverkeer Belastingdienst[43] ingevoerde verplichte digitale aangifte niet meer plaatsvindt op basis van vrijwilligheid. Er is dus nu wel een publiekrechtelijke regeling en deze biedt als zodanig de gebruiker, homo digitalis, wel al meer waarborgen en rechtszekerheid dan de daarvoor gehanteerde gebruiksvoorwaarden. Uit de toelichting bij de regeling blijkt echter dat deze primair beoogt om de bestaande, in de praktijk reeds gehanteerde voorschriften, een wettelijke basis te geven. Daardoor zijn de gevolgen ervan, volgens de toelichting, beperkt. En we zien dan ook dat de regeling nog steeds nogal eenzijdig opgestelde voorwaarden bevat. Zo kan er 'bij het vermoeden van misbruik of oneigenlijk gebruik' de toegang tot MijnOverheid.nl of DigiD worden onderbroken of 'bij geconstateerd misbruik of oneigenlijk gebruik' de toegang tot de voorziening worden beëindigd. Er is in de regeling wel aandacht voor de beveiliging van één en ander, en voor de wijze waarop ongebruikelijke patronen kunnen worden onderkend die mogelijk duiden op misbruik of oneigenlijk gebruik.[44] Heel weinig aandacht is er echter voor de waarborgen van de burger tegen zo een onderbreking of beëindiging (zeg: de rechtsmiddelen daartegen of de maximale duur van zo een onderbreking of beëindiging etc.).[45] Dat geeft te denken.

Risico II. Het risico is dat de toegang tot steeds essentiëler wordende diensten van de digitale overheid wordt beheerst door regelingen met maar weinig waarborgen voor de gebruikers van deze diensten (de burgers)

---

40. Besluit vaststelling aansluitvoorwaarden MijnOverheid.nl van 4 december 2007, 249.
41. Besluit beheer Persoonlijke Internetpagina, 25 mei 2007, *Stcrt*. 2007, 102, p. 8.
42. Regeling voorzieningen GDI, *Stcrt*. 2015, 37158.
43. Wet elektronisch berichtenverkeer belastingdienst, *Stb.* 2015, 378.
44. NvT Regeling voorzieningen GDI, *Stcrt*. 2015, 37158, resp. p. 7-8 en p. 11.
45. In de kamerbrief van 4 december 2015 (*Kamerstukken II* 2015/16, 26 643, nr. 373) wordt een wet aangekondigd die een juridische basis beoogt te leggen onder wat wordt genoemd de Generieke Digitale Infrastructuur of GDI. De zgn. Wet GDI moet een bijdrage leveren aan de totstandkoming van een in de Awb vast te leggen 'recht op elektronisch zakendoen met de overheid'. Afgaand op de schets die in de brief van deze beoogde wetgeving wordt gegeven, zou het daarin niet zozeer gaan om waarborging van rechten van burgers, maar vooral om de afstemming van uitvoeringsprocessen, herkenbaarheid van overheidsdienstverlening, aansluiting bij standaarden, omschrijving van functionaliteiten, en dergelijke. We kunnen deze Wet GDI niet in onze beschouwingen betrekken, de formulering is nog niet bekend. Wel kunnen we de hoop uitspreken dat de risico's die we in dit preadvies inventariseren zijn onderkend.

3.4 Wie bepaalt de selectie?

Van andere orde zijn de vragen over de overheidsinformatie waarover iedereen moet kunnen beschikken en die daarom en in beginsel zonder beperkingen aan iedereen ter beschikking wordt gesteld. Een probleem is dat onduidelijk is of alle overheidsinformatie die daarvoor in aanmerking komt door de desbetreffende overheid uit eigen beweging wordt aangeboden. De verwachting lijkt gerechtvaardigd dat, mede dankzij open-data wetgeving,[46] voor de categorieën van overheidsinformatie waarvoor een markt is (zoals parlementaire stukken en wet- en regelgeving) betrekkelijk gemakkelijk kan worden gewaarborgd dat de informatie goed en volledig beschikbaar is.

Toch is daarmee niet verzekerd dat alle relevante overheidsinformatie inderdaad beschikbaar is. Van alle in Nederland geproduceerde rechtspraak werd in 2010 minder dan 3 procent via rechtspraak.nl beschikbaar gesteld. Inmiddels is dat, naar wij begrijpen, nog steeds niet meer dan enkele procenten.[47] Voor rechtspraak, die in principe in het openbaar wordt gedaan,[48] is het uitgangspunt kennelijk '*niet digitaal, tenzij…*' Vanuit de rechterlijke macht wordt daarvoor wel als verklaring gegeven dat de niet gepubliceerde rechtspraak 'onbetekenende zaken' betrof (want toch ongemotiveerd of faillissementen enz.), en dat deze rechtspraak alleen maar het beeld op de wel relevante rechtspraak zou vertroebelen, of dat het veel te duur is om alles te anonimiseren, en dergelijke.[49] Deze overwegingen, hoewel uitvoerig uitgewerkt in een indrukwekkend proefschrift,[50] overtuigen ons niet – ook niet omdat zelden aandacht wordt besteed aan het verlies van de mogelijkheid tot wetenschappelijk en journalistiek onderzoek naar de rechtspraak als geheel.[51] En, ook al is in 2012 vanuit de rechtspraak opgehelderd wat de publicatiecriteria zijn,[52] dan nog komt het

46. Wet hergebruik overheidsinformatie, *Stb*. 2015, 271.
47. Er werden in 2014 ca. 31.330 uitspraken gepubliceerd via rechtspraak.nl (bron: Legal Intelligence) en uit het overzicht op p. 36 van het Jaarverslag Rechtspraak 2014 (www.jaarverslagrechtspraak.nl/verslag/productie-en-werkvoorraadontwikkeling) kan worden opgemaakt dat de 'instroom' in dat jaar ca. 1,8 miljoen zaken bedroeg. We leiden daaruit af dat het aantal gepubliceerde uitspraken vermoedelijk nog steeds niet meer dan enkele procenten bedraagt.
48. Art. 121 Grondwet: Met uitzondering van de gevallen bij de wet bepaald vinden de terechtzittingen in het openbaar plaats en houden de vonnissen de gronden in waarop zij rusten. De uitspraak geschiedt in het openbaar.
49. Zie de reacties op Mommers et al. (2010a), p. 2072: Philippart (2010) p. 2356 en van der Hoek (2010) p. 2357, en de reactie daar weer op van Mommers et al. (2010b), p. 2358.
50. Van Opijnen (2014), p. 151 e.v.
51. Aldus recent ook: F. Jensma, 'Machines zijn eerder op te lichten dan mensen', NRC 2 januari 2016
52. Zie Besluit selectiecriteria uitsprakendatabank Rechtspraak.nl, te vinden via www.rechtspraak.nl/Uitspraken-en-nieuws/Uitspraken/Paginas/Selectiecriteria.aspx

vanuit een rechtstatelijk perspectief geloofwaardiger voor dat in beginsel alle uitspraken worden gepubliceerd, en dat de vraag wat relevant of irrelevant is wordt beantwoord door de gebruiker van rechtspraak.nl (homo digitalis). Inmiddels lijken de algoritmes van zoekmachines hem heel goed in staat te stellen de belangrijke van de onbelangrijke zaken te scheiden. Het is voorts de vraag of álle rechtspraak áltijd moet worden geanonimiseerd. Bovendien kunnen, als bij de productie van uitspraken al rekening wordt gehouden met anonimiseren, de kosten daarvan waarschijnlijk substantieel worden teruggebracht.[53]

Maar daarom gaat het niet eens. Het gaat erom dat de selectie van welke informatie wordt bekendgemaakt, en de keuze van de daarbij te gebruiken selectiecriteria, níet zouden moeten liggen bij degenen die deze informatie hebben geproduceerd. En dat is natuurlijk niet beperkt tot rechtspraak. Ook van andere overheden en overheidstoezichthouders hebben we gezien dat sommige besluiten en rapporten om onverklaarbare redenen niet, of na verloop van enige tijd niet meer, zijn te vinden op de website of in de administratie. Als daarnaar navraag wordt gedaan, al dan niet met een beroep op de Wet openbaarheid van bestuur of onder politieke druk, leidt dat soms ertoe dat het gezochte alsnog boven tafel komt.[54] Maar omdat we nou eenmaal niet weten wat we niet weten, valt niet te zeggen wat er nog meer bekend had kunnen worden gemaakt. En wat de redenen waren om iets niet openbaar te maken. Of niet gemakkelijk vindbaar te maken.[55]

Risico III. Een risico voor de homo digitalis is dat digitale overheden in hun verhouding met burgers en ondernemers zich weten te onttrekken aan checks and balances door selectief hen betreffende informatie in meer of mindere mate toegankelijk te maken

---

3.5 Samenvatting

Als eerste wordt de transitie naar gedigitaliseerd bestuur (en naar 'de' homo digitalis) zichtbaar in de wijzen waarop de communicatie wordt gerealiseerd. Dat impliceert dat de manieren waarop overheid, ondernemer en burger beschikbaar en bereikbaar zijn veranderen. We vatten de kern van het hoofdstuk hier samen door de geïdentificeerde risico's onder elkaar te zetten en een soms ongenuanceerde 'sound byte' (cursief) mee te geven om er later verkort mee te kunnen werken. Het gaat om:

53. Zie Mommers et al. (2010b), p. 2358.
54. Een sprekend voorbeeld is natuurlijk het "bonnetje" van de betaling aan Cees H., jaren geleden, dat uiteindelijk leidde tot het aftreden van twee bewindspersonen. Zie daarover o.a. A. Eigenraam, 'What's the deal met de deal van Cees H. en wie is Cees H.?' *NRC* 9 maart 2015.
55. Zwenne (2009), p. 31; Persbericht: OPTA past beveiligingsniveau online-documenten aan wensen gebruikers aan, 17 juni 2009 en daarover Zwenne (2011), p. 3; Zwenne (2013), p. 67.

Risico I. *Digibeten de dupe*. Digitalisering met besparingsambities kan ertoe leiden dat een grote groep minder digivaardigen (offline burgers en ondernemers) *de facto* wordt uitgesloten
Risico II. *Digitale dwangbuizen*. Het risico is dat de toegang tot steeds essentiëler wordende diensten van de digitale overheid wordt beheerst door regelingen met maar weinig waarborgen voor de gebruikers van deze diensten (de burgers)
Risico III. *Troebel in plaats van transparant*. Een risico voor de homo digitalis is dat digitale overheden in hun verhouding met burgers en ondernemers zich weten te onttrekken aan checks and balances door selectief hen betreffende informatie in meer of mindere mate toegankelijk te maken.

De genoemde risico's spelen vooral doordat de digitalisering en de kennis daarover niet resulteren in gradueel veranderende communicatieprocessen die we gemakkelijk kunnen leren kennen. Het gaat met horten en stoten die niet iedereen kan bijbenen. Omdat voorts enerzijds de verwachting bestaat dat grote efficiencywinsten te behalen zijn en anderzijds de mogelijkheden zich voor de overheid voordoen om condities te bepalen waaronder (DigiD) en waarover (digitale formulieren) kan worden gecommuniceerd lijkt een speelveld te zijn ontstaan waarin de offline burger het spoor bijster kan raken en het online bestuur kansen ziet zich *de facto* te onttrekken aan toezicht.

4. Informatieveiligheid en identiteitsinfrastructuur

4.1 DigiD / eID-stelsel

In zijn visiebrief onthult Plasterk dat DigiD, met 10 miljoen aansluitingen, een basisvoorziening is geworden die de sleutel is voor digitale toegang van burgers tot de e-overheid. Er moet dan ook, vervolgt de brief, continu aandacht zijn voor veiligheidsmaatregelen, alsmede voor de kans op misbruik van bijvoorbeeld DigiD. Daarmee kan niemand het oneens zijn. Maar er is waarschijnlijk meer nodig dan dat. Een homo digitalis, ook (of: juist) als die een marginaal niveau van digivaardigheid heeft, moet erop kunnen vertrouwen dat de communicatie met de overheid betrouwbaar en veilig is. In elk geval kan het niet zo zijn dat de veiligheidsrisico's daarvan eenzijdig bij de burger worden gelegd.

In dat verband wordt in de brief in één adem het "stelsel eID" genoemd. Dat doelt op een hoogwaardig authenticatiemiddel dat burgers, bedrijven en overheidsdiensten in staat moet stellen om, vanaf 2017, alle communicatie over-en-weer digitaal te kunnen doen.[56]

56. *Kamerstukken II* 2013/2013, 26 643, nr. 280, p. 6.

Analogie tussen data- en wegverkeer

Informatieveiligheid lijkt op het eerste gezicht inderdaad een noodzakelijke voorwaarde om alles 'digitaal te doen.' Maar dat is alleen zo, wanneer we ons voorstellen dat informatieveiligheid iets is dat volkomen haalbaar zou zijn. Dat is echter niet zo (waarover later). Net zo min als '100% verkeersveiligheid' een noodzakelijke voorwaarde is voor wegvervoer is '100% informatieveiligheid' een noodzakelijke voorwaarde voor 'dingen digitaal doen.'

Net zoals het aanbevelenswaard is te voorkomen dat wie beschonken is, of wie anderszins niet rijvaardig is, toch aan het verkeer gaat deelnemen, kan het verstandig zijn om onder ogen te zien of er condities bestaan waardoor iemand niet informatievaardig is (en als gevolg beter maar niet aan het informatieverkeer kan deelnemen). En net zoals het aanbevelenswaard is, voor wie aan het verkeer deelneemt, om zich aan de verkeersregels te houden en om een wet Mulder in te richten die de veelvoorkomende overtredingen beboet, kan het verstandig zijn om onder ogen te zien of er regels zijn voor het informatieverkeer die strafrechtelijk, en misschien ook bestuursrechtelijk kunnen worden overtreden en vervolgens bestuursrechtelijk worden afgedaan.

Het stellen van die vragen is niet populair en leidt onmiddellijk tot opwinding en beschouwingen over de inperking van grondrechten omdat veel informatierechten daar nu eenmaal worden gerangschikt. Maar het niet stellen, en het niet beantwoorden, van die en dergelijke vragen leidt tot het soort vruchteloze discussies over internet governance waar we nu al geruime tijd getuige van zijn en die de eigenlijke vraag uit te weg gaan: wie zorgt voor een communicatie-infrastructuur waarover een geoefende en oplettende gebruiker veilig en in vrijheid kan communiceren? En: is de zorg daarvoor een overheidstaak? En als dat zo is, wat zijn de eisen die worden gesteld aan de veiligheid van informatieverkeer over die infrastructuur? En wat is eigenlijk geoefend en oplettend gebruik? En als de zorg voor die infrastructuur geen bestuurs- of overheidsopdracht is, wat zijn dan de eisen die aan de private partijen die de infrastructuur aanbieden kunnen worden gesteld? En hoe kan worden toegezien op het naleven van die eisen?

Omdat dit soort vragen wel kunnen worden gesteld, en beantwoord, voor het wegverkeer gebruiken we ze ook als een kader om beveiliging van informatieverkeer te bezien. We gaan er daarbij van uit dat de analogie met het wegverkeer een bruikbare is, ook om na te gaan wat de risico's zijn voor een gecombineerd streven naar 'informatieveiligheid' én 'alles digitaal willen gaan doen.' We zijn ons ervan bewust dat er grote verschillen zijn, maar we denken dat de voordelen van het inzetten van een herkenbaar en werkzaam juridisch arrangement voldoende meerwaarde heeft.

We bespreken de bestuursrechtelijke risico's aan de hand van enkele citaten uit overheidsmissives. De visiebrief wijdt een paragraaf aan informatieveiligheid en een eID stelsel:

> *Het elektronisch contact met de overheid moet goed beveiligd zijn. De lessen uit het DigiNotarincident, maar ook na Lektober en de recente Ddos-aanvallen op DigiD laten zien dat het beveiligen van informatie en de beschikbaarheid van de digitale dienstverlening urgent en blijvend op de agenda moeten staan.*
> *Bestuurders en topmanagers in het openbaar bestuur moeten zich hiervan bewust zijn. Om dit bewustzijn en de kennis over informatieveiligheid bij deze groep te verbeteren en te borgen is de taskforce Bestuur en informatieveiligheid dienstverlening ingericht. Voor de komende twee jaar gaat deze taskforce de ministeries, uitvoeringsorganisaties, gemeenten, provincies en waterschappen bijstaan bij het verbeteren van hun bewustzijn van informatieveiligheid. [TK 26643, nr. 280]*

Als we de gekozen vergelijking doorzetten zou de aanhef, overgezet naar het wegverkeer zo kunnen komen te luiden:

> *Het vervoer moet goed beveiligd te zijn. De lessen van 9/11 (2001), maar ook de brand in de Mont Blanc tunnel (1999), en de treinbommen in Spanje (2004) laten zien dat het beveiligen van verkeersroutes en de beschikbaarheid van vervoersdiensten urgent en blijvend op de agenda moeten staan. Bestuurders en topmanagers in het openbaar bestuur moeten zich hiervan bewust zijn.*

Een dergelijke paragraaf gaan we waarschijnlijk als het gaat om verkeersveiligheid niet snel in het echt tegenkomen, omdat we het vanzelfsprekend vinden dat de overheid allang grote aandacht heeft, heeft gehad en zal blijven hebben voor het beveiligen van verkeersroutes en de beschikbaarheid van vervoersdiensten.

Wat uit deze exercitie zou kunnen worden afgeleid is dat leidinggevende bestuurders eigenlijk niet goed weten wat onder informatieveiligheid te verstaan, wat het maatschappelijk en economisch belang ervan kan zijn en waar de verantwoordelijkheden liggen wanneer de openbare infrastructuur om veilig te transigeren wegvalt of wordt gecorrumpeerd. Of, zoals de Onderzoeksraad voor veiligheid het in de ondertitel van het rapport over het Diginotar-drama, uitdrukte: digitale veiligheid bereikt de bestuurstafel te weinig. Op zichzelf is dit een eerste risico.[57]

Risico IV. Het bestuur weet niet goed wat informatieveiligheid is, wat het maatschappelijk en economisch belang ervan kan zijn en waar de verantwoordelijkheden liggen als het echt mis gaat.

Het DigiD-drama

Misschien is het zo, dat het om een zo ingewikkeld vraagstuk gaat dat we nauwelijks van bestuurders kunnen verwachten dat ze er voldoende van

57. Onderzoeksraad voor Veiligheid (2012).

weten. Misschien is het goed om ten aanzien van die onzekerheid, en over de bijbehorende bestuurlijke dynamiek een paar kengetallen te noemen: Het zo-even genoemde kamerstuk heeft dossiernummer TK 26 643, nr. 280 en is, als gezegd van 13 mei 2013. Op 24 december 2015 had dit kamerdossier nr. 382 bereikt. Er zijn dus in 32 maanden 103 kamerstukken aan ICT gewijd, waarvan er niet minder dan 53 gaan over informatiebeveiliging of DigiD/eID (of beide). Er waren daarbij meer dan 27 bijlagen bijgevoegd, de meeste daarvan in de vorm van omvangrijke rapportages. Als er iets uit deze getallen kan worden afgeleid is het wel dat het ófwel om een onmogelijk complexe materie gaat, ófwel over een materie die als onmogelijk complex wordt voorgesteld. In zijn visiebrief bevestigt de bewindspersoon dit met het understatement dat '*[t]echnologische expertise [..] schaars en duur is*'.[58] Dit leidt tot een verzwaring van het eerdergenoemde risico:

Risico V. Voor bestuurders is de materie (veel te?) ontoegankelijk en bewerkelijk

---

En dat houdt in dat van bestuurders zou moeten worden gevraagd veel tijd en aandacht te investeren in het beter leren kennen en doorgronden van de materie. Wanneer dat achterwege wordt gelaten zouden deze twee risico's tot heel eigenaardige gevolgen kunnen leiden, tenminste vanuit een traditioneel bestuursrechtelijk perspectief. We nemen het DigiD-drama als voorbeeld.

We ontlenen daarbij onze beschrijving aan de managementsamenvatting van het rapport dienaangaande van Fox IT:

> *DigiNotar B.V. was founded as a privately-owned notarial collaboration in 1998. DigiNotar provided digital certificate services as a Trusted Third Party and hosted a number of Certificate Authorities (CAs) [...]. The services that DigiNotar provided included […] issuing accredited qualified certificates that could be used as the legal equivalent of a handwritten signature … for various Dutch eGovernment purposes. In June and July of 2011 DigiNotar suffered a breach, which resulted in rogue certificates being issued that were subsequently abused in a large scale attack in August of 2011.*
>
> *Following the detection of the breach on July 19 of 2011 […] On August 28, 2011, the content of a rogue wildcard certificate for the google.com domain was posted publicly, which had been issued by DigiNotar but which had not yet been revoked. For weeks the rogue certificate had been abused in a large scale Man-In-The-Middle (MITM) attack on approximately 300,000 users that were almost exclusively located in the Islamic Republic of Iran […]*

58. *Kamerstukken II* 2013/2013, 26 643, nr. 280, p. 7.

