2011

Privacy na de 'computationele wending'

Mireille Hildebrandt, *Radboud University Nijmegen*

Privacy na de 'computationele wending'?

Mireille Hildebrandt

"Het tijdschrift dat jou leest."

Evelyn Rusli (2011)

Inleiding[i]

In deze bijdrage zal ik mij richten op de gevolgen van het doorzoeken van grote datasets en het toepassen van de kennis die daaruit wordt 'gemijnd'. Zowel het bedrijfsleven als de overheid verwachten veel van dit soort kennis, respectievelijk als marketing-instrument dan wel als manier om criminaliteit te voorspellen. In beide gevallen gaat het vooral om een techniek waarmee zo snel en zo precies mogelijk maatwerk 'op de persoon' kan worden geleverd. De vraag in hoeverre de betreffende computationele technieken die belofte waarmaken – de effectiviteitsvraag – staat in deze bijdrage niet centraal. Voor de goed orde ga ik er hier vanuit dat toepassing van technieken zoals datamijnen, machinaal leren, neurale netwerken en multi-agent systemen interessante kennis kan opleveren, maar vaak ook incomplete dan wel incorrecte kennis die door een gebrek aan transparantie niet als zodanig aan het licht komt. Bij voortschrijdend gebruik van dit soort technologie zou zich dan ook wel eens de volgende situatie kunnen voordoen (met een knipoog naar Merton 1948): 'if machines define a situation as real, it is real in its consequences'. Daarmee verschijnt de vraag hoe deze nieuwe computationele infrastructuur zich verhoudt tot grondbeginselen van de rechtsstaat, in het bijzonder tot onze privacy. Kernpunt van de analyse is de manier waarop dit soort technieken individuele personen gaan 'lezen' en 'begrijpen' en de conclusie zal zijn dat traditionele opvattingen van informationele privacy zoals controle over of beperkte toegang tot persoonsgegevens geen adequate bescherming bieden. Om privacy te beschermen in een wereld die voortdurend op de zaken vooruit wil lopen, moet de link worden gelegd met identiteitscontructie en autonomie, zonder in de valkuil van neo-liberale dan wel liberteinse vrijheidsdromen te vallen. Tegelijkertijd wordt duidelijk dat effectieve

juridische bescherming onvoldoende gewaarborgd is wanneer die wordt beperkt tot articulatie in de technologie van de drukpers (het geschreven recht, zie daarover Hildebrandt 2008a). Voortbouwend op noties als privacy by design, value sensitive design en constructive technology assessment moeten juristen, computer wetenschappers en designers van ICT infrastructuur zich gaan buigen over de vraag hoe juridische – democratisch gelegitimeerde – bescherming kan worden gearticuleerd in de ICT infrastructuur.

Het visioen van 'Omgevingsintelligentie'

Ambient Intelligence betekent letterlijk 'Omgevingsintelligentie' en verwijst dus naar omgevingen die een vorm van intelligentie ontwikkelen. Om discussies te vermijden over de vraag of door mensen gemaakte computersystemen 'intelligent' mogen heten, kies ik meestal voor de term 'slim'. Onder een slimme omgeving versta ik hier een omgeving die op basis van lerende computersystemen in staat is op haar gebruikers te anticiperen.

Volgens het 'narratief' van de ontwerpers van Ambient Intelligence is die anticipatie kenmerkend voor proactieve omgevingen die daarmee in staat zijn om diensten op maat te verlenen, zelfs voordat de gebruiker zich van haar behoeften bewust is (Aarts and Marzano 2003; Van den Berg 2010). In die zin is de omgeving slimmer dan bijvoorbeeld een thermostaat, of een eenvoudige zoekmachine die een door de ontwerper gedetermineerd stappenplan volgen. Het verschil is dat de slimme omgeving in staat is te leren van de manier waarop haar bewoners of gebruikers zich gedragen en dat dit leerproces de slimme omgeving een zekere onvoorspelbaarheid geeft (D. J. Hand *et al.* 2001). Slimme omgevingen hebben een 'eigen wil' zou je metaforisch kunnen zeggen. Daarom zijn ze ook in staat om oplossingen te vinden voor problemen die de ontwerper niet had voorzien en in beginsel kunnen ze die oplossingen ook zelfstandig uitproberen. Concreet betekent het dat de omgeving zich voortdurend proactief aanpast, bijvoorbeeld door deuren te ontsluiten als het 'slimme huis' de bewoner herkent, verlichting af te stemmen op de voorkeuren van de gebruiker, muziek af te spelen die de ontspanning of de productiviteit van de gebruiker verhoogt of bestellingen te doen om voorraden op peil te houden. Allerlei preventieve gezondheidsbevorderende maatregelingen kunnen worden

