Technologie en wetgeving in cyberspace

Hildebrandt, M.; Leenes, R.E.; Lokin, M.H.A.F.

Published in:
RegelMaat

Document version:
Publisher's PDF, also known as Version of record

Publication date:
2012

ARTIKELEN

Technologie en wetgeving in cyberspace: verstandshuwelijk of innige relatie?

M. Hildebrandt, R.E. Leenes & M.H.A.F. Lokin

1. Inleiding

Technologische ontwikkelingen en digitalisering van de samenleving hebben steeds meer invloed op recht en wetgeving. Omgekeerd zou het recht steeds meer invloed op technologische ontwikkelingen moeten hebben, om te zorgen dat bepaalde waarborgen die het recht beoogt te bieden door oprukkende techniek niet teloorgaan.
De wetgever lijkt de zich in sneltreinvaart voltrekkende digitalisering van de samenleving als een voldongen feit te beschouwen, en is nogal eens geneigd achter die vermeende feiten aan te hollen. Per domein en beleidsdoel wordt wetgeving op maat gemaakt en waar deze in het ene domein ophef veroorzaakt (het elektronisch patiëntendossier (EPD)), wordt deze in het andere tamelijk geruisloos ingevoerd (het Digitaal Klantdossier in de sociale zekerheid, dat in opzet en werking niet wezenlijk verschilt van het EPD).
Het verder ontwikkelen van algemene kaders zoals in de Wet elektronisch bestuurlijk verkeer (Webv), de Wet bescherming persoonsgegevens (WBP) en de Wet openbaarheid van bestuur (WOB) lijkt vooralsnog geen hoge prioriteit te hebben. Het regeerakkoord benoemt technologie en digitalisering vooral als een instrument ter ondersteuning van ondernemerschap en het economisch klimaat in Nederland,[1] als een medium om tot een efficiëntere overheid te komen (*shared services* op ICT-gebied) of ter ondersteuning van het veiligheidsbeleid (cameratoezicht). Concrete maatregelen die het akkoord onder het kopje 'informatieveiligheid en bescherming van persoonsgegevens' noemt, zijn vrij traditioneel van aard:

- Voorgenomen maatregelen inzake opslag, koppeling en verwerking van persoonsgegevens worden zo veel mogelijk voorzien van een horizonbepaling en bij de voorbereiding nadrukkelijk getoetst aan effectiviteit.
- Het kabinet komt met een voorstel voor een meldplicht voor alle diensten van de informatiemaatschappij, waaronder de overheid, in geval van verlies, diefstal of misbruik van persoonsgegevens, waarbij alle datalekken worden gemeld aan de nationale toezichthouder, die boetes kan opleggen indien de meldplicht niet wordt nageleefd.
- Het toezicht op grootschalige informatiseringsprojecten en het oplossen van automatiseringsproblemen wordt structureel aangescherpt.
- Het kabinet komt met een integrale aanpak van cybercrime.

1 *Kamerstukken II* 2010/11, 32 417, nr. 14.

Het kabinet lijkt de wetgever het gebaande pad op te willen leiden van 'regels maken en (repressief) handhaven' om problemen die de ontwikkeling van cyberspace met zich brengt op te lossen. De vraag is of dat nog een begaanbare weg is. Een serieuze bezinning op de manier waarop het recht in een informatiegestuurde samenleving tegelijk zijn instrumentele en waarborgfunctie kan waarmaken, is noodzakelijk. Daarbij past anticipatie in plaats van na-ijlen, in combinatie met een gezonde dosis scepsis. Wat in ieder geval niet past is om onder druk van 'de markt' of onbewezen efficiency- en effectiviteitsdromen allerlei nieuwe ICT-systemen door te voeren.
In deze bijdrage schetsen we enkele lijnen rond de ontwikkeling van cyberspace en daarbij opkomende dilemma's voor de wetgever. Na een korte bespreking van wat wordt bedoeld met cyberspace (par. 2) gaan we in op de interactie tussen technologie en wetgeving (par. 3). Daarna komt de positie van de burger in het steeds meer uitdijende domein van cyberspace aan de orde, waarbij de nadruk ligt op de burger als leverancier van gegevens waarmee bedrijven rijk hopen te worden en waarmee de overheid effectiviteit en efficiency denkt te bevorderen (par. 4). We gaan in op de merites van (nog meer) geschreven regels als oplossing voor de geschetste dilemma's en op mogelijke alternatieven (par. 5 en 6). In de laatste twee paragrafen besteden we aandacht aan de toenemende inzet van technoregulering bij het voorschrijven en afdwingen van bestuurlijke wetgeving (par. 7), met aandacht voor de caveats die daarbij passen (par. 8). We sluiten af met een beschouwing over de in onze optiek wenselijke rolverdeling tussen recht en technologie in cyberspace (par. 9).

2. Cyberspace?

We noemden in de inleiding al een paar keer het begrip *cyberspace*. Daarover eerst wat meer. De term is ouder dan het fenomeen dat we er nu mee aanduiden, namelijk de informatie-*gestuurde* samenleving die zich in razend tempo heeft ontwikkeld in het verlengde van de informatiesamenleving. Het woord cyberspace is geïntroduceerd door de schrijver W. Gibson in zijn roman *Neuromancer* uit 1984. Hoewel de eerste netwerken die zouden uitgroeien tot het *world wide web* al met elkaar verbonden waren en zelfs de eerste e-mailspam al een feit was,[2] maakte informatie- en communicatietechnologie toen nog lang niet zo'n omvangrijk en ingrijpend deel uit van ons dagelijks leven. En hoewel cyberspace ook nu nog associaties oproept met *Star Trek*, *1984* en andere sciencefictionfilms en -boeken is onmiskenbaar dat we er deel van uitmaken. Ons dagelijkse doen en laten, de aanspraken die we hebben en de verplichtingen waaraan we moeten voldoen jegens de private partijen en de overheid, de wijze waarop we met elkaar communiceren, alles wordt in hoge mate bepaald door technologische mogelijkheden om informatie – al dan niet in bits en bytes – te genereren, transporteren, combineren, profileren en archiveren.

