

Vrije Universiteit Brussel

From the Selected Works of Mireille Hildebrandt

2014

ICT en Rechtsstaat

Mireille Hildebrandt, *Radboud University Nijmegen*



Available at: https://works.bepress.com/mireille_hildebrandt/55/

ICT en rechtsstaat

Mireille Hildebrandt

1. Inleiding

Onderling gekoppelde computersystemen, vaak online verbonden, bepalen in toenemende mate de omgeving van staat en recht. Sterker nog, staat en recht worden voor een steeds groter deel bemiddeld, vertaald of zelfs *gemaakt* door volautomatische beslissystemen die intussen grotendeels aan het zicht zijn onttrokken. De profetische woorden van Weiser uit 1991 lijken steeds accurater. Weiser schreef over ‘calm computing’,¹ en kondigde een nieuwe werkelijkheid aan waarin computersystemen de fysieke omgeving voortdurend afstemmen op en aanpassen aan hun gebruikers terwijl hun complexiteit verborgen blijft en het toetsenbord en zelfs het beeldscherm niet meer nodig zijn.² Mogelijke wensen en voorkeuren worden in zo’n omgeving immers moeiteloos meegenomen op basis van statistische gedragsanalyses. Menselijk handelen, het aanknopingspunt voor recht en staat, wordt met dit alles steeds meer afhankelijk van ICT. De keten van beslissingen die ICT systemen voor ons nemen wordt steeds langer en complexer, waardoor ICT ook voor de overheid niet alleen een instrument is om beleidsdoelen te verwezenlijken maar een computationele tussenlaag vormt die naast toenemende functionaliteiten ook een eigen onvoorspelbaarheid ontwikkelt. Waar recht en staat sinds de uitvinding van de boekdrukkunst sterk leunen op tekst als middel tot uniformering en centralisering van juridische normering, zullen zij de komende jaren in sneltreinvaart afhankelijk worden van netwerkmachtige computersystemen. Het lijdt geen twijfel dat daarmee ook de verhouding tussen staat en recht schoksgewijs zal worden opgebroken.

Deze bijdrage gaat in op de implicaties van een *datagestuurde* infrastructuur voor de rechtsstaat, met bijzondere aandacht voor twee centrale beginselen: legaliteit en doelbinding. In paragraaf 2 worden twee opvattingen van de rechtsstaat besproken (legalisme en legaliteit) en wordt kort ingegaan op een derde opvatting van de staat, waarbij het recht ondergeschikt is aan door de politiek aangewezen beleidsdoelen (instrumentalisme). Paragraaf 3 bespreekt de overgang van de informatiesamenleving naar de datagestuurde samenleving, en gaat in op de rol van de iOverheid, gedefinieerd als een datagestuurde overheid. In paragraaf 4 worden legaliteit en doelbinding besproken met het oog op de iOverheid en paragraaf 5 sluit af met een aantal bedenkingen.

2. Over legalisme, instrumentalisme en legaliteit in de rechtsstaat

De idee van de rechtsstaat is een containerbegrip, waar gemakkelijk heel verschillende ‘dingen’ onder worden verstaan. Tegelijk is het een historisch verschijnsel met een gemeenschappelijke kern, uitgewerkt in twee richtingen. In deze paragraaf gaan we kort in op die historische kern, die nog steeds grote invloed heeft

¹ Weiser, *The Computer for the 21st Century* 1991.

² Het blijft voorlopig spannend welke rol Google Glass hierbij zal spelen, maar de introductie van een bril die de rol van muis en toetsenbord overbodig maakt geeft aan dat de zoektocht naar intuïtieve interfaces voortgaat. Zie <http://www.google.com/glass/start/>.

op ons begrip van zowel de staat als het recht.³ Vervolgens bespreken we een derde opvatting van de staat, die de interne verbinding tussen recht en staat loslaat.⁴ In de volgende paragrafen komt dan steeds de vraag aan de orde wat de digitalisering en de ‘verslimming’ van de omgeving betekenen voor de rechtsstaat.

De historische kern van de rechtsstaat ligt in de samenhang tussen staat en recht, die elkaar sinds het einde van de middeleeuwen in vergaande mate bepalen. Enerzijds laat het recht zich handhaven door de staat, dankzij de institutie van het geweldmonopolie. Daarmee is de positiviteit van het recht gegeven en de afhankelijkheid van het recht ten opzichte van de staat. Anderzijds zet de staat het recht in om haar macht te institutionaliseren en te legitimeren: *macht wordt bevoegdheid* en daarmee *schept en beperkt* het recht de macht van de staat.⁵ Daarmee zijn zowel het rechtskarakter van de moderne staat als de afhankelijkheid van de staat ten opzichte van het recht gegeven.

In de loop van de negentiende en twintigste eeuw zijn verschillende visies op de rechtsstaat tot ontwikkeling gekomen, die zich ruwweg laten indelen in formele en materiele opvattingen. De formele opvatting gaat ervan uit dat rechtsnormen gelden als zij voldoen aan de procedurele eisen voor de totstandkoming van geldige rechtsnormen; de inhoud wordt in beginsel niet getoetst. Dat laatste kan zijn uit angst voor de moralisering van het recht (rechtspositivisme), of omdat de democratische wetgever nu eenmaal het hoogste en het laatste woord hoort te hebben (volkssoevereiniteit). De formele opvatting neigt tot de idee dat de overheid vrij moet kunnen handelen als er maar een juridische bevoegdheid is waarop die handeling gebaseerd kan worden en hangt aldus samen met *legalisme*, dat wil zeggen een sterke nadruk op de naleving door de overheid van door de wetgever gestelde regels.⁶ Onder overheid worden dan in ieder geval verstaan het bestuur en de rechter, maar eventueel kan ook de wetgever zelf onder de wet worden gebracht door toetsing van de wet aan de grondwet mogelijk te maken. Zolang door de wetgever gestelde regels door de overheid worden nageleefd, althans niet worden overtreden, is dan sprake van een rechtsstaat. Deze toets is formeel omdat de nadruk ligt op procedurele eisen, zodat legalisme gemakkelijk vervalt tot proceduralisme (als de procedure is gevolgd kan niemand iets worden verweten).

De materiele opvatting gaat ervan uit dat rechtsnormen niet alleen in de wet zijn te vinden, maar ook in het ongeschreven recht. Dat ongeschreven recht wordt meestal samengevat onder de noemer van de rechtsbeginselen die de grondstructuur van het recht bepalen. Zulke beginselen hebben een hoog abstractie niveau om operationalisering in een veranderende omgeving mogelijk te maken. Rechtvaardigheid, rechtszekerheid en doelgerichtheid zijn drie voorbeelden van dragende beginselen, maar ook beginselen zoals de goede trouw, het verbod van terugwerkende kracht, de onschuldpresumptie, hoor en wederhoor en ‘fair play’ behoren tot het ongeschreven recht. Zelfs wanneer deze beginselen worden gecodificeerd behouden zij hun status van ongeschreven recht, omdat codificatie

³ Chevallier, *L'Etat de Droit* 1994. Chevallier bespreekt zowel de Duitse en Franse ontstaansontwikkeling van de ‘Rechtsstaat’ en de ‘Etat de Droit’, als het onderscheid tussen de continentale rechtsstaat en de Anglo-Amerikaanse ‘Rule of Law’. Over dat laatste bijvoorbeeld ook Grote, *Rule of Law, Rechtsstaat and ‘Etat de Droit’* 1999, p. 269–306. Zie ook Hildebrandt, *Straf(begrip) En Procesbeginsel* 2002, hoofdstuk 6.

⁴ Overeem, *The Politics-Administration Dichotomy: Toward a Constitutional Perspective* 2012.

⁵ Zie bijvoorbeeld Cleiren, *Artikel 1 Sv* 1994, over de constitutieve en limitatieve aard van de bevoegdheidstoekenning.

⁶ Shklar, *Legalism* 1964.