geprogrammeerd, waarbij vrijwel permanente meting van bloedwaarden, hartritme, temperatuur en transpiratie tot de mogelijkheden behoort. Persoonlijke digitale assistenten kunnen alle inkomende communicatie sorteren op urgentie en belang, op basis van eerder gedrag en/of ingestelde voorkeuren; berichten kunnen worden weggefilterd of opgeschort totdat het de gebruiker uitkomt.

De anticipatie is gebaseerd op complexe softwareprogramma's die op basis van computeralgoritmes databestanden doorzoeken waarin voortdurend allerlei gegevens worden opgeslagen. De analyse van deze gegevens levert een veelheid van patronen op die met het blote oog niet zichtbaar zijn en die alleen dankzij het enorme rekenvermogen van computers ontdekt kunnen worden (David J. Hand 2007). De gebruiker wordt echter niet lastig gevallen met deze computationele onderbouw; in beginsel zouden het toetsenbord en het computerscherm zelfs kunnen verdwijnen omdat alle voorwerpen in de omgeving zelf als 'interface' gaan functioneren (Greenfield 2006). De beïnvloeding is in het kader van de gebruiksvriendelijkheid *subliminaal*. De gegevens waar het om gaat worden grotendeels door sensoren in de omgeving opgepikt en niet expliciet door de gebruiker aangedragen; gegevens worden 'gelekt' in plaats van 'verstrekt'. De idee is dat alle dingen in de omgeving door middel van draadloze communicatie (RFID) voortdurend kunnen aangeven waar ze zich bevinden (het 'Internet der Dingen', ITU 2005). Hoewel de omgeving dus is vergeven van de laatste technologische snufjes zal de bewoner daar weinig van merken; het narratief van Ambient Intelligence spreekt graag van 'verborgen complexiteit' en van het primaat van de gebruiker, wiens (door de software afgeleide) wensen centraal zouden staan. Daar passen echter wat caveats bij. Zo is het maar de vraag in hoeverre de data waar deze preferenties uit zijn afgeleid correct zijn, relevant en compleet. In het verlengde is voor de gebruiker onduidelijk hoe haar voorkeuren, en bijvoorbeeld haar zwakke en sterke kanten precies zijn afgeleid en in hoeverre die inferentie correct, relevant en gepast is. Wanneer overschrijdt de slimme omgeving de grenzen van de persoonlijke autonomie van de gebruiker? Dat laatste hangt ook samen met de wijze waarop de gebruiker wordt bediend: is er sprake van participatie of is de slimme omgeving de gebruiker voortdurend 'te slim af'?

Gedragsgestuurd adverteren & gepersonaliseerde nieuwsvoorziening

De lezer kan zich afvragen of het allemaal zo'n vaart gaat lopen. Om de gedachten te bepalen ga ik in op twee online voorproefjes van wat ons te wachten staat. Op dit moment is het grote verschil tussen online en offline dienstverlening dat online voortdurend gegevens worden 'gelekt', met name van websurf gedrag. Lekken betekent in dit verband dat de internetgebruiker die gegevens niet hoeft op te geven of in te typen. Zolang de sensortechnologie en de RFID systemen die Ambient Intelligence mogelijk moeten maken nog niet in functie zijn, kan alleen de online 'wereld' zich op basis van grote hoeveelheden gelekte gegevens proactief aanpassen.

