REDACTIONEEL

Juridische bescherming 'by design'?

Mireille Hildebrandt

Recht en technologie

Het thema van de wereldconferentie van de IVR 2010 in Frankfurt is *Law, Science, Technology*. Dat nodigt onder meer uit om de normatieve implicaties van bestaande en nieuwe communicatie- en informatie-infrastructuren nader te onderzoeken in verhouding tot het recht. Eind jaren negentig heeft Lawrence Lessig voor enige opschudding gezorgd met zijn *Code and other laws of cyberspace*,[1] waarin hij vaststelt dat het recht geen monopolie heeft op het reguleren van menselijk gedrag. Naast markt, sociale normen en recht onderscheidt hij ook technologie in het algemeen en computercode in het bijzonder als factoren met een normerende werking. We zouden dit af kunnen doen als een triviaal inzicht en op kunnen merken dat de manier waarop die regulering tot stand komt toch nogal verschilt. Kenmerkend voor juridische regulering in een constitutionele democratie is in ieder geval dat de regels tot stand komen op basis van democratische besluitvormingsprocessen en dat het mogelijk is om zowel de geldigheid van de regel als de beslissing dat een bepaalde handeling onder de regel valt aan te vechten bij de rechter. Democratische legitimatie en de mogelijkheid tot contestatie doen rechtsnormen aldus verschillen van de normen van het niet-juridisch genormeerde sociale verkeer en van de regulerende werking van de markt. Vanuit analytisch oogpunt lijkt Lessig bovendien een categoriefout te maken, wanneer hij marktwerking, sociale normen en recht op één lijn stelt: marktwerking is immers afhankelijk van de manier waarop het recht de mogelijkheidsvoorwaarden schept voor het sluiten van contracten en het verhandelen van vermogensrechten, en zowel rechtsnormen als de tucht van de markt zijn uiteindelijk sociale normen.
Onder normerende of regulerende werking versta ik hier het uitnodigen of afdwingen dan wel het ontmoedigen of uitsluiten van bepaalde gedragspatronen. Regels of normen begrijp ik als bewust of onbewust richtinggevend voor menselijk handelen, waarbij normatief overigens niet gelijk staat aan moreel.[2] *Online* sociale netwerken kunnen – afhankelijk van de manier waarop ze het gedrag van de gebruiker sturen – de privacy van gebruikers aantasten. Of dat moreel wenselijk of onwenselijk is, vraagt een moreel oordeel, maar dat de *default* instellingen van de *online* omgeving het handelen in vergaande mate reguleren kan los van dat

1 L. Lessig, *Code Version 2.0*, New York: Basic Books 2006. Ook J.R. Reidenberg, Lex Informatica: The Formulation of Information Policy Rules Through Technology, *Texas Law Review* 76 (1998), p. 553-585.

2 M. Hildebrandt, Legal and technological normativity: more (and less) than twin sisters, *Techné: Journal of the Society for Philosophy and Technology* 12 (2008), p. 169-183.

morele oordeel worden vastgesteld. Hoewel de regulerende werking van technologie vaak een neveneffect is, kan ze vele malen groter zijn dan de normerende werking van talig gearticuleerde rechtsnormen. Zoals Lessig en anderen hebben aangegeven, kan dit de effectiviteit van rechtsregels op allerlei manieren ernstig ondermijnen.[3] Dat speelt met name als de technologie in kwestie nieuwe, verstrekkende en grotendeels onzichtbaar normerende implicaties heeft.[4] De erkenning dat ICT-infrastructuren een normerende werking hebben, heeft in de ethiek geleid tot de ontwikkeling van de notie *value sensitive design*, inmiddels geoperationaliseerd in de technische ondersteuning van privacy door middel van *privacy by design*.[5] Het is van belang dat niet alleen ethici, maar ook juristen, wetgevers en rechters zich bewust worden van de normerende werking van technologie en van het feit dat ontwerpkeuzes niet alleen bepalend zijn voor de functionaliteit, maar ook voor de manier waarop menselijk handelen wordt gereguleerd.
Hierna zal ik mij richten op de implicaties van de zogenoemde 'computationele wending' in de wetenschap, de economie en de samenleving, die door 'slimme' technologie mogelijk wordt gemaakt. Naar mijn mening vraagt die computationele wending om het inbouwen van juridische bescherming in de ICT-infrastructuur, omdat het articuleren van rechtsnormen in de technologie van schrift en drukpers in een aantal gevallen niet meer voldoet.[6] Het spreekt vanzelf dat aan zo'n juridische bescherming *by design* vele haken en ogen zitten, die om serieuze doordenking vragen, bijvoorbeeld in samenspraak met techniekfilosofen.[7]