2 Cf. <http://nl.wikipedia.org/wiki/Geschiedenis_van_het_internet>.

Cyberspace is dus een feit. De vraag is hoe we de rechtsstaat er een goede plaats in geven.[3] Daarvoor is het van belang om te bekijken op welke wijzen technologie en recht met elkaar samenhangen.

3. Technoregulering en juridische bescherming by design

De interactie tussen technologie en recht kan vanuit twee perspectieven worden bezien. De eerste invalshoek is die van *juridische bescherming by design*.[4] Technologie biedt ons mogelijkheden om juridische waarborgen tot hun recht te laten komen, bijvoorbeeld door software en systemen zo te ontwikkelen dat zij de publieke en private belangen op het gebied van privacy, transparantie, verantwoording en dergelijke als het ware automatisch, oftewel *by default* beschermen.
Door te spreken van juridische bescherming wordt de nadruk gelegd op het feit dat computercode wordt ingezet in opdracht van de democratische wetgever. Daarmee ordent deze bijvoorbeeld het speelveld voor bedrijven, zodat het inbouwen van privacy of andere grondrechten geen concurrentienadeel hoeft op te leveren. Daarnaast kan de wetgever de nodige voorwaarden scheppen voor het digitale verkeer tussen burgers en bedrijven en tussen burgers en overheid, ter bescherming van fundamentele waarden in onze samenleving.
De concept-EU-Verordening gegevensbescherming[5] illustreert deze visie op de verhouding tussen technologie en recht. Daarin is een apart hoofdstuk ingericht dat *privacy by design* en *privacy by default* voorschrijft bij alle technologie waarmee persoonsgegevens worden verwerkt. Als de verordening wordt aangenomen, hebben de desbetreffende bepalingen directe werking in de Nederlandse rechtsorde; de nationale wetgever zal zich moeten bezinnen op de vraag wat dat precies betekent.
Juridische bescherming *by design* betekent in feite dat de democratische wetgever zich bezig gaat houden met de wijze waarop de ICT-infrastructuur interfereert met de grondrechten en een gepast beschermingsniveau afdwingt. En dan niet alleen met traditionele regels en handhaving daarvan, maar door concreet richting te geven aan en invloed uit te oefenen op de manier waarop deze worden geïncorporeerd in de specificaties van software en systemen. Dat vraagt om te beginnen om meer aandacht voor de manier waarop technologische infrastructuren onze handelingsmogelijkheden verruimen en inperken.
Juridische bescherming *by design* gaat er namelijk van uit dat codes in software en ICT-systemen steeds vaker invloed uitoefenen op ons gedrag, zelfs zonder dat we dat doorhebben, en vaak ook zonder dat het de bedoeling was. Het gaat dan om niet door een democratische wetgever ingezette technoregulering. Dit wordt wel '(computer)*code as regulation*' genoemd. Te denken valt aan dvd-recorders die zodanig geprogrammeerd zijn dat zij in Europa geen Amerikaanse dvd's kunnen

3 M. Hildebrandt, *De rechtsstaat in cyberspace?* (oratie Nijmegen), 2011, uitgegeven in eigen beheer, <http://works.bepress.com/mireille_hildebrandt/39/>.
4 M. Hildebrandt, 'Juridische bescherming "by design"?', *Rechtsfilosofie & Rechtstheorie* 2010/afl. 2, p. 101-106.
5 Beschikbaar via <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm>.

afspelen, en omgekeerd. Daarmee wordt op effectieve wijze een segmentering van de markt bewerkstelligd, met omzeiling van mededingingsregels.
Niet bedoeld, maar wel invloedrijk is bijvoorbeeld het netwerkeffect van het delen van informatie op online sociale netwerken zoals Facebook en Hyves, dat onverwachte gevolgen kan hebben voor de privacy van derden. We zien daarbij dat deze netwerken niet alleen de kern van het recht op privacy raken omdat (jonge) mensen er veel persoonlijke informatie op delen, maar vooral omdat het verdienmodel inmiddels drijft op de verkoop van geregistreerd websurfgedrag. Dat laatste wordt mogelijk gemaakt door de technische infrastructuur (codes) die het voortdurend loggen en opslaan van onlinegedrag mogelijk maakt. De inbreuk op de privacy is hier niet het doel, maar wel het neveneffect van een bewust toegepast verdienmodel dat eigenlijk pas goed op stoom komt als surfgedrag overal en altijd kan worden opgeslagen en doorzocht. Juridische bescherming *by design* is erop gericht dit soort 'neveneffecten' in kaart te brengen en op het niveau van de technische infrastructuur de erosie van grondrechten tegen te gaan.
Ten slotte kan *code as regulation* ook expliciet en wettelijk worden geregeld, zoals een alcoholslot tegen rijden onder invloed, rekeningrijden om congestie tegen te gaan en elektronische detentie. Het wettelijk opleggen van technische maatregelen om bedrijven en burgers tot naleving te dwingen wordt ook wel technoregulering genoemd.[6] In beginsel is technoregulering een neutrale term, die bijvoorbeeld verwijst naar het gebruik van technologie als middel voor het bereiken van beleidsdoelen. Vanuit het perspectief van rechtsstaat en democratie is van belang te onderkennen dat noch het geschreven recht, noch technoregulering een neutraal instrument is. Met het concept van 'juridische bescherming *by design*' wordt beoogd de instrumentele en beschermende functies van het recht niet als *tradeoffs* te zien, maar vanuit een coherent kader samen te nemen.[7]