> *The investigation by Fox-IT showed that all eight servers that managed Certificate Authorities had been compromised by the intruder[…] While the approach to protecting the potential targets from this type of intrusion does not differ significantly from other threats, the range of scenarios that need to be taken into account is rapidly expanding.*

Het gaat om een serieus probleem. De digitale identiteit van de Nederlandse overheid is gecorrumpeerd en is vermoedelijk in handen van een buitenlandse geheime dienst (in hackerskringen worden zowel die van de USA als die van Iran genoemd[59]). Een ernstiger vertrouwensbreuk als gevolg informatie-onveiligheid van het digitale verkeer met, en onder de hoede van, de Nederlandse overheid is nauwelijks denkbaar.

Het gaat om een kwetsbaarheid waarvan het misbruik onmiddellijk had moeten zijn opgemerkt, en waarover de alarmbellen onmiddellijk hadden moet klinken om de schade zoveel mogelijk te beperken. Dat is niet gebeurd. Eerst heeft Diginotar (zonder succes) geprobeerd de zaak zelf te regelen en vervolgens heeft de Nederlandse overheid erop aangedrongen om de daartoe ingerichte protocols nog even buiten werking te houden omdat anders het digitale verkeer met de Nederlandse overheid teveel schade zou ondervinden.[60] Dit optreden werd (en wordt) overigens niet als het welbewust negeren van veiligheidsprotocols gepresenteerd, maar als een adequaat en doortastend optreden van onze overheid in een noodsituatie die wordt verondersteld niet aan haar te kunnen worden toegerekend. Het wordt tijd om met het DigiD-drama in het achterhoofd enkele van onze vragen puntsgewijs af te lopen.

– Wie zorgt voor een communicatie-infrastructuur waarover een geoefende en oplettende gebruiker veilig kan communiceren? De betreffende communicatie-infrastructuur was internet. Die wordt aangeboden en verzorgd door het bedrijfsleven over een publiek netwerk. Netwerk en infrastructuur functioneerden prima.
– Wat bedoelen we dan met infrastructuur? Infrastructurele diensten zijn diensten die een platform vormen voor inhoudelijke diensten en zijn als zodanig zelf weer een infrastructuur. Dat kan dus in verschillende lagen. In dat licht bieden niet alleen internet, TCP/IP en DNS infrastructurele diensten, ook Google, Facebook en Twitter doen dat, voorts is de Diginotardienst waarbij certificaten worden uitgegeven eveneens een infrastructurele dienst (voor veilig transigeren over internet), net als de dienst (in casu van Microsoft) die de besmette certificaten had moeten intrekken.
– Wie zorgt voor de relevante infrastructurele dienst waarover een geoefende en oplettende gebruiker veilig met overheidsdiensten kan com-

59. Aldus blijkt bijvoorbeeld uit de wikipedia-pagina's over 'Hack bij DigiNotar', https://nl.wikipedia.org/wiki/Hack_bij_DigiNotar (laatst geraadpleeg 21 december 2015).
60. Zie Dirkx (2012), beschikbaar onder kenmerk RAD/2012/161 op www.overheid.nl. Het bevestigt veel van onze *misgivings*.

municeren? De betreffende infrastructurele dienst identificeert overheidsdiensten als overheidsdienst op internet. Diginotar is de private partij die de dienst levert.
- Wie is civielrechtelijke aansprakelijk voor welke gevolgschade van een fout in de relevante infrastructurele dienst? Dat is afhankelijk van contracten, algemene voorwaarden en exoneratieclausules tussen de dienstaanbieders en de afnemers.
- Wie is bestuursrechtelijk aansprakelijk voor welke gevolgschade van een fout in de relevante infrastructurele dienst? Dat is afhankelijk van de vraag of het civielrechtelijk 'outsourcen' van de infrastructurele dienst die betrouwbaar transactieverkeer met de overheid mogelijk moet maken door een bestuursrechtelijke bril een zorgvuldig besluit kan worden genoemd. Van belang zal daarbij kunnen zijn in hoeverre gebruikers als belanghebbenden tegen zo'n outsourcingsbesluit zouden kunnen opkomen.
- Wie is politiek aansprakelijk voor welke gevolgschade van een fout in de relevante infrastructurele dienst? Dat is afhankelijk van de vraag hoe het corrumperen van de veilige infrastructuur voor betrouwbaar transactieverkeer met de overheid onder de politieke verantwoordelijkheid van de betreffende minister wordt geoordeeld.

We menen dat het DigiD-drama laat zien dat (1) de politieke aansprakelijkheid geen vorm kreeg (Donner kon geruisloos afmarcheren naar de Raad van State),[61] dat (2) de bestuursrechtelijke aansprakelijkheid niet werd beproefd ten tijde van het outsourcingsbesluit door partijen die later direct werden getroffen door het tijdelijke uitvallen van de infrastructuur en dat (3) de civielrechtelijke aansprakelijkheid is vervaagd in het faillissement van Diginotar en dat (4) de (mogelijke) schade die werd geleden door Iraniërs wier vertrouwelijke berichtenverkeer door hun geheime dienst werd onderschept zich aan ons blikveld onttrekt.

We menen dat hiermee enkele belangrijke risico's zijn aangestipt:

Risico VI. De politieke en bestuursrechtelijke aansprakelijkheid rond informatiebeveiliging en eID is niet eenvoudig te realiseren

---

Wat hier een rol lijkt te spelen is de mate waarin beveiligingstechniek voor bestuurders en ambtenaren als een belemmering wordt ervaren om duidelijk stelling te nemen en aansprakelijkheden toe te delen en te aanvaarden. Mogelijk wordt gezichtsverlies gevreesd. Het lijkt erop dat onze bestuursrechtelijke gewoontes en cultuur niet zijn opgewassen tegen de tendens om

61. Inmiddels is de Minister van BZK op grond van art. X van de Wet elektronisch berichtenverkeer belastingdienst jo. art. 6 van de Regeling voorzieningen GDI verantwoordelijk voor de veiligheid en betrouwbaarheid van o.a. MijnOverheid.nl en DigiD.

gezag te ontlenen aan technologische scholing in plaats van aan de waarneming en duiding van maatschappelijke verhoudingen. We menen dat de bedorven verhoudingen tussen bestuursdiensten en de ICT-sector, zoals die aan het licht treden in de voortdurende reeks mislukkende ICT-projecten die door overheidsdiensten worden aanbesteed,[62] een aanwijzing zijn voor hoe moeilijk het kennelijk is om hierin verbetering aan te brengen.

Risico VII. De bestuursrechtelijke zorgvuldigheid bij (naar achteraf blijkt) relevante besluiten kon niet (of nauwelijks) ter discussie worden gesteld op het geëigende moment.

Dit vierde risico lijkt ons mede een gevolg van hoe het bij het verhelderen van politieke verantwoordelijkheid is misgelopen (als boven aangegeven). In een zich op basis van technologische innovatie voortdurend specialiserende wereld is het onvermijdelijk dat besluiten worden genomen over wat wel en wat niet kan worden geoutsourced aan het gespecialiseerde bedrijfsleven (of kan worden ondergebracht in een bijzondere civielrechtelijke organisatievorm waarin het bedrijfsleven en het bestuur samenwerken). Daarbij moet steeds de vraag onder ogen worden gezien of het besluit tot outsourcen een bestuursrechtelijk besluit is dat dient te voldoen aan de eisen die de Awb daaraan stelt – en zo ja, of die zorgvuldigheid tot uitdrukking komt in de arrangementen die rond dat besluit worden bepaald. En ook moet daarbij worden nagedacht over wie als belanghebbenden kunnen gelden en van het voorgenomen besluit op de hoogte worden gesteld c.q. in staat moeten worden gesteld hun visie te geven.

Risico VIII. De civielrechtelijke risico's rond informatiebeveiliging kunnen vergaand worden geminimaliseerd via exoneratieclausules

---

Als het derde en vierde risico zich hebben laten gelden kan dit vijfde risico, dat immers een standaardvorm is waarin de civielrechtelijke aansprakelijkheden tussen ondernemingen worden geregeld, het lek vormen waardoor aansprakelijkheden en verantwoordelijkheden weglopen.

4.2 DDoS aanvallen en botnets

Het komt ons voor dat we in het kader van bestuursrechtelijke risico's rond informatiebeveiliging moeilijk voorbij kunnen gaan aan wat DDoS aanvallen worden genoemd. Het gaat dan om via botnets uitgevoerde aanvallen, gelijktijdig, als het tegenzit door honderdduizenden gehackte machines, op

62. *Kamerstukken II* 2014/15, 33 326, nr. 5. www.tweedekamer.nl/sites/default/files/field_uploads/33326-5-Eindrapport_tcm181-239826.pdf

een doelwit waarvan, daardoor, de communicatiecapaciteit wordt verlamd, soms voor langere tijd.

Een overheid die de ambitie heeft om 'alles digitaal te gaan doen' moet zijn houding bepalen ten aanzien van deze risico's. De causale keten die dergelijke risico's in het leven roept begint bij een kwaadwillende. De activiteiten van zo een kwaadwillende zijn weliswaar strafrechtelijk te kenmerken, maar daarmee is het risico op de verstoring van de door de overheid gebruikte informatie-infrastructuur niet uitgebannen. Opnieuw doet zich de vraag voor naar de bestuurlijke zorgvuldigheid van de digitale overheden die besluiten om hun toegankelijkheid en vermogen tot dienstverlening geheel laten verlopen via een infrastructuur waarvan de kwetsbaarheid (via aanvallen van botnets) reëel is en van tevoren als zodanig vaststaat, vooralsnog zonder uitzicht op een effectieve oplossing.

De tweede schakel in de causale keten wordt gevormd door de individuele computergebruikers die met behulp van malware worden gehackt en waarvan de gehackte (gekaapte) computers worden gebruikt om de aanvallen uit te voeren. Mogelijk zou het aantal computers dat kan worden gehackt worden beperkt door eisen te stellen aan de vaardigheden van wie aan het digitale verkeer deelnemen. Die weg naar een oplossing lijkt evenwel om veel redenen onhaalbaar. Van belang zijn hier bijvoorbeeld de vaststelling dat de doorsnee homo digitalis wél de vaardigheden heeft om apparatuur en programmatuur effectief te gebruiken, maar onvoldoende om die te kunnen beschermen tegen hacking en malware infecties. Daarbij komt dan dat beschermingsmaatregelen tegen hacking en malware onvermijdelijk een beperking inhouden van (en daarmee: een *chilling effect* kunnen hebben op) verworven informatievrijheden (zoals rechten op toegang tot informatie en de vrijheid van meningsuiting). We menen dat, ook gelet op de maatschappelijke discussie rond filteren van het internet, het van belang is vast te stellen dat het politieke klimaat rond grondrechtelijke informatievrijheden vooralsnog het verplicht stellen van essentiële beheersvaardigheden en beheerstaken onmogelijk maakt.[63] Ook dit is een risico.

Risico IX. Het voor een verantwoord gebruik van de digitale overheidsdienstverlening vereiste niveau van digitale beheervaardigheden wordt de facto niet gehaald, en kan ook niet worden geëist van de offline burger omdat dat in strijd wordt geacht met verworven informatievrijheden.

Risico X. Dit impliceert een risico voor hacking en botnets en daarmee ook voor de informatieveiligheid van communicatie tussen burgers en overheden en tussen overheden onderling.

---

63. En één van de andere redenen die hier een rol zouden kunnen spelen wordt misschien wel – vergeef ons dit wantrouwen – gevormd door de voordelen die door opsporingsdiensten worden ervaren wanneer informatiediensten niet al te sterk zijn beveiligd.

Juist die onhaalbaarheid leidt ertoe dat we ons zullen moeten zien te redden in een wereld waarin een hoge vorm van informatieveiligheid vooralsnog niet bestaat. De voortdurende reeksen van onthullingen van via hacking of phishing illegaal en illegitiem verkregen verzamelingen creditcard- en logingegevens ondersteunt deze stelling. Er is bovendien inmiddels een beveiligingsindustrie ontstaan die rond het opsporen en vervolgens verhelpen van zogenoemde *vulnerabilities* zijn eigen infrastructurele diensten aanbiedt, een industrie die er onder de huidige condities dan ook geen belang bij heeft dat het aantal vulnerabilities volledig verdampt.
Overigens, veelal wordt als vanzelfsprekend aangenomen dat de risico's rond digitale beheervaardigheden voor de online bestuurder niet bestaan. Het DigiD-drama, en naar wij menen ook de extreem hoge faalpercentages van ICT-projecten van de overheid,[64] laten echter zien dat het geenszins om een bagatelrisico gaat.

Tenslotte. Een zeer voor de hand liggende aanpak van het als zesde genoemde risico kan erin worden gevonden om de zorg voor beheerkritische taken over te dragen aan infrastructurele dienstverleners.[65] Die tendens wordt al wel zichtbaar (bijvoorbeeld bij DigiD), met name waar het gaat om diensten die worden verwezenlijkt via wat de 'cloud' wordt genoemd. Maar clouddiensten leiden weer tot nieuwe risico's die samenhangen met asymmetrieën die de informatieverhoudingen op geheel eigen wijze kunnen verstoren. Een overheidsdienst die een infrastructurele beheerdienst uitbesteedt (outsourcet), bindt zich aan de eisen die de dienst stelt. Dat hoeft niet altijd overeen te stemmen met autonome taakvervulling. En bovendien: hierbij dient zich weer het risico aan van machtsmisbruik jegens de overheid door de dienstverlener, als randverschijnsel van het outsourcen aan clouddiensten door het bestuur. Dit risico is nog niet helder te duiden. Daarvoor is het op het moment nog te onzeker hoe de risico's van *lock-in* en van bijbehorende kennisasymmetriën tussen opdrachtgevende bestuursdiensten en technisch geavanceerde dienstverleners kunnen worden begrepen en beheerst. Gelet op wat over grote overheidsprojecten op het gebied van de ICT boven tafel komt zijn we er niet erg gerust op.[66]

64. Kamerstukken II 2014/15, 33 326, nr. 5. http://www.tweedekamer.nl/sites/default/files/field_uploads/33326-5-Eindrapport_tcm181-239826.pdf
65. Maar het betreffende risico is ook civielrechtelijk geen bagatelrisico. Per 21 september 2015, bijvoorbeeld, werd ons vertrouwen in hoogwaardige beheervaardigheden bij belangrijke commerciële infrastructurele diensten ernstig geschaad. Toen werd bekend dat door een hack in veelgebruikte ontwikkelsoftware (die wordt gebruikt om iOS apps (Apple apps) te bouwen) de gebouwde apps worden/werden voorzien van een zogenoemde 'back doors.' De hack heeft geruime tijd ongemerkt zijn gang kunnen gaan.
66. Zie voor de ICT-faalprojecten bij de rijksoverheid weer: Kamerstukken II 2014/15, 33 326, nr. 5. http://www.tweedekamer.nl/sites/default/files/field_uploads/33326-5-Eindrapport_tcm181-239826.pdf en voor de ICT-problemen bij lokale overheden de berichtgeving in NRC, zoals: D. Stokmans, 'PinkRoccade en Centric misbruiken marktmacht' en 'Gegijzeld door de softwareboer' NRC 17 oktober 2015.

4.3 Samenvatting

De transitie naar gedigitaliseerd bestuur (en de evolutie naar de homo digitalis) wordt zichtbaar in de wijzigingen die optreden in het verwezenlijken van betrouwbare communicatie. Daarbij zijn van belang een veilige communicatie-infrastructuur en betrouwbare mechanismen waarmee de identiteit van de deelnemers kan worden vastgesteld en bevestigd. Dat blijken in de digitale wereld ingewikkelde en ook organisatorisch moeilijk te realiseren vereisten te zijn.[67]
We vatten weer samen met behulp van de gesignaleerde risico's.

Risico IV. *Professioneel bestuur op basis van onwetendheid.* Het bestuur weet niet goed wat informatieveiligheid is, wat het maatschappelijk en economisch belang ervan kan zijn en waar de verantwoordelijkheden liggen als het echt mis gaat.

Risico V. *Complexiteit van materie*. Voor bestuurders is de materie (veel te?) ontoegankelijk en bewerkelijk

Risico VI. *Bestuurlijke aansprakelijkheid glipt weg.* De politieke en bestuursrechtelijke aansprakelijkheid rond informatiebeveiliging en eID is niet eenvoudig te realiseren

Risico VII. *Bestuurlijke zorgvuldigheid post hoc.* De bestuursrechtelijke zorgvuldigheid bij (naar achteraf blijkt) relevante besluiten kon niet (of nauwelijks) ter discussie worden gesteld op het geëigende moment.

Risico VIII. *Exoneratievergiet*. De civielrechtelijke risico's rond informatiebeveiliging kunnen vergaand worden geminimaliseerd via exoneratieclausules

Risico IX. *Beheervaardigheid is informatiefiltering*. Het voor een verantwoord gebruik van de digitale overheidsdienstverlening vereiste niveau van digitale beheervaardigheden wordt de facto niet gehaald, en kan ook niet worden geëist van de burger, omdat dat in strijd wordt geacht met verworven informatievrijheden.

Risico X. *Informatievrijheid impliceert botnets*. Dit impliceert een risico voor hacking en botnets en daarmee ook voor de informatieveiligheid van communicatie tussen burgers en overheden en tussen overheden onderling.

Informatieveiligheid is dus moeilijk en ingewikkeld, zeker ook als het gaat om infrastructurele informatiediensten waarmee burgers en bestuurders zichzelf in een digitale omgeving identificeren en authentiseren. Voldoende ervan weten is voor bestuurders en voor burgers vaak een brug te ver. Als gevolg is er vanuit de bestuurszijde nogal eens een streven, meestal effectief, gericht op het minimaliseren van verantwoordelijkheden. De besluiten van de digitale overheden om werkzaamheden of verantwoordelijkheden uit te besteden (outsourcing) zijn zelden bij belanghebbenden bekend en worden niet steeds ingebed in een praktijk van continu, toereikend toe-

67. In aanvulling op het DigiD-drama openbaren zich op het moment van schrijven twee corruptieschandalen rond handel in politiële informatie en in douane-autorisaties – en het aantal ontdekte corruptiegevallen bij de politie baart zorgen, meldt de NOS (http://nos.nl/artikel/700526-politie-verdacht-van-corruptie.html) .

zicht. Als gevolg wordt de schade die kan ontstaan door misbruik van onveilige infrastructurele diensten doorgaans op de burger afgewenteld – we zagen dat al in hoofdstuk 3 van dit preadvies. Opmerkelijk is dat beheerkennis bij zowel burger als bestuurder achterblijft, wat de kans op onveilige infrastructuren doet toenemen (botnets), en/of de autonomie van de overheid bij outsourcecontracten aan (onwenselijke) beperkingen kan binden. Het lijkt erop dat de risico's van onveilige infrastructuren in de huidige bestuursrechtelijke praktijk niet transparant zijn en dus evenmin effectief kunnen worden beheerst.

5. Overheidsgegevensgebruik

5.1 Het gebruik van digitale gegevens binnen en door de overheid

In de visiebrief wordt uiteengezet dat de digitale overheid meer en beter gebruik moet gaan maken van de beschikbare digitale gegevens. Dit omdat – we parafraseren de brief – het voor de burger onbegrijpelijk is dat hij of zij aan de overheid elke keer dezelfde gegevens moet doorgeven. En ook omdat overheidsorganisaties niet aansluiten bij gemeenschappelijk ontwikkelde voorzieningen, zoals de basisregistraties en MijnOverheid, wat onnodig veel tijd en ergernis kost en voor de overheid als geheel onnodig ook nog eens duur is.[68]

Voor Plasterk gaat het dus om het vergroten van het gebruiksgemak voor de burger en het efficiënter en betrouwbaarder maken van de overheidsbedrijfsvoering. De overheid moet de burger niet steeds weer dezelfde gegevens vragen. De burger verwacht 'één overheid' en 'daarbij hoort eenduidigheid en hergebruik van generieke voorzieningen'. Ook om redenen van consistentie, veiligheid en stabiliteit is het beter als binnen de overheid gebruik wordt gemaakt van dezelfde voorzieningen en infrastructuur, basisregistraties en gegevensuitwisseling.

Het gaat echter niet alleen over gebruiksgemak, efficiëntie, betrouwbaarheid en kostenbesparingen. Andere kamerstukken laten zien dat het verbeteren van het overheidsgegevensgebruik ook wordt gerelateerd aan controle en toezicht op burgers, en andere meer repressieve doelstellingen. Het meer en beter gebruik maken van digitale gegevens moet ook worden bezien in het kader van het mogelijk maken van gegevensuitwisseling, tussen overheden en met private partijen, om toe te zien op de naleving van allerlei wet- en regelgeving. Het gaat dan, bijvoorbeeld, om de bestrijding van belastingfraude en het tegengaan van misbruik en oneigenlijk gebruik van overheidsvoorzieningen en -toeslagen, en allerlei andere vormen van fraude en criminaliteit, zoals daar zijn: illegale hennepteelt, vastgoedfrau-

68. *Kamerstukken II* 2013/2013, 26 643, nr. 280, p. 7.

de, verzekeringsfraude, zorgfraude, alsmede milieucriminaliteit, cybercrime en voertuigcriminaliteit, zelfs snelheidsovertredingen.