De computationele wending: als het tapijt uw dokter belt

Voor zover de vorige eeuw die van de *linguistic turn* was, lijkt zich op dit moment in wetenschap, bedrijfsleven en samenleving een *computational turn* voor te doen.
In februari van dit jaar verscheen een speciale aflevering van *The Economist*, onder de titel 'Data, data, everywhere', waarin de spectaculaire gevolgen van de explosie aan digitale gegevens in kaart worden gebracht.[8] De biomedische wetenschappen (de genetica, moleculaire biologie, epidemiologie, enz.), astronomie, geografie, economie, de neurowetenschappen, milieukunde en inmiddels zelfs de geestes-

3 Brownsword, *Rights, Regulation, and the Technological Revolution*, Oxford: Oxford University Press 2008.
4 D.J. Solove, *The digital person: technology and privacy in the information age*, New York: New York University Press 2004; C. Sunstein, *Republic.com*, Princeton and Oxford: Princeton University Press 2001; T.Z. Zarsky, '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 (2002-2003), p. 17-47.
5 M. Flanagan, D. Howe e.a., Values in Design: Theory and Practice, in: J. van den Hoven en J. Weckert (red.), *Information Technology and Moral Philosophy*, Cambridge: Cambridge University Press 2007, over privacy-by-design zie <www.privacybydesign.ca>.
6 C. Houtekamer, Privacy-lessen voor technici, *NRC Handelsblad*, 1 en 2 mei 2010, p. 8-9.
7 R. Leenes, *Harde lessen. Apologie van technologie als reguleringsinstrument*, Tilburg: Universiteit van Tilburg 2010; M. Hildebrandt en A. Rouvroy, *The philosophy of law meets the philosophy of technology. Autonomic computing and transformations of human agency*, London: Routledge, te verschijnen in 2010).
8 K. Cukier, A special report on managing information, *The Economist*, 27 februari 2010, p. 2.

wetenschappen raken steeds meer in de ban van de informatica. Daarbij gaat het minder om de gegevens zelf en steeds meer om de verbanden, correlaties, patronen of clusters die dankzij allerlei computationele technieken aan onvoorstelbaar grote databestanden worden ontfutseld. Sommige auteurs beweren in een poging tot provocatie zelfs dat hier sprake is van een nieuwe vorm van wetenschappelijke kennis, die geen nood meer heeft aan causale verbanden of theorievorming.[9] Daar is uiteraard veel op af te dingen, maar dat wil niet zeggen dat we de computationele wending niet serieus hoeven te nemen.

Ook het bedrijfsleven lijkt betoverd door de mogelijkheden die het doorzoeken van digitale databestanden zou bieden; verdienmodellen worden dankzij diezelfde technieken gebaseerd op verfijnde klantsegmentering en onverhoedse, subliminale manieren van beïnvloeding hebben hun intrede gedaan in de vorm van gericht adverteren. Lerende software maakt het mogelijk om nauwkeurig en automatisch uit te zoeken welk product en welk type mail of 'advertorial' met grote waarschijnlijkheid uw aandacht zal trekken en tot 'aankoopgedrag' zal leiden.[10] De mantra van dit verdienmodel is dat slim, gepersonaliseerd adverteren gaat leiden tot gratis diensten en producten, waarbij u bijvoorbeeld een gratis mobiele telefoon en een gratis abonnement krijgt in ruil voor uw persoonsgegevens, die met uw toestemming gebruikt mogen worden om u te voorzien van op uw persoon gerichte informatie, aanbiedingen en reclame.

Gepersonaliseerd adverteren is een voorbode van wat Philips en de Europese Commissie 'omgevingsintelligentie' (*Ambient Intelligence*) hebben genoemd, wat neerkomt op omgevingen die dankzij ingebouwde sensoren en draadloze chips voortdurend 'weten' wat er zich voordoet en daarop inspelen met proactieve aanpassingen.[11] Dat kan gaan om aangepaste verlichting, het ontsluiten van deuren, het bestellen van eten (de slimme koelkast), het voorzien in gepersonaliseerde informatievoorziening, maar ook om het bewaken van de gezondheid van een diabetespatiënt. In april van dit jaar besprak *The Economist* de convergentie van draadloze communicatie, sociale netwerksites en gezondheidszorg onder de titel 'When your carpet calls your doctor'.[12] De idee is dat patiënten langer en veiliger thuis kunnen blijven wonen als zij onder voortdurend elektronisch toezicht staan en via de nieuwste technische snufjes zorg op maat kunnen krijgen. Omdat het tapijt voorzien is van draadloze chips die communiceren met het netwerk van *online* verbonden elektronica in uw 'slimme' huis, kan het alarm slaan als het uit bepaalde verschuivingen afleidt dat u bent gevallen. Dit soort gezondheidszorg op afstand past goed bij het streven naar een preventieve benadering van ziekte en gezondheid, want een omgeving die voortdurend gegevens opslaat, kan daar allerlei 'kennis' uit distilleren en als 'voorkennis' gaan toepassen. Het kenmerk van de

9 C. Anderson, The End of Theory: The Data Deluge Makes the Scientific Method Obsolete, *Wired Magazine* 16 (2008). Vgl. R.D. King, J. Rowland, e.a., The Automation of Science, *Science* 324/5923 (2009), p. 85-89.