4. De burger als cognitieve bron van een slimme omgeving

In deze paragraaf gaan we kort in op de manier waarop de ICT-infrastructuur zich tot een computationele in*kijk*structuur heeft ontwikkeld. Als we surfen op het internet laten we een massa aan informationele vingerafdrukken achter en het internet nestelt zich door middel van cookies ook comfortabel in onze computer. Muziek die we downloaden, recepten die we raadplegen voor een etentje met vrienden, informatie die we opzoeken over kwalen waaraan we lijden, alles wordt vastgelegd.
De technologie om de gegevens op te slaan die wij bewust en onbewust verstrekken, wordt steeds goedkoper. Dat heeft ertoe geleid dat het verzamelen van en voorsorteren op onze online- en offlinegedragsgegevens een hoge vlucht hebben genomen. Daarmee worden ons aankoopgedrag, reisgedrag, rijgedrag (TomTom), medisch relevant gedrag en allerlei andere manieren van doen en laten tot op grote hoogte transparant voor de (commerciële) buitenwereld.

6 R. Leenes, *Harde lessen – apologie voor technologie als reguleringsinstrument* (oratie Tilburg), 2010.
7 R. Foqué & A.C. 't Hart, *Instrumentaliteit en rechtsbescherming*, Arnhem/Antwerpen: Gouda Quint/Kluwer Rechtswetenschappen 1990.

Daarnaast wordt de technologie om de grote hoop gegevens (meestal met enig gevoel voor understatement *Big Data* genoemd) te doorzoeken, aangeduid als *data mining* of het 'mijnen' van informatie, steeds slimmer en steeds beter in staat om patronen te vinden en te valideren in zowel gestructureerde als ongestructureerde data. Onder gestructureerde data verstaan we voor bepaalde doelen of bedrijfsprocessen ingewonnen of verzamelde gegevens die in gedefinieerde structuren machinaal verwerkt worden of opgeslagen zijn, bijvoorbeeld de belastingaangifte. Onder ongestructureerde data verstaan we informatie in documenten, op websites, in tweets, blogs, enzovoort, maar ook films en muziek.
Een mooi voorbeeld van de kracht van dit soort technologie is IBM's Watson, een supercomputer die is gebouwd voor het beantwoorden van vragen in natuurlijke taal. Hij is niet verbonden met het internet, maar beschikt wel over 200 miljoen pagina's gestructureerde en ongestructureerde informatie, waaronder de volledige tekst van Wikipedia. IBM liet Watson begin 2011 meedoen aan de populaire Amerikaanse kennisquiz Jeopardy, die hij overtuigend won.[8]
Maar ook (veel) dichter bij huis is die kracht merkbaar. Als twee personen hetzelfde trefwoord intypen op Google, zullen ze verschillende *hits* gepresenteerd krijgen, omdat deze mede gebaseerd zijn op eerder surf- en zoekgedrag. En als we in januari bij Wehkamp een spijkerbroek een maatje groter bestellen dan gebruikelijk, zou het zomaar kunnen dat bij ons volgende bezoek aan de site een advertentie verschijnt voor een dieet(product) om onze kerstkilo's weer kwijt te raken.
Enerzijds fungeren onze online- en offlineomgeving dankzij deze technologieën steeds meer als een fantastische cognitieve bron, die onze vermogens om nieuwe informatie te vinden en te interpreteren exponentieel doet toenemen. Letterlijk met een paar muisklikken hebben we de wereld in huis. Anderzijds lijken we zélf steeds meer te functioneren als cognitieve bron voor de onzichtbare *data analytics*, die het mogelijk maken onze omgevingen geruisloos en subtiel af te stemmen op onze afgeleide voorkeuren.
Die onzichtbaarheid doet af aan onze autonomie,[9] omdat we (evidente gevallen daargelaten) niet kunnen beoordelen op grond van welke statistische inferenties[10] beslissingen worden genomen of informatie wordt aangeboden. Dit speelt zowel in de commerciële als in de publieke sector. Het algoritme van Google dat bepaalt welke zoekresultaten we voor ons zien, iTunes die onze muziekvoorkeuren stuurt, maar ook de acceptatie van onze zorgverzekering en de opleidingskansen voor onze kinderen.

8 IBM White Paper, 'Watson – A System Designed for Answers. The Future of Workload Optimization', 2011, <www-03.ibm.com/innovation/us/watson/what-is-watson/a-system-designed-for-answers.html>; zie ook J. Markoff, 'On "Jeopardy!" Watson Win Is All but Trivial', *The New York Times* 16 februari 2011, sec. Science, <www.nytimes.com/2011/02/17/science/17jeopardy-watson.html>.

9 En zou onder omstandigheden zelfs een inbreuk op de persoonlijke levenssfeer kunnen vormen.

10 Dat wil zeggen generalisaties, door het gelijkstellen van de eigenschappen van een populatie aan die van een individu. Het probleem van statistische inferenties is dat de sprong van geaggregeerd naar individueel niveau altijd een hachelijke zaak is: of de eigenschappen van de populatie voor het individu gelden, weten we immers niet; het kan, maar het hoeft niet. Zie B. Custers, *The Power of Knowledge*, Nijmegen: Wolf Legal Publishers 2004.

