Autonomie en Transparantie

Prof. dr. Bart Jacobs,
Hoogleraar computerbeveiliging, Radboud Universiteit Nijmegen
Contact: : bart@cs.ru.nl, www.cs.ru.nl/~bart
31 maart 2011

Wetten lopen achter de feiten aan. Wetten reguleren het maatschappelijke verkeer en worden gewoontelijk pas geformuleerd in reactie op bepaalde aspecten van dat maatschappelijke verkeer die als onwenselijk of juist wenselijk ervaren worden. In geen enkele sector lijkt dit na-ijlen van wettelijke regulering zo prominent als in de informatie en communicatietechnologie (ICT). Bijvoorbeeld, pas in het begin van de jaren negentig van de vorige eeuw werden in Nederland computercriminaliteitswetten van kracht. Deze stellen het binnendringen in een computer van een ander strafbaar (als 'computervredebreuk'), en ook het veroorzaken van stoornis in een geautomatiseerd werk, of het afluisteren van communicatie. Het eerste hackersblad van Nederland[1] schreef destijds uitvoerig over methoden om computer- en telefoon-systemen binnen te dringen en te manipuleren die aanvankelijk moeilijk, enkel via indirecte weg, vervolgd konden worden.

Er zijn verschillende redenen aan te geven waarom nu juist in de ICT-sector wetten zo sterk achterlopen op de praktijk. Ten eerste gaan de ontwikkelingen in de ICT razendsnel en zijn ze voor iedereen, en niet alleen voor juristen, moeilijk bij te benen. Ten tweede dienen wetten bij voorkeur techniek-onafhankelijk geformuleerd te worden. Wetgeving die commerciële profilering door adverteerders probeert te reguleren en zich enkel richt op het gebruik van cookies in webbrowsers is achterhaald op het moment dat adverterdeerders andere methoden gebruiken om surfgedrag in kaart te brengen. Zulke techniek-onafhankelijk formulering vergt een zekere distantie tot de materie die pas na enige mate van stabilisatie bereikt wordt. Een derde hiermee samenhangende reden is dat er niet zo veel mensen zijn die een redelijk inzicht hebben in zowel de juridische als de computertechnische aspecten van de materie. Ook dit werkt vertragend. Dit alles brengt het risico met zich mee van *ad hoc* maatregelen die niet gebaseerd zijn op inzicht, overzicht en visie.

De vraag dient zich aan hoe te handelen bij na-ijlende wetgeving, met name op ICT-gebied, waar dit na-ijlen structureel is[2]. Hierbij maak ik een grof onderscheid tussen bedrijfsleven en overheid. In zeer algemene termen zou men kunnen stellen dat in het bedrijfsleven bij ontbreken van wetgeving enthousiast gebruik wordt gemaakt van de afwezigheid van beperkende regulering. Ook hier is het profileren van klanten ten behoeve van persoonsgerichte advertenties een treffend voorbeeld, waarbij zelfs de mogelijkheid van een opt-out (klant moet nee zeggen en wordt anders geacht mee te willen doen) meestal niet geboden wordt --- om van een opt-in (klant moet expliciet ja zeggen) nog maar te zwijgen. Websites voor boekverkoop brengen op opzichtige wijze onder de aandacht wat andere klanten bij eenzelfde boek (en vergelijkbare aankoopgeschiedenis) ook gekocht hebben, zonder daarbij de mogelijkheid te bieden om verschoond te blijven van dergelijke opgedrongen bemoeizuchtige 'service'. Wetgeving op zulke gebieden zal zich typisch richten op transparantie en opt-in of opt-out mogelijkheden. Ook bij de overheid komt dit opzoeken van de randen van het toelaatbare voor, bijvoorbeeld bij zogenaamde *crimefighter* officieren van justitie. Soms zullen zij in hun handelen

1 *Hack-Tic,* tijdschrift voor techno-anarchisten 1989-1994, zie www.hacktic.nl.

2 Feitelijk gaat het niet alleen om het introduceren van nieuwe regelingen maar ook om het herinterpreteren of expliciteren van bestaande regels. Zo zijn privacywetten welbewust als open regels geformuleerd die om en constante herinterpretatie vragen in het licht van technische ontwikkelingen.

bewust grenzen overschrijden, juist om via een rechterlijke uitspraak duidelijkheid te verkrijgen. Echter, van de overheid wordt vooral verwacht dat zij zich ook bij het ontbreken van regulering 'netjes' gedraagt, en handelt in lijn met bestaande wetsartikelen en daaraan ten grondslagliggende waarden en normen. Het is juist dit grijze niet-gereguleerde gebied dat hieronder verkend zal worden, aan de hand van een aantal vragen en voorbeelden die met name individuele autonomie en transparantie betreffen.