meestal een toespitsing en dus verenging met zich meebrengt. Dankzij dit type beginselen zijn recht en rechtsstaat adaptieve systemen, die dan ook voortdurende inzet vragen om het geheel van op elkaar betrokken rechtsregels door middel van nieuwe wetgeving, nieuwe rechterlijke uitspraken en nieuwe doctrinaire analyse te herschikken, met het oog op nieuwe toepassingen. Dit alles dan ook nog zonder de eigen identiteit als rechtsstaat te verliezen. Die identiteit impliceert dat het niet alleen om formeel geldige regels gaat, maar ook om het doorzetten van beginselen die inhoudelijk verbonden zijn met een specifieke ethiek ten aanzien van de machtsverhoudingen die in het geding zijn. Je zou kunnen zeggen dat die beginselen de interface of bemiddeling zijn tussen recht, politiek en moraal. Maar dan toch niet om het even welke bemiddeling, want de materiele opvatting van de rechtsstaat stelt een aantal morele eisen, die institutioneel verankerd moeten worden. Over de vraag welke morele eisen hier aan de orde zijn is geen overeenstemming, maar ze hebben te maken met wat Radbruch heeft bestempeld als de drie antinomieën van de rechtsidee, de hierboven al even genoemde *rechtvaardigheid* in de zin van een gerichtheid op gelijke behandeling, de *rechtszekerheid* in de zin van een gerichtheid op voorspelbaarheid en ‘doorzetbaarheid’ (positiviteit), en de *doelmatigheid* of instrumentaliteit in de zin van een gerichtheid op het algemeen belang.⁷ Radbruch gaf daarbij direct aan dat het hier niet kan gaan om een natuurrechtelijk af te leiden invulling van het algemeen belang. Hier moet de politiek dus keuzes maken. Hij waarschuwde dat rechtszekerheid geen onvoorwaardelijk rechtspositivisme kan rechtvaardigen, ook al is de positiviteit van het recht van groot belang voor de effectiviteit van het recht. Tot slot wijst Radbruch op het feit dat de vraag naar rechtvaardigheid in concrete gevallen vaak tot verschillende antwoorden leidt. Het belang van Radbruch’s beginselen steekt onder meer in zijn erkenning dat hun toepassing in specifieke gevallen tot incompatibiliteiten zal leiden, waardoor knopen moeten worden doorgehakt. In plaats van het ‘oplossen’ of ‘overstijgen’ van de tegenstrijdigheden die inherent zijn aan de eisen die aan het recht worden gesteld, bepleit Radbruch aandacht voor het feit dat het recht in ieder geval *steeds zowel is gericht op* een instrumentele inzet *als op* een rechtvaardige *en* op een voorzienbare inzet. Wanneer die gerichtheid ontbreekt is volgens Radbruch geen sprake meer van recht. Vele andere beginselen zijn door vele andere auteurs genoemd als bepalende uitgangspunten voor recht en rechtsstaat, waarbij het spel van macht en tegenmacht binnen de overheid een voorname rol speelt, als ultieme waarborg tegen monopolisme, absolutisme of totalitaire machtsuitoefening. Het gaat dan vooral om waarborgen die het handelen van de overheid principieel zowel transparant als aanvechtbaar maken *in rechte*. Daarbij gaat het niet alleen om de vraag of er een specifieke wettelijke grond is voor overheidsoptreden (legalisme), maar of dat optreden kan worden nagerekend en eventueel ook kan worden aangevochten als zijnde in strijd met het recht. De vereiste wettelijke bevoegdheid voor inbreukmakend overheidsoptreden zal dan wel een belangrijke rol spelen, maar het enkele bestaan ervan is nooit voldoende. De materiele opvatting van de rechtstaat is dan ook verbonden met een veel breder legaliteitsvereiste dan de formele opvatting die we hierboven als legalisme hebben bestempeld. Vanuit dat brede legaliteitsvereiste wordt aan wettelijke bevoegdheden een aantal kwaliteitseisen gesteld. We zien dat bijvoorbeeld terug bij de institutionalisering en afdwingbaarheid van de mensenrechten, die alleen mogen worden aangetast als aan een aantal voorwaarden is

⁷ Radbruch, *Rechtsphilosophie* 1950. Vgl. ook Fuller, *The Morality of Law* 1969.

voldaan, die tezamen de *legaliteit* van de inbreuk bewaken.⁸ De juridische bevoegdheid moet niet alleen kenbaar zijn en de inbreuken voorzienbaar maken, maar eist ook dat de uitoefening van de bevoegdheid wordt ingeperkt en voorzien van een aantal waarborgen (bijvoorbeeld rechterlijke toetsing). Ook de eis dat sprake moet zijn van een legitiem doel, dat daadwerkelijk met de inbreuk gediend moet worden en de eis dat de inbreuk proportioneel moet zijn in relatie tot het te dienen doel, maken deel uit van de legaliteitseis. Legaliteit verwijst niet alleen naar de wet, maar – conform de materiele opvatting van de rechtsstaat – naar het recht. In de rechtsstaat hoort het recht, kortom, altijd zowel instrumenteel als beschermend te zijn.⁹

Los van de theorievorming inzake formele en materiele opvattingen van de rechtsstaat is nog een derde opvatting ontstaan omtrent de verhouding tussen recht en staat, hoewel het wellicht geen zin meer heeft om hier van een rechtsstaat te spreken. Het gaat daarbij niet om legalisme of proceduralisme, of om legaliteit, maar om pure doelmatigheid. In deze opvatting is het recht slechts een middel tot het bereiken van een politiek doel. De kwaliteitseisen die aan het recht worden gesteld berusten in die visie vooral of zelfs alleen op de effectiviteit en de efficiency van het recht als middel om door de politiek gestelde doelen te bereiken.¹⁰ Het ligt voor de hand dat er naast het recht vele andere middelen zijn, waarmee eenzelfde doel kan worden gerealiseerd. Deze rechtsopvatting kan dan ook *instrumentalisme* worden genoemd en is nauw verbonden met het zogenaamde reguleringsparadigma. Voor een jurist betekent ‘regulering’ hetzelfde als normering; regulering stelt grenzen en eisen aan bepaalde *handelingen* met het oog op mogelijke rechtsgevolgen. Vanuit de cybernetica en de bestuurskunde heeft regulering echter een geheel andere betekenis.¹¹ In de vaak aangehaalde definitie van Julia Black gaat het bij regulering om *gedragsbeïnvloeding*. De politiek of de overheid in brede zin (beleidmakers en -uitvoerders) hebben een bepaald beeld voor ogen van hoe mensen zich zouden moeten gedragen en ontwikkelen instrumenten (maatregelen, regelgeving, financiële prikkels, technologie) om zulk gedrag ‘gedaan’ te krijgen. Vanuit rechtsstatelijk perspectief kan een dergelijk bestuurskundig perspectief problematisch zijn, omdat het gedrag wil sturen en daartoe detailkennis zoekt die zulke sturing mogelijk maakt. De materiele opvatting van de rechtsstaat is hecht verbonden met de mensenrechten, die een fundamentele onkenbaarheid en onbepaalbaarheid van individuele burgers garanderen. Deze onkenbaarheid en onbepaalbaarheid komen tot uitdrukking in het

⁸ Wintgens, *Legisprudentie* 2010, p. 42, onderscheidt tussen twee versies van het legaliteitsbeginsel. Enerzijds een beginsel dat eenvoudigweg verwijst naar de suprematie van de wet, anderzijds een beginsel dat verwijst naar de rechtsstaatsdoctrine waarmee de staat onderworpen wordt aan het recht. Zijn eerste uitleg valt grofweg samen met legalisme, de tweede uitleg sluit aan bij legaliteit (hoewel hij zelf weer een andere betekenis toekent aan legaliteit en niet spreekt over legalisme).

⁹ Foqué en 't Hart, *Instrumentaliteit en rechtsbescherming* 1990.

¹⁰ Vaak kort samengevat als New Public Management (NPM), waar *markets, managers* en *measurement* hoog in het vaandel staan. NPM is – onder bepaalde voorwaarden – in te passen in het gedachtengoed van de rechtsstaat in materiele zin, namelijk wanneer het marktdenken geen doel op zich is en de normatieve keuzes die gemoed zijn met financiële afwegingen goed in het vizier worden gehouden. Zie voor een toepassing van zowel klassiek-rechtsstatelijke als NPM beginselen op de rechterlijke organisatie Mak, *De Rechtspraak in Balans* 2008. Voor een analyse van het belang van effectiviteit en efficiency in de rechtsstaat Zijlstra, *Zelfstandige bestuursorganen in een democratische rechtsstaat* 1997.

¹¹ Cybernetica is ‘the science of communication and control theory that is concerned especially with the comparative study of automatic control systems (as the nervous system and brain and mechanical-electrical communication systems)’. “Cybernetics.” in: Merriam-Webster.com. Merriam-Webster, n.d. Web. 18 Aug. 2013. <http://www.merriam-webster.com/dictionary/cybernetics>.

onderscheid tussen gedrag en handeling. *Gedrag* is observeerbaar, verklaarbaar en voorspelbaar. *Handelen* is verbonden met wederzijdse verwachtingen die het mogelijk maken betekenis toe te kennen aan bepaald gedrag. Handelen veronderstelt een zekere mate van zelfbepaling, die samenhangt met de mogelijkheid zichzelf opnieuw uit te vinden. Die mogelijkheid is verbonden met een fundamentele onkenbaarheid, die verloren zou gaan wanneer een persoon volledig in beeld kan worden gebracht. Zoals hierboven uiteengezet, betreft de rechtsstaat – anders dan de democratie – niet zozeer de doelstellingen die politiek en bestuur ontwikkelen, maar de eisen waaraan de instrumenten moeten voldoen waarmee die doelstellingen worden nagestreefd. Daarmee is de idee van de rechtsstaat een variatie op Kant's categorische imperatief, die zegt dat je een ander mens nooit uitsluitend als middel tot een doel mag gebruiken maar altijd tegelijk als doel op zich moet behandelen.¹² Anders dan vaak wordt gesuggereerd zegt Kant niet dat je anderen helemaal niet mag gebruiken. Zo is het ook met het recht in de rechtsstaat. Uiteraard is het recht een instrument om doelen te bereiken, maar tegelijk heeft het recht een eigen waarde die verband houdt met de manier waarop het machtsverhoudingen bemiddelt en wederzijdse verwachtingen stabiliseert. Instrumentalisme is om die reden problematisch. Het suggereert dat het recht als instrument inwisselbaar is met – bijvoorbeeld – technologische middelen om bepaald beleid of specifiek gedrag af te dwingen (techno-regulering).¹³

De materiele opvatting van de rechtsstaat onderscheidt zich dus van zowel het instrumentalisme dat voortvloeit uit het reguleringsparadigma, als van het legalisme van de rechtsstaat in formele zin. In het vervolg verwijzen we naar de materiele opvatting onder de noemer van legaliteit.