10 R.H. Guttman, A.G. Moukas, e.a., Agent-mediated electronic commerce: a survey', *The Knowledge Engineering Review* 13 (1998), p. 147-159.

11 B. van den Berg, *The Situated Self: Identity in a world of Ambient Intelligence*, Nijmegen: Wolf Legal, te verschijnen in 2010.

12 Wireless health care. When your carpet calls your doctor, *The Economist*, 8 april 2010.

slimme technologie die op het punt staat door te breken, is dat zij anticipeert op de gebruiker op basis van geraffineerde computationele modellen.[13]

Problemen

Proactieve omgevingen genereren verschillende soorten problemen. Enerzijds kan er misbruik worden gemaakt van de mogelijkheid om vergaande kennis van individuele personen te verkrijgen, hetgeen kan leiden tot ernstige inbreuken op de privacy. Anderzijds kan misbruik worden gemaakt van de mogelijkheid om burgers op basis van verfijnde groepsprofielen uit te sluiten van aanbiedingen, kortingen, verzekeringen, werk, toegang tot allerlei diensten. Dergelijke groepsprofielen kunnen ook worden gebruikt om de preventieve opsporing verder uit te bouwen en in het verlengde van de reeds bestaande actuariële justitie correlaties te zoeken tussen bijvoorbeeld genprofielen en recidive.[14] Inbreuken op grondrechten als het verbod op ongerechtvaardigde discriminatie en privacy lijken de meest voor de hand liggende problemen. Over beide gevaren zijn inmiddels bibliotheken volgeschreven, waarbij discriminatie en uitsluiting met name binnen de zogenoemde *surveillance studies* worden bestudeerd.[15]
Een probleem dat minder aandacht krijgt, maar direct met genoemde gevaren samenhangt, is het totale gebrek aan transparantie van de computationele onderbouw op grond waarvan slimme omgevingen ons inschatten. Een van de buzzwoorden van omgevingsintelligentie is gebruikersvriendelijkheid, die vaak wordt verbonden met de notie van 'verborgen complexiteit'. De idee is dat de gebruikers van dit soort omgevingen niet worden lastig gevallen met vragen over hun wensen en voorkeuren en niet worden geconfronteerd met de technische systemen die het mogelijk maken om die wensen en voorkeuren proactief af te leiden uit opgeslagen en geanalyseerde gedragsgegevens. Hoewel de opgeslagen gegevens deels onjuist en vaak incompleet zullen zijn, zal het feit dat we op grond van een analyse van die gegevens worden gecategoriseerd en behandeld een zekere normerende werking hebben die vergelijkbaar is met Merton's *self fulfilling prophecy*: 'If machines define a situation as real, it is real in its consquences.'[16] Het verschil is dat waar we in het dagelijks leven wel weten dat anderen op ons anticiperen, en daar bij ons handelen ook rekening mee kunnen houden, we niet gewend zijn aan artefacten die op ons anticiperen. Terwijl wij ten aanzien van mensen en organisaties voortdurend en grotendeels onbewust anticiperen op hoe anderen op ons anticiperen, lijkt dat bij slimme omgevingen veel moeilijker.

13 Hierover M. Hildebrandt en S. Gutwirth, *Profiling the European Citizen. Cross-disciplinary Perspectives*, Dordrecht: Springer 2008.

14 B.E. Harcourt, *Against prediction : profiling, policing, and punishing in an actuarial age*, Chicago: University of Chicago Press 2007; Y. Buruma, Veiligheid en privacy, *Delikt en Delinkwent* 32 (2002), p. 329-339.

15 Zie het online tijdschrift voor Surveillance & Society: <www.surveillance-and-society.org/ojs/index.php/journal>.

16 Ik heb daarbij Mertons 'men' vervangen door 'machines'. Zie R.K. Merton, The Self-Fulfilling Prophecy, *The Antioch Review* 8 (1948), p. 193-210, die voortbouwt op W.I. Thomas en D. S. Thomas, *The Child in America*, New York: Knopf 1928.