Hoe dit in het publieke domein plaatsvindt, laat de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) zien in het rapport iOverheid.[11] Informatie over personen en entiteiten waarover overheidsorganisaties beschikken, raakt steeds meer vernetwerkt en verknoopt: gegevens worden een-op-een hergebruikt, of er worden – al dan niet geanonimiseerd – profielen van gemaakt die voor andere doelen en in andere contexten worden ingezet.
De consequenties hiervan kunnen verstrekkend zijn. Voorbeelden als het EPD, de database voor vingerafdrukken uit het paspoort en het dossier rekeningrijden bevestigen dat. Het stelt zware eisen aan beveiliging van informatie die in systemen of websites opgeslagen ligt. Wat er gebeurt als deze onvoldoende is, hebben de DigiNotar-kwestie en problemen bij het gebruik van DigiD laten zien.
In de meeste gevallen wordt de praktijk van het vernetwerken en verrijken van grote hoeveelheden data – zowel door het bedrijfsleven als door de overheid – gepresenteerd als dienstverlening. De vraag is echter of ons wel een dienst wordt bewezen, zeker nu de onzichtbaarheid van de criteria op grond waarvan we worden benaderd, evenzeer geldt voor de criteria op grond waarvan wij (of onze gegevens) eventueel weer uit databestanden verdwijnen. De vraag is dus hoe we onze autonomie weer terugkrijgen. De huidige oplossing, bijvoorbeeld gecodificeerd in de ePrivacy-richtlijn,[12] is een uitdrukkelijke toestemming vooraf (*opt in*) voor het 'mijnen'[13] van al die gegevens. Dat levert echter weinig op zolang we niet weten welke consequenties de opslag en het doorzoeken van die gegevens hebben. Het vraagt dus om adequate (technische) mogelijkheden voor de burger om snel en intuïtief te achterhalen welke conclusies bedrijven en overheid hebben getrokken op basis van de vloed aan gegevens, hoe die informatie wordt gebruikt en hoe hij fouten kan (laten) rechtzetten.

5. Pavlov: meer geschreven regels?

De gebruikelijke reactie van juristen, politici en misschien ook wel burgers is om bij elk serieus probleem – en daar kunnen we hier wel van spreken – de oplossing te zoeken in nieuwe geschreven regels. De in de inleiding genoemde voorbeelden uit het regeerakkoord illustreren dit.
Deze reactie is begrijpelijk, maar het is de vraag of regels in de klassieke zin van het woord ons in staat stellen de uitdagingen die cyberspace met zich brengt het hoofd te bieden. We beschrijven hier twee voorbeelden die ons inziens aantonen dat we daarmee niet meer toekomen. Het eerste voorbeeld laat overigens tegelijk zien dat sommige geschreven regels adequater zijn dan andere.

11 Zie <www.ioverheid.nu>.

12 D 2002/58/EC, artikel 5 en 6. Zie hierover bijv. *Opinie* 2/2010, WP 171, van de art. 29 Werkgroep inzake gedragsgestuurd adverteren.

13 Het Engelse 'mining' laat zich moeilijk vertalen, omdat het verder gaat dan het delven of blootleggen van iets wat er al is. Het is veeleer de constructie van patronen die met het blote oog niet zichtbaar zijn en waarvan we pas na empirisch toetsen weten of ze niet 'vals' zijn (waarbij het toepassen van die patronen bovendien invloed zal hebben op de werkelijkheid, dus zelfs die toets is niet zuiver).

Het eerste voorbeeld is ontleend aan de wetgeving inzake gegevensbescherming. Artikel 35 WBP, gebaseerd op artikel 12 van de EU-Richtlijn gegevensbescherming, bepaalt:

> 'Desgevraagd doet de verantwoordelijke mededelingen omtrent de logica die ten grondslag ligt aan de geautomatiseerde verwerking van hem betreffende gegevens.'

Deze bepaling biedt degene die hier een beroep op doet weinig soelaas als hij bij wijze van antwoord een cd vol algoritmes in machinetaal krijgt aangereikt, waarmee misschien aan de letter van de verplichting is voldaan, maar waarmee hij uiteraard weinig kan uitrichten.
De Duitse wetgever heeft al wat meer handen en voeten gegeven aan deze bepaling. In artikel 34 van de Datenschutzgesetz is, ter implementatie van artikel 12 van de EU-privacyrichtlijn, een helder geformuleerd en redelijk adequaat transparantierecht opgenomen, dat verplicht tot het bieden van inzicht in de manier waarop onze gelekte[14] en verstrekte gegevens 'matchen' met de profielen die uit de grote hoop gegevens worden afgeleid.
Het artikel bepaalt concreet dat wanneer een 'score' ten aanzien van toekomstig gedrag wordt gebruikt bij beslissingen over het aangaan, uitvoeren of beëindigen van een overeenkomst, degene die het betreft recht heeft op de volgende informatie:

> '1. die innerhalb der letzten sechs Monate vor dem Zugang des Auskunftsverlangens erhobenen oder erstmalig gespeicherten Wahrscheinlichkeitswerte,
> 2. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten und
> 3. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.
>
> Satz 1 gilt entsprechend, wenn die für die Entscheidung verantwortliche Stelle
> 1. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder
> 2. bei einer anderen Stelle gespeicherte Daten nutzt.'

Hier wordt in elk geval een aantal problemen opgelost:
- De informatieverplichting is ook van toepassing als de 'score' is gebaseerd op geanonimiseerde gegevens. Dit maakt dat de verantwoordelijke voor de gegevensverwerking zich niet kan verschuilen achter het feit dat geen persoonsgegevens in het geding zijn.
- De statistische inferenties ten aanzien van toekomstig gedrag moeten worden verstrekt, zoals opgeslagen gedurende de laatste zes maanden, mét een

14 Dat wil zeggen: onbewust op het web achtergelaten.

> begrijpelijke uitleg over de wijze waarop die inferenties zijn afgeleid. Dit houdt in dat niet volstaan kan worden met het verstrekken van onbegrijpelijke algoritmes. Dat heeft als bijkomend voordeel dat de verantwoordelijke zich er niet op kan beroepen dat hij door het verstrekken van de informatie in strijd zou handelen met bedrijfsgeheim of auteursrecht van hemzelf of van degene die de software of het systeem voor gegevensverwerking geleverd heeft.
>
> Verder moet een expliciete verwijzing worden opgenomen naar de typen gegevens die zijn gebruikt.[15]

De Duitse uitwerking van dit transparantierecht biedt een handzamer en effectiever recht, maar de vraag blijft hoe de burger zich tot dit soort informatie gaat verhouden. Het is nog steeds een kwestie van tekst en nog meer tekst, waardoor ook deze oplossing gemakkelijk tot cognitieve overspanning leidt.