Vaak vindt deze gegevensuitwisseling plaats binnen samenwerkingsverbanden van overheden en anderen. De bedoeling is dat de gegevens waarover ieder van de deelnemers beschikt met elkaar in verband kunnen worden gebracht voor gemeenschappelijke analyses. Wat daarbij als praktisch probleem wordt opgevat is dat de onderliggende wetgeving, op basis waarvan de onderscheiden deelnemers over de relevante gegevens kunnen beschikken, in veel gevallen eraan in de weg staat dat deze gegevens kunnen worden gedeeld met andere deelnemers aan het samenwerkingsverband. Om dit op te lossen wordt een Kaderwet gegevensuitwisseling voorgesteld. Er moet daarmee worden voorzien in een generieke grondslag voor de gegevensverstrekking aan samenwerkingsverbanden en mogelijk maken dat gebruik kan worden gemaakt van 'moderne analysetechnieken als datamining en profiling'. En daarmee kan bijvoorbeeld een lijst worden gegenereerd van de personen ten aanzien waarvan wordt vermoed dat er sprake is van een bijzonder groot risico dat zij fraude plegen. Of, het staat er echt, dat zij vermoedelijk *gaan* plegen.[69]

5.2 De Kaderwet gegevensuitwisseling

Er is nog geen Kaderwet gegevensuitwisseling, en omdat daarop nogal wat kritiek is geuit,[70] moeten we nog zien of die er in de vorm die is voorgesteld gaat komen. Met de inwerkingtreding van het SyRI-besluit[71] op 12 september 2014 is er wel al de mogelijkheid dat gemeentebesturen, bestuursorganen of sociale zekerheids- of belastingtoezichthouders een samenwerkingsverband aangaan dat is gericht op het voorkomen en bestrijden van onrechtmatig gebruik van overheidsvoorzieningen op het terrein van de sociale zekerheid en inkomensafhankelijke regelingen en

69. In de brief waarin de verkenning van de Kaderwet gegevensuitwisseling aan de Tweede Kamer wordt aangeboden (*Kamerstukken II* 2014/15, 32 761, nr. 79) wordt inderdaad gezinspeeld op 'predictive policing', getuige deze opmerkingen: "*[Er is] het voornemen een profiel van beroepsfraudeurs te ontwikkelen, maar zou het zo'n profiel op basis van de huidige wetgeving niet kunnen matchen met alle data waarover zij rechtmatig de beschikking heeft. Hierdoor kan er geen lijst gegenereerd worden van personen met een bijzonder groot risico dat zij fraude (gaan) plegen.*" In de fiscale vakliteratuur werden al eerder methodes besproken gericht op het 'construeren van patronen op basis van (potentiële) toekomstige gedragingen' en het 'conceptualiseren van toekomstige noncompliante gedragspatronen', zie: Berkhout en Van Engers (2012). In één en ander zien we hoe enthousiast wordt voorgesorteerd op de donkere science fiction wereld van Steven Spielberg's Minority Report (Dreamworks SKG/20th Century Fox 2002).
70. Zie bijv. de brief van het Cbp aan de Minister van Veiligheid en Justitie van 25 februari 2015, kenm. z2015-00155; Martijn en Goslinga (2015).
71. Besluit van 1 september 2014 tot wijziging van het Besluit SUWI in verband met regels voor fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens met inzet van SyRI, *Stb*. 2014, 320.

dergelijke. In het kader van dit samenwerkingsverband kunnen op grond van het SyRI-besluit maar liefst zeventien categorieën van gegevens (zoals: arbeidsgegevens, detentiegegevens, gegevens over roerende en onroerende goederen, inburgeringsgegevens, nalevingsgegevens, onderwijsgegevens, pensioengegevens, re-integratiegegevens, schuldenlastgegevens, etc.) worden gekoppeld en vervolgens geanalyseerd, om zogeheten 'risicomeldingen' te genereren.[72]

Zo een risicomelding geeft aan dat een rechtspersoon of een natuurlijk persoon 'onderzoekswaardig' wordt geacht in het licht van de doelstellingen van het betrokken samenwerkingsverband.[73] De gegenereerde risicomeldingen worden aan de betreffende bestuursorganen en personen van het samenwerkingsverband verstrekt, voor zover deze voor hen relevant zijn. Op verzoek kunnen de risicomeldingen ook worden verstrekt aan het OM en de politie, voor zover dat noodzakelijk is voor de uitvoering van hun wettelijke taken.[74]

Voor de homo digitalis betekent dit dat de analyses die eerst niet konden worden gedaan, of alleen grotendeels handmatig in een beperkt aantal specifieke gevallen en waarschijnlijk alleen door een beperkt aantal deskundigen, als gevolg van digitalisering nu met aanmerkelijk minder moeite en veel vaker kunnen worden gedaan. Een door de Raad van State aangeduid risico daarbij is dat de categorieën van te verwerken gegevens nogal ruim en veelomvattend zijn omschreven en diep kunnen ingrijpen in iemands persoonlijke levenssfeer: "*De opsomming van gegevens is weliswaar*", zo zegt het adviescollege het in zijn advies over het ontwerpbesluit, "*bedoeld om de gegevensverwerking in te perken (dataminimalisatie), maar is in feite zo ruim dat er nauwelijks een persoonsgegeven te bedenken is dat niet voor verwerking in aanmerking komt.*" Dat is nogal wat. Ook al wordt bij ieder afzonderlijk project en samenwerkingsverband nader bepaald welke gegevens daarvoor nodig zijn, dan nog is daarmee het risico van sleepnet-acties (*fishing expeditions*) helemaal niet weggenomen.[75]

72. Art. 5a.1, derde lid, onder a t/m q, Besluit SUWI, het gaat in alfabetische volgorde om achtereenvolgens: arbeidsgegevens, gegevens inzake bestuursrechtelijke maatregelen en sancties, detentiegegevens, fiscale gegevens, gegevens over roerende en onroerende goederen, handelsgegevens, huisvestingsgegevens, identificerende gegevens, inburgeringsgegevens, nalevingsgegevens, onderwijsgegevens, pensioengegevens, re-integratiegegevens, schuldenlastgegevens, uitkerings- toeslagen- en subsidiegegevens, vergunningen en ontheffingen, en zorgverzekerings-gegevens. Zie daarover T, Wieringa (2015).
73. NvT bij SyRI-besluit, *Stb.* 2014, 320, p. 14, 21-24.
74. Zie resp. art. 65, derde lid, onderdelen a en b, Wet SUWI; NvT bij SyRI-besluit, *Stb*. 2014, 320, p. 15
75. Advies Raad van State, nr. W12.14.0102/III, 's-Gravenhage, 15 mei 2014, *Stcrt*. 2014, nr. 26306.

Het Nader Rapport bij het besluit gaat daarop wel in maar stelt niet gerust. Er wordt opgemerkt dat de desbetreffende gegevens op grond van andere regelingen ook al aan gemeenten of UWV en Svb moeten worden verstrekt[76] en dat het niet wenselijk is om op voorhand gegevens uit te sluiten, omdat SyRI-projecten zich kunnen richten op verschillende thema's. De vereiste dataminimalisatie[77] moet worden gewaarborgd doordat de samenwerkingsverbanden die gebruik maken van SyRI geacht worden zelf te toetsen welke gegevens nodig zijn voor het welbepaalde en nadrukkelijk omschreven doel van de samenwerking, dat weer moet passen binnen de in de wet genoemde doelen van het tegengaan van onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen op het terrein van sociale zekerheid en inkomensafhankelijke regelingen, het bestrijden van belasting- en premiefraude en niet naleving van arbeidswetten.[78]

Al met al lijken de waarborgen die de wet biedt betrekkelijk. Een samenwerkingsverband dat gebruik wil maken van SyRI moeten binnen de ruime wettelijke kaders voor zichzelf de beperkingen stellen waarbinnen de gegevensanalyse mag plaatsvinden. En de vraag is dan natuurlijk of we erop kunnen vertrouwen dat deze samenwerkingsverbanden, die worden aangegaan om heel uiteenlopende vormen van fraude en misbruik te bestrijden, bereid zijn zichzelf daarbij inderdaad gebruiksbeperkingen op te leggen. Er is, menen wij, een risico dat deze samenwerkingsverbanden niet vanzelfsprekend geneigd zijn het belang van fraudebestrijding ondergeschikt te maken aan de bescherming van de persoonlijke levenssfeer van degenen over wie gegevens kunnen worden verwerkt. En dat is een risico dat toeneemt als deelnemers aan het samenwerkingsverband per saldo veel te winnen hebben, of denken te hebben, bij de analyse en maar weinig bij de bescherming van de persoonlijke levenssfeer.

Risico XI. Als het gaat om gegevensgebruik door en binnen de overheid is de wetgever maar in beperkte mate geneigd te voorzien in beperkingen met betrekking tot gegevensuitwisseling en gegevensanalyse.

Één en ander roept natuurlijk ook vragen op met betrekking tot rechtsbescherming van burgers, en meer in het bijzonder de waarborging van de onder meer in het Europees Handvest vastgelegde recht op gegevensbe-

76. O.g.v. resp art. 64 Wet werk en bijstand art. 54 Wet Structuur uitvoeringsorganisatie werk en inkomen.
77. Art. 11 Wbp.
78. Zie Nader Rapport, opgenomen bij de publicatie van Advies Raad van State inzake het ontwerpbesluit houdende regels voor fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens (Besluit SyRI), *Stcrt* 2014, nr. 26306.

scherming.[79] Ook is er de vraag in hoeverre de overheid voldoet aan de strenge voorwaarden die worden gesteld, en straks in de nieuwe Europese privacyregels[80] gaan worden gesteld, aan risicoprofilering. In haar bespreking van de verhoudingen tussen belastingdienst en digitale burger stelt Overkleeft-Verburg dan ook onomwonden dat "*de rechtmatigheid [van deze risicoprofilering] derhalve vooralsnog aan twijfel onderhevig [blijft]*".[81]

Risico XII. Als het gaat om gegevensgebruik door en binnen de overheid is de wetgever maar in beperkte mate geneigd rekening te houden met beperkingen verband houdend met fundamentele rechten en vrijheden, zoals die waarin het Europees Handvest voorziet.

Voor de digitale overheid is er daarmee het risico dat deze SyRI- en andere wetgeving, en de daarop gebaseerde gegevensuitwisselingssystemen en -arrangementen, geen stand blijken te kunnen houden.[82] Dat dit geen denkbeeldig risico is kan wellicht worden opgemaakt uit het voorbeeld van de Wet bewaarplicht telecomgegevens, die vanwege strijdigheid met artikel 7 en 8 van het Handvest buiten werking werd verklaard nadat het Hof van Justitie al eerder de daaraan ten grondslag liggende Richtlijn 2006/24/EC ongeldig had verklaard.[83] Een ander, recenter voorbeeld is de ongeldigverklaring van het Safe Harbor-besluit van de Europese Commissie op grond waarvan persoonsgegevens konden worden doorgegeven naar ondernemingen in de Verenigde Staten.[84]

Risico XIII. De wetgeving waarin te weinig rekening wordt gehouden met de bescherming van fundamentele rechten en vrijheden is kwetsbaar en loopt het risico door een rechter buitenwerking te worden gesteld. Voor de op basis daarvan gebouwde gegevensuitwisselingssystemen is dit een potentiële faalfactor.

Weer ander risico ligt in het vermoeden dat digitale bestuurders, binnen de door de wetgever toch al ruim gestelde kaders, de neiging hebben om de grenzen op te zoeken van wat toelaatbaar is, en daar nogal eens overheen gaan. Een voorbeeld daarvan zagen we bij de aanleg door de belastingdienst van een verzameling met de inkomensgegevens van alle huurders in Nederland ten behoeve van de uitvoering van de regeling met betrekking

79. Art. 8 van Handvest van de Grondrechten van de EU (2007/C 303/01), PbEG 2007, C 303/1.
80. Zie art. 20 van de General Data Protection Regulation (consolidated compromise text of December 15th, 2015).
81. Overkleeft-Verburg (2014), p. 318.
82. Zwenne and Steenbruggen (2015).
83 Resp. HvJEU 8 april 2014, C-293/12 en C-594/12 en vz Rb Den Haag, 1 maart 2015, ECLI:NL:RBDHA:2015:2498.
84 HvJEU 6 okotober 2015, C-362/14.

tot de inkomensafhankelijke huurverhoging in het kader van het tegengaan van scheefwonen. In de gegevensverzameling werden gemakshalve ook de gegevens opgenomen van huurders in de vrije sector die niet onder de regeling vallen.[85] Een ander voorbeeld zagen we in het gebruik van de gegevens die de ene overheidsorganisatie niet meer mag bewaren, maar die nog wel beschikbaar zijn bij een andere overheidsorganisatie, als in: de kentekengegevens die de politie na vier weken moet verwijderen, maar die de politie vervolgens nog wel zonder veel moeite kan verkrijgen bij de belastingdienst.[86]

In deze voorbeelden zien we dat er weinig betekenis wordt toegekend aan het beginsel van dataminimalisatie en het daarmee verband houdende uitgangspunt dat er selectie moet plaatsvinden voordat er wordt verzameld (*'select-before-you-collect'*). Alles wordt verzameld en pas dan wordt bezien wat door de desbetreffende overheid kan worden gebruikt. We hebben het dan over sleepnet-acties ('*fishing expeditions*'). En daarbij speelt ook het doelbindingsbeginsel, dat verlangt dat gegevens niet mogen worden verwerkt voor doeleinden die onverenigbaar zijn met het doel waarvoor ze zijn verzameld, geen rol van betekenis meer.

Risico XIV. Digitale bestuurders hechten weinig betekenis aan beginselen als select-before-you-collect en hebben weinig moeite met sleepnet-acties, als die effectief lijken om de door hen gestelde doelen te bereiken.

Waar gaat het naar toe? We kunnen ons een voorstelling proberen te maken van wat het voorgaande gaat betekenen in een wereld waarin exponentieel meer gegevens dan thans gaan worden vastgelegd, omdat er nu eenmaal steeds meer digitaal wordt gedaan en gemaakt (*datafication*).[87] De digitale sporen daarvan kunnen worden gebruikt, en gaan waarschijnlijk zonder nadere maatregelen ook inderdaad worden gebruikt door overheden die daarover kunnen beschikken op basis van bevoegdheden die zijn gemaakt in (en: voor) een offline wereld. We hebben het over de gegevens die zijn te vinden in de systemen die worden gebruikt voor wat wordt aangeduid als het internet-van-dingen (*Internet-of-Things* of *IoT*), smart-cities, quantified communities en dergelijke. Denk dan aan: de kwartierwaarden uit slimme energiemeters, huisthermostaatgegevens, locatiegegevens van smartphones, sensoren in de fietsenstalling, de sentimenten die zijn af te leiden uit social media, online boodschappenlijstjes, rijgedraggegevens uit autonavigatieapparaten en interconnected auto's, lichaamstemperatuur- en hartslaggegevens, 'wearables', etc.

85. Cbp Rapport Onderzoek Belastingdienst - aanpak scheefwonen, 5 februari 2014 te vinden via https://cbpweb.nl/nl/nieuws/cbp-belastingdienst-gebruikte-inkomensgegevens-strijd-met-de-wet (geraadpleegd 1 januari 2016).
86. Martijn (2014).
87. Mayer-Schönberger and Cukier (2013).

We kunnen dat niet los zien van de digitalisering ten behoeve van het verbeteren van de beschikbaarheid van overheidsinformatie en de bereikbaarheid van overheden (hoofdstuk 2 van dit preadvies). We denken daarbij bijvoorbeeld aan de digitale aangifte, bijvoorbeeld via een aangifte-app op tablet. Zo een digitale aangifte stelt de belastingdienst in staat om niet alleen te beschikken over de door aangifteplichtigen verstrekte gegevens, maar ook over gegevens betreffende de wijze waarop het digitale aangifteformulier is ingevuld. We kunnen dan denken aan de snelheid waarmee en de volgorde waarin de verschillenden vragen zijn beantwoord, de tijd die de beantwoording van bepaalde vragen heeft gekost, de verbeteringen die op verschillende momenten zijn aangebracht, het aantal toetsaanslagen per minuut, locaties waar het biljet werd ingevuld, het taalgebruik, etc. Voor een belastingdienst die uitgaat van 'een informatiegestuurde subjectgerichte handhavingsregie' en het streven om 'iedere belastingplichtige de behandeling te geven die hij verdient',[88] zijn daaruit ongetwijfeld bruikbare signalen af te leiden. Het is niet onaannemelijk dat er bij de belastingdienst op zijn minst de wens is van die signalen gebruik te maken bij de controle van de aangifte.[89]

Ook als we ons beperken tot de gegevens waarover de overheid nu al beschikt, of zonder al teveel moeite kan beschikken, is duidelijk dat de burger meer dan ooit te voren door de overheid wordt gekend, door middel van sms-perkeergegevens, trajectcontroles, ov-chipkaartgegevens, sociale media-berichten, smartphonelocaties, televisiekijkgedrag, etc. Een digitale overheid kan, als de wet of rechter daaraan geen beperkingen stelt, in niet eerder vertoonde mate inzicht hebben in haar digitale burgers. Omdat dit leidt tot meer mogelijkheden om gedrag van digitale burgers en ondernemingen te beïnvloeden of te sturen, kan dat op zichzelf, menen wij, als risico worden geduid. Er is sprake van een uitbreiding van (nieuwe) machtsinstrumenten en dwangmiddelen, zonder dat duidelijk is in hoeverre daar passende waarborgen tegenover staan.

Risico XV. Er komen heel veel meer gegevens beschikbaar die door digitale overheden kunnen worden gebruikt, en waarschijnlijk ook gaan worden gebruikt, om macht uit te oefenen over burgers en ondernemers, zonder dat duidelijk is of daar tegenover voldoende waarborgen staan.

5.3 Aftapdilemmas (of: de geheimhoudersgesprekkencasus)

De wijze waarop overheden het gebruik van de voor hen beschikbare gegevens inrichten leidt tot praktische problemen die binnen de huidige wette-

88. Martijn (2015).
89. Vgl. Berkhout en van Engers (2012); Martijn (2015).

lijke kaders niet goed oplosbaar lijken. Illustratief daarvoor zijn de gesprekken van degenen van wie de communicatie geheim moet blijven, de zogeheten geheimhouders zoals onder andere advocaten. In deze 'geheimhoudersgesprekkencasus' gaat het om het spanningsveld tussen enerzijds het belang van opsporingsinstanties en het openbaar ministerie om op grote schaal vertrouwelijke telecommunicatie te kunnen aftappen, en anderzijds het belang dat advocaten en andere geheimhouders hebben erop te kunnen vertrouwen dat hun communicatie niet wordt afgetapt en afgeluisterd. In het verlengde daarvan is er natuurlijk het belang van het openbaar ministerie dat steevast niet ontvankelijk wordt verklaard wanneer het strafdossier transcripts van geheimhoudersgesprekken bevat.[90]

Een praktisch probleem is dan het volgende. Voor geheimhoudersgesprekken is het zaak dat deze, in het geval van een overigens rechtmatige 'tap', worden weggefilterd, althans meteen worden verwijderd nadat deze zijn opgenomen. Maar om dat te kunnen doen moet uiteraard bekend zijn dat er inderdaad sprake is van zo een geheimhoudersgesprek. En om dat te weten te komen, moet ofwel het gesprek inhoudelijk worden verwerkt ofwel moeten de door advocaten gebruikte telefoonnummers bekend zijn gemaakt aan het openbaar ministerie. In Nederland is enkele jaren geleden voor de laatste oplossing gekozen.[91]

Risico XVI. Een fundamenteel risico is dan dat er een ontwikkeling is ingezet waarin degenen die aanspraak maken op geheimhouding of, in meer algemene zin bescherming van persoonlijke levenssfeer, dat alleen kunnen krijgen als zij zich als zodanig bekend willen maken.

En juist door die bekendmaking is er, zo wordt wel gevreesd, weer een risico dat aan die aanspraak voorbij wordt gegaan. Zo kan nu, omdat de geheimhoudnummers bekend zijn, onderzoek worden gedaan naar gebruiksprofielen van de betreffende dataretentiegegevens, iets wat voorheen voor het OM onmogelijk was. Ook wordt gericht afluisteren door de veiligheidsdiensten vergemakkelijkt. Dat deze vrees geen paranoïde fantasie hoeft te zijn blijkt uit enkele zaken die recent aan het licht kwamen.[92]

90. Rb Amsterdam 20 december 2007 ECLI:NL:RBAMS:2007:BC0685 http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2007:BC0685 .
91. College van Afgevaardigden van de Nederlandse Orde van Advocaten, Verordening van 1 april 2011, *Stcrt.* 2011, 6728. (Verordening op de nummerherkenning).
92. Zie brief van Pestman aan Plasterk d.d 8 april 2014 (kenm. Prakken D'Oliveira/AIVD) te vinden via: www.prakkendoliveira.nl/user/file/140408_-_kantoorklacht_aivd_(mp_-_prakken_doliveira).pdf (geraadpleegd 1 januari 2016). En vervolgens: Vzr. Rechtbank Den Haag 1 juli 2015, ECLI:NL:RBDHA:2015:7436 te vinden via http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2015:7436 (geraadpleegd 1 januari 2016) en daarover o.a: AIVD ging te ver in afluisteren advocaten' NRC 19 december 2014); 'AIVD luistert advocaten al jaren af' De Volkskrant 19 december 2014; 'Advocaten dagen staat om afluisterpraktijken AIVD' NRC 22 april 2014.