Een actuele illustratie van zo'n nog-niet-gereguleerde kwestie betreft computervredebreuk door de politie. Hiervoor wordt soms de ietwat opportunistische kreet 'terug-hacken' gebruikt. Een voorbeeld is het inbreken in de computer van een verdachte om via een zogenaamde *keylogger* toetsaanslagen en daarmee wachtwoorden te achterhalen waarmee bestanden versleuteld zijn. Een ander voorbeeld betreft het verstoren van een computer die ongewenste of kwaadaardige acties uitvoert, mogelijk vanuit het buitenland. Het moge duidelijk zijn dat een dergelijke bevoegdheid voordelig kan zijn. Derhalve wordt door het huidige kabinet in het kader van de wetsaanpassing 'computercriminaliteit III' zo'n bevoegdheid voorbereid. Enige voorzichtigheid, terughoudendheid en reflectie is hier echter op zijn plaats. Een belangrijk deel van de voorgestelde bevoegdheid tot computervredebreuk lijkt gericht te zijn op het kunnen *lezen* van informatie binnenin de computer van een verdachte. Er is echter in dit verband een dunne, moeilijk te controleren scheidslijn tussen *lezen* en *schrijven*. Het valt te voorspellen dat bij ieder gebruik van deze bevoegdheid de politie zich zal moeten verdedigen tegen het verwijt dat belastende gegevens (kinderporno, problematisch emailverkeer, etc.) op afstand in de binnengedrongen computer geplaatst zijn[3]. Hoe wordt hierbij vormgegeven aan de controlerende rol van de rechter-commissaris? Meekijken over de schouder van de digitale rechercheur is volstrekt inadekwaat omdat op de achtergrond allerlei verborgen programma's actief kunnen zijn. Daarom zullen eerst effectieve middelen voor logging en reconstructie van al het digitale handelen in een dergelijke computervredebreuk-operatie geconstrueerd moeten worden. Ook is deze bevoegdheid in hoge mate agressief en kan ze zeker in internationale context tot sterke, onvoorziene reacties leiden. Daarnaast zal in de persoonlijke sfeer een dergelijke bevoegdheid als zeer indringend ervaren worden. Het (sociale) leven van de moderne mens speelt zich immers in aanzienlijke mate af in de digitale wereld en het op afstand benaderen van de daarbij horende privé gegevens, opgeslagen op eigen persoonlijke apparaten (mobiel, tablet, laptop, PC), zal ervaren worden als het 'onder de eigen huid' kruipen door rechercheurs. Tenslotte is het mogelijke grootschalige, geautomatiseerde gebruik van een dergelijke binnendring-bevoegdheid zorgelijk, zeker in het licht van het mogelijke misbruik. De Duitse filosofe Hannah Arendt heeft in haar uitgebreide studies van totalitaire regimes (Arendt 1951) juist deze wens om in het privéleven van de burger binnen te dringen als kenmerkend aangeduid.

In dit verband is het relevant te wijzen op de zorgvuldige discussie die hierover in Duitsland al langer loopt. Daar is het *Bundesverfassungsgericht* gevraagd zich over deze materie te buigen. Dit hoogste Duitse rechtscollege heeft het grijze, ongereguleerde gebied van computervredebreuk door politie benaderd vanuit de bestaande wetgeving en daarbij een nieuw recht geëxpliciteerd, namelijk een recht op confidentialiteit en integriteit van eigen computersystemen[4]:

> *Das allgemeine Persönlichkeitsrecht (...) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.*

Overigens is dit recht niet absoluut: onder specifieke omstandigheden zijn inbreuken gerechtvaardigd. Maar het genoemde recht is het uitgangspunt: het *Bundesverfassungsgericht* heeft een zodanig moderne opvatting over individuele personen dat daar het recht op een onaangetaste tablet bijhoort.

---

3 De beoordeling door rechters van aangetroffen kinderporno op computers is onderzocht in (Stevens en Koops, 2009); aldaar wordt een overkoepelend criterium geformuleerd dat enige bescherming biedt tegen heimelijke plaatsing: "Degene op wiens harde schijf kinderporno is aangetroffen, is strafbaar wegens het opzettelijk in bezit hebben van deze kinderporno, indien hij zich bewust is van de aanwezigheid van de bestanden, hierover beschikkingsmacht heeft, en de bedoeling heeft ze in bezit te hebben." Daarbij is het doorslaggevend of de verdachte al dan niet op zoek is geweest naar kinderporno. De surfgeschiedenis speelt dan een belangrijke rol.

4 BVerfG, 1 BvR 370/07 van 27 feb. 2008, zie www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html:

Vragen

In het onderstaande komen vijf vragen aan bod die te maken hebben met individuele autonomie en ontwikkelingen op ICT gebied. Een rode lijn wordt gevormd door de toenemende intelligentie en autonomie van omgevingen waarin wij als individuen functioneren. Steeds zal eerst de relevante context besproken worden. De lezer wordt uitgenodigd bij het stellen van de vraag even te pauzeren en tot een eigen standpuntbepaling te komen. Deze vragen zijn eerder aan de orde geweest in verschillende lezingen van de auteur over deze materie. Hieronder komt soms ook aan de orde hoe het publiek daarbij reageerde. Dit geeft natuurlijk niet meer dan een oppervlakkige indruk en vormt op geen enkele wijze een representatief beeld, van, bijvoorbeeld, de opvattingen van de gehele Nederlandse bevolking.