Het tweede voorbeeld betreft de artikelen 2:14 en 2:15 van de Algemene wet bestuursrecht (Awb), zoals ingevoegd bij de Webv.[16] Het derde lid van artikel 2:14 Awb regelt een belangrijk uitgangspunt bij het elektronisch bestuurlijk verkeer, namelijk betrouwbaarheid en vertrouwelijkheid. Indien een bestuursorgaan een bericht elektronisch verzendt, dan dient dit op een voldoende betrouwbare en vertrouwelijke manier te geschieden, gelet op de aard en inhoud van het bericht en het doel waarvoor het wordt gebruikt. Het tweede en derde lid van artikel 2:15 Awb geven weigeringsgronden voor een elektronisch bericht. Het bestuursorgaan kan een bericht weigeren indien verwerking ervan tot onaanvaardbare last zou leiden, of indien de betrouwbaarheid en de vertrouwelijkheid van het bericht onvoldoende gewaarborgd zijn. Onder 'voldoende betrouwbaar en vertrouwelijk' wordt hier hetzelfde verstaan als in artikel 2:14 lid 3 Awb.

Deze bepalingen beogen bestuursorganen de nodige ruimte te geven voor het invullen van beveiligingseisen en het stellen van eisen aan identificatie en authenticatie van de ontvanger of afzender van een elektronisch bericht. Ze bieden echter niet veel houvast bij de beantwoording van de vraag wat in de praktijk bijvoorbeeld adequate niveaus voor identificatie en authenticatie zijn, en met wat voor technische middelen die gerealiseerd kunnen worden. Dat leidt ertoe dat voor het aanvragen van een afvalcontainer op een gemeentelijke website soms hetzelfde authenticatieniveau (en -middel, namelijk 'DigiD basis') wordt gevraagd als voor het ophalen van je vooringevulde aangifte bij de Belastingdienst, of voor het raadplegen van je GBA-gegevens via Mijnoverheid.nl. Dat dit qua aard en omvang van de geleverde en getoonde gegevens nogal een verschil maakt, mag duidelijk zijn.

In februari van dit jaar is een Handreiking betrouwbaarheidsniveaus bij authenticatie voor elektronische overheidsdiensten verschenen,[17] die een classificatiemodel biedt voor het bepalen van het gewenste authenticatieniveau voor overheidsdiensten, op basis van de voor de desbetreffende dienst geldende wettelijke

15 Hildebrandt 2011, p. 22-23.

16 *Stb.* 2004, 14.

17 <www.forumstandaardisatie.nl>, te downloaden via link op de homepage.

eisen, de aard van de gegevens, eventuele waarborgen in het vervolgproces enzovoort. Dit biedt bestuursorganen houvast bij het eenduidig invullen van de open norm uit de Awb-artikelen. De handreiking zal nog worden aangevuld met een (omwille van flexibiliteit separaat) overzicht van authenticatiemiddelen die corresponderen met de gedefinieerde betrouwbaarheidsniveaus. Dat zal het bepalen van een adequate *default* voor authenticatie bij elektronisch verkeer voor bestuursorganen nog eenvoudiger maken.

6. Juridische bescherming *by design*

De in de vorige paragraaf beschreven uitwerking van wettelijke normen biedt zeker kansen om de interactie tussen wetgeving en technologie te ondersteunen en versterken. Het bieden van handreikingen en in aanvulling daarop het aanleggen van openbare catalogi met *best practices* die zowel overheid als bedrijf en burger inzicht geven in technologische oplossingen die een goede vertaling vormen van eisen en waarborgen in recht en wetgeving is een begin. Met name waar het gaat om de *defaults* van de technologische omgevingen van burgers menen we dat nog een stap extra nodig is.
Naast een adequaat wettelijk kader is dringend behoefte aan intuïtieve interfaces die bijvoorbeeld met behulp van visualisering (*visual data analytics*) snel laten zien waar publieke en private beslissers hun kennis vandaan halen. Je zou je kunnen voorstellen dat een knop in je browser of op een site toegang geeft tot een dynamisch plaatje dat laat zien met welke relevante profielen je matcht en wie die profielen beheren.[18] Die knop gaat dan functioneren als een digitale assistent die in staat is om op relevante profielen te anticiperen. Bij een profiel gaat het om slimme stereotypen, gebaseerd op statistische inferenties: als ik herhaaldelijk te hard rijd, match ik een profiel dat risicoverhogend is voor de verzekeringsmaatschappij en als ik bovendien snel mijn geduld verlies, match ik misschien wel het profiel van personen met neiging tot gewelddadig gedrag. Dat dit alles geen sciencefiction is maar harde werkelijkheid, mag blijken uit de investeringen die het ministerie van Defensie in de Verenigde Staten doet in het *future attributes screening technology* (FAST)-project. Uit biometrische gedragspatronen (de manier waarop je loopt, praat, lacht, beweegt) worden correlaties met crimineel gedrag 'gemijnd' teneinde daar op den duur voorspellingen uit af te leiden, met als doel crimineel gedrag steeds een stap voor te zijn. Wanneer dit soort 'preventieve technologie' proactief wordt ingezet, wordt het tijd om de vertraging die eigen is aan het geschreven recht in te bouwen in de architectuur van de slimme omgeving en wel zo dat de onschuldpresumptie en het recht op tegenspraak gewaarborgd blijven. Toepassingen als de hiervoor genoemde 'profielknop' kunnen (en moeten) daarbij helpen. Die mogen dan ook niet worden overgelaten aan 'de markt' of aan de burger die tijd en zin heeft om zich daarmee bezig te houden.