3. De opkomst van de informatiegestuurde overheid

3.1. Van informatiesamenleving naar datagestuurde samenleving

In zijn oratie *De digitale rechtsstaat* van 1998 bespreekt Bovens de traditionele noties van de liberale, de democratische, en de sociale rechtsstaat.¹⁴ Hij constateert dat wat hij noemt 'het huis van de rechtsstaat' geconfronteerd wordt met een aantal implicaties van de oprukkende ICT, die zich moeizaam verhouden tot de traditionele vormen van de rechtsstaat. Zijn analyse betreft uiteraard de stand van zaken aan het eind van de vorige eeuw, die samengevat kan worden als de opkomst en de uitbouw van de *informatiesamenleving*. Kenmerken daarvan zijn de toenemende hoeveelheid informatie die beschikbaar is voor een toenemend aantal mensen, het steeds grotere belang van de economische waarde van informatie en de mate waarin het internet en het world wide web dankzij de toepassing van de hyperlink leiden tot een steeds lastiger te voorspellen netwerkeffect, dat bovendien weinig of geen rekening houdt met landsgrenzen. Zijn analyse kan worden samengevat in termen van deterritorialisering, turbulentie, horizontalisering en dematerialisering. Deterritorialisering verwijst naar het grensoverschrijdende karakter van internet en het web en de daarmee gepaard gaande internationalisering. Dit genereert problemen in relatie tot territorialiteit, het geweldmonopolie, en daarmee samenhangende problemen van handhaving en rechtsstatelijke begrenzing. Turbulentie verwijst naar

¹² Kant, *Grundlegung Zur Metaphysik Der Sitten* 1999 (eerste uitgave 1785), p. 52.

¹³ Leenes, *Harde Lessen* 2010. Hildebrandt, *Technologische En Juridische Normativiteit* 2011.

¹⁴ Bovens, *De Digitale Rechtsstaat* 1999.

de onvoorspelbaarheid die eigen is aan het netwerkeffect, en levert problemen op voor het legaliteitsbeginsel en de rechtszekerheid (waarbij hij de legaliteitseis overigens lijkt te reduceren tot de eis van een wettelijke grond). Bovens zoekt de oplossing in de richting van een transparante overheid en meer aandacht voor kenbaarheid van overheidshandelen voor de burger. Horizontalisering verwijst naar het feit dat de overheid zich in toenemende mate gedwongen voelt om te onderhandelen met private partijen en steeds vaker optreedt als partner in horizontale netwerken. Hij constateert dat democratie in essentie een hiërarchie veronderstelt waarbij de democratische wetgever het laatste woord heeft, terwijl de praktijk van alledag inmiddels meer weg heeft van interactieve beleidsontwikkeling en onderhandelend bestuur. Dat roept de bekende vraag op waar het heengaat met het primaat van de politiek.

Dematerialisering verwijst naar de relatieve onafhankelijkheid van informatiedragers die met online gegevensopslag en -toegang lijkt te ontstaan. Dit leidt volgens Bovens tot problemen van uitsluiting van burgers die geen toegang hebben tot de digitale infrastructuur en impliceert dat verdergaande informatierechten nodig zijn. Dit vraagt een proactieve opstelling van de overheid bij de informatievoorziening aan burgers. Hij bepleit als cruciaal element van digitaal burgerschap dan ook de toepassing van het regime van universele dienstverlening op de toegang tot ICT infrastructuur (internet). Verder wijst hij nog op de technocratisering van werkprocessen, die leidt tot steeds meer geautomatiseerde beslisprocessen, waarbij de zogenaamde ‘street level’ bureaucraat lijkt te verdwijnen, evenals de expertise die dit soort veldwerkers op grond van persoonlijke ervaring en interactie opbouwen. Tot slot formuleert hij een aantal beginselen van behoorlijke informatisering: integriteit, authenticiteit, transparantie en privacy.

Inmiddels lijken de problemen die Bovens noemt te verbleken in het licht van een nieuw type ICT, dat mogelijk is gemaakt door de steeds verdere integratie van onderling verbonden online en offline netwerken, de toenemende rekenkracht van computers, miniaturisatie van de apparatuur, exponentieel toenemende verwerkingscapaciteit en nieuwe technieken van kunstmatige intelligentie zoals met name data mijnen en machinaal leren. Het gaat daarbij om de overgang van een *informatiesamenleving* naar een *datagestuurde* samenleving. De exponentiele toename van data (machinaal leesbare gegevens) impliceert dat data niet meer samenvallen met informatie. Integendeel, een van de grote uitdagingen van de data explosie is om weer informatie te ‘maken’ van de beschikbare data. Dat gebeurt bijvoorbeeld met behulp van technieken van kunstmatige intelligentie, zoals de algoritmes van zoekmachines. Dat soort technieken bepalen ook in toenemende mate een groot aantal beslissingen die volautomatisch worden genomen, bijvoorbeeld over de prijs van diensten en producten die we overwegen aan te schaffen of de advertenties die we aangeboden krijgen. Op het moment dat onze online omgeving grotendeels wordt bemiddeld door dit soort technieken kunnen we spreken van een datagestuurde omgeving. Cyberspace valt bovendien allang niet meer samen met het internet en de daarop gebouwde virtuele wereld van het world wide web, maar is doorgedrongen tot in de haarvaten van de offline wereld.¹⁵ Enerzijds leidt dit tot een

¹⁵ Hildebrandt, *De Rechtsstaat in Cyberspace?* (Nijmegen: RU, 2011). Denk aan de gegevensverwerking die mogelijk wordt gemaakt door de OV chipkaart, het slimme energienetwerk, het meten van aankoopgedrag via de klantenkaart, het gebruik van camera's om kentekens te herkennen, elektronische patiëntendossiers, de zwarte doos in de personenauto, het gebruik van software om werknemers te monitoren.

nog verdere deterritorialisering (denk aan cybercriminaliteit en cybersecurity),¹⁶ nog grotere turbulentie (denk aan de financiële markten),¹⁷ nog meer aandacht voor horizontale netwerkachtige publiek-private samenwerking (denk aan veiligheid),¹⁸ en toenemende dematerialisering (denk aan cloud computing).¹⁹ Anderzijds doemen geheel andersoortige problemen op, die te maken hebben met de opkomst van een alomtegenwoordige datagestuurde infrastructuur, die bedrijven en overheden in staat stelt om gedrag tot in detail te voorspellen en daar zo mogelijk real-time op in te spelen.²⁰ Daarbij worden drie type data steeds belangrijker en wordt de handel daarin steeds bepalender.²¹ *Ten eerste* de vrijwillig verstrekte gegevens, bestaande uit in te vullen naam, adres, creditcard nummer of op ‘social networking sites’ (SNSs) of blogs geposte teksten en afbeeldingen. Dit type gegevens is het meest zichtbaar voor de eindgebruikers of bewoners van cyberspace, omdat ze deze zelf hebben verstrekt. Vaak is niet goed voorspelbaar wie welke gegevens uiteindelijk te zien krijgt en veel zorgen over privacy hebben daarop betrekking. Het blijkt echter dat gebruikers van SNSs zich meestal goed bewust zijn van de privacy instellingen van hun account en hier lijkt eerder sprake van reputatie management dan van de zorgeloze verspreiding van persoonsgegevens uit de begintijd van SNSs.²² *Het tweede* type data betreft geobserveerde data, meestal bestaande uit online en offline gedragsgegevens. Bij ‘gedrag’ moeten we online denken aan clickstream gedrag of het gebruik van zoektermen online (hoelang staat iemand op welk onderdeel van welke site, vanaf welke site kwam de bezoekers, naar welke site klikt zij door, hoe correleert dit met het aankoopgedrag), en offline aan bewegingen die bijvoorbeeld bij de OVChipkaart worden geregistreerd of via een navigatiesysteem, energieverbruiksgegevens die door de slimme meter worden doorgegeven of medicijngebruik dat via het Landelijk Schakel Punt kan worden ingezien. Het gaat dus altijd om meetbare en machinaal leesbare gedragsdata, die meestal niet handmatig worden ingevoerd maar rechtstreeks door computersystemen worden opgemeten op basis van de digitale sporen die gebruikers achterlaten. Terwijl dienstverleners dit type gegevens door hun software laten optekenen, zijn de eindgebruikers zich vaak nauwelijks bewust van het feit dat hun gangen worden nagegaan, je zou kunnen zeggen dat zij deze gegevens onbewust ‘lekken’. Hoewel dit type gegevens net als het eerste type vaak onder het juridische kader van de gegevensbescherming vallen, is het voor individuele personen lastig om zicht te krijgen en te houden op de onmetelijke hoeveelheid gedragsgegevens die aldus worden geregistreerd en opgeslagen, laat staan om te voorzien waar die opslag uiteindelijk toe gaat leiden. Het *derde type* data betreft de afgeleide data, die dankzij zogenaamde ‘analytics’ tot nieuwe kennis leiden. Hierbij gaat het om de resultaten van meestal statistisch geïnspireerde technieken waarmee grote hoeveelheden data

¹⁶ Hildebrandt en Koning, *Universele Handhavingsjurisdictie in Cyberspace* 2012; Hildebrandt, *Extraterritorial Jurisdiction To Enforce in Cyberspace?* 2013.

¹⁷ Esposito, *The Future of Futures* 2011.

¹⁸ ENISA, *Give and Take* 2012.

¹⁹ Uiteindelijk is ook bij Cloud Computing natuurlijk geen sprake van dematerialisering. De gegevens, software en andere diensten staan op de server bij de ‘cloud provider’ in plaats van op de eigen harde schijf. Er is dus sprake van verplaatsing en reorganisatie, niet van dematerialisering.

²⁰ Uiteraard gaat het hier om statistische voorspellingen. Hoewel deze voorspellingen op zichzelf genomen vaak onjuist zullen zijn wanneer zij op een individu worden toegepast, leidt het feit dat ze worden gebruikt voor een scale aan volautomatische beslissingen ertoe dat ze als het ware met terugwerkende kracht ‘juist’ worden. Zie over de implicaties van het veelvuldig gebruik van ‘data science’ Hildebrandt en De Vries (red.), *Privacy, Due Process and the Computational Turn* 2013.