5.4 Samenvatting

De transitie naar gedigitaliseerd bestuur (en naar de homo digitalis) leidt ertoe dat naarmate transacties tussen overheid, ondernemers en burgers worden gedigitaliseerd de hoeveelheid digitaal beschikbare data in omvang zozeer toeneemt dat er wel van Big Data wordt gesproken. Zonder daaraan te willen meedoen kan toch worden vastgesteld dat de overheid als geheel gaat beschikken over steeds dekkender informatiesystemen die (gedrag van) burgers en ondernemers beschrijven. En dat de mogelijkheid bestaat om al die informatie te koppelen en te analyseren.

We vatten weer samen op basis van de gesignaleerde risico's.

Risico XI. ***Weinig wettelijke beperkingen***. Als het gaat om gegevensgebruik door en binnen de overheid is de wetgever maar in beperkte mate geneigd te voorzien in beperkingen met betrekking tot gegevensuitwisseling en gegevensanalyse.

Risico XII. ***Wetgever laat bestuur te vrij.*** Als het gaat om gegevensgebruik door en binnen de overheid is de wetgever maar in beperkte mate geneigd rekening te houden met beperkingen verband houdend met fundamentele rechten en vrijheden, zoals die waarin het Europees Handvest voorziet.

Risico XIII. ***Kwetsbare wetgeving***. De wetgeving waarin te weinig rekening wordt gehouden met de bescherming van fundamentele rechten en vrijheden loopt het risico buitenwerking te worden gesteld. Voor de op basis daarvan gebouwde gegevensuitwisselingssystemen is dit een potentiële faalfactor.

Risico XIV. ***Sleepnetpraktijken***. Digitale bestuurders hechten weinig betekenis aan beginselen als select-before-you-collect en hebben weinig moeite met sleepnet-acties, als die effectief lijken om de door hen gestelde doelen te bereiken.

Risico XV. ***Waarborgenerosie***. Er komen heel veel meer gegevens beschikbaar die door digitale overheden kunnen worden gebruikt, en waarschijnlijk ook gaan worden gebruikt, om macht uit te oefenen over burgers en ondernemers (offline, online en digitaal), zonder dat duidelijk is of daar tegenover voldoende waarborgen staan.

Risico XVI. ***Databeschermingparadox***. Een fundamenteel risico is dan dat er een ontwikkeling is ingezet waarin degenen die aanspraak maken op geheimhouding of, in meer algemene zin bescherming van persoonlijke levenssfeer, dat alleen kunnen krijgen als zij zich als zodanig bekend willen maken.

We vrezen dat op het moment met de digitalisering bij de overheid een *Quod Licet Jovi* cultuur opbloeit – d.w.z. een cultuur van de dubbele standaard, waarin de overheid zich niet aan de regels hoeft te houden die voor de anderen gelden. Dan gaat het om het zich niet of *contre coeur* storen aan informatiebeperkingen die beogen de burger en de ondernemer te beschermen. Onze vrees berust op het kennelijke appèl dat uitgaat van een logica

als gehanteerd door Fred Teeven bij de bonnetjesafaire: " … *Met de deal was overigens niets mis. Ook dat is gebeurd voor volk en vaderland …* "[93]

Deel III. BESCHOUWING

6. Evenwichtige informatieverhoudingen

6.1 Op zoek naar tegenwicht

Het gaat in deze bijdrage over digitalisering en de vraag wat dat betekent voor de verhoudingen van burgers en overheden. We hebben in de voorgaande drie hoofdstukken van dit preadvies een groot aantal risico's in kaart willen brengen en bespreken in dit hoofdstuk welke positiefrechtelijke middelen het bestuursrecht te bieden heeft om aan enkele ervan het hoofd te bieden, en of daaraan iets hapert. We vatten dit ruim op. We gaan het dus hebben over burgers en andere bestuurden (organisaties, ondernemingen etc.) die als gevolg van digitalisering een andere positie krijgen c.q. innemen ten opzichte van de gedigitaliseerde overheid. Ons uitgangspunt is daarbij dat het een taak van het bestuursrecht is om eraan bij te dragen dat die verhoudingen zich ook in tijden van digitalisering evenwichtig ontwikkelen, dat wil zeggen: op een wijze die past binnen de grenzen die worden gesteld door grondrechten en beginselen van behoorlijk bestuur.

In reactie op de door digitalisering versterkte informatiepositie van de overheid wordt in de visiebrief van Plasterk gepleit voor het versterken van de informatiepositie van de burger.[94] Vanuit de gedachte van machtsevenwichten is dat goed te volgen. De wijze waarop dit in de brief wordt ingevuld stelt evenwel, gelet op de mate waarin de informatiepositie van de overheid wordt versterkt, teleur. In de brief wordt ervoor gepleit dat burgers eenvoudig moeten kunnen zien welke gegevens over hen bij de overheid zijn vastgelegd en aan wie deze worden verstrekt. Verder moeten zij de mogelijkheid hebben om fouten te corrigeren. En dat moet worden gerealiseerd door burgers via MijnOverheid inzage te geven in de kerngegevens die overheden over hen vastleggen, met de mogelijkheid om online correcties door te geven. Er wordt aldus invulling gegeven aan het inzage- en correctierecht uit de Wet bescherming persoonsgegevens.[95]

Waarom is dit teleurstellend? Omdat het versterken van de informatiepositie van burgers en het bewaken van evenwichtige informatieverhoudingen in een tijd van digitalisering naar ons gevoel meer omvat dan het

93. Aldus redeneert de aftredende staatssecretaris nog op de persconferentie van 9 maart 2015.
94. *Kamerstukken II* 2012/13, 26643, nr. 280, p. 5.
95. Art. 35 en 36 Wbp.

invulling geven aan inzage- en verbeteringsrechten waarover burgers allang beschikken. Het gaat erom dat we informatieposities en -verhoudingen van burgers tegenover de overheid zinvol kunnen duiden in een bestuursrechtelijke context, met bijbehorende effectieve rechtsbescherming.

In onze rechtssystemen zijn die machtsevenwichten min of meer organisch gegroeid aan de hand van de verschillende verhaallijnen die zijn ingezet door onder andere Hobbes, Locke, Montesquieu en Rousseau. De machtsevenwichten hebben zich natuurlijk doorontwikkeld, ook onder invloed van niet-juridische, vooral natuurwetenschappelijke, biologisch-medische en economische – en laatstelijk misschien ook cultureel-religieuze verhalen. Een digitale overheid vraagt om de inpassing van een aanvullend verhaal over de betekenis van wijzigende informatieposities. Evenals onze opvattingen over grondrechten, individuele veiligheid en individuele vrijheid ontwikkelt het bestuursrecht zich. En dat kan, zoals alles, onder voldoende druk vloeibaar worden. Zijn er onder de risico's die we inventariseerden zorgenkinderen die bijdragen aan het opvoeren van die druk?

6.2 Zorgenkinderen

We vatten nog even samen wat we in het voorgaande hebben vastgesteld.

Risico's bij beschikbaarheid en bereikbaarheid

Risico I. Digibeten de dupe. Digitalisering met besparingsambities kan ertoe leiden dat een grote groep minder digivaardigen (offline burgers en ondernemers) *de facto* wordt uitgesloten
Risico II. Digitale dwangbuizen. Het risico is dat de toegang tot steeds essentiëler wordende diensten van de digitale overheid wordt beheerst door regelingen met maar weinig waarborgen voor de gebruikers van deze diensten (de burgers)
Risico III. Troebel in plaats van transparant. Een risico voor de homo digitalis is dat digitale overheden in hun verhouding met burgers en ondernemers zich weten te onttrekken aan checks and balances door selectief hen betreffende informatie in meer of mindere mate toegankelijk te maken.

De genoemde risico's spelen vooral doordat digitalisering en de kennis daarover niet resulteren in gradueel veranderende communicatieprocessen die we gemakkelijk kunnen leren kennen. Het gaat met horten en stoten en niet iedereen kan die bijbenen. Ook omdat digitalisering vormen van 'formulierdwang' met zich brengt die moet worden gehoorzaamd omdat anders de door de burger gezochte overheidsdienst buiten bereik blijft.

Welke bestuursrechtelijke rechtsbescherming geniet een minder digivaardige homo digitalis, wanneer zijn gemeente besluit alles digitaal af te handelen en om het gemeentehuis alleen nog op donderdagmiddag open te stellen voor publiek? Welke bestuursrechtelijke rechtsbescherming geniet

een burger of ondernemer tegen de vormgeving van digitale formulieren die – direct in strijd met de beginselen van behoorlijk bestuur – onnodige verplichtingen op onvoldoende transparante motieven opleggen? Welke rechtsbescherming en rechtsmiddelen hebben we als het gaat om de vormgeving van die formulieren? Moeten we voor deze dingen naar de Ombudsman?

Kortom: is het bestuursrecht voldoende toegesneden op de strubbelingen die de vergrote inzet van informatietechnieken in termen beschikbaarheid en bereikbaarheid met zich mee kan brengen? We menen van niet. Traditionele bezwaarschiftenprocedures lijken, metaforisch gesproken, op kanonnen gericht op muggen, terwijl het ongemoeid laten van de muggen een malaria-epidemie zou kunnen veroorzaken.

Risico's met informatieveiligheid

Risico IV. Professioneel bestuur op basis van onwetendheid. Het bestuur weet niet goed wat informatieveiligheid is, wat het maatschappelijk en economisch belang ervan kan zijn en waar de verantwoordelijkheden liggen als het echt mis gaat.

Risico V. Complexiteit van materie. Voor bestuurders is de materie (veel te?) ontoegankelijk en bewerkelijk

Risico VI. Bestuurlijke aansprakelijkheid glipt weg. De politieke en bestuursrechtelijke aansprakelijkheid rond informatiebeveiliging en eID is niet eenvoudig te realiseren

Risico VII. Bestuurlijke zorgvuldigheid post hoc. De bestuursrechtelijke zorgvuldigheid bij (naar achteraf blijkt) relevante besluiten kon niet (of nauwelijks) ter discussie worden gesteld op het geëigende moment.

Risico VIII. Exoneratievergiet. De civielrechtelijke risico's rond informatiebeveiliging kunnen vergaand worden geminimaliseerd via exoneratieclausules

Risico IX. Beheervaardigheid is informatiefiltering. Het voor een verantwoord gebruik van de digitale overheidsdienstverlening vereiste niveau van digitale beheervaardigheden wordt de facto niet gehaald, en kan ook niet worden geëist van de offline en online burger (wel van de online en digitale bestuurder?), omdat dat in strijd wordt geacht met verworven informatievrijheden.

Risico X. Informatievrijheid impliceert botnets. Dit impliceert een risico voor hacking en botnets en daarmee ook voor de informatieveiligheid van communicatie tussen burgers en overheden en tussen overheden onderling.

Genoemde risico's spelen vooral omdat het bewaken van informatieveiligheid en van een veilige digitale identificatie-infrastructuur veel kennis vraagt uit uiteenlopende, zich nog sterk ontwikkelende gebieden (bijv. informatica, organisatiekunde).

Wanneer we de Diginotar-kwestie of het DigiD-drama als casus nemen (en afzien van beschouwingen over politieke verantwoordelijkheid) gaat het er niet alleen om hoe een burger of ondernemer beschermd wordt tegen de nadelige gevolgen van bestuurlijk onzorgvuldig digitaal handelen, maar

ook om hoe het bestuur, burger en ondernemer worden beschermd tegen hacking door kwaadwillenden en criminelen. Deze vormen van rechtsbescherming zijn problematisch – ook omdat de technologisch-organisatorische complicaties omvangrijk zijn en meestal verhinderen dat causaliteit gemakkelijk aannemelijk kan worden gemaakt. Wie het slachtoffer is geworden van identiteitsfraude als gevolg van het DigiD-drama zal die oorzaak niet of moeilijk voldoende aannemelijk kunnen maken. Wie de oorzaak van veiligheidsfalen is of was zal zich daarvan doorgaans uit onwetendheid niet eens bewust zijn.

De vraag is dan, kortom, of het bestuursrecht voldoende is toegesneden op de strubbelingen die de vergrote inzet van informatietechnieken in termen van informatieveiligheid met zich mee kan brengen. We menen opnieuw van niet. Het lijkt te gaan om vragen die betrekking hebben op de praktijk van behoorlijk besturen, maar hun invloed hebben buiten de context van de besluitvorming door bestuurders. Het gaat om vereiste kennisniveaus. Een heikel onderwerp. We bespreken aanbevelingen hieromtrent in het laatste hoofdstuk.

Risico's van overheidsgegevensgebruik

Risico XI. Weinig wettelijke beperkingen. Als het gaat om gegevensgebruik door en binnen de overheid is de wetgever maar in beperkte mate geneigd te voorzien in beperkingen met betrekking tot gegevensuitwisseling en gegevensanalyse.

Risico XII. Wetgever laat bestuur te vrij. Als het gaat om gegevensgebruik door en binnen de overheid is de wetgever maar in beperkte mate geneigd rekening te houden met beperkingen verband houdend met fundamentele rechten en vrijheden, zoals die waarin het Europees Handvest voorziet.

Risico XIII. Kwetsbare wetgeving. De wetgeving waarin te weinig rekening wordt gehouden met de bescherming van fundamentele rechten en vrijheden loopt het risico buitenwerking te worden gesteld. Voor de op basis daarvan gebouwde gegevensuitwisselingssystemen is dit een potentiële faalfactor.

Risico XIV. Sleepnetpraktijken. Digitale bestuurders hechten weinig betekenis aan beginselen als select-before-you-collect en hebben weinig moeite met sleepnet-acties, als die effectief lijken om de door hen gestelde doelen te bereiken.

Risico XV. Waarborgenerosie. Er komen heel veel meer gegevens beschikbaar die door digitale overheden kunnen worden gebruikt, en waarschijnlijk ook gaan worden gebruikt, om macht uit te oefenen over burgers en ondernemers (offline, online en digitaal), zonder dat duidelijk is of daar tegenover voldoende waarborgen staan.

Risico XVI. Databeschermingsparadox. Een fundamenteel risico is dan dat er een ontwikkeling is ingezet waarin degenen die aanspraak maken op geheimhouding of, in meer algemene zin bescherming van persoonlijke levenssfeer, dat alleen kunnen krijgen als zij zich als zodanig bekend willen maken.

Genoemde risico's spelen vooral, menen we, omdat het bestuur een belangrijke rol speelt bij wetgeving en in beleidsvormende processen. Daarbij worden de mogelijkheden van digitalisering enerzijds ervaren als een kans om de doelmatigheid van het overheidshandelen te vergroten en besparingsambities te realiseren, en anderzijds als een mogelijkheid om de handhaving te verbeteren op basis van een verbeterde informatiepositie. Voeg daar bij dat bestuurders nogal eens ervan overtuigd zijn dat het directe belang van hun werk vanzelfsprekend van meer gewicht is dan het belang van grondrechtelijke bescherming, en we hebben door de digitalisering een zichzelf versterkend mechanisme. Als gezegd vrezen we dat op het moment bij de overheid een *quod licet jovi* cultuur (dubbele standaard)[96] opbloeit met de toegenomen handhavingsmogelijkheden op basis van digitalisering. Dan gaat het om het zich niet of *contre coeur* storen aan informatiebeperkingen die beogen de burger en de ondernemer te beschermen, hetgeen op de werkvloer van overheden al snel als hinderlijk wordt ervaren.

Wanneer we de in hoofdstuk 5 beschreven *geheimhoudnummerkwestie* als voorbeeld nemen, gaat het om de bescherming tegen afluisteren van gesprekken tussen advocaten en hun cliënten, een bescherming die kennelijk alleen kan worden gegarandeerd wanneer bekend wordt gemaakt van welke telefoons voor geheimhoudgesprekken gebruik wordt gemaakt. Een dergelijk arrangement werkt alléén als erop kan worden vertrouwd dat van die kennis, van het weten waar geheimhoudgesprekken worden gevoerd, geen misbruik wordt gemaakt, ook niet onder de logica dat dit 'voor volk en vaderland' gebeurt. Eén en ander schreeuwt om nog meer onafhankelijk toezicht, zoals ook blijkt uit de recente uitspraak van het Hof Den Haag over het niet zonder onafhankelijk toezicht door de AIVD afluisteren van een advocatenkantoor.[97]

De vraag is dan, kortom, of het bestuursrecht voldoende is toegesneden op het stelsel van verlokkingen dat de vergrote inzet van informatietechnieken in termen van informatiegebruik door de overheid met zich mee brengt? We denken dat hier twee gezichtspunten kunnen worden verdedigd. Door een positiefrechtelijke bril komt het ons voor dat er voldoende bestuursrechtelijke regels zijn waaraan de burger en de ondernemer rechtsbescherming zouden kunnen ontlenen wanneer de overheid in zijn gege-

96. Uit wikipedia: 'Quod licet Iovi non licet bovi' of 'Wat Jupiter is toegestaan, is het rund nog niet toegestaan' is een Latijns spreekwoord dat in feite zegt dat wat een als belangrijk aangemerkt persoon mag, niet zomaar ook iedereen toegestaan is < https://nl.wikipedia.org/wiki/Quod_licet_Iovi_non_licet_bovi > (geraadpleegd op 30 oktober 2015).
97. Hof Den Haag 27 oktober 2015, ECLI:NL:GHDHA:2015:2881.

vensgebruik over de juridische schreef gaat. Maar door een rechtsrealistische bril menen we toch vooral te zien dat de overheid zich aan het aanwennen is om beperkende regels in de wind te slaan en om de sporen daarvan aan het zicht te onttrekken. We zouden aanbevelingen hieromtrent in het laatste hoofdstuk wel willen bespreken, maar realiseren ons dat we daar in de context van dit preadvies nog niet heel ver mee komen.

Wat uit één en ander naar voren komt is de betekenis van de kwaliteit van iemands *informatie*positie waar het gaat om het verwezenlijken van een *rechts*positie. Dit verwondert helemaal niet, en is ook niet nieuw. Het verkeerd inlichten van de Kamer door een bewindspersoon is niet voor niets al twee eeuwen een politieke doodzonde. Wat nieuw is, is dat informatieposities veranderen onder de druk van de digitalisering. En dat die digitalisering zozeer om zich heen grijpt dat iedereen aan de gevolgen voor zijn rechtspositie aandacht zal moeten besteden. Die aandacht gaat wat ons betreft uit naar het bewerkstelligen van evenwichtige informatieverhoudingen. Of het scheppen van condities waarin sprake kan zijn van digitaal ondersteund *fair play*.

Eén en ander brengt ons tot een voorlopige conclusie: door het verwezenlijken van de geïnventariseerde risico's bestaat de niet te verwaarlozen kans dat de informatieverhoudingen tussen enerzijds overheid en anderzijds de burger en ondernemer uit evenwicht raken, dat wil zeggen dat die niet meer passen binnen de grenzen die worden gesteld door grondrechten en beginselen van behoorlijk bestuur. Deze conclusie staat op twee benen. Tegen de risico's voor de burger en de ondernemer op de gebieden van toegang en veiligheid bestaan eigenlijk geen toegesneden bestuursrechtelijke instrumenten. En tegen de risico's voor de burger en de ondernemer die voortvloeien uit informatiegebruik binnen en tussen overheden voorziet het bestuursrecht weliswaar wel in allerlei regels, maar blijkt in de praktijk een adequate handhaving problematisch.

Enkele oorzaken zijn bekend. Ten eerste (*i*) is er natuurlijk de enorme toename aan informatie, informatietransacties en –bewerkingen. Ten tweede (*ii*) is er de aanmerkelijke dynamiek in aangeboden ICT-functionaliteit: het is moeilijk, zo niet onmogelijk geworden om als individuele burger, bestuurder of ondernemer de ontwikkelingen voldoende bij te houden. Deze oorzaak valt nagenoeg samen met de toegenomen noodzaak om over specialistische kennis te beschikken voor wie individueel verantwoordelijk wil zijn voor zijn deelname aan de digitale samenleving. Ten derde (*iii*) zijn er bij bestuursdiensten te veel visioenen of veronderstellingen over efficiëntie en effectiviteit van bestuurstoezicht op basis van digitale informatieverzamelingen en is er te weinig bewustheid van mogelijke rampscenario's, zoals dat van het DigiD-drama, en van de beperkte beveiliging

tegen kwaadwillige DDOS-aanvallen waarvan er één nog recentelijk de uitbetaling van toeslagen door de belastingdienst langdurig vertraagde.[98]

De vraag die voorligt is of, en zo ja, in hoeverre de algemene en universele maatschappelijke transitie van offline bestuurders, burgers en bedrijven naar digitale bestuurders, burgers en bedrijven risico's met zich meebrengen voor ons begrip (en voor de hanteerbaarheid en dus flexibiliteit) van de bestuursrechtelijke beginselen en de via het bestuursrecht (dat immers op die beginselen rust) te beschermen rechten van burgers en ondernemers.[99]

7. Wat kunnen we ermee?

7.1 In grote lijnen

We hebben aangewezen waar het bestuursrechtelijke bouwwerk onder druk komt te staan wanneer de samenleving en de overheid digitaliseren. Wat naar voren komt is de betekenis van de kwaliteit van iemands informatiepositie wanneer het gaat om het verwezenlijken van zijn rechtspositie. Daarbij speelt een drietal categorieën van vragen, zijnde:

– vragen van institutionele aard (bestuursrechtelijke instrumenten lijken in sommige gevallen bijvoorbeeld ontoereikend);
– vragen van vereiste kennisniveaus (ook hier schieten traditionele rechtsmiddelen tekort, zo laat het zich aanzien);
– vragen van bestuursmorele aard (een bestuurlijke bedrijfscultuur die opgewassen is tegen de verlokkingen die de digitalisering met zich mee brengt).