18 De Firefox plug-in Collusion die visualiseert welke websites je online volgen, is daarvan een rudimentair voorbeeld, zie <http://collusion.toolness.org/>.

Nationale en internationale wetgevers zouden zich moeten laten inspireren door de notie van juridische bescherming *by design* en werk moeten maken van een goed doordachte aanpassing van dit soort infrastructuur, gebaseerd op technologische standaarden, organisatorische protocollen en ondersteunende regelgeving. Doel moet zijn de positie van het individu binnen en tegenover de slimme ICT-infrastructuur te beschermen en de rechten en vrijheden van burgers niet alleen de jure, maar ook de facto effectief handen, voeten en tanden te geven.
Cruciaal is dat het verwerken van juridische bescherming in de architectuur van cyberspace niet wordt gezien als een uitvoeringsmaatregel, maar in eerste instantie als een opgave voor de democratische wetgever. Daarbij moet wel scherp in de gaten worden gehouden dat de wetgever geen technische klusjesman wordt. De eerdergenoemde ePrivacy-richtlijn eist bijvoorbeeld een *opt in* voor het plaatsen van cookies, terwijl *tracking* en *tracing* van gebruikers inmiddels ook met allerlei andere technieken gebeurt. In die zin moet wetgeving technologieneutraal zijn; het gaat hier om de juridische normering van *tracking* en *tracing*, niet om de vraag met welke middelen dat gebeurt. Zoals Reed al eens heeft verzucht, betekent technologieneutrale wetgeving niet dat de wetgever zich niets hoeft aan te trekken van de ontwikkeling van de ICT-infrastructuur.[19] Integendeel, de wetgever moet een vinger aan de pols houden om te voorkomen dat de werking van de grondrechten dankzij technologische ontwikkelingen erodeert en in goed overleg met de ontwerpers van de desbetreffende ICT het juridisch kader aanpassen.

7. Regulering door technologie

Daar waar de overheid slechts schoorvoetend stappen zet op het reguleren van menselijk gedrag door de technologie zelf, maakt de private sector daar in toenemende mate gebruik van. De al eerder genoemde dvd-speler die weigert om dvd's gekocht in een andere geografische zone af te spelen, omdat de door de entertainmentindustrie ingestelde zonering is ingebakken in de software van zowel de speler als de dvd's, is daarvan een sprekend voorbeeld. Maar ook antikopieermaatregelen op digitale content (muziek, films), gebruiksbeperkingen in e-readers, en *lock-in*-mechanismen in software (zoals *proprietary*[20] bestandsformaten) zijn daar voorbeelden van.
Toch rijst ook bij de overheid het besef dat het reguleringsinstrumentarium uit meer bestaat dan regelgeving, massacommunicatie (denk aan Postbus 51-spotjes) en economische prikkels, en dat ook heil verwacht kan worden van technoregulering, zeker in cyberspace. In de strijd tegen onlinekinderporno en tegen piraterij op het gebied van auteursrecht worden filtering van internetverkeer en blokke-

19 Ch. Reed, 'Taking Sides on Technology Neutrality', *SCRIPT-ed 4* 2007/afl. 3, p. 263-284.

20 Het gaat hier om intellectuele rechten op software, firmware of hardware. Daarmee kan de rechthebbende (persoon of bedrijf) een eigendomsrecht doen gelden op het desbetreffende product en daarmee het gebruik door anderen beperken. Voorbeelden zijn het bestandsformaat van Microsoft Word of met DRM (Digital Rights Management) beschermde filmbestanden. Een gevolg van *proprietary* bestandsformaten is een gebrek aan interoperabiliteit, software van derden kan niet of onvoldoende uit de voeten met beschermde bestandsformaten.

ring van onwelgevallige websites expliciet als middel gezien om maatschappelijke problemen aan te pakken. De overheid lijkt daarbij op controversiële wijze te leunen op implementatie van technische maatregelen door vooral private partijen. Internet Service Providers (ISP's) lijken in sommige jurisdicties zelfs technisch uitvoering te moeten geven aan het filteren en blokkeren van informatie in cyberspace,[21] hoewel met name het monitoren en filteren van internetverkeer in rechtsstatelijke, democratische samenlevingen buiten de orde zijn. Dit bevestigt dat technoregulering, op zichzelf genomen, tot onwenselijke dwang kan leiden. In de fysieke wereld is het lokale effect van een verkeersdrempel mogelijk groter dan van een 30 km-bord. Als technoregulering buiten de idee van juridische bescherming *by design* om wordt ingezet, dreigt het handhavingslandschap dan ook stevig te veranderen: ISP's kunnen bijvoorbeeld hun rol van neutrale boodschapper verliezen voor zover zij in toenemende mate een rol van (verkeers)politie in cyberspace vervullen. Dat brengt ISP's in een onwenselijke positie tussen klanten, vertegenwoordigers van rechthebbenden van auteursrecht en justitie. Zoals het Europese Hof van Justitie inmiddels in meerdere uitspraken heeft bepaald, past het systematisch filteren en monitoren van internetverkeer niet in een rechtsstatelijke democratie.[22] Hoe effectief dat – op de korte termijn – ook zou kunnen zijn. Het is dan ook aan de wetgever om sturing te geven aan deze ontwikkelingen en daarbij niet voor de verleiding te bezwijken om de eigen dan wel private handhaving uit te (laten) besteden aan ISP's.

Een beleidsterrein waar technoregulering erg voor de hand ligt, maar waar het om andere redenen op verzet stuit, is het verkeer. Deze fysieke werkelijkheid lijkt op het eerste gezicht misschien buiten cyberspace te liggen, maar door de grote hoeveelheid ICT die tegenwoordig in auto's en verkeerssystemen is verwerkt, maakt ze integraal deel uit van de informatiegestuurde samenleving.