²¹ World Economic Forum, *Personal Data* 2013.

²² Zie bijvoorbeeld <http://nutech.nl/internet/3411687/vooral-jongeren-wijzigen-privacyinstellingen-facebook.html>.

(‘Big Data’) worden doorzocht om relevante, niet-triviale patronen te vinden. Met de gevonden patronen wordt het mogelijk om gedrag te voorspellen en tegelijk de validiteit van de patronen te testen, door steeds opnieuw te checken onder welke condities de voorspellingen al dan niet uitkomen. Een voorbeeld is zogenaamd A/B onderzoek ten behoeve van geoptimaliseerde websites. Daarbij worden twee versies (A en B) van een website aangeboden.²³ Bezoekers worden doorgeleid naar een van beide versies (zonder dat ze dat doorhebben), en wel zodanig dat beide versies door evenveel bezoekers worden bezocht. Vervolgens wordt doorgemeten hoe bezoekers zich gedragen en wordt berekend welke versie de meeste impact heeft (bijvoorbeeld door te onderzoeken welke versie tot het meest lucratieve koopgedrag leidt). Hoewel A/B onderzoek evident tot verbetering van de dienstverlening kan leiden, is ook duidelijk dat bezoekers hier ongemerkt als proefpersoon worden ingezet voor real-time experimenten. Daarbij komt dat deze drie typen gegevens inmiddels op grote schaal worden gemonetariseerd, dat wil zeggen dat zij op basis van verfijnde ‘predictive analytics’ verhandeld worden tegen wisselende prijzen.²⁴ Grote delen van de economie, maar ook kritische infrastructuur staan op het punt deel uit te maken van een nieuwe economische orde, waarin verstrekte, geobserveerde en afgeleide data een hoofdrol spelen als ruilmiddel en/of als grondstof of halffabricaat voor de oprukkende personalisering van cyberspace.²⁵

De datagestuurde infrastructuur die op velerlei terreinen is doorgedrongen, heeft vergaande implicaties voor privacy, non-discriminatie en transparantie. Het lijkt erop dat consumenten in toenemende mate *doorzichtig* worden, omdat dit soort technologie in staat is om dwars *doorheen* de individuele persoon te kijken naar het soort gedrag dat zij waarschijnlijk zal gaan vertonen.²⁶ Een veelheid van gepersonaliseerde beslissingen die op het niveau van de software genomen zal worden heeft rechtstreeks invloed op de toegang tot informatie, de prijs die voor bepaalde diensten betaald moet worden, verzekeraarbaarheid, kansen op de arbeidsmarkt en andere zaken, waarbij voor de betrokken burger vaak niet duidelijk zal zijn op basis van welke profielen zij bejegend wordt. Lessig’s waarschuwing dat ons gedrag deels gereguleerd wordt door de nieuwe ICT infrastructuur is hier wellicht nog meer op zijn plaats dan bij het internet en het web. Tussen persoon en werkelijkheid is een computationele laag in ontwikkeling die de uitoefening van bepaalde grondrechten weleens helemaal buiten beeld zou kunnen brengen. De kenniskloof tussen degenen die, dankzij het monetariseren van data, nieuwe kennis verkrijgen en degene op wie allerlei statistisch gegenereerde profielen worden toegepast, wordt steeds groter. Het is nog niet eenvoudig te bepalen hoe de rechtsstaat – diep verankerd in de eervorige ICT infrastructuur van schrift en drukpers – hier nog iets te betekenen heeft. Wat kan de notie van legaliteit hier toevoegen? Is die niet vooral aan de orde waar het gaat om het handelen van de overheid zelf? In de volgende paragraaf komt eerst de notie van de iOverheid aan de orde, opgevat als een datagestuurde overheid, voordat we in de laatste paragraaf nog kort ingaan op de mate waarin een gegevensbescherming ‘by design’ sturing kan bieden bij het waarborgen van een aantal grondrechten binnen horizontale verhoudingen.

²³ Zie bijvoorbeeld http://www.google.com/analytics/apps/about?app_id=2032001.

²⁴ World Economic Forum, *Personal Data* 2013.

²⁵ Hildebrandt, O’Hara, Waidner (red.), *The Value of Personal Data* 2013.

²⁶ Hildebrandt, *The Dawn of a Critical Transparency Right for the Profiling Era* 2012. Over transparantie van en voor burgers, hoofdstukken 8 en 9 in Hildebrandt and De Vries, *Privacy, Due Process and the Computational Turn*.

3.2. De iOverheid als datagestuurde overheid

Sinds eind jaren '90 zijn overheden onder de noemer van de eOverheid het internet gaan inzetten bij het communiceren met hun burgers.²⁷ De eOverheid past bij wat heet de informatiesamenleving, en heeft vooral betrekking op online verstrekking van informatie en andere diensten. De informatiesamenleving en de eOverheid moeten niet worden verward met de zogenaamde iOverheid, die veel meer is gericht op het creëren van toegevoegde waarde op basis van de onmetelijke hoeveelheid gegevens die verschillende overheden in handen hebben en eventueel met elkaar zouden kunnen delen. De iOverheid past in de datagestuurde samenleving en staat voor een *informatiegestuurde* Overheid. Omdat we er niet van uit kunnen gaan dat data automatisch samenvalt met informatie, gaat het eigenlijk om een datagestuurde overheid. Met die benaming komt ook duidelijker tot uitdrukking dat overheden informatie mijnen uit data, hetgeen de aandacht mede richt op de stap van data naar informatie, die zeker niet evident is.²⁸

In het rapport van de WRR over de *iOverheid* wordt gesproken over de vernetwerking en verrijking van gegevens en het daardoor mogelijk gemaakte proactieve optreden van de overheid.²⁹ *Vernetwerking* is de nieuwe term voor bestandskoppeling en publiek-private samenwerking, toegespitst op het delen en uitwisselen van gegevens die betrekking hebben op het gedrag van burgers. De idee is enerzijds dat het erg vervelend is om burgers steeds weer om dezelfde gegevens te vragen als ze toch al bij een onderdeel van de overheid bekend zijn. Anderzijds kunnen op deze manier beslissingen worden genomen op basis van een veel vollediger beeld van de burger die aanspraak maakt op uitkeringen en toeslagen of de burger die aan haar belastingverplichtingen moet voldoen. Ook in de sfeer van de handhaving van de openbare orde en de strafrechtelijke aanpak zou veel winst te behalen zijn als de overheid snel toegang heeft tot informatie vanuit verschillende contexten, zodat eerder en proactiever kan worden opgetreden bij verwachte problemen. *Verrijking* van gegevens ziet op het genereren van nieuwe kennis uit grote gegevensbestanden, waarin de vernetwerkte data – bij voorkeur geanonimiseerd – worden geaggregeerd. In hun recente *Big Data. A Revolution That Will Transform How We Live, Work and Think* vatten Viktor Mayer-Schönberger en Kenneth Cukier de zogenaamde 'Big Data' revolutie samen.³⁰ Onder 'Big Data' verstaan zij niet zomaar een hoop gegevens, maar een verwijzing naar:³¹

things one can do at a large scale that cannot be done at a smaller scale.

Daarmee doelen ze op het feit dat de onwaarschijnlijke hoeveelheid data die doorzocht kan worden op relevante patronen de aloude steekproef overbodig maakt: 'N = all'. Door de grote hoeveelheden is minder precisie nodig (want fouten worden vanzelf gecorrigeerd door nieuwe data), en door de aanhoudende stroom nieuwe data is de zoektocht naar causaliteit vervangen door de focus op correlatie. Alles en iedereen wordt 'gedatificeerd' en relevant bevonden data worden vervolgens

²⁷ Uiteraard worden computersystemen en internet ook gebruikt tussen overheden onderling.

²⁸ Hierover Hildebrandt and De Vries, *Privacy, Due Process and the Computational Turn*, hoofdstuk 2.

²⁹ Wetenschappelijke Raad voor het Regeringsbeleid, *iOverheid* 2011.

³⁰ Mayer-Schönberger, Cukier, *Big Data* 2013.

³¹ Ibid. 6.

gemonetariseerd. Op alle fronten wordt de rol van data analisten groter, ten koste van inhoudelijk experts. Ten slotte, hoewel ze eschatologische verwachtingen lijken te koesteren ten aanzien van deze revolutie,³² komen de auteurs toch met een aantal caveats. Zo waarschuwen ze voor de verlamdende werking die 'Big Data' zou hebben op privacy, de mogelijkheid dat straffen gebaseerd worden op statistieken, en het gevaar dat 'dataficatie' het aura versterkt van objectiviteit en waarheid dat vaak ten onrechte aan cijfers, kwantitatief onderzoek en door computers berekende uitkomsten wordt toegekend. Dit hangt samen met de suggestie, in het rapport over de *iOverheid*, dat overheden op basis van voortgaande 'dataficatie' proactief kunnen gaan optreden,³³ omdat de actuariële kennis van klantenprofielen en digitale klantendossiers de overheid in staat stelt de toekomst beter in kaart te brengen.³⁴ Het is niet ondenkbaar dat sommigen uit alle enthousiaste berichten over vernetwerking en verrijking afleiden dat regulering een stuk gemakkelijker zal worden; het beïnvloeden van burgers zou eenvoudiger worden als 'de' data inzicht geven in hoe de burger zal reageren op verschillende typen prikkels. Het doet denken aan het 'Behavioural Insights Team', ook wel genoemd de 'Nudge Unit' bij de regering van het Verenigd Koninkrijk.³⁵

The Behavioural Insights Team, often called the 'Nudge Unit', draws on insights from academic research in behavioural economics and psychology, to apply them to public policy making. The team works across all areas of government policy, developing policy and testing it empirically, where possible using randomised controlled trials.