Waar we mee te maken krijgen is dat complexiteit en kennisgebreken bestuursrechtelijk op een zorgvuldige manier moeten kunnen worden behandeld. We weten nog niet goed hoe, maar denken dat daaraan vanuit verschillende richtingen wel kan worden bijgedragen. Bijvoorbeeld door weldoordachte mechanismen te organiseren voor het inrichten van bestuurlijke taken, in gezamenlijkheid met ofwel specialistische overheidsdiensten ofwel gespecialiseerde commerciële diensten. En bovendien door het inrichten van weldoordachte kaderscheppende mechanismen voor het outsourcen van publieke dienstverlening, maar dan zonder het politiek en

98. We doelen op de storing van 20 november 2015 bij banken en belastingdienst, waardoor mogelijk zo een 7 miljoen toeslagengerechtigden werden geraakt. Over de oorzaak ervan werd opmerkelijk zuinigjes gerapporteerd. Zie o.a. RTL-nieuws, 'Toeslagen later overgemaakt door storing Belastingdienst', 20 november 2015, te vinden via http://www.rtlnieuws.nl/nieuws/binnenland/toeslagen-later-overgemaakt-door-storing-belastingdienst (geraadpleegd 1 januari 2016).
99. Zie bijvoorbeeld Cliteur (2002).

bestuurlijk weglekken van verantwoordelijkheden. We zijn daar nog lang niet, zo blijkt uit de zorgwekkende afhankelijke positie die overheden innemen ten opzicht van bijvoorbeeld ondernemingen als Diginotar en Ordina of, als het gaat om van cybersecurity, van een specifieke dienstverlener als Fox IT.

We kunnen de rollen van de verantwoordelijke individuen onderscheiden in die van burger, ondernemer en bestuurder. We doen dit niet alleen omdat dit onderscheid in toenemende mate ook bij beleid en regelgeving van belang is geworden. Ook voor onze benadering, die ziet op bewust, verantwoord handelen is het van belang om te onderscheiden naar wat tegenwoordig wel *prikkels* worden genoemd, of in minder tegen de economische discipline aanhangende formulering: *motiveringstructuren*. Zonder terug te vallen op sociaalwetenschappelijke inzichten kunnen we hier uit de voeten met wat de rechtstraditie heeft opgeleverd. In grote lijnen draagt de individuele burger individueel de verantwoordelijkheid voor wat zij of hij doet, behalve wanneer zij of hij een onderneming met rechtspersoonlijkheid leidt of ervoor handelt (dan draait het bedrijf ervoor op) en behalve wanneer hij of zij als ambtenaar in functie handelt, in welk geval de overheid ervoor opdraait (met dien verstande dat wanneer het een politiek gevoelig mistasten betreft de ministeriële verantwoordelijkheid eveneens in werking kan worden gesteld.)

Wij menen dat het onderscheiden in burger-ondernemer-bestuurder van belang is omdat de onderlinge verschillen in motiveringstructuren aanzienlijk zijn, en hun rollen in termen van onder andere specialisatie en delegatie onontbeerlijk zijn in het steeds complexer wordende netwerk van interacties dat onze samenleving vormt en verwezenlijkt. En we menen ook dat we naast een consumentenrecht-achtige rechtsbescherming voor de homo digitalis ook een vorm van rechtsbescherming moeten kunnen bespreken waarin garanties te vinden zijn dat hij of zij zich op zijn eigen, individuele wijze kan blijven ontplooien en ontwikkelen.

7.2 Kritische aspecten

We hebben in het voorgaande 16 risico's gevonden waarmee de homo digitalis te maken krijgt. We hebben een aantal mogelijke oorzaken genoemd en in grote lijnen een drietal vraagstukken voor het bestuursrecht en bestuurspraktijk benoemd. En we hebben daarbij aangegeven dat de institutionele inrichting en vertegenwoordigingsarrangementen daarbij een rol spelen.

Wanneer we het in grote lijnen hebben over bestuursrechtelijke rechtsbescherming denken we, als gezegd, aan het legaliteitsbeginsel, de beginselen van behoorlijk bestuur en grondrechten als kaderscheppend. Kunnen we al die resultaten en overwegingen die we in de vorige paragraaf opsom-

den in verband brengen met de functionaliteiten van één en ander? Om dat overzichtelijk te houden benoemen we eerst een vijftal kritische aspecten.

Als eerste is van belang zich te realiseren dat er met de toenemende digitalisering vanuit het gezichtspunt van de verantwoordelijke individu een dynamiek ontstaat in wat hij of zij ervaart als eigen bevoegdheid en opgedrongen verplichtingen. Heel vaak worden efficiency, doeltreffendheid en controleerbaarheid als belangen in stelling gebracht. En heel vaak gaat dat ten koste van de discretionaire ruimte (autonomie, vrijheid). Een standaardvoorbeeld in dit verband is de lijst van zogeheten diagnose-behandel-combinaties, waaraan de vergoeding van het werk van een huisarts is gekoppeld en waardoor de huisarts die betaald wil worden blind moet zijn voor diagnoses die zijn kennis en ervaring hem voorhouden maar die in die lijst niet voorkomen – en zich dan ofwel bij de beperkingen neerlegt, ofwel in de verleiding komen kan om administratieve kunstgrepen te gaan toepassen die als valsheid in geschrifte kunnen worden geïnterpreteerd. Wij hebben in dezen geen oordeel over de verhouding autonomie-veiligheid bij digitale dienstverlening. We wijzen erop dat het gaat om een culturele kwestie die kan veranderen, en die vloeibaar lijkt te kunnen worden onder druk.

Over *evenwichtige informatieverhoudingen* als kritisch aspect hebben we het meeste wel gezegd in de vorige hoofdstukken. We merken alleen hier nog op dat het gaat om iets dat wel kan worden begrepen wanneer het wordt getoond, maar moeilijk kan worden gedefinieerd. Het zou goed zijn, denken we, wanneer daartoe door de wetgever een poging zou worden gedaan. Het hele begrip verdient hoe dan ook meer aandacht. We leven inmiddels in een wereld waarin de belangrijkste grondstof niet meer olie, maar informatie is.

Over *kennisvereisten* als broodnodige context *voor bestuurlijke zorgvuldigheid in digitale zaken* spraken we reeds. Maar ook over de omstandigheid dat de digitale wereld steeds ingewikkelder en complexer wordt en bovendien snel verandert. Het is onzeker in hoeverre van een individu (bestuurder, burger of ondernemer) kan worden verwacht van de meeste digitale zaken voldoende op de hoogte te zijn. Hier openbaart zich de noodzaak van samenwerking, institutionalisering en/of uitbesteding c.q. outsourcing naar specialisten.

Een daarmee samenhangend kritisch aspect is dan *de institutionele inbedding*. Economen hebben laten zien dat een rationale benadering mogelijk is. Oneerbiedig samengevat leiden hun (in respectievelijk 1991 en 2005 Nobelprijswaardig geoordeelde) bevindingen[100] tot de volgende heuristieken: (a) organisaties ontstaan voor wat een organisatie (institutie) efficiënter kan doen dan de markt, (b) eenmaal bestaande organisaties besteden iets dat ze nodig hebben uit aan een andere organisatie als daar

100. Coase (1937); Williamson (2005).

een markt voor bestaat en als een uitbestedingsovereenkomst geloofwaardig juridisch kan worden gehandhaafd. Die heuristieken lijken *mutatis mutandis* zo gek nog niet wanneer wordt nagedacht over institutionele veranderingen – bijvoorbeeld in het spoor van de Kaderwet zelfstandige bestuursorganen,[101] die expliciet werd opgesteld voor het kunnen inrichten van onafhankelijke instituties die over specialistische kennis beschikken[102] en voor het kunnen inrichten van bijzondere bestuursdiensten onder de hoede van een of enkele ministeries (we denken aan figuren die tot de inrichting van overheidsinstituten als het CIOT, ICTU en Luris hebben geleid). Trouwens, de ervaringen met die instituties laten zien hoe moeilijk het is om over de departementale grenzen heen werkelijk effectieve samenwerkingsverbanden te realiseren. Kennisdeling, kenniscapaciteit, outsourcing en specialisatie zijn elementen van een belangrijk organisatorisch kernaspect van onze bestuurspraktijk zolang die in transitie is door de digitalisering. Samenwerking over de soms nog parochiaal bewaakte departementale grenzen heen blijkt bovendien extra lastig.

Een ander belangrijk kernaspect van de transitie naar digitalisering betreft de steeds weer opduikende ambities en verwachtingen rond de volledigheid en toekomstbestendigheid van onze inzichten en daarmee samenhangende maakbaarheden van onderdelen van onze samenleving. Heel vaak wordt dan gedacht in de lijnen van wat we hier *de juridische Nirvana fallacy* noemen,[103] bijvoorbeeld wanneer wordt aangenomen dat maatschappelijke problemen door regelgeving kunnen worden opgelost of weggenomen. Dat dit in de praktijk maar zelden opgaat valt om ons heen waar te nemen. En daarvoor is een bijzondere reden wanneer we kijken naar digitaliseringsprocessen. Die houden altijd in dat er netwerken ontstaan. En dat leidt vooral tot complicaties wanneer de knooppunten in zo'n netwerk zich in verschillende tempi ontwikkelen.

Alles kent zijn tijd. Het gaat om het verwezenlijken van technologische innovatie, de behandeling van een rechtsgeschil, het aanpassen van beleid, van de wet, een cultuuromslag, etc. Dat allemaal loopt niet zonder meer synchroon. En toch hebben al de genoemde processen invloed op elkaar, als ze deel uitmaken van zo'n netwerk.[104]

101. Stb. 2006, 587.
102. *Kamerstukken II* 2005/06, 27426, nr. 3.
103. In navolging van Demsetz (1969):1.
104. Een beroemd voorbeeld is de mededingingszaak in de Verenigde Staten die in de jaren 1960 door CDC tegen IBM werd aangespannen en die ging over de beschikbaarstelling van de interface-protocollen voor randapparatuur, zie bijvoorbeeld: Baase (1974). Deze zaak werd na 12 jaar procederen geschikt, op een moment dat er technisch inmiddels heel andere dingen speelden. Voor zover wij kunnen overzien heeft dit voorbeeld zich decennia later in Europa opnieuw voorgedaan in de Microsoft-zaak (Page and Lopatka (2009)). Dit soort complexiteit blijkt lijkt veel hardnekkige politiek-juridische vraagstukken te kenmerken (privacy, ICT-aanbestedingen, duurzaamheid, vluchtelingen). Maakbaarheid en voorspelbaarheid blijken beperkt (zie ook Appendix 3).

Er zijn dan dus vragen en onzekerheden over behoud van discretionaire bevoegdheden van gebruikers, over motiveringstructuren en effectieve institutionele inbedding, en over het tegengaan van de juridische *Nirvana fallacy*. Eén en ander leidt tot het vermoeden dat we niet al te veel moeten hopen op een enkele bestuursrechtelijke '*silver bullet*' waarmee we de problemen snel en effectief uit de wereld kunnen helpen.

Maar dat is niet alles. Er zijn ook meer positieve 'bottom-up' ontwikkelingen. Ze rusten óók op de mogelijkheden van de digitalisering (denk aan de manier waarop de inhoud van Wikipedia op basis van enkele regels en afspraken door de gebruikers zelf wordt bewaakt op kwaliteit, en tegen kwaadwillige aanvallen[105]) die zouden kunnen bijdragen aan verbetering van de hanteerbaarheid van de complexiteit. Omdat we menen dat het van betekenis is om daarop te anticiperen bespreken we een mogelijke ontwikkeling hieronder aan de hand van een voorbeeld waarvan het maatschappelijk belang moeilijk kan worden overschat: de app-revolutie.

7.3 De app revolutie

We gaan op zoek naar een functionele ontwikkeling in de digitalisering die thans gaande is en waarschijnlijk van grote betekenis gaat worden om de gesignaleerde complexiteit te beteugelen, dat eigenlijk al is en doet, maar die daarbij tegelijkertijd weer nieuwe risico's voor onevenwichtige informatieverhoudingen met zich brengt. We gebruiken die ontwikkeling als demonstratiemateriaal. We kiezen de *app*-ontwikkeling en geven aan waarom die van zo grote betekenis is voor de verschijningsvormen van de digitale wereld.

Proprietary én open source bedrijfsmodellen voor smartphones: institutionele inbedding (i)

In 2007 kwam de eerste iPhone op de markt die werkte op iOS (het *proprietary* smartphone platform van Apple); in 2008 de eerste HTC die werkte onder Android (het *open source* smartphone platform dat Google haast onmiddellijk als tegenhanger van iOS beschikbaar stelde).

Zowel iOS als Android bieden 'toolkits' die het vervaardigen van apps ondersteunen en standaardiseren. Beide bieden een distributie-en-betaalpad. En beide bieden een zekere mate van toezicht op kwaliteit. Vooral het kwaliteitstoezicht én het bedrijfsmodel verschillen: iOS Apps moeten door Apple worden getoetst en gedistribueerd, en een aanmerkelijk percentage van de opbrengst moet aan Apple worden afgedragen. Vergelijkbare inmenging van Android is aanmerkelijk minder of afwezig. Wat opmerke-

105. Zie bijvoorbeeld Heaberlin en DeDeo (2015). Hun aanpak wordt nader geplaatst in Appendix 3.

lijk genoemd kan worden is dat de twee platforms iOS en Android, die naar hun bedrijfsmodel zo verschillen, naar functionaliteit haast niet van elkaar verschillen, althans niet voor de meeste gebruikers c.q. consumenten.

Ontwikkeling van Apps vanaf 2007 tot heden

Vanaf 2007, toen de markt voor apps ontstond, is deze stormachtig gegroeid. Medio 2015 wordt gerapporteerd dat in de voorafgaande 12 maanden 25 miljard iOS apps werden gedownload, en 50 miljard apps voor Android. [106] Dat is samen 75 miljard(!) In 2014-2015 werden (op een wereldbevolking van 7.3 miljard) iets meer dan 10 apps per wereldburger gedownload. De platforms iOS en Android, die medio 2014 respectievelijk zeven en zes jaar bestonden, hebben dus een explosieve groei doorgemaakt en voor een explosieve groei gezorgd. We hoeven dan ook niet meer aan juristen uit te leggen wat smartphones en apps zijn. Er zijn, vermoeden wij, maar weinig juristen in Nederland die geen gebruik maken van tenminste één smartphone en een tiental apps of meer.

Smartphones als voorbeeld van Internet of Things: institutionele inbedding (ii)

Apps leveren diensten die zo kunnen zijn ingericht, dat ze samenwerken met andere apps en/of toegang nodig hebben tot informatie van elders ('the cloud') en dat voor die samenwerkingsmogelijkheden meestal keurig netjes toestemming wordt gevraagd en verkregen.[107] Dit in overeenstemming met de wettelijke regelingen die de persoonlijke levenssfeer beogen te beschermen.

Maar omdat het verlenen van toestemming is gerelateerd aan het verwerven van functionaliteit wordt die toestemming doorgaans vrij gemakkelijk verleend en verkregen. Veel apps vragen en krijgen toestemming om toegang tot foto's, netwerkfuncties, adressen, locatiegegevens. Eigenlijk weet niemand op dit moment het antwoord op twee belangrijke vragen: (1) wat mogen de app-aanbieders die toestemming kregen met de verkregen gegevens doen en wat niet, en (2) wat doen die app-aanbieders er in feite mee. Het is meer dan aannemelijk dat rechtmatig verkregen (persoons) gegevens worden doorverkocht of -geleverd (doorgaans als voedsel voor de voor consumenten weinig transparante geautomatiseerde carrousels met veilingen van profielinformatie, of als voedsel voor de ook proactief georienteerde analyses van politie- en veiligheidsdiensten). En daarmee, dat de

106. Google Play downloads reached 50 billion in the last 12 months, while Apple's app store downloads totaled 25 billion. Amy Gesenhues on June 16, 2015 at 1:12 pm at: http://marketingland.com/google-play-gaining-ground-against-apple-as-android-app-downloads-outnumber-ios-2-to-1-132307.
107. Dit geldt inmiddels ook voor Android apps, tenminste vanaf versie 6.0 [Lollipop].

wereld van de smartphones een belangrijk voorbeeld is geworden van wat het 'Internet of Things' of 'IoT'[108] wordt genoemd.

De 'use-case' dimensie

Apps zijn dan, als onderdeel van dat IoT, als knooppuntjes in een wereldwijd netwerk, een emergent verschijnsel. Het succes is vermoedelijk mede ingegeven door de omstandigheid dat toepassingen in de vorm van apps aan beperkingen onderhevig zijn. Want smartphones hebben – hoewel deze *devices* qua architectuur volwassen computers zijn – beperkte mogelijkheden (batterij, schermgrootte, processor, geheugen e.d.), evenals smartphonegebruikers te maken hebben met beperkingen (tijd, aandacht, ICT-kennis, soorten digitale behoeften etc.). Door die wederzijdse beperkingen op elkaar af te stemmen is een nieuw standaardformaat voor programma's (*applications* d.w.z. 'apps') op mobiele apparatuur ontstaan dat buitengewoon effectief en succesvol is. Zo succesvol, dat ze onderweg zijn een nieuwe *de facto* standaard te worden voor digitale diensten.

Apps zijn doorgaans programma's met een beperkte functionaliteit, je kunt ze niet voor alles gebruiken, maar wel voor een zogeheten *use case,* dat wil zeggen: voor een dienst met de dimensie van de een of andere standaardtaak, van iets wat de gebruiker goed kent en vaak doet en waarvoor je een digitaal steuntje in de rug kunt gebruiken. Voor wanneer je wilt weten wat voor weer het is in Den Haag, als je een SMS wilt lezen, een tweet wilt twitteren, wanneer je wilt weten of je nog een mailtje hebt gekregen, of voor het bekijken van je banksaldo, of de digitale post van de belastingdienst.

Het gebruik van dat soort dienstjes is vaak heel intuïtief. Er zijn meer dan een anderhalf miljoen verschillende apps beschikbaar voor Android en vermoedelijk meer dan half zoveel voor iOS. Vaak hebben ze via internet toegang tot de servers en databases van een 'back office.' De wereld van computergebruikers is razendsnel aan het veranderen in de richting van een wereld van app-gebruikers.

Standaard objectarchitectuur

De term 'use case' laat zich niet gemakkelijk vertalen en is afkomstig uit het domein van de informatica in de jaren 1980, toen er een beweging opkwam onder informatici om programmatuur zo te gaan inrichten dat bouwstenen hergebruikt konden worden. Die bouwstenen werden 'objecten.' En de standaardarchitectuur van objecten bestaat uit een compartiment voor data en voor functionaliteit ('methods') en voor input en output ('message'). Object oriëntatie werd een doorslaand succes, mede doordat in de afgelopen twintig jaar omvangrijke bibliotheken met objecten (en dus: methods) beschikbaar kwamen en omdat computertalen als Java

108. Morgan (2014).

gericht werden op het bouwen en integreren van objecten. Zowel iOS (met objective C) als Android (met Java) ondersteunen het programmeren van objecten.

Samengevat komt de apps-explosie van 2015 met kansen en met bedreigingen. De kansen worden geboden door de 'use-case' dimensie van apps, die er tezamen met de standaard objectarchitectuur toe lijkt te leiden dat de digitalisering voor consumenten, bedrijven en dienstaanbieders aanmerkelijk transparanter kunnen worden dan ze tot nu toe waren, tenminste, wanner er standaarden ontstaan voor functies waarvoor toestemming nodig is en voor de protocols waarvan dat soort functies gebruik maken om te communiceren. De bedreigingen bestaan in de kans dat die standaarden *niet* ontstaan en *niet* worden omhelsd, en dat de apps wereld verder tot een volkomen ondoorzichtige en onveilige kluwen van onderling verbonden diensten (en via die diensten verbonden belangen) zal uitgroeien.

Belangrijke vragen gaan dan natuurlijk in de toekomst ook (en nog steeds) over evenwichtige informatieverhoudingen tussen app gebruikers en app aanbieders. En dat evenwicht berust op het effectief kunnen authentiseren van gebruikers, aanbieders en apps, het hebben van toegang, het bestaan van transparantie en van betrouwbare, integere communicatie. We menen dat zulks alleen mogelijk is op basis van effectieve standaarden en *protocols*. En we menen dat het bestuursrecht hier een rol heeft te spelen, al was het alleen maar om bestuurlijke taakvervulling digitaal te kunnen uitvoeren op een digitale wijze die tegelijkertijd recht doet aan elementaire beginselen van bestuurlijk behoren.

7.4 Apps van de overheid

De digitale overheid gaat zelf natuurlijk ook apps aanbieden om haar dienstverlening voor burgers (gebruikers) beschikbaar te maken. De overheid kan daarbij, eventueel zelfs zonder dat voor te leggen aan wetgever of belanghebbende, informatiefunctionaliteiten inbouwen, zonder om toestemming te vragen, dat wil zeggen: de toegang tot de dienst te weigeren wanneer de toestemming niet wordt gegeven. Apps van overheden kunnen, doorgaans zonder democratische of bestuursrechtelijke toetsing, toegang tot informatiefunctionaliteit van burgers en ondernemers claimen. Alsdan kan een situatie ontstaan waarin de machtsverhoudingen tussen het bestuur (als app-aanbieder) en de burger of ondernemer (als app-gebruikers) uit evenwicht raken.