In geval van gedragsgestuurd adverteren gaat dat als volgt in zijn werk (Office of Fair Trading 2010).[ii] Adverteernetwerken plaatsen software op zoveel mogelijk websites. Deze software registreert – bijvoorbeeld door het plaatsen van cookies op de computer van de gebruiker – vanuit welke andere site of zoekmachine de bezoeker op een bepaalde site landt, hoelang die daar blijft, welk deel van de inhoud wordt aangeklikt en hoe dat zich verhoudt tot aankoopgedrag. Op die manier kunnen klantenprofielen worden gemaakt waaruit blijkt wat voor type klanten welk soort aankoopgedrag vertonen. Adverteerders (die diensten of producten aanbieden) kunnen vervolgens 'bieden' op advertentieruimte bij voor hen lucratieve websites, wanneer duidelijk is dat dit voordeel op gaat leveren. Alle registratie van websurf gedrag, het analyseren van de gegevens, het aanbieden van advertentieruimte en het bieden daarop gaan volautomatisch. Praktisch gezien betekent het dat behalve geografisch aangepaste advertenties (geen bontjassen aanbieden in de tropen) en contextuele advertenties (dure producten aanbieden op de site van een krant die door kapitaalkrachtige bezoekers wordt gelezen) nu ook gedragsgestuurde advertenties mogelijk zijn, die veel specifieker afstemmen op een bepaald type gebruiker. Daarmee is het mogelijk zeer gepersonaliseerde reclame te maken, zonder dat de bezoeker van een website door heeft dat haar buurman waarschijnlijk andere aanbiedingen krijgt. Door het voortdurend matchen van online gedragspatronen met door data-analyse verkregen klantenprofielen kan met een grote of minder grote mate van waarschijnlijkheid worden voorspeld hoe de klant zich zal gedragen. Dit kan uiteraard leiden tot uitsluiting van bepaalde diensten of goederen, waarbij we kunnen denken aan verzekeringen of aankopen op krediet. Meestal zullen de gevolgen echter subtieler zijn: bepaalde zaken worden niet aangeboden, of tegen een andere prijs aangeboden, zonder dat de gebruiker dit doorheeft. In het verlengde hiervan kan ook worden uitgezocht aan welke inhoud (content) individuele personen waarschijnlijk de

voorkeur geven, zodat nieuws en andere vormen van berichtgeving hierop kunnen worden afgestemd. Dan gaat het om gepersonaliseerde – gefilterde – nieuwsvoorziening. In plaats van het aanbieden van de mogelijkheid om op eigen initiatief bepaalde voorkeuren aan te geven die tot gefilterde nieuwsvoorziening leiden, zoeken apps als *Flipboard* of *Editions* zelf bij elkaar wat geacht wordt in de interesse sfeer van een gebruiker te liggen (Rusli 2011).[iii] Net als slimme omgevingen en advertentienetwerken 'lezen' deze tijdschriften de lezer, waarna deze wordt voorzien van artikelen 'op maat'. Sunstein (2001) heeft al eens geschreven over de dreiging die uitgaat van zo'n ver doorgevoerde personalisering van de nieuwsvoorziening, hoewel hij daarbij vooral oog had voor filters die gebruikers zelf als zodanig kunnen instellen. Zijn bezwaren zijn desondanks relevant voor software die zelf uitzoekt waar de voorkeuren van de gebruiker liggen. Ten eerste is het in een levensvatbare democratie van belang dat burgers geconfronteerd worden met onverwachte meningen en onderwerpen, anders raken ze het contact met de werkelijkheid kwijt; ten tweede is van belang dat burgers beschikken over gedeelde kennis en ervaring hetgeen bij vergaande filtering steeds minder waarschijnlijk wordt. Gepersonaliseerde informatievoorziening kan ertoe leiden dat mensen steeds meer bevestigd worden in eenmaal ingenomen standpunten, eenvoudigweg omdat de slimme online omgeving meent dat die het meest bij de betreffende persoon aansluiten.

De computationele wending

Waarom heeft het zin om vooruit te lopen op omgevingsintelligentie en alvast te bedenken welke bedreigingen daaruit voortkomen voor privacy en de rechtsstaat? De reden is dat de computationele infrastructuur die dit alles mogelijk maakt op dit moment wordt ontworpen en als de investeringen eenmaal gedaan zijn en de toepassingen eenmaal 'aan de man gebracht' wordt het moeilijk die infrastructuur alsnog achteraf te gaan voorzien van transparantie-technologie. Het is dus zaak om al tijdens het ontwerp van deze technologie mee te kijken en mee te bouwen aan een structuur die zo min mogelijk kansen biedt om gebruikers op onzichtbare wijze te manipuleren. Om duidelijk te maken wat nu precies met een computationele infrastructuur wordt bedoeld volgt hier nog een korte uitleg over data mijnen, profileren en de kennis die daaruit voortkomt. 'Knowledge discovery in databases'