In Nederland is vanaf begin jaren negentig in steeds uitgebreidere vorm gebruik gemaakt van stemcomputers, totdat ze in 2007 vrij plotseling werden afgeschaft (Jacobs en Pieters, 2009). Daarbij had een zeer effectief opererende actiegroep www.wijvertrouwenstemcomputersniet.nl gewezen op het gebrek aan transparantie en controleerbaarheid bij het gebruik van dergelijke computers[5]. Een groot probleem ontstond toen de actiegroep aantoonde dat de destijds gebruikte stemcomputers het stemgeheim niet garandeerden: door het opvangen en interpreteren van de uitgezonden elektromagnetische straling (*tempest*) kon de groep aantonen dat op afstand informatie verkregen kan worden over de uitgebrachte stem. Dit was een juridisch probleem. Stemgeheim en autonomie zijn immers belangrijke onderdelen in de Nederlandse kieswet, bijvoorbeeld in artikel J15 “Het stemlokaal is zodanig ingericht dat het stemgeheim is gewaarborgd” of in artikel J28 “In het stemlokaal worden geen activiteiten ontplooid die erop gericht zijn de kiezers in hun keuze te beïnvloeden”.

De kieswet bevat meer bepalingen over de inrichting van, en de wijze van handelen in, het stemlokaal. Zo mag er in het stemlokaal dus geen politiek werving plaatsvinden en mogen kiezers enkel in hun eentje een stemhokje betreden. Ingeval toch twee personen tegelijk een stemhokje betreden dienen de leden van het stembureau in te grijpen. Deze en andere bepalingen zijn erop gericht om een zone te creëren waarin burger in volstrekte autonomie, vrij van beïnvloeding, de eigen stem uit kan brengen. Men wordt hier letterlijk gedwongen autonoom te zijn. Deze uitgebreide regels en maatregelen die erop gericht zijn deze autonome keuze mogelijk te maken wijzen erop dat autonomie niet vanzelfsprekend is. Integendeel, individuele autonomie is fragiel en kwetsbaar, en dient, althans in democratische rechtsstaten, actief beschermd te worden.

In veel landen is de afgelopen jaren geëxperimenteerd met verschillende vormen van elektronisch stemmen. Niet alleen in Nederland is daarover discussie gevoerd. In vergelijkingen tussen elektronisch stemmen (via stemcomputer of internet) en traditioneel stemmen (met potlood en papier) zijn onderliggende assumpties en eisen expliciet gemaakt en afgewogen zijn. Soms werd daarbij ook het belang van het stemgeheim aan de orde gesteld: waarom is het eigenlijk zo belangrijk dat het niet bekend wordt wie wat gestemd heeft? We zijn tegenwoordig toch allemaal vrije en onafhankelijke mensen die zich niet laten beïnvloeden en zich niet schamen voor onze politieke opvattingen? Er zijn veel vormen van stemmen die in het openbaar plaatsvinden.

Vraag 1: Is stemgeheim een essentiële eis in het stemproces in een democratische rechtstaat?

Een zeer grote meerderheid vindt dit stemgeheim inderdaad essentieel. Enigszins overdreven kan men stellen dat het stemgeheim ‘heilig’ is en misschien wel het duidelijkste voorbeeld waar aan

5 Ook over deze kwestie heeft het *Bundesverfassungsgericht* zich overigens in heldere termen uitgelaten: de burger moet inzicht hebben in de werking van zulke systemen.

afgedwongen transparantie van burgers een harde grens gesteld wordt. Inderdaad, wanneer zou blijken dat politie of inlichtingendiensten of commerciële partijen systematisch zouden proberen individueel stemgedrag van burgers in kaart te brengen zou dat tot grote verontwaardiging en protest leiden. Overigens hielden de inlichtingendienst in Nederland tot in de jaren tachtig wel degelijk bij wie lid was van, of stemde op, de communistische partij (Hoekstra 2004, Engelen 2007). En in de moderne tijd kunnen online stemwijzers op basis van IP-adressen politieke voorkeuren bijhouden. In 2007 heeft stemwijzer.nl zijn werkwijze onder druk van het College Bescherming Persoonsgegevens dienaangaande aangepast.

Het tweede onderwerp betreft de aard en wijze van toegang tot de media. Ook dit is een belangrijk punt in een democratie, waarbij de overheid geacht wordt een redelijke mate van pluriformiteit en toegankelijkheid te garanderen. Traditioneel worden die media aangeleverd via een *broadcast* model, waarbij bijvoorbeeld een zendmast voor radio of TV alle kanalen uitzendt en de ontvanger lokaal een selectie maakt uit het brede aanbod. Belangrijk hierbij is dat de verzender niet kan zien welke selectie lokaal gemaakt wordt en dus ook niet van individuele luisteraars of kijkers kan bijhouden wanneer en hoe lang waar naar geluisterd of gekeken wordt. Net zo weet men bij de krant waarop ik geabonneerd ben niet welk artikel ik wel of niet lees (en wanneer en hoe lang).