Hier komt opnieuw naar voren wat Locke en Montesquieu van belang oordeelden als randvoorwaarde voor het domesticeren van bestuursmacht: het primaat van de 'liberty' (we begrijpen *liberty* als samengesteld uit vrijheid en autonomie) boven '*security'* (wat we begrijpen als samengesteld uit zekerheid en veiligheid). We kunnen ons niet aan de indruk onttrekken dat wat de digitalisering vooral met zich meebrengt een terugkeer is naar

het waarderen van veiligheid boven *liberty*,[109] mogelijk doordat het doorzien en beïnvloeden van digitale diensten moeilijk is. En we vragen ons ook af of die omgekeerde tendens mede het gevolg is van de mate waarin onzekerheid in de samenleving toeneemt ten aanzien van terrorismedreigingen, maar ook ten aanzien van ondoorzichtige en nauwelijks door het recht beteugelde digitalisering bij bedrijfsleven en bij de overheid, en misschien ook doordat de betreffende overheden er niet in lijken te slagen de burger ervan te overtuigen dat de problemen onder controle zijn. We vragen ons af of de app revolutie de mogelijkheid opent dat de burger hierbij de overheid te hulp schiet.

We herinneren ons nog levendig de tijd waarin heftig werd gedebatteerd over de wenselijkheid van het elektronische patiëntendossier (EDP). De discussie liep erop uit dat de Eerste Kamer het project zo goed als afblies. Ergens gedurende dat proces bood Google aan om een EDP als clouddienst aan te bieden. Daarop is niet ingegaan – vermoedelijk ook omdat er geen aanbesteding was waarop Google had ingeschreven en als winnaar te voorschijn was gekomen – maar ondenkbaar is het niet dat de overheid die immers baat heeft bij het zoveel mogelijk doen uitvoeren van de haar opgedragen taken op digitale wijze, er toe komt die taken via cloud-diensten te outsourcen als aan de daaraan te stellen eisen zou zijn voldaan.

In een app benadering zou dat EDP er als volgt kunnen uitzien: een EPD-app op je smartphone die het EDP van de eigenaar bevat als data en die via messages over het internet in verbinding staat met *devices* van de medici van dienst. In een app-benadering zou het systeem voor het niet-afluisteren van advocatengesprekken er eveneens anders kunnen uitzien: de betreffende app zou dan de afluisterdienst van het geheimhoudkarakter van de voorliggende smartphone aan de afluisterdienst kunnen signaleren. Op die wijze zou in de app-benadering een belangrijk deel van het werk door de burger of ondernemer worden gedragen en beheerd op zijn smartphone.

Ook dan blijven de belangrijkste rechtsvragen nog onvoldoende beantwoord. Ze betreffen niet alleen het effectief authentiseren van gebruikers (burgers, ondernemers), aanbieders (overheden) en apps, en het garanderen van betrouwbare communicatie, maar ook het betrouwbaar monitoren en archiveren van digitale transacties ten behoeve van eventuele bewijs-

109. Dit lijkt te worden gekoesterd: in december 2015 kregen we een paniekbericht onder de vlag van NL-Alert op onze smartphone met de vraag of we de rampeninformatie-app wilden activeren – het was een proef, maar het weigeren van de dienst bleek een heel gedoe waarvan wij vermoeden dat menige offliner daarin niet zal zijn geslaagd. We vragen ons trouwens wel af of zo'n proef aan de eerste beginselen van het recht op een persoonlijke levenssfeer voldoet. Mag een overheid ongevraagd paniek zaaien om een overheids-app te testen? Het lijkt ons een illustratie van het toenemende belang dat de overheid ziet in zijn rol van beveiliger, ten koste van het belang van zijn rol als bewaker van onze autonomie/vrijheid.

voering achteraf. Die dingen zijn er nu, bij de bestaande ICT infrastructuur waarvan overheid, bedrijven en burgers gebruik maken, niet. Misschien kan dat bij een ICT-infrastructuur gebaseerd op apps wel, of beter. Dit (anno 2016) lijkt het jaar om dat uit te vinden. In de volgende paragraaf laten we daarom onze verbeelding spreken ten aanzien van de mogelijkheden van een gestandaardiseerde app-benadering voor overheden.

7.5 Waarheen?

Eerder concludeerden we dat door het verwezenlijken van de geïnventariseerde risico's de niet te verwaarlozen kans bestaat dat de informatieverhoudingen tussen overheid, burger en ondernemer uit evenwicht raken. Dat is betekenisvol omdat evenwichtigheid van informatieverhoudingen bijdraagt aan individuele vrijheid. Immers wanneer er een verschil van inzicht bestaat tussen een burger of bedrijf met de overheid over een overheidsbesluit of -regeling (of de manier waarop die wordt gehandhaafd) is het resultaat mede afhankelijk van de mate waarin de informatieposities van beide partijen in evenwicht zijn. Equality of digital arms is noodzakelijk voor het kunnen verdedigen, tegen de digitale overheid, van de individuele vrijheden van homo digitalis.

Maar wat moeten we daar nu mee? Een vraag die ons, bij wijze van gedachtenexperiment, relevant voorkomt is wat een burger, homo digitalis, kan doen als hij of zij meent dat de informatieverhouding met de overheid uit evenwicht is geraakt. Kan deze homo digitalis met enige kans op succes een beroep doen op een beginsel van behoorlijk bestuur? Kan een evenwichtige informatieverhouding worden geëist, bijvoorbeeld in het kader van het verbod op détournement de pouvoir? Zou zo een bijzondere interpretatie kunnen postvatten, bijvoorbeeld onder de noemer *détournement de pouvoir digitale* of *equilibre de relation*s *digitale*?

Détournement de pouvoir digitale?

We zijn dan op zoek naar een uitwerking van het verbod van de détournement de pouvoir waarmee informatieverhoudingen in evenwicht kunnen worden gebracht. We denken dan bijvoorbeeld aan de daaraan verwante vereisten van doelbinding of doelverenigbaarheid en transparantie (resp. art. 9, eerste lid, Wbp en art. 33 en 34 Wbp). Die vereisten verlangen dat persoonsgegevens, die voor een bepaald doel zijn verzameld, niet mogen worden gebruikt voor een ander, daarmee onverenigbaar doel, alsmede dat de wijze waarop en het doel waarvoor persoonsgegevens worden gebruikt transparant wordt gemaakt. Voor wat we ermee willen bereiken zouden we dan kunnen denken aan de uitwerking dat de informatie verkregen in het kader van de éne publiekrechtelijke taak alléén mag worden gebruikt voor andere publiekrechtelijke taken, als er is voorzien in passende waarborgen en effectieve mogelijkheden van verantwoording van hoe de informatie is

gebruikt. Voor deze waarborgen kan dan aansluiting worden gezocht bij de voor het doelbindingsbeginsel ontwikkelde criteria. Verdergaande waarborgen zijn passend als gevolgen van het verdere gebruik van de gegevens voor de burger ernstiger kunnen zijn, als de gegevens niet rechtstreeks van de burger zijn verkregen, als de aard van de gegevens gevoelig is, als er minder verwantschap is tussen de verschillende publiekrechtelijke taken (vgl. art. 9, tweede lid, Wbp).[110]

We menen dat de huidige stand van de Nederlandse rechtsstaat in de praktijk nog ver verwijderd is van dit ideaalbeeld, en dat er weinig uitzicht is op spontaan herstel. We menen ook dat het de moeite waard zou zijn na te gaan of, wanneer de digitale overheid er toch toe overgaat zijn diensten in de vorm van apps aan te bieden, de bijbehorende standaarden en communicatieprotocols niet zo kunnen worden ingericht dat de verzwakking van de informatiepositie van de burger tenminste voor een deel wordt hersteld, bijvoorbeeld door hem meer zeggenschap te geven en hem aldus mede-verantwoordelijk te maken voor het bewaren en beheren van eigen persoonsgegevens.

Digitaal-materiële zorgvuldigheid?

Een andere vraag is of we, wanneer de overheidsdienst blijk geeft van te weinig kennis van informatica en/of organisatiekunde, een beroep kunnen doen op het vereiste van materiële zorgvuldigheid, d.w.z. het vereiste van art. 3:4, tweede lid, Awb. Op grond daarvan worden bestuursorganen geacht de rechtstreeks bij een besluit betrokken belangen af te wegen, voor zover niet uit een wettelijk voorschrift of uit de aard van de uit te oefenen bevoegdheid een beperking voortvloeit. Daarbij mogen de voor een of meer belanghebbenden nadelige gevolgen van zo een besluit niet onevenredig zijn in verhouding tot de met het besluit te dienen doelen.

We vragen ons, weer bij wijze van gedachtenexperiment, af hoe deze bepaling zou kunnen worden gelezen als het gaat om een Iraanse burger die ernstig is gedupeerd door het DigiD-drama en daarom rechtsmiddelen zou willen instellen tegen het ‘besluit’ van de minister om er in het kader van het DigiD-drama bij Microsoft op aan te dringen níet over te gaan tot het intrekken van valse certificaten? Is hij geen belanghebbende? Zijn bij de besluitvorming door de minister de belangen van Iraanse burgers afgewogen? Is er bewijsmateriaal? Hebben we een begin van een idee wat we bedoelen wanneer we het over digitaal-materiële zorgvuldigheid hebben?

110. Zie daarover bijv. Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013.

7.6 Een conclusie en enkele aanbevelingen

Wij denken dat dergelijke vragen, vragen naar concrete claims, naar interpretaties en naar rechtsontwikkeling van groot belang zijn. Maar we denken ook dat wij daarover op deze plaats, en op dit moment, nauwelijks iets met gezag kunnen zeggen omdat er, voorzover wij overzien, nog maar weinig gerichte klachten over de risico's die wij inventariseerden werden voorgelegd aan de rechter.

Ons algemene beeld is, dat het in veel individuele gevallen moeilijk zal zijn om handvaten te vinden die toereikend zijn voor de homo digitalis om zijn rechtspositie te verdedigen. We denken ook dat dit een cruciale uiting is van verstoorde en onevenwichtige informatieverhoudingen tussen burger en bestuurder. De voornaamste problemen hierbij zijn vermoedelijk direct terug te voeren op asymmetrische informatieposities. Dit geldt in elk geval wanneer onduidelijk is of een besluit is genomen, of een juiste belangenafweging heeft plaatsgevonden en of er bewijsmateriaal beschikbaar kan worden gemaakt. En die onduidelijkheden gelden voor veel van wat de *homo digitalis* kan overkomen als gevolg van overheidsdigitalisering.

Onze hoofdconclusie is dan ook onthutsend. Onze democratie en onze rechtspraktijk blijken, oog in oog met de huidige maatschappelijke transitie naar een digitale samenleving kwetsbaar voor belangrijke en mogelijk schadelijke bijeffecten zonder zich daarop effectief voor te bereiden.
Hiermee raken we aan het eind van ons Latijn.

Wel hebben we nog enkele aanbevelingen die uit het voorafgaande volgen. Deze gaan erover hoe, als jurist, om te gaan met de voortschrijdende digitalisering van de wereld en het bestuur. Wij zien twee actielijnen, die geen van beide wetswijzigingen omvatten, wel beleidsaanpassingen.

1. Ad hoc rechtsontwikkeling op basis van feitelijke situaties die zijn ontstaan.
Het is van het grootste belang dat de rechter en de rechtspraak veel actiever worden ingezet om antwoorden te vinden op het beteugelen van de bestuursrechtelijke risico's die we inventariseerden en die de transitie naar een digitale samenleving met zich meebrengt. We leven in turbulente tijden, zowel juridisch als digitaal, waar de rechtsontwikkeling in belangrijke mate hangt op de rechtspraak, op individueel juridisch talent, oog in oog met een verrassende en aansprekende digitale casus die al dan niet toevallig een centraal probleem treft en via de rechtspraak tot een vruchtbare uitkomst leidt. We vermoeden dat de materiële bestuurlijke zorgvuldigheid wel wat opheldering *in digitalibus* kan gebruiken.

We vermoeden ook dat onder de huidige omstandigheden niet te veel van wetgeving hoeft worden verwacht omdat daarmee vaak doelen worden beoogd in een omgeving die waarschijnlijk al van kleur is verschoten nog

voordat tot handhaving kan worden overgegaan. Omdat zowel de techniek als de politieke verhoudingen inmiddels op hun eigen wijze en in hun eigen tempo blijken te zijn veranderd. Een schoolvoorbeeld lijkt de ontwikkeling van de wettelijke bescherming van de persoonlijke levenssfeer te bieden, tegen de achtergrond van de ontwikkelingen van economische en technologische bedrijfsmodellen die zijn gebaseerd op de verwerking van persoonsgebonden informatie.

We menen daarom dan ook dat het aanbeveling verdient te bevorderen dat de rechter vaker wordt ingezet door of namens de homo digitalis, wanneer die zich op digitale wijze buiten spel voelt gezet en aan den lijve de gevolgen ondervindt van het uit evenwicht raken van informatieverhoudingen.

2. Standaardisering van ICT op een wijze die tegemoet komt aan vereisten voor herstel van maatschappelijk vertrouwen in de digitale overheid.
Alle geïnventariseerde risico's kunnen eraan bijdragen dat een bestuurlijke praktijk ontstaat waarin wantrouwen en misverstand tussen burgers, ondernemers en bestuurders de overhand krijgen. Wij vermoeden dat we die route in de praktijk al aan het verkennen zijn wanneer we denken aan de mislukte ICT-projecten van de overheid, aan de verplichte digitalisering van communicatie tussen de burger (met inbegrip van de minder digivaardige offliner) en de belastingdienst, en aan de weinig bemoedigende handhavingstatistieken bij cybercriminaliteit.

Wanneer we in aanmerking nemen dat er zelfs onder de huidige, gebrekkige beveiligingsmogelijkheden een ontwikkeling gaande is naar een digitale overheid menen we dat daarmee de noodzaak is ontstaan om effectief te werken aan behoud (of herstel) van vertrouwen. Die noodzaak rust op het besef dat, wanneer alle risico's die we hebben geïnventariseerd *tegelijkertijd* zouden gaan spelen, de gevolgen onrustbarend, om niet te zeggen: ontwrichtend zouden zijn. We vermoeden dat hiermee een politieke noodzaak bestaat om tot een gelaagd fundament van betrouwbare infrastructurele protocollen en diensten te geraken waarop de individuele transacties in vrijheid en veilig kunnen worden aangegaan. In elk geval, en tenminste, voor de transacties van en met overheden.

Het verdient daarom aanbeveling om deze weg serieus te onderzoeken, met name nu we de overgang naar bestuurlijke dienstverlening via apps meemaken, wat een waterscheiding zou kunnen markeren. Een waterscheiding die als het goed gaat de stroom in de richting stuurt van effectief authentiseren van gebruikers (burgers, ondernemers), aanbieders (overheden) en apps, van het garanderen van betrouwbare communicatie, en van het betrouwbaar monitoren en archiveren van digitale transacties door de overheid ten behoeve van eventuele verantwoording en bewijsvoering achteraf, maar die als het fout gaat de stroom ook een richting in kan sturen

van een digitale jungle, waarbij de wetten van de jungle de overhand krijgen.[111]

Ten slotte
En voor wie nu, aan het einde van ons betoog, zich teleurgesteld realiseert dat we geen enkele positiefrechtelijke vraag concreet en gezaghebbend hebben beantwoord, geen enkele vraag die hij of zij in zijn of haar commerciële praktijk zou mogen hebben, resteert terugverwijzing naar onze aanbeveling om rechtsvragen *in digitalibus* aan de rechter voor te leggen. En daarbij nog een aansporing – wees vooral vasthoudend als een terriër, wanneer de 'inequality of digital arms' een omvang aanneemt die naar uw oordeel niet door de beugel van de bestuurlijke behoorlijkheid gaat.

APPENDICES

Appendix 1. Iets over de homo digitalis (of de menselijke natuur) als voorwerp van rechtswetenschappelijke overweging

In dit preadvies verdiepen wij ons in de rechtspositie van de *homo digitalis*, de mens die in een gedigitaliseerde wereld zijn weg moet vinden en zich moet zien te handhaven. Het is ons inziens noodzakelijk uiteen te zetten wat we verder bedoelen met de notie van *homo digitalis* (als bestuurder en als bestuurde). We ontlenen daarbij inzichten aan menstyperingen zoals die in andere disciplines wel een bijzondere rol spelen, zoals de *homo economicus*, de *homo ludens*, de *homo universalis,* de homo sapiens , etc. Deze bijlage heeft dan drie delen. In het eerste (*Welk beeld past bij het begrip homo digitalis?*) bezien we hoe het begrip homo digitalis thans wordt begrepen, op basis van het gebruik ervan op het internet. In het tweede (*Waarom een homo digitalis?*) gaan we op zoek naar een functie die het begrip deelt met zusterbegrippen (economicus, ludens, sapiens). In het derde gedeelte (*De homo digitalis als autonoom individu*) van deze bijlage geven we aan in welk opzicht de homo digitalis een bijzondere karakterisering van de mens als voorwerp van rechtswetenschappelijke studie is.

1. Welk beeld past bij het begrip homo digitalis?

Juristen zijn niet de eersten die aangetrokken bleken door de term *homo digitalis*. Antropologen, bijvoorbeeld, waren ons voor. We geven hier een

111. Om te voorkomen de indruk te wekken dat we zelf inmiddels ook slachtoffer zijn geworden van een Nirvana fantasie (die doorgaans resulteert in de Nirvana fallacy) hebben we enkele beschouwingen hierover opgenomen in Appendix 3.

paar citaten uit Antroplogi.info,[112] een blog of webforum van antropologen:

> *"How do people in Britain use the internet? How do they behave online?* ***The new Digital Anthropology Report****. The Six Tribes of Homo Digitalis gives some answers.*
>
> *The British communication company Talk Talk sent researchers from the University of Kent into the homes of people around the UK to ask them questions about their attitudes towards digital technology and to watch them use it. They also commissioned anthropology professor* ***David Zeitlyn*** *to analyse the findings.*
>
> *They found that "homo digitalis" consists of Six Tribes with very different attitudes, usage patterns and modes of behaviour. Some of these tribes have embraced technology and put it at the centre of their lives. For other tribes, 'the internet' is a rather frightening jungle.*
>
> *The* ***E-ager Beavers*** *are the largest tribe by quite a distance, with 29% of the UK adult population. They use the internet heavily, but they are more passive users. They lack the confidence or the drive to get involved with uploading their own content or producing their own blogs.*
>
> *The* ***Timid Technophobes*** *are the second largest group (23%). They have only limited internet skills and will only use it when they really need to. They still prefer to use pen and paper and prefer to send and receive letters. They don't read blogs and are not interested in facebook either.*
>
> *The tribe of the* ***Digital Extroverts*** *(9%) consists of people who are "always-on". They are active bloggers, use twitter, flickr etc. "Regularly updating their online profile is as much a part of their daily routine as eating." The ability to interconnect and share data is a prerequisite.*
>
> *According to Zeitlyn, your willingness to embrace technology and integrate it into your life will dictate your success in life far more than your social class will. As class structures change quickly, he writes in his analysis, the extent to which people use social networking and promote themselves online will become more important in determining their careers than what school or university they went to."*

Daaruit kan worden afgeleid dat het begrip homo digitalis in de sociale wetenschappen al wordt gebruikt als een overkoepelend begrip om, op basis van gedragskarakteristieken in relatie tot de digitalisering, groepen te kunnen onderscheiden en hun sociale betekenis te beoordelen.

112. http://www.antropologi.info/blog/anthropology/2009/digital-anthropology-report.

Een ander citaat: Natasha Friis Saxberg betoogt bij TEDx[113] naar aanleiding van een door haar uitgebracht (Deens) boek dat in vertaling is getiteld: Homo digitalis, mapping our human basic needs with our digital behavior:

> *"[...] There are three universal relational structures that are the same across borders across demographics and across cultures. The first is called intimate connectedness, that's the one we have with our spouses and sweethearts. The other is relational connectedness, which we have among friends or colleagues. [...] The third and most interesting relational structure in this context is collective connectedness. That's the one we experience when we gather in groups and it can be spread online and does not need to be based on physical meeting. Collected connectedness gives us a sense of belonging during events where we feel united whether it's people protesting in the streets of Tehran, Tahrir square or [...] That gives us a sense of purpose and passion that is not matched on our daily social streams [...] makes us feel lonely [...] we can avoid becoming lonely if we believe someone will take care of us when we are in need."*

De pointe van Saxberg's betoog (eveneens sociaal-wetenschappelijk van aard) lijkt te zijn dat onze gevoelens van eenzaamheid via sociale media kunnen worden verdrongen door gevoelens van 'erbij horen.' Deze stelling zou een deel van de verklaring kunnen zijn van waarom eerst SMS (1982) en later enkele andere grote sociale media zoals Wikipedia (2000), Facebook (2003), Twitter (2006) en WhatsApp (2009) zulke spectaculaire successen zouden worden. Opmerkelijk blijft het dat de grote telecomaanbieders en/of ICT-giganten die vraag kennelijk over het hoofd hebben gezien of het commerciële belang ervan hebben onderschat.