We kunnen opmerken dat hierbij wellicht sprake is van de nieuwe kleren van de oude keizer. De gedragseconomische aanpak verzet zich weliswaar tegen de rationalistische vooronderstellingen die ten grondslag ligt aan de rechtseconomische inspiraties van bijvoorbeeld Lessig, maar met het vervangen van de *homo economicus* door de *homo bias* blijft deze nieuwe benadering binnen het kader van het reguleringsdenken. Op het moment dat een *bias* kan worden afgeleid uit de beschikbare 'Big Data',³⁶ kan de burger de goede kant op worden *genudged*. Daar is niets mis mee, als de burger maar door heeft dat zij, wanneer zij en hoe zij wordt aangestuurd, zodat zij zich daar eventueel in rechte tegen kan verzetten. Daarmee komen we aan bij de drie typen beginselen die het rapport over de *iOverheid* onderscheidt:

³² Net als Ayres, *Super Crunchers* 2007.

³³ 'Datificatie' is een term die niet in het *iOverheid* rapport wordt gebruikt. Desondanks lijkt het rapport daarop aan te sturen. Onder datificatie verstaan we hier het vertalen van de analoge, vloeiende, continue en multi-interpretable werkelijkheid in discrete, digitale, machinaal leesbare data, om deze vervolgens te gaan bewerken, vanuit de gedachte dat ze de werkelijkheid adequaat representeren.

³⁴ 'Predictive analytics' op basis van Big Data is nauw verwant met de actuariële wetenschappen, die zich bezighouden met de wiskundige berekening van verzekerbare risico's. Feeley and Simon spreken van 'actuarial justice' om aan te geven dat dit type calculaties het strafrechtelijk beleid doordringen, zie Feeley, M. and J. Simon, 'Actuarial Justice: The Emerging New Criminal Law', in *The Futures of Criminology*, D. Nelken (red.), London: Sage, 1994, 173–201.

³⁵ <https://www.gov.uk/government/organisations/behavioural-insights-team>. Zie ook aanmaningen om deze aanpak in Nederland te introduceren, op het blog van Economisch Statistische Berichten: <http://www.econometrie.nl/weblog/gedragseconomie-en-beleid-tijd-voor-actie>. Vgl. Thaler and Sunstein, *Nudge* 2008).

³⁶ Gedragseconomische inzichten verwijzen naar een aantal cognitieve bias die inherent zouden zijn aan menselijke cognitie. Zij bouwen voort op het werk van met name Kahneman, *Maps of Bounded Rationality* 2003, maar zie bijvoorbeeld de kritiek van Gigerenzer, *How to Make Cognitive Illusions Disappear* 1991.

[S]tuwende beginselen (zoals veiligheid, effectiviteit en efficiëntie), verankerende beginselen (privacy en keuzevrijheid) en procesmatige beginselen (transparantie en accountability). Stuwende beginselen zijn verbonden met de drive van de overheid om ict in tal van domeinen in te zetten en staan in het teken van verbetering en kwaliteitswinst. Verankerende beginselen staan voor het waarborgen van vrijheden, het in kaart brengen van ‘stille verliezen’ bij voortgaande digitalisering en voor het vrijwaren van de autonomie van het individu. Ze vormen als het ware een tegenwicht voor de stuwende beginselen. Procesmatige beginselen ten slotte staan voor de procedurele omlijsting die het mogelijk maakt dat afweging tussen de stuwende en verankerende beginselen met name inzichtelijk en toetsbaar is.

Hoewel de indeling in stuwende, verankerende en procesmatige beginselen aantrekkelijk is omdat het meer instrumentele beginselen (die ons voortstuwten bij het realiseren van beleidsdoelen) onderscheidt van meer beschermende beginselen (die rechten en vrijheden verankeren, onder meer door transparantie en verantwoording), blijft onduidelijk hoe deze beginselen zich tot elkaar verhouden en tot de hierboven besproken legaliteit als kern van de rechtsstaat. Het rapport spreekt – conform veel beleidsrapportages en -adviezen – van borging, van ketenpartners,³⁷ van het digitaal klantdossier,³⁸ van eenmalige uitgaaf en hergebruik van gegevens, van misbruik en oneigenlijk gebruik van gegevens en van correctieverzoeken en terugmeldingen.³⁹ Voorop staat steeds de combinatie van effectiviteit, efficiency en bescherming. Het gaat dan al gauw over de noodzakelijke afwegingen, zoals ongetwijfeld die waarbij bescherming tegen effectiviteit en efficiency wordt afgewogen en die waarbij instrumentele beginselen tegen beschermende beginselen worden afgewogen. Het beeld van de weegschaal doemt op, dat enerzijds een toonbeeld van redelijkheid en zorgvuldigheid lijkt, maar anderzijds kritisch bevraagd moet worden voor zover prangende kwesties ermee worden verbloemd. De vraag bij dit soort afwegingen is immers (1) of het opofferen van bescherming wel leidt tot de grotere veiligheid die vaak wordt beloofd, (2) of de precisie die wordt gesuggereerd onder verwijzing naar de notie van de afweging wel waargemaakt kan worden, (3) of rechten en vrijheden überhaupt wel opgeofferd mogen worden om de enkele reden dat hierdoor beleidsdoelen kunnen worden bereikt, (4) of de bescherming van de een niet wordt opgeofferd voor de beveiliging van de ander, (5) of meer uitgebreide bevoegdheden om veiligheid na te streven zelf geen veiligheidsrisico meebrengen en (6) of het pleiten voor stuwende maatregelen niet tot symboolwetgeving leidt die alleen de perceptie van veiligheid beïnvloedt, maar geen aantoonbaar effect heeft op de veiligheid zelf.⁴⁰ Hoewel afwegingen onvermijdelijk zijn, eist een afweging binnen het juridische kader van de legaliteit om te beginnen dat inbreuken op grondrechten

³⁷ Over het verschil tussen ketens (gezamenlijk doel) en netwerken (losse samenwerking), zie *iOverheid* 2011, p. 72.

³⁸ Het digitaal klantdossier maakt informatie-uitwisseling mogelijk tussen alle organisaties binnen de zogeheten Structuur Uitvoeringsorganisatie Werk- en Inkomen (SUWI).

³⁹ Over de spanningsverhouding tussen hergebruik en doorlevering van gegevens enerzijds en bescherming van persoonsgegevens anderzijds, zie bijvoorbeeld het Inspectierapport van het Ministerie van Sociale Zaken en Werkgelegenheid *Informatie-uitwisseling van de SUWI-keten met andere partijen. Programmarapportage Informatieprocessen*, 2012.

⁴⁰ Cf. Waldron, *Security and Liberty* 2003. Zie overigens de heldere analyse van effectiviteit en efficiency in *iOverheid* 2011, p. 76-77, idem dito inzake veiligheid, p. 77-79. Zie verder over afwegingen p. 85-87 en 210-214.

een legitiem doel hebben, noodzakelijk en proportioneel zijn in een democratische samenleving, en berusten op een voor de betreffende maatregel bestemde juridische grondslag. Indien deze afweging ertoe leidt dat de inbreuk inderdaad noodzakelijk en legitiem is, eist de materiele opvatting van de rechtsstaat dat tegenover de inbreuk een aantal effectieve waarborgen zijn geïnstitutionaliseerd. Een van die waarborgen is het doelbindingsbeginsel, dat helaas geen evidente rol lijkt te spelen in het rapport van de *iOverheid*.⁴¹ Dit beginsel is hecht verbonden met het legaliteitsbeginsel. Niet in die zin dat de overheid alle bewegingsruimte wordt ontnomen of dat de overheid alles mag als er maar een wettelijke bevoegdheid is (dat zijn twee vormen van legalisme), maar in de zin dat al het handelen van de overheid integer moet passen binnen het kader van de rechtsstaat. Dat betekent dat de vernetwerking en de verrijking van persoonsgegevens en het daardoor mogelijk gemaakte proactieve optreden van de overheid altijd mede getoetst moet worden aan het legaliteitsbeginsel en de daarmee verbonden doelbinding. Doelbinding is echter geen waarborg die alleen van toepassing is wanneer inbreukmakende handelingen aan de orde zijn. Als uitvloeisel van de legaliteitseis betekent doelbinding dat alle interventies van overheden een legitiem en uitdrukkelijk doel moet hebben, waar de overheid op kan worden aangesproken en waaraan haar handelen getoetst kan worden. De vrije ruimte die aan individuele burgers toekomt om hun leven naar eigen inzicht en op basis van eigen doelstellingen in te richten, komt niet toe aan de overheid. Waar burgers zich vrij moeten weten hun eigen doelen na te streven binnen de grenzen van de wet, zijn overheden gehouden alleen die doelen na te streven die hen door de democratische wetgever en de geschreven en ongeschreven constitutie zijn opgedragen.

4. Legaliteit, doelbinding en de rechtsstaat in cyberspace

4.1. Bestandskoppeling ten behoeve van fraudebestrijding

In het rapport over de *iOverheid* stellen de auteurs dat het vernetwerken en verrijken van informatie en het voeren van preventief en proactief beleid de *iOverheid* in staat stellen om ‘een omvattend beeld te verkrijgen van burgers’.⁴² Het staat er echt. Hoewel het rapport uitgebreid ingaat op verankerende beginselen die – zo constateren de auteurs – vaak het onderspit delven bij afweging tegen meer instrumentele beginselen, blijkt de informatiepositie van de *iOverheid* toch gericht op het verkrijgen van een omvattend beeld van burgers. Dat verklaart dan gelijk waarom de beschermende beginselen het afleggen. Het mag duidelijk zijn dat overheden met een omvattend beeld van burgers het grondrecht op privacy op ontoelaatbare wijze schenden.⁴³ Daarover is genoeg geschreven en het zijn natuurlijk niet alleen overheden die steeds omvattender profielen aanleggen van hun ‘klanten’.