Steeds meer wordt dit *broadcast* model vervangen door een *point-to-point* model. Daarbij maakt de mediaconsument zijn keuze bekend aan een centrale aanbieder en wordt daarop alleen het geselecteerde item aan de consument verzonden. De webserver van een nieuwssite als nu.nl beantwoordt mijn kliks met de bijbehorende items. Deze items worden speciaal voor mij naar het IP-adres van mijn computer gestuurd. Daarbij houdt nu.nl op basis van mijn IP-adres precies bij op welke nieuwsberichten ik klik en hoe lang ik daar op welk moment naar kijk. Ik lees bijvoorbeeld nooit over sport maar wel over buitenlandse politiek. Ik krijg daarmee op nu.nl dan ook nooit reclame voor sportevents of sportartikelen, maar wel over buitenlandse reizen. Ongetwijfeld worden ook subtielere, voor mij haast onbewuste, zaken geregistreerd, bijvoorbeeld of ik wel of niet tot een klik te verleiden ben met een foto van een rondborstige dame bij de aankondiging van een item. Sommigen zijn zich wel degelijk bewust van dit soort zaken en klikken daarom juist niet op dat soort items. Leidt surveillance van media consumptie hier tot een vorm van zelfcensuur? Doordat mediaproducenten over langere termijn dergelijke gegevens registreren en analyseren kunnen zij profielen opbouwen die vanuit marketing perspectief goud waard zijn: er wordt uit afgeleid van welke merk auto, of van welk product dan ook, men het beste reclame gericht kan versturen.

Dit *point-to-point* model wordt ook toegepast bij internetradio, bij betaaltelevisie voor sport of films, en ook bij sommige vormen van digitale televisie (zeker wanneer sprake is van interactieve TV). Het is te verwachten dat kranten steeds minder in papieren vorm en steeds meer in digitale vorm gelezen zullen worden. Bij een digitale krant kan, net als op nu.nl, de aanbieder precies zien wat ik lees en daar zijn conclusies uit trekken. Ook kan ik mij mogelijk gehinderd voelen om bepaalde items te bekijken (over bijvoorbeeld ‘foute’ politieke opvattingen of historische gebeurtenissen) omdat ik daar niet mee geassocieerd wil worden. Is hierbij vrije onbevangen toegang tot de media in het geding?

Vraag 2: Is onbespiede media-toegang beschermenswaardig in een vrije samenleving?

Een kleine meerderheid lijkt hier voor te zijn. In sommige situaties kan ik mijzelf tegen bespieding wapenen door bijvoorbeeld een *anonimiser* zoals Tor[6] te gebruiken, zodat mijn surfgedrag gemaskeerd wordt en een site als nu.nl niet kan zien van welk IP-adres mijn kliks afkomstig zijn. Maar zulke individuele beschermingsmiddelen zijn alleen te gebruiken op een open netwerk als internet, waarop

6 zie www.torproject.org

transport gratis is[7]. Op een gesloten netwerk als van een digitale TV-aanbieder kan ik niks maskeren en ben ik overgeleverd aan de profileringsdrang van de aanbieder. De overheid zou in deze kwestie onbespiede toegangsmogelijkheden kunnen bevorderen door een opt-in voor profilering bij mediaconsumptie[8] af te dwingen, of door het verplicht te stellen dat het *broadcast* model waar mogelijk gebruikt wordt. Concreet zou dat bijvoorbeeld kunnen betekenen dat krantenabonnees hun digitale krant in zijn geheel kunnen downloaden (en niet enkel per artikel), zodat nog steeds een lokale onbespiede selectie gemaakt kan worden.

Het volgende onderwerp richt zich op beprijzing. We zijn redelijk gewend geraakt aan vaste prijzen in winkels. Velen van ons hebben de sport van het afdingen verleerd en laten zich in landen waar dat afdingen meer voorkomt gemakkelijk afzetten door de eerstgeboden prijs te accepteren. Wel zijn we steeds meer *overlay websites* gewend die een overzichtelijke prijsvergelijking bieden door systematisch te zoeken in onderliggende websites van aanbieders. Met name op het gebied van vliegtickets zijn er verschillende van zulke *overlay sites*. Zo'n website kan een onderscheid maken tussen klanten die twee keer per jaar naar Benidorm vliegen en klanten die zes keer per jaar naar New York, Kyoto, Sydney etc. vliegen. Dit onderscheid kan gemaakt worden op basis van het gebruikte IP-adres, zonder de identiteit van de klant te kennen. De *overlay site* kan nu besluiten bij de waarschijnlijk rijkere klanten van de tweede categorie af en toe 50 Euro bij de prijs op te tellen --- en die 50 Euro voor zichzelf te houden --- in de hoop dat de betreffende internationaal georiënteerde reiziger het te druk heeft om dit te herkennen of te controleren. Dit is een voorbeeld van *behavioural price differentiation*.

Vraag 3: Is deze gedragsafhankelijke beprijzing ongewenst en moet die aan banden gelegd worden?

Veel mensen die hier voor het eerst van horen reageren enigszins geschokt en willen een verbod. De zaak is echter niet zo eenvoudig. Ook de marktkoopman keurt eerst zijn klanten en noemt dan zijn prijs. Mag dit ook niet? Een gevoel van ongemakkelijkheid en oneerlijkheid echter blijft aanwezig bij geautomatiseerde gedragsafhankelijke beprijzing, mede vanwege de informatie-asymmetrie en het gebrek aan transparantie: als klant weet je niet welke gegevens van jou gebruikt worden, mogelijk over langere perioden en ook van andere bronnen, en op welke wijze daar conclusies uit getrokken worden. Het gevoel van oneerlijkheid lijkt vooral gebaseerd te zijn op ongelijke behandeling, en niet zozeer op eventuele aantasting van autonomie. Het is waarschijnlijk vanwege zulke negatieve reacties dat commerciële partijen vooralsnog terughoudend zijn met gedragsafhankelijke beprijzing. Er zijn geen harde voorbeelden voorhanden. Wel worden indirecte gedragsafhankelijke methoden gebruikt, waarbij alleen geselecteerde klanten extra voordeel, spaarpunten, of coupons krijgen.