(KDD) is een techniek waarmee patronen kunnen worden ontdekt in zeer grote datasets (Custers 2004). Het gaat daarbij niet om het opvragen van informatie die als zodanig in de dataset is opgeslagen, bijvoorbeeld hoeveel mensen een inkomen genieten boven de 50.000 euro, of wat voor opleiding mensen hebben die meer dan 75.000 euro per jaar verdienen. Het kan wel gaan om de vraag of het klopt dat mensen die meer dan 60.000 euro bruto per jaar verdienen minder vaak een beroep doen op de huisarts. In dat geval wordt een vooraf opgestelde correlatie getoetst. Wat datamijnen echter pas echt interessant maakt is dat dankzij statistische en andere computationele technieken ook kan worden gezocht naar nieuwe verbanden, omdat correlaties kunnen worden ontdekt die niet waren voorzien. De idee is dat door dit soort 'blinde' algoritmische zoekopdrachten mogelijke 'bias' of vooringenomenheid kan worden voorkomen en dat onverwachte patronen zichtbaar kunnen worden die met het blote oog niet vindbaar zijn. De uitkomsten lijken daarom objectiever dan wanneer eerst een correlatie wordt geponeerd wordt.

Hierbij passen twee opmerkingen. Ten eerste melden onderzoekers vanuit de hoek van machinaal leren dat de computationele technieken die gebruikt worden om een omgeving 'slim' te maken altijd een zekere bias zullen hebben (Sculley and Pasanek 2008). Die bias hangt samen met het feit dat geautomatiseerde leerprocessen steeds gebaseerd zijn op een specifieke modellering van de dataset waaraan zij hun leervermogen ontlenen. Die modellering maakt sommige verbanden zichtbaar maar andere juist onzichtbaar. In wezen is het juist deze modellering en de daarmee samenhangende 'bias' die zorgt voor nieuwe inzichten, maar – onvermijdelijk – ook voor blinde vlekken. Binnen het domein van machinaal leren staat dit bekend als het *no-free-lunch theorema van* Wolpert en Macready (1997). Dit theorema leert dat er geen algoritme is dat in alle gevallen de beste uitkomst oplevert; je kunt dus wel proberen je programma te optimaliseren voor de oplossing van een bepaald type problemen, maar je zult daar nooit volledig in slagen. Wie gebruik maakt van dit soort technieken moet zich dus steeds bewust blijven van het feit dat de slimheid van de omgeving berust op het ontdekken, vooropstellen en prioriteren van specifieke verbanden en voor zover de omgeving steeds verdergaat op de ingeslagen weg is de kans op ongelukken dan ook steeds groter. Een mogelijke remedie is om datasets steeds op verschillende manieren te modelleren en met regelmaat alternatieve uitkomsten te vergelijken. Dat kan natuurlijk alleen als daarin wordt geïnvesteerd en

afscheid wordt genomen van de gedachte dat computationele technieken objectieve waarheden aanleveren (Hildebrandt 2011 forthcoming).

Ten tweede zal het meestal zo zijn dat de uitkomsten van dit soort technieken statistisch van aard zijn en wel kloppen op een geaggregeerd niveau, maar niet bij toepassing op een individu. De kennis die wordt gegenereerd betreft non-distributieve profielen van een groep individuen (Vedder 1999). Zo kan bijvoorbeeld een verband worden gevonden tussen vrouwen en borstkanker: 1 op de 8 vrouwen krijgt borstkanker. Dat betekent echter niet dat iedere vrouw een kans van 1 op 8 heeft om borstkanker te bekomen; afhankelijk van allerlei andere factoren zal die kans hoger of lager zijn. Het kans is niet gelijk verdeeld over alle vrouwen; leeftijd, levensstijl, ziektegeschiedenis van de voorouders of verwanten, medicijngebruik of nog andere zaken kunnen de kans veranderen. Dat betekent dat toepassing van het profiel op een vrouw, als zou haar kans 1 op 8 zijn, simpelweg onjuist is. In de praktijk zijn de meeste profielen die op basis van statistische inferenties gevonden worden non-distributief. Dat betekent dat toepassing in veel gevallen onterecht is. Het gebruik van dergelijke profielen kan worden gezien in het verlengde van onze eigen cognitieve economie, die ons dwingt om voortdurend te categoriseren en te generaliseren ten einde enige orde aan te brengen in de chaos van dagdagelijkse bevindingen. Als het goed is zijn we ons echter bewust van de beperktheid van onze kennis en staan we open voor 'het andere verhaal'. Handzame, goed getrainde intuïtie wordt een handicap zodra we ongevoelig worden voor nieuwe informatie die om bijsturing vraagt (Gigerenzer 2007). De vraag is of slimme omgevingen slim genoeg zijn om zo'n ander verhaal een kans te geven. Kan een machine 'buiten de doos' denken?