In deze bijdrage gaat het echter specifiek om de vraag in hoeverre de staat op grond van het legaliteitsbeginsel enerzijds is gehouden om de eigen informatiepositie te versterken om specifieke beleidsdoelen te verwezenlijken, en anderzijds is

⁴¹ Maar zie bijvoorbeeld *iOverheid* 2011, p. 59, 62, waar het gaat over de (beleids)doelen die bepalend zijn voor de vernetwerking en verrijking van gegevens.

⁴² Ibid. p. 16 en 215.

⁴³ Zo oordeelde het Duitse Constitutionele Hof in Karlsruhe, BVerfG, 27 februari 2008, 1 BvR 370/07, 1 BvR 595/07, dat ongelimiteerde toegang tot allerlei gegevens waarmee omvattende profielen van individuele burgers kunnen worden gemaakt in strijd is met het recht op gewaarborgde integriteit en vertrouwelijkheid van computersystemen.

gehouden om de fundamentele onkenbaarheid en de onbepaalbaarheid van individuele burgers te respecteren. Het mag duidelijk zijn dat er een evidente spanningsverhouding is tussen deze beide aspecten van het legaliteitsbeginsel. Onkenbaarheid en onbepaalbaarheid verwijzen niet zomaar naar een kennisgebrek of een gebrek aan sturingsvermogen. Het gaat hier om normatieve uitgangspunten die de staat de toestemming ontzeggen om enerzijds gedetailleerde kennis van individuele burgers te zoeken (onkenbaarheid) en om anderzijds – bijvoorbeeld dank zij die kennis – individuele burgers als pionnen over een schaakbord te schuiven ten einde bepaalde beleidsdoelen te bereiken (onbepaalbaarheid). Het recht op privacy en het ermee verbonden respect voor de persoonlijke autonomie van individuele burgers zijn gegrond in de idee dat de overheid de handen af moet houden van de persoonlijke levenssfeer en daar alleen in mag treden wanneer daarvoor expliciete bevoegdheden bestaan die met de nodige waarborgen zijn omgeven. De idee van onbepaalbaarheid is verbonden met het hierboven besproken verschil tussen juridische normering en regulering; waar juridische normering appelleert aan bereidheid om te handelen in overeenstemming met het recht, poogt regulering mensen te beïnvloeden door ze als mechanismen te beschouwen die kunnen worden aangestuurd. Kennis van die mechanismen is dan een eerste vereiste om goed te kunnen sturen. Een datagestuurde overheid zal dus zorgen dat zoveel mogelijk kennis uit de databergen wordt gemijnd, ten einde burgers te kunnen verleiden of desnoods dwingen om ‘compliant gedrag’ te vertonen.⁴⁴ Het feit dat het hier gaat om *gedrag* en niet om *handelen* verraadt een extern perspectief en een zekere desinteresse in het perspectief van de aan te sturen burger. Het uitgangspunt van de onkenbaarheid en onbepaalbaarheid van individuele burgers impliceert echter dat de staat zich nooit ten doel mag stellen om een omvattend beeld te verkrijgen van burgers. Het legaliteitsbeginsel brengt de staat onder het recht en eist daarmee dat de staat deze normatieve uitgangspunten van het recht bij *al haar handelen* handhaaft. Tegelijk biedt het legaliteitsbeginsel ook de mogelijkheid om welbepaalde kennis en zelfs aanstuurbaarheid na te streven. De voorwaarden daarvoor zijn dat de betreffende kennis of aanstuurbaarheid noodzakelijk en proportioneel is voor het nastreven van specifieke legitieme doelen, mits daarbij de nodige waarborgen zijn geïnstitutionaliseerd. Het beginsel van doelbinding vloeit dus voort uit het legaliteitsbeginsel en is hecht verbonden met de proportionaliteitseis; het *beperkt* de mate waarin gegevens kunnen worden genetwerkt en verrijkt, alsmede ook de mate waarin de overheid op basis van risicoprofielen handelend op kan treden. Daarbij kan het niet gaan om de afweging of de overheid zich in een voorliggend geval wel of niet aan het legaliteitsbeginsel zal houden. Dat moet de overheid in een rechtsstaat altijd. Binnen het kader van dat legaliteitsbeginsel kan wel een afweging aan de orde zijn, maar die afweging mag er nooit toe leiden dat de overheid streeft naar omvattende kenbaarheid en aanstuurbaarheid van haar burgers.

4.2. De Waterproof

⁴⁴ Berkhout, Van Engers, *Onderzoeksmethodologie voor informatiegestuurd fiscaal toezicht* 2012. De auteurs stellen voor om middels het in kaart brengen van ‘toekomstige non-compliance gedragspatronen’ tot proactief beleid te komen (p. 828). Het gaat daarbij om ‘[h]et dynamiseren van een risicogerichte aanpak [die] bestaat uit het op basis van transacties activeren van een verzameling abstracte risicopatronen’ (p. 830).

In de late middeleeuwen werden mensen soms onderworpen aan de zogenaamde waterproef,⁴⁵ waarbij hun onschuld pas kwam vast te staan als zij naar de bodem zonken na in het water te zijn gegooid; bovendien was een teken van hekserij en bewees aldus de schuld. Inmiddels kennen wij onder de titel ‘Waterproof’ de bestandskoppeling van waterverbruiksgegevens en opgegeven vervuilingseenheden met gegevens van ontvangers van een uitkering op grond van de Wet werk en bijstand (WWB), met gegevens van ontvangers van een huurtoeslag, en met gegevens van alleenwonende AOW’ers. Meer precies gaat het hierbij om het vergelijken van waterverbruiksgegevens die – gezien de in het GBA opgenomen bewonersaantal dat de vervuilingseenheden bepaalt – extreem hoog of extreem laag zijn, met gegevensbestanden van personen die een uitkering, AOW of huurtoeslag ontvangen. De gedachte is dat extreem hoog of extreem laag waterverbruik een mogelijke indicatie is van schijnbewoning, dat wil zeggen dat meer of minder personen op het adres verblijven dan bekend bij de GBA.

Het College Bescherming Persoonsgegevens (CBP) achtte de bestandskoppeling in 2007 in strijd met de noodzakelijkheidseis van art. 8(e) Wet bescherming persoonsgegevens (Wbp), en – wat betreft de gegevens van de waterschappen - onverenigbaar met het doel waarvoor de gegevens in eerste instantie waren verzameld, zoals vereist in art. 9 Wbp.⁴⁶ Kort gezegd meent het CBP dat het voor burgers niet duidelijk was dat hun waterverbruik gebruikt zou kunnen worden voor detectie van fraude met bijstand, AOW of huurtoeslagen. Het CBP merkt daarbij op dat de gegevens niet werden verwerkt naar aanleiding van een concrete verdenking van fraude, of naar aanleiding van een statistisch relevante risico analyse. De gegevens werden juist gebruikt om daaruit een ‘risicosignaal’ te bekomen, op basis waarvan nader onderzoek kon worden gedaan, wat dan weer zou kunnen leiden tot een concrete verdenking. Dit is een bijzonder relevant voorbeeld van de manier waarop doelbinding in het kader van de legaliteitseis moet worden uitgelegd en van de manier waarop doelbinding en proportionaliteit zich verhouden tot ‘Big Data’. Het is ook een voorbeeldig geval omdat de omschakeling naar slimme meters en slimme energienetwerken tot een explosie van digitaal beschikbare energieverbruiksgegevens zal leiden, die in beginsel eveneens kunnen worden ingezet voor fraude detectie.⁴⁷

Bij de toetsing van het Waterproof project gaat het volgens het CBP om een bestandskoppeling waarbij persoonsgegevens van hele groepen onverdachte burgers worden doorgelicht ‘om risicosignalen te verkrijgen’. Dat mag niet.⁴⁸

Argument hiervoor is dat bij bestandskoppelingen met als doel het verkrijgen van risicosignalen de feitelijke inbreuk op de persoonlijke levenssfeer al heeft plaatsgevonden terwijl de vraag of deze gerechtvaardigd was nog moet worden beantwoord. De noodzaak tot het raadplegen en koppelen van

⁴⁵ Van de Vrugt, *Aengaende Criminele Saken* 1982, p. 6.

⁴⁶ CBP, *Bevindingen Ambsthalve Onderzoek Waterproof*, 2007. Zie ook CBP, *Notitie fraudebestrijding door bestandskoppeling* 2006. Het CBP meent overigens kennelijk dat wanneer sprake is van een inlichtingenplicht naast de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit geen verenigbaarheidseis geldt (ibid, p. 2). Onduidelijk is waarom dat het geval is, tenzij het CBP meent dat we ervan uit moeten gaan dat in dat geval de onverenigbaarheidstoets door de wetgever is verricht en daarmee niet meer toetsbaar is.

⁴⁷ Vgl. ook F. Jensma, Binnenkort: het totale burgervolgsysteem, *NRC Handelsblad* 23 februari 2013 over automatische kentekenregistratie op basis van ‘een landelijk dekkend cameranetwerk boven de wegen om er daders mee te pakken’.

⁴⁸ CBP, *Bevindingen Ambsthalve Onderzoek Waterproof*, p. 9.

bestanden dient vooraf, in de vorm van een verdenking van fraude of een risicoanalyse, te kunnen worden aangetoond.