Op natuurlijke wijze komt hiermee het vierde onderwerp aan de orde. Profilering van klanten wordt niet zozeer gebruikt om een individueel afgestemde prijs te bepalen, maar veeleer voor een individueel aanbod (of het uitblijven daarvan). Steeds meer van mijn gedragingen worden door mijn omgeving

7 Al mijn reisgedrag met het openbaar vervoer blijft, zoals bekend, jarenlang geregistreerd via mijn OV-chipkaart. Ik kan daarbinnen mijn 'werkelijke' reisgedrag proberen te maskeren door kris-kras rond te reizen. Zoiets kost niet alleen veel tijd en moeite, maar ook veel geld indien ik althans geen abonnement bezit. Op internet kan zulk verhullend kris-kras verkeer wel zonder veel moeite gecreëerd worden.

8 De beoogde bescherming (bijv. via een opt-in) zal zich primair moeten richten tegen het niet op mijn belangen gerichte gebruik van mijn mediaconsumptiepatroon. Mogelijk wil ik juist wel dat een krant mijn patroon herkent en mij geheel onbevooroordeeld en zonder eigenbelang direct juist die artikelen voorschotelt waarvan de krant denkt dat ze voor mij interessant zijn. Zulke belangeloosheid en onbevooroordeeldheid bestaat natuulijk niet. Mogelijk zal de manier van omgaan met gebruikersprofielen deel uit gaan maken van het ideologische of commerciële imago van een krant. Zo'n ontwikkeling werkt alleen bij een grote mate van transparantie mbt. profilering (zie later) en is natuurlijk geen argument om misbruik niet aan banden te leggen.

geregistreerd, gecombineerd en geanalyseerd. Soms gebeurt dit expliciet, zoals bij mijn aankoopgedrag via een klantenkaart of bij mijn reisgedrag via de OV-chipkaart of bij een televisieabonnement, maar soms ook impliciet. Moderne telefoons hebben een bewegingssensor waarmee met een redelijke mate van nauwkeurigheid kan worden vastgesteld wat de eigenaar aan het doen is: wandelen, hardlopen, zitten, autorijden, treinreizen, slapen, etc. Applicatiesoftware op de telefoon kan deze patronen herkennen en (ongemerkt) aan andere partijen doorgeven. Inderdaad, een mobiele telefoon is niet alleen via dataretentie een ideaal middel voor individuele surveillance. Steeds meer van dergelijke registraties vinden ongemerkt plaats, waarbij degene die de gegevens opneemt er vanzelfsprekend van uit lijkt te gaan alle rechten te hebben om de gegevens te exploiteren.

In een commerciële context leidt profilering tot steeds verdere verfijning van het reclame aanbod. Dit kan relatief onschuldige of zelfs creatieve vormen aannemen, waarbij bijvoorbeeld een slimme camera in de openbare ruimte uit mijn loopgedrag mijn stemming afleidt (gehaast, vrolijk, terneergeslagen) en daarop een reclameboodschap aanpast, op een elektronisch reclamebord in mijn looprichting. Echter, wanneer adverteerders een zeer gedetailleerd individueel beeld hebben samengesteld van ons doen en laten, van onze sterke en zwakke kanten, en van onze stemmingen, kunnen ze persoonlijke, op het geobserveerde gedrag gebaseerde aanbiedingen construeren die er zeer verleidelijk uitzien en niet alleen inhoudelijk afgestemd zijn, maar ook op het moment komen dat we het meest geneigd zijn tot (impuls)aankopen. In deze context wordt gesproken van *predictive modeling*. Er is wel gesuggereerd (Zarsky 2010) dat de bankencrisis van de afgelopen jaren mede veroorzaakt is door het gebruik van dit soort agressieve, gepersonaliseerde verkooptechnieken bij mensen die het eigenlijk niet konden betalen.

Je zou kunnen zeggen dat mensen er altijd nog zelf bij zijn en er zelf voor kunnen kiezen of ze wel of niet ingaan op een (vilein) aanbod. Tot op zekere hoogte is dat ook zo, al dient er altijd rekening gehouden te worden met kwetsbare groepen, zoals bijvoorbeeld kinderen. De zaken liggen anders als, bij mensen met een bepaald risicoprofiel, sommige mogelijkheden (zoals een hypotheek) helemaal niet eens geboden worden. De vraag is of individuele autonomie op dit punt expliciete bescherming behoeft. Daarnaast spelen veel andere lastige zaken een rol, zoals gelijkheid van behandeling (niet-discriminatie), de mogelijkheid om verhaal te halen bij een mogelijk oneigenlijke behandeling (Gutwirth en Hildebrandt 2010, Hildebrandt en Koops 2010), en het recht op vergetelheid (Buruma, 2011).