Een ander citaat komt uit de hoek van de journalistiek. Het expertisecentrum voor de journalistiek, een digitaal informatiecentrum voor de journalist wijdt een artikel[114] aan het begrip homo digitalis:

> *"De vervagende grens tussen mens en machine. Nog even en je leefstijlcoach- app bepaalt dat je gaat sporten. De auto oordeelt dat je niet meer kan rijden na een vrijdagmiddagborrel. De computer grijpt in wanneer je aandacht op het werk verslapt. En zelf modificeer je straks je yoghurtbacteriën met DNA dat je via internet hebt bestelt." (sic!)*

Het citaat besteedt aandacht aan de kwetsbaarheid van de autonomie van wie diensten gebruikt die gedigitaliseerd zijn en waarschuwt, zo lijkt het, voor al te grote afhankelijkheid. De journalistiek beweegt zich hier in de richting van de filosofie.

113. Vindbaar achter adres https://www.youtube.com/watch?v=xCoR0bI9mAo (laatstelijk geraadpleegd op 18 december 2015).
114. Vindbaar achter www.expertisecentrumjournalistiek.nl/homo-digitalis/ (laatstelijk geraadpleegd op 18 december 2015).

Tegenover wat we toch maar als technologiepessimisme lezen bij de journalistiek treffen we ook onverbloemd techno-optimisme. We geven als voorbeeld een citaat van Rydell op een website die zich Mind Control noemt en gepubliceerd wordt door MindTech Sweden:[115]

> *"But soon the technology will not only prepare us, it will also improve. [...] A man who can move things with thought and read your mind. A man who sees more [...] There are no fantasies, the properties are within scientific reach. We have already taken the first steps towards a new man. Homo digitalis."*

Hoewel wij niet zo gevoelig zijn voor dit soort beschouwingen, die er zonder veel reflectie van uit lijken te gaan dat een wereld vol machines die onze gedachten kunnen lezen een wenselijke toestand zou opleveren, vermelden we het hier volledigheidshalve, omdat de term homo digitalis voor techno-optimisten een weer heel andere betekenis gaan aannemen dan die welke wij voor ogen hebben.

Tenslotte nog een citaat dat een speculatie bevat over een tweedeling die van nog groter belang lijkt dan die welke de econoom Piketty ons heeft voorgerekend.[116] Het citaat is ontleend aan Carsten Corneliussen, *Homo sapiens digitalis*, een boek uit 2004:[117]

> *"Those individuals that have evolved beyond the present social political correctness (as standard psychological beings of normative existential maturity) are about to reach a stage where they are able to decide and do what they want to become (used as a distinct psychological terminology) and they hold the power to do so [for themselves]. The rest of the world will be left in a vacuum, and if they do not evolve further and become smarter, they will stay there." (p. 29).*

Onze korte verkenning naar hoe het begrip homo digitalis inmiddels op het internet is ingeburgerd leverde dus een aantal uiteenlopende resultaten, zozeer uiteenlopend dat we ons nog niet wagen aan een eigen definitie. Maar als de betekenis varieert per gebruikersgroep, heeft het begrip dan tenminste een constante functie?

2. Waarom het begrip homo digitalis?

Er bestaan verschillende veel beter ingeburgerde samenstellingen met de Latijnse *homo*. We laten enkele de revue passeren om na te gaan of dat

115. Te vinden achter www.mindcontrol.se/?page_id=17 (geraadpleegd op 26 december 2016).
116. Thomas Piketty, Capital in the Twenty-First Century, Harvard University Press 2014
117. Achter www.strategix.dk/pdf/digitalisuk.pdf (geraadpleegd op 26 december 2016) is een Engelse samenvatting te vinden.

beter licht werpt op waarom en hoe we het concept homo digitalis kunnen begrijpen en gebruiken.

Het concept ***homo economicus*** is in de economie een *modelmatige* eigenschap van de menselijke soort, een eigenschap waarvan de aanvaarding door de economische wetenschap niet gelijk wordt geschakeld met de psychologische werkelijkheid, maar wel noodzakelijk wordt gevonden om economische processen te kunnen beschrijven. Persky zegt het zo:

> *"In economics, homo economicus, or economic human, is the concept in many economic theories of humans as rational and narrowly self-interested actors who have the ability to make judgments toward their subjectively defined ends. Using these rational assessments, homo economicus attempts to maximize utility as a consumer and economic profit as a producer. [...] The term 'economic man' was used for the first time in the late nineteenth century by critics of John Stuart Mill's work on political economy."*[118]

In het domein van de politieke economie worden de rollen omgedraaid: in samenhang met een naïeve conceptualisering van de onzichtbare hand van Adam Smith wordt de homo economicus een ideaalbeeld dat - mits nageleefd - zal leiden tot optimalisering van de welvaart. Hieronder het citaat waarnaar in het vorige citaat wordt verwezen:

> *"[Political economy] does not treat the whole of man's nature as modified by the social state, nor of the whole conduct of man in society. It is concerned with him solely as a being who desires to possess wealth, and who is capable of judging the comparative efficacy of means for obtaining that end."*[119]

Met andere woorden: Occam's scheermes is toegepast op de menselijke natuur (en daarmee op de vrije wil en de menselijke waardigheid) in de economische wetenschap op een wijze die in de populair-politieke arena (en soms ook in de economische wetenschap zelve, zie hierover bijvoorbeeld Bowles (2006) of Beinhocker (2006)) de betekenis heeft verworven van *een universeel wenselijke verworvenheid* omdat de economie als geheel daar beter van zou worden. Het canonieke citaat is hier de slogan "*Greed is good* " van Gordon Gekko in de film *Wallstreet* (20th Century Fox 1987).[120]

Het begrip *homo economicus* heeft – mede door de impliciete projectie van model naar norm – geleid tot heftige debatten, en doet dat nog. Wij

118. Persky (1995).
119. John Stuart Mill. "On the Definition of Political Economy, and on the Method of Investigation Proper to It," *London and Westminster Review*, October 1836. Essays on Some Unsettled Questions of Political Economy, 2nd ed. London: Longmans, Green, Reader & Dyer, 1874, essay 5, paragraphs 38 and 48].
120. Zie voor een onderbouwing van popularisering en de bijbehorende betekenisprojectie http://en.wikipedia.org/wiki/Gordon_Gekko.

mengen ons daarin niet. Maar we stellen wel vast dat het begrip homo economicus een centraal model is geworden voor de economische wetenschap van een rationeel handelende en denkende economische actor.

Huizinga (1938) schreef zijn ***homo ludens*** in het interbellum. Het is een uitzonderlijk werk voor een historicus, en heeft internationaal erkenning gevonden, onder meer door een vertaling in het Engels en een lemma in Wikipedia.

> *"Homo Ludens or "Man the Player" (alternatively, "Playing Man") is a book written in 1938 by Dutch historian and cultural theorist Johan Huizinga. It discusses the importance of the play element of culture and society. Huizinga suggests that play is primary to and a necessary (though not sufficient) condition of the generation of culture. Play is older than culture, for culture, however inadequately defined, always presupposes human society, and animals have not waited for man to teach them their playing. Huizinga begins by making it clear that animals played before humans. One of the most significant (human and cultural) aspects of play is that it is fun."* [121]

Wij menen dat de *homo ludens* een conceptualisering is die complementair is aan wat we zullen zien bij de *homo sapiens*: Huizinga bespreekt het belang van de universele predispositie van de *homo sapiens* om als *homo ludens* bij te dragen aan de beleving en ontwikkeling van zijn cultuur. Hij benadrukt daarbij vijf karakteristieken van "spelen:" als een uiting van vrijheid, van verbeelding, als buiten het normale leven staand in plaats en tijd, als ordenende activiteit, als profijtloos. Spelen in deze zin amuseert en animeert en heeft, omdat het een sociale activiteit is, onbedoeld betekenis voor een cultureel *trial* en *error* gebeuren. De overeenkomst van Huizinga's *homo ludens* en de *homo economicus* is dat ze beide een centrale rol vervullen bij de theorievorming over de wijzen waarop het gedrag van actoren in verschillende disciplines wordt onderzocht. De economie is gebaat bij berekenbaarheid en eenvoud. De historicus is op zoek naar rijkere analyses. Maar ook dan is het geschiedkundig perspectief op de handelende mens als een *homo ludens* een modelmatige, sterke vereenvoudiging.

Het begrip ***homo sapiens*** is een technische term in de biologie voor de menselijke soort, (tegenwoordig eigenlijk homo sapiens sapiens), en daarmee vooral een aanduiding voor individuen met dezelfde DNA structuur.

> *"Homo sapiens, (Latin: "wise man") the species to which all modern human beings belong. Homo sapiens is one of several species grouped into the genus Homo, but it is the only one that is not extinct [...] The name Homo sapiens was applied in 1758 by the father of modern biological classification [...], Carolus Linnaeus."* [122]

121. Zie http://en.wikipedia.org/wiki/Homo_Ludens. (geraadpleegd op 22 februari 2015).
122. Zie http://www.britannica.com/EBchecked/topic/1350865/Homo-sapiens (geraadpleegd op 22 februari 2015.)

Die DNA-structuur (het genotype) bepaalt voor een belangrijk deel hoe individuen in de soort eruit gaan zien (het fenotype) en welke universele eigenschappen de individuen uit de soort zullen hebben. Deze zullen zich onder invloed van de omgeving tot individuele vermogens ontwikkelen. Vermoedelijk is het *kunnen* ontwikkelen van juridisch besef, net als het *kunnen* leren van een taal een erfelijk bepaalde, biologische predispositie.[123] Het individueel en feitelijk ontwikkelde juridische besef is dan dus, net als de individueel geleerde taal, deels biologisch en deels cultureel bepaald.

Het begrip homo sapiens gaat over het biologische deel, over de populatie, niet over een groep, en past dus in het biologische discours. Met de toename van onze kennis over evolutionaire processen, en de samenhangende popularisering ervan is het begrip ook deel gaan uitmaken van het algemene debat. Zo zijn de ongeschonden universele, biologische eigenschappen van de homo sapiens de noodzakelijke voorwaarden om zich tot een *homo ludens* te kunnen ontwikkelen.

Onze korte verkenning van de wijzen waarop samenstellingen met de Latijnse *homo* zich een blijvende plaats verwierven hangt, menen we, samen met het antwoord op de vraag of die samenstellingen een sleutelrol spelen in de modellering van het domein van de desbetreffende discipline. *Wij* gebruiken het begrip homo digitalis dan omdat het een centrale rol kan gaan spelen in het rechtswetenschappelijk debat.

3. De homo digitalis als autonoom individu

We zijn dan *de facto* op zoek naar een *voor de rechtswetenschap* bruikbare definitie van de *homo digitalis*. Bruikbaar in de zin dat hij geen verbazing wekt bij normaal gebruik, en dat hij een onvermijdelijk aanknopingspunt biedt voor rechtswetenschappelijke overwegingen. We menen dat die definitie daarom moet aansluiten bij wat zowel techno-pessimisten als techno-optimisten na aan het hart ligt, en wat centraal is voor het bestaande recht (dat mogelijk bedreigd wordt in de toekomst). We denken dat de individu als autonome beslisser *in digitalibus* in deze puzzel past. Daarmee wordt de homo digitalis een kwestie van de-mate-waarin, van de mate waarin een individu zich laat vertegenwoordigen en/of laat leiden door gedigitaliseerde processen.

Het gaat ons in deze bijdrage om verantwoorde besluitvorming, de legitimering daarvan en de rechtsbescherming in verband daarmee. In onze aanpak wordt derhalve met de term *homo digitalis* allereerst gerefereerd aan een verantwoordelijk individu, maar verder als dat zo uitkomt ook aan de individuen die deel uitmaken van instituties en instellingen, rechtspersonen, bestuursdiensten, ondernemingen en andere organisatievormen. In

123. In deze geest ook Pagel (2012).

voorkomende gevallen zal dat met zich brengen dat we dergelijke organisatievormen in het taalgebruik in minder of meerdere mate vereenzelvigen met de desbetreffende individuen die alleen of met anderen invloed hebben op de wijze waarop deze in het maatschappelijk verkeer optreden. Een andere benadering, waarbij we het begrip rigide zouden opvatten, heeft het risico dat ons blikveld te beperkt wordt en dat we geen zicht hebben op belangrijke rechtspositionele implicaties die het gevolg zijn een toenemende verdichting van de digitale dienstverlening en van digitale organisatievormen.

We gaan dus ervan uit dat de homo digitalis als autonoom individu voor zich handelt, maar zijn ons ervan bewust dat zijn rol lijkt te verminderen en te veranderen wanneer hij optreedt als functionaris c.q. vertegenwoordiger van bijvoorbeeld een onderneming of overheidsdienst.

Appendix 2. Veiligheid, vrijheid en grondrechten

Het spreekt waarschijnlijk niet helemaal vanzelf dat ons betoog kan passen in een meer algemeen beeld van de krachten en beginselen die een rol hebben gespeeld (en nog spelen) bij de ontwikkeling van onze Westerse rechtssystemen, en de rollen (bevoegdheden, taken, plichten) die bij de ontwikkeling ervan aan het bestuur werden en worden toegekend. We menen dat het zoeken naar hoe ons betoog kan passen in wat de mainstream hierover denkt behulpzaam kan zijn om het in de rechtswetenschappelijke traditie te plaatsen.

In het onderwijs van de Leidse rechtenfaculteit wordt bij de vakgroep Encyclopedie[124] de nadruk gelegd op enkele belangrijke ontwikkelingen in het rechtsdenken over het sociaal contract. Wat ons daarbij van belang voorkomt is dat in die ontwikkeling een aantal stappen kan worden herkend die laten zien dat er een aantal centrale concepten spelen: soevereiniteit, een geweldsmonopolie, de Rule of Law, de scheiding der machten en de algemene wil van een volk.

We geven een grove, functionele schets van hoe en waarom de rol van het bestuur in de trias tot stand is gekomen, hoe die functionele positionering heeft geleid tot positiefrechtelijk bevestigde beginselen die ook steunen op moderne wetenschappelijke en economische inzichten. We hangen dit verhaal op aan enkele jaartallen

1581 Het Plakkaat van Verlatinghe: Soevereiniteit wordt voorwaardelijk
In 1581 hadden de Verenigde Provinciën er genoeg van en zwoeren Philips

124. Wat hieronder volgt is ontleend aan en geïnspireerd door een hoorcollege dat onze Leidse collega mr. dr. A.J. Kwak aan buitenlandse masterstudenten gaf in 2015, wiens commentaar op deze bijlage we in dank hebben verwerkt.

II af als hun soeverein vorst. Een deel van de tekst van het Plakkaat is veelzeggend (we citeren eclectisch uit de tekst die Wikipedia geeft) omdat er duidelijk uit wordt dat aan het einde van de zestiende eeuw iets als een rechtssysteem (op zoek naar dynamisch evenwicht tussen de belangen van de prins en van zijn onderdanen), onder voorwaardelijk gezag van een soeverein (die dus kon worden afgezet):

> *[...] En so wanneer hy sulx niet en doet, maer in stede van zijne ondersaten te beschermen, deselve soeckt te verdrucken, t'overlasten, heure oude vryheyt, privilegien ende oude herkomen te benemen, ende heur te gebieden ende gebruycken als slaven, moet ghehouden worden niet als Prince, maer als een tyran ende voor sulx nae recht ende redene magh ten minsten van zijne ondersaten […] voor egheen Prince meer bekent, maer verlaeten […]*

Als we aannemen dat in die tijd het bestuur onderdeel was van de bevoegdheden van de soeverein, wordt vanaf 1581 verdedigd dat wanneer de soeverein niet voor de veiligheid van zijn onderdanen zorgt, en hun verworven privileges schendt, hij rechtmatig (als tyran) kan worden afgezet. Het bestuur heeft vanaf 1581 in Nederland een functie: het beschermen van de burgers (en hun verworven rechten).

1651 Hobbes' Leviathan: Het Zwaard en het Recht – twee hiërarchieën
Soevereinen worden vervangen. Dat gebeurde ook al in 1581. Soevereinloze gemeenschappen worden onwenselijk geacht. Hobbes stelde de vraag waarom we een soeverein (of een hiërarchisch georganiseerde macht) nodig hebben. Daarzonder maatschappelijke chaos, oorlog van man tegen man

> *"… and the life of man, solitary, poor, nasty brutish and short …"*

Om dit alles tegen te gaan is er een soeverein nodig, die beschikt over een geweldsmonopolie ("het Zwaard") dat de veiligheid van de burger garandeert. Veiligheid is de enige bron van legitimiteit voor Hobbes en alleen als de vrede en veiligheid niet effectief worden gehandhaafd mag de burger in verzet komen. Recht is vrijwel geheel ondergeschikt aan veiligheid, we zien dit terug in hedendaagse instituties als 'noodtoestand' en "noodweer." Hobbes ziet de staat en diens soevereiniteit wel *bottom up* rustend op de redelijkheid van de burgers.

1689 Locke's Treatises on Government: van Veiligheid naar Vrijheid via de Rule of Law
Maar de organisatie in termen van soeverein met een geweldsmonopolie is niet voldoende. De soeverein kan het recht zodanig vorm geven dat de tirannie legitiem wordt. Er moet iets van doelbinding komen voor wetge-

ving. Voor Locke is het respecteren van de natuurlijke vrijheid van de burger de belangrijkste bron van legitimiteit. Locke pleit dus voor een recht op verzet tegen de staat als individuele vrijheden en eigendommen worden aangetast. Het legaliteitsbeginsel volgt als vanzelf: de burger heeft natuurlijke rechten (op veiligheid, vrijheid en eigendom). Locke zoekt het dus in een verandering van focus waar het de taak van de soeverein (en het recht) betreft: het recht is er niet om te verbieden en te beschermen, maar om een zo groot mogelijke vrijheid van burgers te garanderen. Van daaruit kunnen wettelijke regels worden geformuleerd waaraan zowel Het Zwaard als het Recht zich te houden hebben. We noemen die de Rule of Law (later worden dat de grondrechten).

1748 Montesquieu's Esprit: Scheiding der Machten, Institutionele systemen

Weer een jaar of zestig later analyseert Montesquieu welke instituties het beste bij de verschillende staatsregimes passen. Hij onderzoekt er drie, de despotie, de monarchie en de republiek. Als individuele burgerlijke vrijheid centraal staat, zo betoogt hij, ontbreekt die geheel in de despotie, is die gecentreerd rond veiligheidsmaatregelen in de monarchie en is die in de republiek afhankelijk van een goede en gescheiden organisatie van de staatsmachten: wetgeving, bestuur, rechtspraak. Opnieuw gaat het om dynamische evenwichten die elkaar in toom moeten houden, en om het maximeren van de individuele vrijheid van de burger.

1768 Rousseau's Contract: Niet het staatshoofd, maar de Rule of Law als souverein; 1786 Democratiën beginnen te komen: We, the people …

Rousseau maakt het verhaal rond door een kunstgreep toe te passen. Hij stelt dat groepen een enkelvoudige algemene wil hebben die gericht is op het behoud van de groep en op het algemene welzijn daarbinnen. Bij Rousseau is niet de staat, en niet het recht, maar het volk soeverein. De algemene wil moet tot wet worden gemaakt en door de staat worden gehandhaafd. Rousseau biedt zo een conceptueel kader voor de democratie. In de moderne democratieën zijn langs deze weg vrijheidsrechten (en het legaliteitsbeginsel) tot grondrecht geworden. Het concept algemene wil staat toe om aan de producten daarvan bijzondere status toe te kennen. Locke's Rule of Law kan zo in een door Rousseau geïnspireerde benadering de rol krijgen van de souverein. In die geest wordt het bestuur dan de institutie die de opdracht heeft om de Rule of Law te verwezenlijken. We onderscheiden vaak het formele rechtsstaatsbegrip – 'rule of law' and not by men' – van het materiële rechtsstaatsbegrip waarin niet alleen het legaliteitsbeginsel maar ook een bepaalde grondrechtencatalogus tot het wezen van de rechtsstaat behoort. De in de Rule of Law gerealiseerde volkswil is zo soeverein geworden, en het bestuur daaraan dienstbaar.

2015 De homo digitalis …

In dit verhaal over de weg naar Westerse democratieën is de verhouding burger-soeverein weergegeven als een zich ontwikkelend concept. Die ontwikkeling verliep langs steeds betere manieren om het nodig geoordeelde geweldsmonopolie te brengen naar een bestuur dat steeds minder het risico in zich bergt van geweldsusurpatie. Ten eerste door de nadruk van bestuurstaken te leggen op het beschermen van vrijheid (vanaf Locke) in plaats van veiligheid. Ten tweede door grondrechten te formuleren (de Rule of Law) die grenzen stellen aan de wetgeving (doelbinding aan verwezenlijking van vrijheid). Ten derde door het bestuur in drie onafhankelijke instituties onder te brengen, en de wetgeving en de rechtspraak los te maken van het eigenlijke bestuur (machtenscheiding). Ten vierde, tenslotte, door de grondrechten als uiting te zien van de algemene wil van een volk.