Om privacy-inbreuken vast te kunnen stellen en discriminatie te kunnen voorzien, is feedback nodig over hoe slimme omgevingen ons gedrag 'interpreteren' en welke consequenties dat kan hebben. 'Bewoners' van proactieve omgevingen horen toegang te hebben tot de 'logica' die bepalend is voor de manier waarop de omgeving haar gebruikers kansen en risico's toedeelt. Een interessante vraag is intussen wie eigenlijk gebruiker is: degene die zich in een slimme omgeving begeeft om dankzij subliminale 'catering' van de laatste gemakken voorzien te worden, of de omgeving die haar 'gebruikers' gebruikt om de gehanteerde verdienmodellen verder te optimaliseren. Het recht op inzicht in de computationele logica volgens welke we bediend worden, is verwoord in artikel 12 van de Richtlijn Gegevensbescherming. Daarover is veel te mitsen en maren, al was het maar omdat de preambule van de richtlijn onder punt 41 al aangeeft dat dit recht op gespannen voet kan staan met het bedrijfsgeheim of de intellectuele rechten van degene die deze logica beheert of inhuurt. Interessanter is dat het technisch op dit moment niet mogelijk is om dit transparantierecht te operationaliseren. Zelfs al zou een bedrijf bereid zijn om informatie te verschaffen over die logica, dan nog is het niet mogelijk om te checken of die informatie klopt. De rechtsnorm is gearticuleerd in de informatie- en communicatie-infrastructuur van het schrift en de drukpers, en lijkt ineffectief in het tijdperk van proactieve omgevingen.

Juridische bescherming 'by design'

Een mogelijke oplossing zou zijn om de implementatie van dit soort rechtsnormen uit te besteden aan *privacy enhancing technologies* (PETs) en *transparency enhancing technologies* (TETs). In allerlei beleidsstukken, zowel op nationaal als Europees niveau, doemt de term PETs steeds vaker op als oplossing voor privacy in relatie tot de toenemende verwerking van persoonsgegevens. Het past in een agenda waarbij technologie wordt ingezet om naleving af te dwingen vanuit de gedachte: als het niet goedschiks lukt, dan maar kwaadschiks. Probleem daarvan is dat de wetgever een deel van zijn regelgevende taak op die manier afstaat aan computerwetenschappers die de desbetreffende rechtsnormen moeten vertalen in door machines te lezen en te implementeren regelsystemen. Die vertaalslag raakt de inhoud van de norm en zal de ambiguïteit en de betekenisdynamiek reduceren, die eigen zijn aan het gesproken en geschreven recht.[17] Tegelijkertijd kan zo'n technisch afgedwongen rechtsnorm mogelijkerwijs niet meer overtreden worden, hetgeen de vraag oproept of dit nog wel recht is. Discipline of administratie lijken meer in de buurt te komen.
Juridische bescherming 'by design' kan dan ook geen kwestie zijn van technische implementatie. Het predicaat 'juridisch' impliceert in een democratische rechtsstaat dat de inhoud van de norm door democratische besluitvormingsprocessen tot stand is gekomen en dat verzet tegen de toepassing van de norm in rechte

17 D.K. Citron, Technological Due Process, *Washington University Law Review* 85 (2007), p. 1249-1313, T. van der Linden-Smith, *Een duidelijk geval: geautomatiseerde afhandeling*, NWO/ITeR-serie 41, Den Haag 2001.

mogelijk is.[18] Dat betekent allereerst dat het ontwerp van nieuwe technologische infrastructuren die grote implicaties hebben voor bestaande rechtswaarborgen niet aan de markt en de technische experts mag worden overgelaten. De wetgever zal zich moeten verdiepen in de vertaalslag die nodig is om bepaalde rechtsnormen op het niveau van hardware en software te articuleren. Dat betekent uiteraard niet dat beleidsmakers, politici en juristen zich moeten omscholen tot computerwetenschapper. Het betekent wel dat veel meer aandacht moet komen voor de computationele onderbouw van de slimme infrastructuren die nu in aanbouw zijn en dat de wetgever zich verantwoordelijk moet weten voor de manier waarop de bescherming van grondrechten daarin gestalte gaat krijgen. Ten tweede zal bij het inbouwen van juridische bescherming altijd de mogelijkheid van verzet tegen een specifieke rechtsnorm moeten worden ingebouwd; zowel het aanvechten van de geldigheid van de norm als het ontkennen dat het eigen handelen onder die norm valt moet in rechte mogelijk zijn. Het geschreven recht heeft daar geen problemen mee, maar het zal geen sinecure zijn om de mogelijkheid van contestatie in te bouwen in de nieuwe ICT-infrastructuur.

18 M. Hildebrandt en B.J. Koops, The challenges of Ambient Law and legal protection in the profiling era, *The Modern Law Review* 73 (2010), p. 428-460.