In 2006 is in de Tweede Kamer op initiatief van kamerlid Vietsch gesproken over het mogelijk aan banden leggen van agressieve leenreclames. Het blijkt dat sommige mensen daar niet goed tegen opgewassen zijn en zichzelf in de problemen brengen. Het valt te verwachten dat bij vergaande *behavioural targeting* in de reclamewereld het aantal slachtoffers toe zal nemen.

Vraag 4: Moet bescherming tegen commerciële beïnvloeding en uitsluiting versterkt worden?

Een meerderheid lijkt voorstander te zijn van additionele bescherming op dit gebied. Adverteerders verdedigen zich typisch door erop te wijzen dat ze mensen juist een dienst bewijzen, door ze niet met allerlei irrelevante reclame lastig te vallen maar alleen met wat mensen zelf willen. Dit is natuurlijk een drogredenering en een overigens tamelijk effectieve vorm van *framing*. Het is niet: ‘u krijgt precies wat u zelf wil’ maar: ‘u krijgt precies wat de adverteerder wil’. Er wordt gepretendeerd dat uw autonomie juist versterkt wordt, terwijl aan alle kanten geprobeerd wordt u te beïnvloeden. Daarbij is de inhoud van de commerciële boodschappen er meestal niet op gericht om u te verheffen of tot een groot vrijdenker te maken, maar eerder tot een afhankelijke volgzame consument. Er wordt u voorgehouden dat het verzamelen van gedragsgegevens in uw voordeel is. Dat is een eenzijdig beeld. Als, bijvoorbeeld, de Nederlandse Spoorwegen u werkelijk van dienst zouden willen zijn met de gegevens die via uw OV-chipkaart verzameld worden zouden ze u automatisch vergoedingen voor vertragingen doen toekomen. Immers, door de database van vertraagde treinen met uw OV-chipgegevens te

vergelijken wordt snel duidelijk of u ernstige vertraging heeft ondervonden en dus recht heeft op vergoeding. Maar die 'service' wordt ons als klanten natuurlijk niet geboden. Die service is namelijk alleen voor ons voordelig[9].

Enige nuancering is hier op zijn plaats. Een vakbekwame adverteerder gaat op zoek naar de pijngrens van de consument, maar gaat er niet overheen. De boodschap moet inhoudelijk redelijk kloppen en niet te schaamteloos op manipulatie gericht zijn. Dit zorgt voor enige demping, in ieder geval voor degenen die langdurig in de sector actief willen zijn. Sommige mensen blijken ongevraagde adviezen ook wel te waarderen. Ik behoor daar zelf niet toe: ik denk bij een boeksuggestie op een boekensite altijd: dat is vast een onverkoopbaar boek waarvan het magazijn nog vol ligt. Het stoort me in hoge mate dat ik niet eens de optie krijg om deze ongevraagde suggesties uit te schakelen. Liever nog heb ik dat me als consument eerst beleefd gevraagd wordt of ik eigenlijk wel suggesties van de boekenboer wil ontvangen (opt-in). Maar uiteindelijk zie ik het liefste een volledig transparante omgang met klanten, waarbij ik op een 'hoe zien wij u?' knop kan drukken en vervolgens inzicht krijg in het profiel dat over mij geconstrueerd is, met daarbij nog een sub-knop 'wat zijn de consequenties?'. De daarbij verschafte uitleg moet helder en eerlijk zijn, bijvoorbeeld van de vorm: 'wij zien u als risicoconsument vanwege (…); uw krediet wordt beperkt indien (…), en weer verruimd als (...); u komt op dit moment niet in aanmerking voor de volgende producten (...)'. Ingeval er sprake is van foute perceptie of onterechte gevolgtrekkingen heeft de consument bij een dergelijke openhartigheid de mogelijkheid om beroep aan te tekenen. De commercieel gevoelige technieken waarmee profielen samengesteld worden hoeven bij deze vorm van transparantie niet onthuld te worden, maar wel de voor de klant relevante conclusies en gevolgen. Ik vermoed overigens dat zulke transparantie niet anders dan door ingrijpen van reguleerders gerealiseerd zal worden[10].

Langdurige en systematische profilering kan zaken onthullen waar de betrokkene zelf nog niet eens van op de hoogte is. Toenemende vergeetachtigheid om met de OV-chipkaart uit te checken, in combinatie met de leeftijd van de kaarthouder, kan tot bepaalde conclusies leiden (beginnende Alzheimer). Het moge duidelijk zijn dat er sprake kan zijn van een informatie-asymmetrie, waarbij ogenschijnlijk onschuldige details, onderling in verband gebracht, voor een profileerder wel degelijk betekenisvol kunnen zijn. Er zal opnieuw nagedacht moeten worden over de beschermingswaardigheid en het gebruik van op zich onbenullige losse stukjes gedragsinformatie. Vaak lijkt degene die ze oppikt nu te denken ook de eigenaar te zijn en er mee te kunnen doen wat hij/zij wil, zonder transparantie, rekenschap of verhaalmogelijkheden. Zie (Gutwirth en Hildebrandt 2010) voor meer informatie en discussie.