In feite, en in grove lijnen, werden de Europese staten bijna allemaal tot ver in de negentiende eeuw bestuurd door nauwelijks door wetgeving ingetoomde absolute vorsten, of hun functionele equivalenten. De ideeën rond hoe regimes te verbeteren hebben in de loop der tijd vorm gekregen en zijn in de daaropvolgende periodes ook verwezenlijkt, in het bijzonder rond de Amerikaanse onafhankelijkheid, de Franse Revolutie, het Weense Congres van 1815 en de 'democratische lente' van 1848. In de geschetste ontwikkeling kan in grote lijnen een accentverschuiving worden waargenomen: van het primaat van de bescherming van individuele *veiligheid* naar het primaat van de bescherming van individuele *vrijheid*.

Eén en ander betekent dat de macht van het offline bestuur van de twintigste eeuw, voorafgaand aan de opkomst van de ICT,[125] werd beperkt door de wet (legaliteitsbeginsel), dat het bestuur een onafhankelijke institutie was naast de wetgever en de rechtspraak (machtenscheiding) en dat het bestuur als opdracht had om de grondrechten van individuele burgers te beschermen.[126]

We hebben deze beschouwing aan de ontwikkeling van onze bestuursrechtelijke arrangementen naar voren gebracht omdat we menen dat de ontwikkeling van onze samenleving van offline naar digitaal een misschien onverwachte wending neemt waar het gaat over hoe het gesteld is met de bescherming van onze individuele veiligheid en de bescherming van onze individuele vrijheid. Die twee waarden vormen een spanningsveld. Veel van onze beschouwingen over de rechtsbescherming van de homo digitalis spelen zich af tegen de achtergrond van dit spanningsveld.

125. Zie voor een analyse van de veranderende rol van de rechter in dit verband ook: Barkhuysen et al. (2014).
126. In deze geest ook Overkleeft-Verburg (1999).

Appendix 3. Iets over de homo digitalis (of de menselijke natuur) als voorwerp van natuurwetenschap

In dit preadvies verdiepen wij ons in de rechtspositie van de *homo digitalis*, de mens die in een gedigitaliseerde wereld zijn weg moet vinden en zich moet zien te handhaven. Het was ons inziens noodzakelijk uiteen te zetten wat we (als juristen) verder bedoelen met de notie van *homo digitalis* (in de rollen van bestuurder en bestuurde). We ontleenden daarbij inzichten aan menstyperingen zoals die in andere disciplines wel een bijzondere rol spelen, zoals de *homo economicus*, de *homo ludens*, de *homo universalis,* de homo *sapiens*, etc. We gaven al aan in welk opzicht de homo digitalis een bijzondere karakterisering van de mens als voorwerp van rechtswetenschappelijke studie verdient. Maar ook dat met die karakterisering het hele verhaal niet is verteld.

Natuurlijk niet, want het hele verschijnsel van maatschappelijke digitalisering was onmogelijk geweest zonder belangrijke ontwikkelingen in de natuurwetenschap. Het concept homo digitalis zou er zonder die ontwikkelingen helemaal niet zijn. En dat betekent dat het begrip homo digitalis óók een centrale (maar vermoedelijk heel andere) rol speelt voor de natuurwetenschappen. We gaan ook vanuit dit perspectief kort een aantal relevante ontwikkelingen na aan de hand van enkele (vanzelfsprekend eclectisch gekozen) jaartallen.

1687. Newton publiceert zijn *Principia* met daarin een bruikbare wiskunde voor het beschrijven van de door hem geformuleerde wetten van de mechanica en de zwaartekracht. In veel opzichten markeert dit jaartal het begin van de moderne tijd, die een natuurwetenschap inluidt die vooral mechanische verklaringen zoekt en vindt. Waar dat niet lukt wordt een intellectueel dualisme (dat Descartes al eerder filosofisch noodzakelijk vond, 1644) aantrekkelijk. Deze ontwikkeling markeert ook de kloof die tussen de natuurwetenschap en de geesteswetenschappen (waaronder we de rechtswetenschap rekenen) kon ontstaan en nog steeds de onderlinge verhoudingen domineert.

1859. Darwin publiceert zijn *On the Origin of Species.* Voor de rechtswetenschap van belang omdat er via de natuurwetenschap een argumentatielijn aan kan worden ontleend die veel van de complexiteit die we om ons heen zien verklaren kan, zonder terug te grijpen naar het beeld van een schepper. Juridisch wordt het beeld van een schepper immers traditioneel ook gebruikt om bestuurlijke soevereiniteit mee te legitimeren. Beide argumentatielijnen leiden tot zorgen over de falsificeerbaarheid. De latere ontrafeling van de structuur en werking van DNA- en RNA-moleculen hebben veel van die zorgen, voor velen, weggenomen.

1945. Von Neumann geeft het *ontwerp voor de computer* als universele rekenmachine. Aangenomen kan worden dat daarmee de digitale tijd werd ingeluid (en de homo digitalis als concept mogelijk werd) omdat dat ontwerp resulteerde in de eerste computer (en nog steeds kan worden herkend in de computers van vandaag de dag). Opmerkelijk is dat von Neumann rond die tijd ook een model van *een zelfreproducerende machine* presenteerde – waarvan later de verwantschap met onze huidige kennis over de werking van DNA en RNA is getoond.

1976. Robert May publiceert zijn "Simple mathematical models with very complicated dynamics" in *Nature,*[127] waarin hij laat zien dat heel eenvoudige mathematische modellen van situaties die voortkomen uit een eerdere versie van zichzelf tot onvoorspelbare resultaten leiden kunnen. We kiezen deze publicatie als het begin van de herkenning (en dus: bestudering) van complexiteit door de natuurwetenschappen.

Veel natuurwetenschappers beschouwen netwerken van mensen als gemeenschappen en, daarmee, als complexe, adaptieve systemen. Sommigen onthouden zich van commentaar en analyse, mogelijk omdat volledige, mathematisch oplosbare modellering van het gedrag van dergelijke systemen onmogelijk is. Anderen zien daar juist een belangrijke taak voor de wetenschap en menen dat de dynamiek in en van gemeenschappen ten minste gedeeltelijk kan worden doorgrond met behulp van de methoden en technieken complexiteitstheorieën als ontwikkeld in de exacte wetenschappen.[128]

Die methoden en technieken slaan niet erg aan in de onze discipline (de rechtsgeleerdheid). Dat zou deels te wijten kunnen zijn aan de selectie van vragen en de wijzen waarop antwoorden worden gezocht. Zo is een centrale vraag bij biologen en economen hoe te verklaren dat veel mensen de neiging hebben ontwikkeld om de kosten van samenwerking voor lief te nemen, ook in die gevallen waarin de resultaten om niet beschikbaar hadden kunnen komen. Voor juristen is die vraag niet zo van belang, omdat wij altijd over kostbare samenwerking kunnen redeneren vanuit het recht (wetgeving en overeenkomsten) dat is gemaakt door en geldt voor verantwoordelijke individuen. We vinden nu eenmaal niet dat het recht een inherent, noodzakelijk voortbrengsel is van universele natuurwetten. We gaan uit van de natuurlijke predispositie in de mens tot bewuste, verantwoordelijk gedragskeuzen en vinden het idee dat die keuzen zelf gepredestineerd zouden zijn in de oerknal nogal excentriek.

127. May (1976).
128. Bijvoorbeeld: Mitchell (2009), Lane et al. (2009), Scheffer (2009), Pagel (2012).

Het soort samenwerking dat biologen verbaast komt op een opmerkelijke wijze tot uiting bij de opbouw van de inhoud van Wikipedia en het bewaken van de kwaliteit ervan tegen ongewilde en kwaadwillig aangebrachte fouten. Belangwekkend onderzoek naar hoe die samenwerking inhoudelijk en bij de ontwikkeling en handhaving van standaarden vorm heeft gekregen, en welke rollen daarbij werden gespeeld door het formuleren en handhaven van regels werd niet gedaan door juristen, maar onder leiding van een in complexiteit geverseerde astrofysicus (die ook onderzoek deed naar rechts-culturele ontwikkelingen in het VK op basis van verschuivingen in taalgebruik in de volledige verzameling uitspraken die door de "Old Bailey" werden gedaan).[129] De ervaringen van Wikipedia en het werk van DeDeo laten zien dat, en hoe, in sommige gevallen handhaving van regels in netwerken door individuele leden uit de gemeenschap worden opgebracht.

We achten het dan ook goed mogelijk dat noties uit de niet-juridische disciplines over complexiteit voor juristen aantrekkelijk worden, wanneer duidelijk is dat de voorliggende problematiek complex is en onoplosbaar lijkende problemen oplosbaar blijken. De behandeling van bijvoorbeeld de vraagstukken van klimaatbeheersing, mensenrechten en economische uitsluiting leidt steeds vaker tot het besef dat het voorwerp van onderzoek complexe co-evoluerende netwerken vormen.[130] En dat ondersteunt het bij de bestudering ervan te hulp roepen van de modellen en de simulatietechnieken uit de wereld van de complexiteit. We denken dat die weg ook moet worden verkend bij de benadering van veel van de door ons geschetste risico's voor de homo digitalis.

We lieten al enkele voorbeelden zien van hoe complex situaties *in digitalibus* zijn. We geven hier ter illustratie drie citaten.

Het eerste citaat voert terug naar de erkenning van ons onvermogen de risico's nauwkeurig te bepalen, laat staan concrete oplossingen aan te wijzen:

> *Wanneer we in aanmerking nemen dat er zelfs onder de huidige, gebrekkige beveiligingsmogelijkheden een ontwikkeling gaande is van een offline wereld naar een digitale wereld menen we dat daarmee de noodzaak is ontstaan om effectief te werken aan behoud (of herstel) van vertrouwen in de betekenis van de materiële zorgvuldigheid. Die noodzaak rust op het besef dat, wanneer alle risico's die we hebben geïnventariseerd tegelijkertijd zouden gaan spelen, de gevolgen onrustbarend, om niet te zeggen: ont-*

129. DeDeo (2015a), Heaberlin en DeDeo (2015), Klingenstein et al. (2014).
130. Complexiteit als van netwerken binnen gemeenschappen en als van netwerken tussen gemeenschappen – als bijvoorbeeld culturen, religies, markten, disciplines, natiestaten.

> *wrichtend zouden zijn. We vermoeden dat hiermee een politieke noodzaak bestaat om tot een gelaagd fundament van betrouwbare infrastructurele protocollen en diensten te geraken waarop de individuele transacties in vrijheid en veilig kunnen worden aangegaan. In elk geval, en tenminste, voor de transacties tussen burgers en overheden*

Het tweede citaat is uit Morgan's schets van wat een Internet-of-Things is. Het vertaalt zich moeiteloos in de karakteristieken van een complex adaptief systeem:

> *"Simply put this is the concept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cell phones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of. […] The IoT is a giant network of connected "things" (which also includes people). The relationship will be between people-people, people-things, and things-things"*

Daarnaar wordt door de natuurwetenschappen en door de rechtswetenschap op heel uiteenlopende wijzen gekeken, terwijl toch aannemelijk is dat voor de inherente problemen die het IoT gaat opleveren de rechtswetenschap en de natuurwetenschappen de handen ineen zouden moeten slaan.

Het derde citaat laat zien dat die complexiteit zich in beginsel in de termen van complex adaptieve systemen, wetenschappelijk zou kunnen laten analyseren

> *… dat leidt vooral tot complicaties wanneer de knooppunten in zo'n netwerk zich in een ander tempo ontwikkelen, wanneer innovatie- of handelingscycli niet synchroon lopen. Alles kent zijn tijd. Het gaat om het verwezenlijken van technologische innovatie, de behandeling van een rechtsgeschil, het aanpassen van beleid, van de wet, een cultuuromslag, etc. Dat allemaal loopt niet zonder meer synchroon. En toch hebben al de genoemde processen invloed op elkaar, als ze deel uitmaken van zo'n netwerk*

Het is onze verwachting dat we samenwerking nodig hebben tussen alpha en beta voor het beter informeren van de politieke processen die uiteindelijk zullen bepalen hoe we de problemen aanpakken waarvoor de digitalisering ons stelt. In dit licht is het misschien nuttig om in herinnering te roepen dat de rechtswetenschap zich al millennia richt op het domesticeren van sociale complexiteit[131]

131. Te vinden achter https://en.wikipedia.org/wiki/Complex_system (geraadpleegd op 27-12-2015).

Although it is arguable that humans have been studying complex systems for thousands of years, the modern scientific study of complex systems is relatively young in comparison to conventional fields of science with simple system assumptions, such as physics and chemistry.

De natuurwetenschappelijke belangstelling voor de homo digitalis en diens maatschappelijke inbedding zou er als gevolg van het besef dat het in essentie gaat om een gedeelde belangstelling wel eens toe kunnen leiden dat de kloof wordt versmald tussen de natuurwetenschappen en de rechtswetenschap. Die kloof zelf blijft even diep, en blijft verhinderen dat we uit wat *is* kunnen afleiden wat *behoort*, maar wordt misschien door de gedeelde behoefte aan inzicht in complexiteit wel zo smal, dat we elkaar over en weer kunnen toeroepen en zelfs, soms, verstaan.

Geraadpleegde literatuur

Baase, S. (1974). IBM: Producer or predator. Reason, 4–10.

Barkhuysen, T., M. van Emmerik, B. van Ettekoven, V. Mul, R. Stijnen, en M. de Werd (2014). Adequate rechtsbescherming bij grondrechtenbeperkend overheidsingrijpen: studie naar aanleiding van de Agenda voor de Rechtspraak. Kluwer.

Beinhocker, E. D. (2006). The origin of wealth: Evolution, complexity, and the radical remaking of economics. Boston: Harvard Business School Press.

Berkhout, T. en T. van Engers (2012). Onderzoeksmethodologie voor informatiegestuurd sociaal toezicht. WFR (824).

Cliteur, P. (2002). Een sociaal grondrecht op veiligheid? niet zo'n goed idee. Regelmaat (3), 83–88.

Coase, R. H. (1937, November). The nature of the Firm. Economica 4(16), 386–405.

DeDeo, S. (2015). Conflict and computation on wikipedia: a finite-state machine analysis of editor interactions. arXiv preprint. arXiv:1512.04177.

Demsetz, H. (1969). Information and efficiency: another viewpoint. Journal of law and Economics, 1–22.

Dennett, D. en M. Kinsbourne (1992). Time and the observer: the where and when of consciousness in the brain. Behavioral and Brain Sciences 15, 183–247.

Dirkx, J. (2012). De zaak 'diginotar': handelde de overheid adequaat? Rapport, Rijksauditdienst.

Franken, H. (1993). Kanttekeningen bij hei automatiseren van beschikkingen. Pre-advies voor de vereniging voor Administratief Recht (VAR), Alphen aan den Rijn.

Fuller, L. (1930). Legal Fictions (pts. 1-3). Illinois Law Review 25, 877.

Gillebaard, H. en A. Vankan (2013, September). De digitale (zelf)redzaamheid van de burger: ondersteuning bij de Digitale Overheid 2017. Dialogic.

Groothuis, M.M. (2013). Op weg naar een digitale overheid. Over waarborgen en randvoorwaarden in bestuursrechtelijk perspectief. De Gemeentestem 2013 (7392), 436-445.

Groothuis, M.M. (2011). De digitale overheid en de Awb. Bestuursrechtelijke aspecten van van elektronische communicatie. In: Groothuis M.M., Prins J.E.J. en Schuyt C.J.M. (Red.), De digitale overheid. Preadviezen uitgebracht voor de algemene vergadering van de VAR op 20 mei 2011. Boom, 9-70.

Heaberlin, B. en S. DeDeo (Submitted on 6 Dec 2015). The evolution of wikipedia's norm network. http://arxiv.org/abs/1512.01725.

Holland, J. H. (2014). Complexity: A very short introduction. Oxford University Press.

Hooper, P. L., S. DeDeo, A. E. Caldwell Hooper, M. Gurven, and H. S. Kaplan (2013). Dynamical structure of a traditional amazonian social network. Entropy 15(11), 4932–4955.

Huizinga, J. (1938). Homo ludens: proeve eener bepaling van het spelelement der cultuur. Haarlem: Tjeenk Willink,.

Kanne, P. en J. van den Berg (2013). Kwaliteit van de overheidsdienstverlening 2013. Technical Report G6765, TNS Nipo.

Klingenstein, S., T. Hitchcock, en S. DeDeo (2014). The civilizing process in london's Old Bailey. Proceedings of the National Academy of Sciences 111(26), 9419–9424.

Lane, D., D. Pumain, S. E. van der Leeuw, and G. West (2009). Complexity perspectives in innovation and social change. Number 7 in Methodos. Springer Science & Business Media.

Loos, E. (2010, 25 juni). De oudere: Een digitale immigrant in eigen land? Een verkenning naar toegankelijke informatievoorziening (oratie UvA).

Martijn, M. (2014). Politie en inlichtingendiensten kunnen via een achterdeur bij gegevens van de belastingdienst. De Correspondent 30 september.

Martijn, M. (2015). Baas belastingdienst over big data: Mijn missie is gedragsverandering. De Correspondent (21 april).

Martijn, M. en M. Goslinga (2015). Hoe fraude het nieuwe terrorisme werd. De Correspondent 30 april.

May, R. M. (1976). Simple mathematical models with very complicated dynamics. Nature 261(5560), 459–467.

Mayer-Schönberger, V. en K. Cukier (2013). Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt.

Mitchell, M. (2009). Complexity: a guided tour. Oxford University Press, USA.

Mommers, L., G.-J. Zwenne, en B. Schermer (2010a). Het best bewaarde geheim van de raadkamer, NJB 2010, 1692, a . 32. NJB 1692(32).

Mommers, L., G.-J. Zwenne, en B. Schermer (2010b). Naschrift. NJB 1696(36).

Morgan, J. (2014). A simple explanation of the internet of things. Forbes (13 May).

Onderzoeksraad voor Veiligheid (2012). Het DigiNotarincident: waarom digitale veiligheid de bestuurstafel te weinig bereikt. Onderzoeksraad voor Veiligheid.

Overkleeft-Verburg, G. (1999). De algemene wet bestuursrecht en de (beperking van) de grondrechten. In H. Kummeling (Ed.), Het bestuursrecht als agenda voor het staatsrecht, pp. 129–153. Kluwer.

Overkleeft-Verburg, G. (2014, augustus). De belastingdienst en zijn digitale burger: spanning tussen ambities, uitvoeringsrealiteit en het juridisch kader. Maandblad Belasting Beschouwingen (7-8).

Page, W. H. en J. E. Lopatka (2009). The Microsoft case: antitrust, high technology, and consumer welfare. University of Chicago Press.

Pagel, M. (2012). Wired for culture: origins of the human social mind. WW Norton & Company.

Panteia (2015) Burgers tussen wal en schip: Het voorkomen en oplossen van knelpunten bij de (digitale) overhead, Panteia, Zoetermeer.

Persky, J. (1995). Retrospectives: the ethology of homo economicus. The journal of economic perspectives, 221–231.

Philippart, R. (2010). Toegankelijkheid van rechtspraak. NJB 1696(36).

Scheffer, M. (2009). Critical transitions in nature and society. Princeton Univ Pr.

Schmidt, A.H.J. (2009). Radbruch in cyberspace: About law-system quality and ICT innovation. Masaryk UJL & Tech. 3, 195.

Schmidt, A.H.J. (2010). Met de kennis van nu, en met de rechtswetenschap als bril: enkele gedachten over de cyberpest (afscheidsrede).

Van der Hoek, F. (2010). Huidige opzet van rechtspraak.nl zo slecht nog niet. NJB 1696(36).

Van Opijnen, M. (2014). Op en in het web. Hoe de toegankelijkheid van rechterlijke uitspraken kan worden verbeterd, (diss. UvA). Boom Juridische uitgevers.

Wieringa, T. (2005). Niemands meester, niemands knecht. De Gids (http://www.de-gids.nl/artikel/niemands-meester-niemands-knecht) Kousbroek-lezing.

Williamson, O. E. (2005). The economics of governance. American Economic Review 95(2), 1–18.

WRR (2011). iOverheid. Rapport 86, WRR, Den Haag / Amsterdam.

Zhang, K. en A. H. J. Schmidt (2015). Thinking of data protection law's subject matter as a complex adaptive system: A heuristic display. Computer Law & Security Review 31(2), 201–220.

Zwenne, G.-J. en W. Steenbruggen (2015). Privacyvoorwaarden voor de iOverheid: Vuistregels voor wet- en regelgevers met betrekking tot overheidsinformatiesystemen. Regelmaat (1), 17–36.

Zwenne, G.-J. (2009). Over kopieerbeperkingen in elektronisch bekendgemaakte besluiten. Tijdschrift voor internetrecht (2).

Zwenne, G.-J. (1998). Belastingheffing en informatieverplichtingen: reikwijdte en begrenzing van informatiebevoegdheden in de verhouding tussen belastingdienst en banken. Diss. Leiden.

Zwenne, G.-J. (2011). Redactioneel. Tijdschrift voor internetrecht 1.

Zwenne, G.-J. (2013a). De verwaterde privacywet (inaugurele rede).

Zwenne, G.-J. (2013b). Nogmaals enige opmerkingen over overheids-internet-publicatie-beleid. Tijdschrift voor internetrecht 3.

Zwenne, G.-J. en A.H.J. Schmidt (2008). Opmerkingen bij het wetsvoorstel wet bewaarplicht telecommunicatiegegevens. Mediaforum-Amsterdam 20(7), 278.