Wat wel is toegestaan, zijn koppelingen tussen geanonimiseerde gegevensbestanden en enquêtes die risicofactoren aan het licht brengen, zodat de groep personen wiens persoonsgegevens daadwerkelijk wordt gecontroleerd beperkt blijft.⁴⁹ We komen daar hieronder nog op terug. De Rechtbank Utrecht meende in 2008 overigens, dat wel degelijk sprake was van proportionaliteit tussen het controle- en verificatiebelang en het opvragen van waterverbruiksgegevens; net als de Centrale Raad van Beroep in haar oordeel van 2010, hecht de Rechtbank Utrecht daarbij belang aan het feit dat een voorselectie is gemaakt (alleen extreem hoge of extreem lage verbruiksgegevens werden gebruikt).⁵⁰

In dit voorbeeld lijkt doelbinding een beperkte rol te spelen, vanwege de focus op proportionaliteit (noodzakelijkheid). Dat is echter schijn, want proportionaliteit ziet hier op de evenredigheid en gepastheid van de verwerking van persoonsgegevens in relatie tot het legitieme doel dat ermee is gediend. Het onderliggende probleem is dan ook de vraag of het juridisch toelaatbaar is om de proportionaliteit van gegevensverwerking te relateren aan een doel waarvoor de gegevens niet zijn verzameld. Mogen gegevens worden verwerkt voor een nieuw doel, gebaseerd op een andere juridische grond (bevoegdheid), door een andere ‘data controller’, wanneer dit nieuwe doel niets te maken heeft met het doel waarvoor de gegevens oorspronkelijk aan een andere ‘data controller’ zijn verstrekt? Wordt hiermee de legaliteit van de gegevensverwerking geschonden of kan een dergelijke gang van zaken onder bepaalde voorwaarden worden gelegitimeerd? Heeft doelbinding nog enige betekenis als dit type bestandskoppeling schering en inslag wordt en met enkele kunstgrepen gelegaliseerd kan worden? Mag de iOverheid bij hergebruik van persoonsgegevens als dat zo uitkomt aanspraak maken op een andere juridische grond en de proportionaliteit alsdan zoeken in de relatie tussen de nieuwe verwerking en het nieuwe doel zonder nog acht te slaan op de eventuele onverenigbaarheid van het nieuwe doel met het oorspronkelijke doel?⁵¹

4.3. Doelbinding en proportionaliteit bij de iOverheid

In zijn *Opinie inzake het beginsel van doelbinding binnen het kader van de gegevensbescherming*, gaat de Art. 29 Werkgroep nader in op deze vragen. Het standpunt van de Werkgroep is, dat verdere verwerking van persoonsgegevens voor een ander doel alleen is toegestaan wanneer deze verwerking verenigbaar is met het oorspronkelijke doel. Ook wanneer sprake is van een nieuwe juridische grond, moet

⁴⁹ CBP, *Notitie Fraudebestrijding Door Bestandskoppeling*, p. 4.

⁵⁰ LJN: BD6227, Rechtbank Utrecht, 9 juni 2008; LJN: BM3881, Centrale Raad van Beroep, 17 april 2010.

⁵¹ Zie ook het wijzigingsvoorstel voor o.a. de Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI, Kamerstukken 33 065, 15 maart 2013), waarin grootschalige vernetwerking en verrijking van persoonsgegevens wordt mogelijk gemaakt met als doel proactieve fraudebestrijding in de sociale zekerheid. Hiertoe wordt het zogenaamde systeem risico indicatie (SyRI) in het leven geroepen (voorgesteld in art. 65). In art. 54 lid 8 wordt een verplichting opgenomen voor leveranciers van water en energie om gegevens door te leveren aan de relevante bestuursorganen, ten einde risico-indicaties te verkrijgen.

het doel van de verwerking verenigbaar zijn met het oorspronkelijke doel.⁵² Een van de voorbeelden die de Werkgroep geeft is het gebruik van energieverbruiksgegevens voor de detectie van belastingfraude en illegale wietplantages. De Werkgroep meent dat dit doel waarschijnlijk onverenigbaar is omdat het in strijd is met de gerechtvaardigde verwachtingen van energieconsumenten en omdat hierbij gegevens worden gebruikt van consumenten waartegen geen enkele verdenking bestaat, noch een indicatie dat zij tot een risicogroep behoren. Het simpele feit dat er een juridische grond is voor de verwerking (hetzij een wettelijke verplichting om gegevens aan te leveren, hetzij de uitvoering van een publieke taak door de uitkeringsverstreckende instantie), maakt de toetsing van de verenigbaarheid van het nieuwe doel met het oorspronkelijke doel nog niet overbodig. Het lijkt erop dat de Werkgroep het Waterproof project – net als het CPB – zou beoordelen als zijnde in strijd met het doelbindingsbeginsel. Een ander voorbeeld betreft het gebruik van energieverbruiksgegevens om patronen te vinden van fraude met de slimme energiemeter, waaruit indicatoren kunnen worden afgeleid voor gedrag dat correleert met fraude. Omdat het hier gaat om fraude met energieverbruiksgegevens meent de Werkgroep dat, mits wordt voldaan aan de nodige waarborgen, hier geen sprake is van een doel dat niet verenigbaar is met het oorspronkelijke doel (het leveren en factureren van energie). Gebruikers van een slimme meter kunnen redelijkerwijs verwachten dat hun gegevens met het oog op het voorkomen en sanctioneren van fraude zullen worden gecontroleerd. Hoewel hier sprake is van een andere juridische grond (de gerechtvaardigde belangen van de belanghebbende energieleverancier of de uitvoering van een publieke taak door de netwerkbeheerder) is het doel aldus verenigbaar.

De toegevoegde waarde van ‘Big Data’ wordt vrijgezet door nieuwe vormen van kunstmatige intelligentie. Kenmerk daarvan is het lerend vermogen van de technieken waarmee grote databestanden worden doorzocht, op zoek naar patronen die toegevoegde waarde kunnen genereren. Het interessante van machinaal leren is dat het correlaties op kan leveren die niet waren voorzien en patronen die met het blote oog niet zichtbaar zijn. Daarmee wordt kennis gegenereerd waarvan we niet wisten dat we er niet van wisten.⁵³ Dit alles verhoudt zich moeizaam tot doelbinding en legaliteit, nu het gaat om kennis die gebruikt kan worden voor doelen waarvan we niet konden vermoeden dat ze door het verwerken van gegevens dichterbij zouden komen. De meerwaarde van een datagestuurde omgeving steekt in de onverwachte nieuwe mogelijkheden die door het verwerken van gegevens worden geschapen. De vraag is dan ook of doelbinding en legaliteit, die uitgaan van vooraf bepaalde beperkingen, niet haaks staan op alles waar de nieuwe, datagestuurde infrastructuur voor staat. De vraag is ook of het toestaan van bestandskoppeling op basis van geanonimiseerde gegevensbestanden niet leidt tot verfijnde risico-analyses die na toepassing op de relevante categorieën van burgers tot een omkering van de bewijslast en een uitholling van de onschuldpresumptie gaan leiden. Anonimisering biedt daartegen

⁵² Art. 29 Werkgroep, WP 203, *Opinie 03/2013 inzake doelbeperking* 2013. De Werkgroep stelt dan ook voor om het vierde lid van art. 6 van de voorgestelde Algemene Verordening Gegevensbescherming te schrappen. De Werkgroep meent dat in het vierde een vrijbrief wordt geboden om een nieuwe verwerking te baseren op een nieuwe juridische grond, zonder toetsing van de verenigbaarheid van het nieuwe doel aan het oorspronkelijke doel. Gezien Overweging 40 is het overigens de vraag of het vierde lid wel zo gelezen moet worden.

⁵³ Zarsky, *‘Mine Your Own Business!’* 2002-2003; Hildebrandt, Gutwirth, *Profiling the European Citizen* 2008.

geen enkele bescherming. Strikte interpretatie van het juridisch kader, zoals voorgestaan door het CBP en de Art. 29 Werkgroep, leidt tot het verbieden van bestandskoppeling als het nieuwe doel onverenigbaar is met het oorspronkelijke doel. Dat zou betekenen dat het nieuwe doel in het vervolg al bij de eerste verwerking bekend moet worden gemaakt, dan wel dat de gegevens niet hergebruikt mogen worden. Mij dunk dat het heel verstandig is om burgers bij het opnemen van de meterstanden te wijzen (bij de slimme meter standaard op het display vermelden) op het feit dat hun gegevens mogelijk wordt gebruikt om specifieke vormen van fraude te detecteren. Als overheden vinden dat dit moet kunnen en de wetgever gaat hiermee akkoord, dan hoeven we daar tegenover de burger ook geen doekjes om te winden. Van zo'n waarschuwing kan bovendien een preventieve werking uitgaan, die het doel van de inbreukmakende verwerking wellicht nog meer dient dan de detectie zelf. Mochten burgers echter menen dat we hiermee in Orwell's *1984* terecht zijn gekomen, dan kan de ophef over dit soort bestandskoppelingen leiden tot democratische besluitvorming om ervan af te zien. Maar, daarmee zijn de problemen zeker niet van de baan. Het grootschalig koppelen van *geanonimiseerde* gegevensbestanden om daaruit verfijnde risicoindicaties te mijnen kan veel grotere implicaties hebben, omdat aldus via geautomatiseerde signaalfuncties allerlei geautomatiseerde beslissystemen in gang kunnen worden gezet, met als doel alleen de aldus gesignaleerde gedragingen nader te gaan monitoren. De combinatie van anonieme gegevens en meer specifieke verdenking kan ertoe leiden dat degene die in de gaten wordt gehouden daar geen idee van heeft en zich daar dus niet tegen kan verzetten.⁵⁴ Juist dan moet het recht om niet aan dit soort beslissystemen te worden onderworpen, in samenhang met het recht om hierover te worden geïnformeerd wanneer een van de uitzonderingen van toepassing is, effectief worden ingebouwd in de datagestuurde overheidssystemen. Zowel de huidige Richtlijn, als de nieuwe Verordening leggen dit recht vast met de bijbehorende transparantieplichting.⁵⁵ Onder de Verordening zullen zowel het recht als de verplichting bovendien als een vorm van gegevensbescherming 'by design' geëffectueerd moeten worden.⁵⁶