Profilering is het afgelopen jaar hoog op de agenda van (privacy)reguleerders gekomen. Ook anderen zien dat er wat gedaan moet worden. Zo zullen de grote webbrowsers binnenkort een *do not track* knop krijgen. Zo'n opt-out is nuttig, maar een opt-in of een transparantie knop 'hoe zien wij u?' geeft betere bescherming. De discussie is inhoudelijk gecompliceerd en de belangen zijn groot, aan verschillende kanten. Een beter begrip van deze materie en de sociale impact is urgent (zie Zarsky 2010). Op de Techonomy bijeenkomst van augustus 2010 zei de Google's topman Eric Schmidt:

9 Een interessante optie is dat reizigers deze 'service' zelf kunnen organiseren, door bijvoorbeeld via een daartoe ingerichte website hun eigen reisgegevens, direct afkomstig van hun kaart of van de *Mijn NS* website, automatisch te vergelijken met een overzicht van vertraagde treinen. De website zou dan de voor compensatie benodigde verzoekbrieven automatisch kunnen genereren.

10 Een lastige kwestie waar hier aan voorbij gegaan wordt is authenticatie van klanten: hoe kun je zeker weten met wie je te maken hebt, voordat je nadere informatie verschaft. Het is bijvoorbeeld onverstandig om alleen op basis van het IP-adres te zeggen "dit is het bijbehorende profiel". IP-adressen kunnen immers vervalst worden. In de context van de WBP dient men bij een opvraag altijd een copie van een identiteitsbewijs mee te sturen. Deze aanpak is niet heel betrouwbaar, verschaft de aanbieder veel extra informatie (van het identiteitsbewijs) en is niet handig in een online omgeving. Authenticatie online vergt meer maatwerk. Zo zou mijn op mijn IP-adres gebaseerde profiel onthuld kunnen worden op het moment dat ik kan bewijzen dat het IP-adres van mij is, bijvoorbeeld via een gewone brief of digitale, ondertekende verklaring van mijn internet provider.

If we look at enough of your messaging and your location, and use Artificial Intelligence, we can predict where you are going to go. (...) But society isn't ready for questions that will be raised as result of user-generated content.

Het vijfde onderwerp betreft surveillance, profilering en datamining (zie (Baker 2008) voor een toegankelijke introductie), niet in het bedrijfsleven, maar bij de overheid voor veiligheidsdoeleinden. Simpel gesteld gaat het hier (onder andere) om vragen als: kun je een terrorist herkennen door te kijken naar bijvoorbeeld: is deze persoon ooit in Pakistan geweest, belt die veel internationaal maar nauwelijks nationaal, bestelt hij een halal maaltijd aan boord van een vliegtuig, of wil hij aan het gangpad zitten? In een gezaghebbende studie (National Research Council 2008) wordt betoogd dat dit soort datamining technieken om met patronen terroristen te herkennen niet effectief zijn: er zijn te weinig terroristen in relatie tot de beschikbare kenmerkende gegevens, er zijn geen betrouwbare kenmerken van terroristisch gedrag, en eventuele kenmerken zijn ook nog eens makkelijk te maskeren of te verhullen. Datamining en profilering zijn geen geschikte technieken om in een grote populatie een extreem kleine groep te vinden die niet gevonden wil worden. Dat wil overigens niet zeggen dat datamining niet nuttig kan zijn voor andere doeleinden, in concrete welomschreven situaties.

De nieuwe ICT-mogelijkheden van de laatste decennia worden zowel door de politie als door 'het geboefte' benut. Kwaadwillenden vinden een digitale bankroof aantrekkelijk, omdat je bij zo'n roof veilig achter je PC in Oost-Europa kunt blijven zitten en je minder fysiek risico loopt dan wanneer je met een afgezaagd geweer een bank binnenstormt. De politie gebruikt ICT voor het verkrijgen van meer gegevens via eigen surveillance, of via opvragingen in de private sector, en voor het beheer, doorzoeken en koppelen van die gegevens.

Vraag 5: Wie heeft het meeste voordeel van moderne ICT: de politie of de boeven?

Van medewerkers bij politie of justitie is het spontane antwoord: de boeven! Hierbij speelt mogelijk een rol dat er bij hen vaak niet zoveel vertrouwen aanwezig is in de bestaande ICT-kennis en infrastructuur van de politie. De vraag gaat echter over een meer principieel punt, op de langere termijn. Het is niet moeilijk te voorspellen dat surveillance en gedragsregistratie, door private en publieke partijen, nog sterk zal toenemen. Daardoor zullen vele gebeurtenissen tot in meer detail reconstrueerbaar zijn uit registraties. Dit zal naar verwachting leiden tot een daling van misdaadcijfers, niet alleen vanwege de preventieve werking van een panopticum, maar ook vanwege de grotere effectiviteit van controle en opsporing. Het is dus verre van vanzelfsprekend dat de politie hier als verliezer naar voren zal komen.

Interessant is dat er een verband lijkt te zijn tussen het antwoord op deze vijfde vraag en de opstelling in debatten over privacybescherming versus publieke veiligheid. Degenen die de politie als verliezers zien pleiten makkelijker voor versterking van bevoegdheden (zoals computervredebreuk door politie) omdat ze vinden dat de politie een *losing battle* voert. Daarentegen hebben degenen die de politie op de langere termijn als winnaar zien een grotere angst voor een alles controlerende politiestaat, met alle bijbehorende mogelijke vormen van misbruik. Het zou derhalve verhelderend kunnen zijn in debatten over privacy versus veiligheid eerst deze vijfde vraag te bespreken, om daarmee mogelijke impliciete vooronderstellingen boven tafel te krijgen.