Verkeerscongestie wordt gezien als een groot maatschappelijk probleem. De aanleg van meer asfalt is de oplossing die tot nu toe werd gekozen om het probleem op te lossen dat primair wordt veroorzaakt door een piekbelasting in de spits en in de tweede plaats aan suboptimaal presterende automobilisten en vrachtwagenbestuurders. Volgens sommige verkeerskundigen valt meer te verwachten van het reguleren van het verkeer door middel van technische maatregelen. Het aangrijpingspunt van de regulering is hierbij niet de automobilist, maar zijn voertuig. Door inzet van middelen zoals communicatie tussen voertuigen, snelheidsregulering van de voertuigen door hun boordcomputer en technisch afgedwongen inhaalbeperkingen (bijvoorbeeld begrenzing van toerentallen en daarmee acceleratievermogen) zou het mogelijk zijn het beschikbare wegoppervlak veel efficiënter te benutten en gelijktijdig het risico van verkeersongelukken te verkleinen. De keerzijde van dergelijke technoregulering is dat veel automobilisten dat ervaren

21 Overigens lijkt dit niet alleen voor ISP's te gelden, maar ook voor dienstenaanbieders. De Hoge Raad heeft op 24 februari 2012 bepaald dat het Engelse Ladbrokes niet in Nederland via internet en telefoon kansspelen mag aanbieden. De implementatie van dit verbod wordt onder meer gezocht in filtering van internetverkeer uit Nederland (HR 24 februari 2012, LJN BT6689, 07/00035).

22 Zie EHJ 29 januari 2008, C-275/06 (Promusicae); EHJ 24 november 2011, C-70/10 (Sabam v. Scarlet); EHJ 16 februari 2012, C-360/10 (Sabam v. Netlog).

als een (sterke) beperking van hun autonomie. Het zal dus niet verbazen dat de slimme auto vooralsnog moeizaam van zijn plaats komt.

8. Vraagstukken voor recht en wetgever

De inzet van technoregulering heeft consequenties voor het recht en de wetgever. In veel gevallen leidt het in technologie verpakken van gedragsnormen tot verlies aan transparantie van diezelfde normen. In een democratische rechtsstaat mogen we verwachten dat de normen waaraan burgers zich moeten houden bekend zijn en dat burgers bovendien weten dat er normen zijn en hoe die hun gedrag beogen te reguleren. De 'verexternalisering' die dat vereist, was eigen aan het schrift en de drukpers, de technologieën bij uitstek van het moderne geschreven recht. De eis van zichtbaarheid en contesteerbaarheid van juridische normen past binnen het ruimere begrip legitimiteit. Bij klassieke wetgeving is kennis over de normen door de normsubjecten noodzakelijk omdat zij immers anders niet kunnen weten wat van hen wordt verwacht. Transparantie van zowel de normen als de achterliggende beleidsdoelen is bovendien noodzakelijk voor een kritische maatschappelijke discussie over de aanvaardbaarheid van de normen.
Voor zover technoregulering buiten de rechtsstatelijke kaders opereert, is kenbaarheid van de normen geen noodzakelijk vereiste voor naleving; die wordt immers afgedwongen door de technologie zelf. In het geval van een blokkade door ISP's van websites die onrechtmatig materiaal aanbieden, hangt het van de implementatie af of de websurfende burger zich bewust is van de regulering. Het filter kan bijvoorbeeld een mededeling produceren waardoor de webbrowser de indruk wekt dat de website niet bestaat:

> 'Safari can't open the page "http://speelmeteenkleuter.co.uk/" because Safari can't find the server "speelmeteenkleuter.co.uk".'

Hiermee blijft de norm impliciet en zal de burger zich niet bewust zijn van het feit dat zijn gedrag feitelijk wordt gereguleerd. Het alternatief is dat het filter een mededeling produceert dat de betreffende website actief wordt geblokkeerd:

> 'Access to server "http://speelmeteenkleuter.co.uk" is blocked because it contains illegal content.'

Daarmee is de norm expliciet gemaakt. De wetgever zou een rol kunnen en moeten spelen bij het afdwingen van transparantie van de ISP over deze norm. Vanwege zijn verdienmodel is het immers niet altijd in het belang van de ISP om deze norm kenbaar te maken.
Een andere consequentie van technoregulering buiten de kaders van democratie en rechtsstaat is de mogelijke inperking van de morele handelingsvrijheid van het individu. Technoregulering maakt niet-conform handelen in veel gevallen feitelijk onmogelijk. Hierdoor worden zaken zoals keuzevrijheid, ongehoorzaam gedrag en kritisch tegenwicht feitelijk geëlimineerd. Maar ook heeft het effect op moraliteit

en kan uiteindelijk de menselijke waardigheid in het gedrang komen.[23] Smith betoogt bijvoorbeeld dat de lage metrobarrières zoals die in Amsterdam bestaan een ander effect op mensen hebben dan de menshoge tourniquets in de metro van Parijs.[24] Bij een fysieke belemmering waar de reiziger in wezen overheen kan klauteren, wordt bij elke reis een moreel beroep op de reiziger gedaan zich netjes te gedragen en te betalen voor zijn reis. In Parijs bestaat dit moreel appèl niet, de reiziger kan niet anders dan betalen. Uit economisch oogpunt is dat effectief, maar het risico is een zekere verschraling van het normbewustzijn.[25]
Technoregulering is potentieel een krachtig reguleringsinstrument, maar de morele en legitimiteitsvraagstukken zoals hierboven kort aangestipt, vragen om een nadere doordenking van de inzet van technoregulering en de consequenties die deze heeft voor de rechtsorde. Wanneer de wetgever zich als gevolg van ondoorzichtige handhaving van ondoorzichtige normen kan onttrekken aan een verantwoordingsplicht en maatschappelijke discussies over de aanvaardbaarheid van normen ontbreken, is dat vanuit democratisch en rechtsstatelijk oogpunt onwenselijk. Net zo onwenselijk als wanneer burgers als robots tot normconform handelen worden gedwongen.