5. Afsluiting

De relatie tussen de informatie en communicatie technologische infrastructuur en de vorming van staat en recht is niet altijd evident, en we staan te weinig stil bij de manier waarop het schrift en de drukpers de aard van recht en staat hebben bepaald. De nieuwe ICT infrastructuur van datagestuurde onderling en online verbonden computerssystemen genereert nieuwe verhoudingen tussen recht en staat. In dit hoofdstuk is vanuit een materiele opvatting van de rechtsstaat nader onderzocht wat de implicaties zijn van de toenemende automatisering van beslissystemen, de toegang

⁵⁴ Zie ook de MvT bij het wetsvoorstel aanpassing SUWI, waar wordt gesteld dat de individuele burger wiens gegevens daadwerkelijk worden verwerkt naar aanleiding van de risico analyse, daarvan niet op de hoogte wordt gesteld 'Niet alleen zou dit een onevenredige inspanning vergen van de overheid, maar het zou ook de modus operandi vrijgeven waaraan calculerende burgers hun gedragingen zouden kunnen aanpassen' (idem p. 37, beschikbaar <http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/03/15/wetsvoorstel-tot-wijziging-van-de-wet-suwi-en-enige-andere-wetten-in-verband-met-fraudeaanpak-door-gegevensuitwisselingen.html>).

⁵⁵ Art. 15 en 12 Richtlijn Gegevensbescherming. Art. 20 voorgestelde Algemene Verordening Gegevensbescherming. Zie ook art. 42 van de Wbp. Hildebrandt, "The Dawn of a Critical Transparency Right for the Profiling Era."

⁵⁶ Art. 23 voorgestelde Algemene Verordening Gegevensbescherming.

tot 'Big Data' en de inzet van machinaal leren. Daarbij ligt de nadruk op de taakvervulling van de overheid in haar rol als datagestuurde overheid, met bijzondere aandacht voor de houdbaarheid van het doelbindingsbeginsel bij de koppeling van gegevensbestanden. Conclusie is dat het steeds moeilijker zal worden om doelbinding als uitvloeisel van het legaliteitsbeginsel te bewaken binnen de gegevensbescherming bij de iOverheid. In een rechtsstaat behoort de overheid individuele burgers, bij de inzet van hun gedragsgegevens als instrument van gedragssturing of fraude detectie, niet alleen zien als te reguleren elementen, maar juist als zelfsturende personen die aanspraak kunnen maken op een fundamentele onkenbaarheid en onbepaalbaarheid. Dat betekent dat zij recht hebben op kennis van de manier waarop de iOverheid probeert hun gedrag te beïnvloeden en rechtsmiddelen moeten hebben om zich daartegen te verzetten.

Literatuurlijst

- Ayres, I., *Super Crunchers : Why Thinking-by-numbers Is the New Way to Be Smart*, New York: Bantam Books 2007.
- Berkhout, T.M., T.M. van Engers, 'Onderzoeksmethodologie Voor Informatiegestuurd Fiscaal Toezicht', *Weekblad Fiscaal Recht* 2012/6958, p. 824-832.
- College Bescherming Persoonsgegevens, *Bevindingen Ambsthalve Onderzoek Waterproof*, Den Haag: 2007.
- Bovens, M., *De Digitale Rechtsstaat. Beschouwingen over informatiemaatschappij en rechtsstaat*, Alphen aan den Rijn: Samsom 1999.
- Chevallier, J., *L'Etat de Droit*, Parijs: Montchrestien 1994.
- Cleiren, C.P.M., 'Artikel 1 Sv', Melai (red.), *Wetboek van Strafvordering* 1994.
- ENISA. *Give and Take. Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime*, 2012, www.enisa.europa.eu.
- Esposito, E. *The Future of Futures: The Time of Money in Financing and Society*, Cheltenham: Edward Elgar Publishing 2011.
- Feeley, M. and J. Simon, 'Actuarial Justice: The Emerging New Criminal Law', in *The Futures of Criminology*, D. Nelken (red.), London: Sage, 1994, 173-201.
- Foqué, R., A.C. 't Hart. *Instrumentaliteit En Rechtsbescherming*, Arnhem Antwerpen: Gouda Quint Kluwer Rechtswetenschappen 1990.
- Fuller, L. L. *The Morality of Law*, New Haven: Yale University Press 1969.
- Gigerenzer, G., 'How to Make Cognitive Illusions Disappear: Beyond 'Heuristics and Biases'', *European Review of Social Psychology*, W. Stroebe, M. Hewstone (red.), Chichester: Wiley 1991.
- Grote, R., 'Rule of Law, Rechtsstaat and 'Etat de Drois'', *Constitutionalism, Universalism and Democracy - A Comparative Analysis*, C. Starck (red.), Baden-Baden: Nomos 1999, p. 269-306.
- Hildebrandt, M. *De Rechtsstaat in Cyberspace?* Nijmegen: RU, 2011.
- . *Straf(begrip) En Procesbeginsel. Een Onderzoek Naar de Betekenis van Straf En Strafbegrip En Naar de Waarde van Het Procesbeginsel*, Deventer: Kluwer/Sanders Instituut 2002.
- . 'Technologische en juridische normativiteit: het tekort van het reguleringsparadigma. Een respons op Leenes' 'Technoregulering'', *Recht Der Werkelijkheid* 2011/1, p. 53-59.
- . 'The Dawn of a Critical Transparency Right for the Profiling Era', *Digital Enlightenment Yearbook 2012*, Amsterdam: IOS Press 2012, p. 41-56.
- . 'Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace', *University of Toronto Law Journal* (63) 2013/2, p. 196-224.
- Hildebrandt, M., M. Koning, 'Universele Handhavingsjurisdictie in Cyberspace?' *Strafblad* 3 2012, p. 195-203.
- Hildebrandt, M., and Serge Gutwirth. *Profiling the European Citizen. Cross-disciplinary Perspectives*. Dordrecht: Springer, 2008.
- Hildebrandt, M., K. de Vries (red.), *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*. Abingdon: Routledge 2013.

- Hildebrandt, M, Kieron O'Hara, and Michael Waidner, eds. *The Value of Personal Data. Digital Enlightenment Yearbook 2013*. Amsterdam: IOS Press, 2013 (te verschijnen).
- Kahneman, D. 'Maps of Bounded Rationality: Psychology for Behavioral Economics', *The American Economic Review* (93) 2003/5: 1449–1475.
- Kant, I. *Grundlegung Zur Metaphysik Der Sitten*, Hamburg: Meiner 1999 (oorspronkelijke uitgave 1785).
- Leenes, R. *Harde Lessen. Apologie van Technologie Als Reguleringsinstrument*, Tilburg: Universiteit van Tilburg 2010.
- Mak, E., *De rechtspraak in balans: een onderzoek naar de rol van klassiek-rechtsstatelijke beginselen en 'New Public Management'-beginselen in het kader van de rechterlijke organisatie in Nederland, Frankrijk en Duitsland*, Nijmegen: Wolf Legal Publishers 2008.
- Mayer-Schonberger, V., K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (1st ed.) London: John Murray 2013.
- College Bescherming Persoonsgegevens, *Notitie Fraudebestrijding Door Bestandskoppeling*, Den Haag 2006.
- Overeem, P., *The Politics-Administration Dichotomy: Toward a Constitutional Perspective*. (2nd ed.) CRC Press, 2012.
- World Economic Forum, *Personal Data: The Emergence of a New Asset Class* 2013, <http://www.weforum.org/reports/personal-data-emergence-new-asset-class>.
- Radbruch, G. *Rechtsphilosophie* (heruitgave Erik Wolf), Stuttgart: Koehler 1950.
- Shklar, J. N. *Legalism*, Boston: Harvard University Press 1964.
- Thaler, R. H., C. R. Sunstein. *Nudge : Improving Decisions About Health, Wealth, and Happiness*, New Haven: Yale University Press 2008.
- Vrugt, Van de, M. *Aengaende criminele saken. Drie hoofdstukken uit de geschiedenis van het strafrecht*, Deventer: Kluwer 1982.
- Waldron, J. 'Security and Liberty: The Image of Balance', *Journal of Political Philosophy* (11) 2003/2, p. 191–210.
- Weiser, M. 'The Computer for the 21st Century', *Scientific American* 265/3 1991: 94–104.
- Wetenschappelijke Raad voor het Regeringsbeleid, *iOverheid* 2011.
- Wintgens, Luc. *Legisprudentie: Opstellen over recht en wetgeving*, Larcier: 2010.
- Zarsky, T. "'Mine Your Own Business!': Making the Case for the Implications of the Data Mining or Personal Information in the Forum of Public Opinion", *Yale Journal of Law & Technology* 5/4 2002-2003, p. 17–47.
- Zijlstra, S.E. *Zelfstandige bestuursorganen in een democratische rechtsstaat. Een onderzoek naar democratisch-rechtsstatelijke en positiefrechtelijke aspecten van het gebruik van zelfstandige bestuursorganen, meer in het bijzonder op gemeentelijk niveau*, 's-Gravenhage: VUGA 1997.