In het bovenstaande is bewust niet of nauwelijks over privacy gesproken. Privacy is een moeizaam begrip, dat in het publieke debat in een kwaad licht is komen te staan, bijvoorbeeld als 'schuilplaats van het kwaad'. Hier is de voorkeur gegeven aan het begrip individuele autonomie (in naïeve, niet-filosofische zin), dat relevanter lijkt: enkel het benadrukken van gegevensbescherming is niet productief in de context van slimme omgevingen die voortdurend ogenschijnlijk onbenullige gegevens oppikken en onderdeel maken van een groter beeld; het lijkt productiever de onderliggende waarden

die je in zulke omgevingen zou willen beschermen centraal te stellen. Daarbij is hier nadrukkelijk gekozen voor het perspectief van individuele autonomie. Het is dan prettig dat autonomie vooralsnog een positievere connotatie heeft dan privacy. Autonoom willen we immers allemaal zijn; in ieder geval zolang er nog geen sprake is van negatieve *framing* (zoals bijvoorbeeld in: 'pedofilie dankzij autonomie'; je kunt er op wachten zodra autonomie een bedreigend sterk argument blijkt).

Nieuwe technologie geeft mensen enerzijds meer mogelijkheden en vrijheid (*empowerment*), zoals bijvoorbeeld bij mobiele telefonie, maar creëert ook nieuwe kwetsbaarheden, afhankelijkheden en machtsverhoudingen. Door de toenemende registraties van gedrag vergt individuele autonomie een steeds grotere mate van schaamteloosheid: ik zet die 'natuurfilm' wel op en het interesseert me geen biet als dit vastgelegd wordt en later een keer naar buiten komt; ik lees dat artikel toch, ook al betekent het dat ik voortaan met maoïsme geassocieerd wordt. Schaamtegevoel en terughoudendheid in het delen van persoonlijke informatie zijn in hoge mate cultureel bepaald en ook aan verandering onderhevig. Ze vervullen echter een nuttige, civiliserende maatschappelijke rol: het is in de omgang vaak prettig en makkelijk als je niet te veel van een ander weet. (Solove 2008) stelt terecht: *Privacy is thus a protection of the individual for the good of society*. Dat geldt net zo voor autonomie. De transparantie waartoe burgers en consumenten meer en meer gedwongen worden dient niet tot afgedwongen schaamteloosheid en afhankelijkheid te leiden. Op zijn minst dient er compenserende transparantie te bestaan aan de kant van *the powers that be* die over ons beslissen. Juist in een democratische samenleving wordt het individu beschermd en afgeschermd om (autonoom) zichzelf te kunnen zijn en past het de autoriteiten om open en transparant te zijn. Hoe we individueel autonoom kunnen zijn in het web van nieuwe registrerende, analyserende en sturende technologie blijft een intrigerende uitdaging. Hier is vooral geprobeerd enige belangstelling en gevoeligheid voor de materie te ontwikkelen.

Literatuur

Arendt, H. (1951), *The Origins of Totalitarianism*. Shocken books: New York.

Baker, S. (2008), *The Numerati*. Boston, New York: Hougthon Mifflin Company.

Buruma, Y. (2011), Het recht op vergetelheid. Politiële en justitiële gegevens in een digitale wereld. In: D. Broeders, C.M.K.C. Cuijpers en J.E.J. Prins (red.) De staat van informatie, WRR-verkenning nr. 25, Amsterdam: Amsterdam University Press, 165-221.

Engelen, D. (2007), *Frontdienst. De BVD in de koude oorlog*. Amsterdam: Boom.

Gutwirth, S. en M. Hildebrandt (2010), Some Caveats on Profiling. In: S. Gutwirth, Y. Poullet en P. De Hert (eds), *Data Protection in a Profiled World*. Dordrecht, Springer, 31-41.

Hildebrandt, M. en E.J. Koops (2010), The challenges of ambient law and legal protection in the profiling era. *Modern Law Review*, *73*(3), 428-460.

Hoekstra, F. (2004), *In dienst van de BVD.* Amsterdam: Boom.

Jacobs, B. en W. Pieters (2009), Electronic Voting in the Netherlands: From Early Adoption to Early Abolishment. In: *Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures*. Springer Lecture Notes in Computer Science, deel 5705, Berlijn, 121-144.

National Research Council (2008), Committee on Technical and Privacy Dimensions of Information

for Terrorism Prevention and Other National Goals. *Protecting Individual Privacy in the Struggle against Terrorists*. Washington, The National Academies Press.

Solove, D. (2009), *Understanding Privacy*. Harvard University Press.

Stevens, L en B.J. Koops (2009), Opzet op de harde schijf: criteria voor opzettelijk bezit van digitale kinderporno. *Delikt en Delinkwent* (7), 669-696.

Zarski, T. (2010), Responding to the Inevitable Outcomes of Profiling: Recent Lessons from Consumer Financial Markets, and Beyond. In: S. Gutwirth, Y. Poullet en P. De Hert (eds), *Data Protection in a Profiled World*. Dordrecht, Springer, 53-74.

Tekstverwerker: OpenOffice 3.2.0
Omvang: ongeveer 5500 woorden.