9. Tot slot

In het voorgaande hebben we getracht inzichtelijk te maken wat technologische ontwikkelingen voor de wetgever betekenen, vanuit de optiek van een tegelijk instrumentele en waarborgscheppende opvatting van recht (juridische bescherming *by design*) als een meer instrumentalistische opvatting van recht. In dat laatste geval kan regulering door technologie (technoregulering) worden ingezet als zij leidt tot effectieve handhaving, zonder al op dat niveau de beschermende functie van het recht mee te nemen.
In zijn oratie somt Leenes[26] een aantal belangrijke vragen op die een democratische wetgever onder ogen moet zien bij de inzet van technoregulering. Het gaat enerzijds om de vraag in welke gevallen technoregulering een geschikt instrument is om juridische normen te belichamen en anderzijds om de vraag onder welke voorwaarden dat zou moeten gebeuren.[27] Daarbij speelt met name de vraag in hoeverre de *open texture* van rechtsnormen in de weg staat aan de meer eendui-

23 R. Brownsword, 'Code, Control, and Choice: Why East Is East and West Is West', *Legal studies* 2005 (25) afl. 1, p. 1-21.

24 D.J. Smith, 'Changing Situations and Changing People', in: A. von Hirsch, D. Garland & A. Wakefield (red.), *Ethical and Social Perspectives on Situational Crime Prevention*, Oxford: Hart Publishing 2000.

25 Een soortgelijke situatie doet zich voor waar mensen alleen nog geneigd zijn snelheidsnormen na te leven als er een camera langs de weg staat.

26 Leenes 2010, p. 30.

27 B.J. Koops, 'Criteria for Normative Technology – The Acceptability of "Code as Law" in Light of Democratic and Constitutional Values', in: R. Brownsword & K. Yeung (red.), Regulating Technologies – Legal Futures, Regulatory Frames and Technological Fixes, Oxford: Hart Publishing 2008, p. 157-174. D.K. Citron, 'Technological Due Process', *Washington University Law Review* 2007 (85), p. 1249.

dige (en daarmee soms beperktere) interpretatie die eigen lijkt te zijn aan ICT-systemen. Een computer kan (vooralsnog) nu eenmaal beter overweg met toepassing van objectieve criteria dan met de afwegingen die discretionaire ruimte eigen zijn.[28] Maar naarmate software intelligenter en dus minder rigide wordt, speelt de vraag in hoeverre de souplesse van die nieuwe software tegemoet kan komen aan de eisen van transparantie en verantwoording. En vanuit democratisch oogpunt: hoe kan worden gewaarborgd dat de in technonormen geïncorporeerde rechtsnormen blijven leven in het maatschappelijk debat en indien nodig worden bijgestuurd?

Juridische bescherming 'by design' is niet alleen van belang voor de ICT-infrastructuur die door private partijen wordt ontworpen als ruggengraat van cyberspace, maar juist ook voor de inzet van ICT door de overheid. Het vernetwerken, verrijken en in risicoprofielen inzetten van allerlei gegevens binnen en tussen verschillende overheidsdiensten is een hachelijke zaak. De grondslagen van het bestuursrecht, zoals het legaliteitsbeginsel, proportionaliteit, fair play en doelbinding, komen gemakkelijk in het gedrang en vragen dus continue aandacht en afweging. De WRR heeft in zijn rapport iOverheid de vinger op de zere plek gelegd.

Om te voorkomen dat de iOverheid de burger transparanter maakt, terwijl de overheid zich tegelijkertijd terugtrekt achter een sluier van onbegrijpelijke ICT, moeten we eisen formuleren die aan een robuust legitiem systeem worden gesteld. Ten eerste zou de broncode beschikbaar moeten zijn van systemen die beslissingen nemen die significante invloed hebben op burgers. Ten tweede moeten de betreffende systemen regelmatig en rigoureus worden getest, bijvoorbeeld op mogelijke vooringenomenheid.[29] Ten derde moeten burgers worden betrokken bij de aanleg van databases en softwaresystemen die hun leven de facto gaan normeren. Ten slotte mogen beslissingen die discretie en een menselijk oordeel vragen om een rechtvaardige, eerlijke uitkomst te garanderen niet worden uitbesteed aan geautomatiseerde systemen.

Technoregulering en de iOverheid vragen om een nieuwe technologische verankering van democratie en rechtsstaat. De technologie van het schrift volstaat niet bij de normering van cyberspace. Dit werkt ook door in de rol die politici, juristen en burgers hebben bij het ontwerp van het juridisch kader dat in nieuwe ICT-infrastructuren wordt ingebed. Wetgevingsjuristen zijn – samen met computerwetenschappers en designers – bij uitstek gekwalificeerd om te waken over de vertaling van juridische normen in technische *requirements*: het inbouwen van bescherming is geen zuiver technische en geen zuiver juridische opdracht. Het vraagt aan beide zijden gepaste distantie om het verstandshuwelijk te behoeden

28 Beslisondersteunende systemen bij grote uitvoeringsorganisaties voorzien met het oog daarop in selectiemodules van zaken die volledig geautomatiseerd, deels handmatig of geheel handmatig moeten worden afgehandeld. Het INDiGO-systeem van de IND functioneert daarnaast als kennissysteem voor medewerkers bij afhandeling van de handmatige zaken.

29 D. Pedreschi, S. Ruggieri & F. Turini, *Discrimination-aware Data Mining*, KDD'08 Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining, New York: ACM Press 2008, p. 560, <http://dl.acm.org/citation.cfm?id=1401959>.

voor ongewenste verstrengeling en serieuze betrokkenheid om de innige relatie tussen ICT en rechtsstaat vorm te geven.