Daarmee komen we ook aan bij de vraag of het feit dat de gebruiker – of liever de bewoner – van een slimme omgeving nog wel enige privacy heeft. Is de omgeving haar niet voortdurend een paar stappen voor? Wat betekent privacy eigenlijk nog in dit verband? Zou het kunnen zijn dat de omgeving een mooie privacy-ervaring kan aanbieden, terwijl de persoon die het betreft in feite al helemaal 'uitgelezen' is?

Traditionele opvattingen van privacy

In een overtuigend betoog stelt (Stalder 2002) dat de traditionele Westerse opvatting van privacy in zekere zin een bijproduct is van de opkomst van de drukpers.[iv] De enorme toename van tekst leidde tot het ontstaan van private bibliotheken waarin mensen zich terug konden trekken om een individuele ontdekkingstocht te ondernemen in de gedachtewereld van andere tijden en plaatsen. Het hardop lezen van handgeschreven manuscripten in publieke bibliotheken (zoals daarvoor gebruikelijk) maakte geleidelijk plaats voor het geluidloos lezen van boeken in de eenzaamheid van het eigen huis of enigerlei andere plaats. Daarmee werd een vergaande individualisering ingezet die afstand schiep tot andere lezers (en tot niet-lezers), waardoor bijvoorbeeld de betekenis van teksten minder vanzelfsprekend werd en uiteenlopende interpretaties van dezelfde tekst ontstaan. De Franse filosofen (Ricœur 1981) en (Lévy 1990) hebben al eerder gewezen op de manier waarop het schrift distantie schept tussen auteur, tekst, lezer en publiek en hoe het tot uitstel leidt bij het vaststellen van de betekenis van een tekst. Het schrift en de drukpers vormen aldus de kiem van een pluriforme samenleving waarin de betekenis van bijvoorbeeld een wettekst niet makkelijk gemonopoliseerd kan worden (Hildebrandt 2008). Daarnaast hebben historici beschreven hoe de behoefte aan sociale afstand vanaf het eind van de middeleeuwen zichtbaar wordt in de fysieke woonomgeving; bij de bouw en inrichting van huizen van de hogere en later ook van de middenklasse wordt steeds meer separate ruimte geclaimd voor gezinsleden (eigen slaapkamers voor de kinderen, separate studeervertrekken en bibliotheken) (Ariès and Duby 1987).

Privacy hangt historisch dus samen met de mogelijkheid om zich terug te trekken uit het sociale verkeer en met het vermogen om op basis van verschillende interpretaties tot een eigenstandige oordeelsvorming te komen over zaken van algemeen of persoonlijk belang. Daarmee is privacy zowel een publiek goed als een individueel belang. Privacy betreft echter niet per definitie ons voelen, denken en handelen in de private ruimte, ook al is ons moderne privacybegrip daar wel op georiënteerd, bijvoorbeeld waar art. 8 EVRM het grondrecht omschrijft als een recht op niet-inmenging in het privéleven, met name binnen de eigen woning. De nieuwe informatie- en communicatie-infrastructuur maakt deze opvatting van privacy - als beperkt tot de private ruimte - op twee manieren problematisch. Enerzijds lopen private, sociale en publieke contexten dwars door private, sociale en publieke ruimtes heen: we werken 's avonds laat thuis op de huis-pc, versturen privémails vanaf ons kantoor, we

bellen met goede vrienden in de trein en houden een online werkbespreking vanuit onze hotelkamer. De context valt niet meer samen met de locatie (Gutwirth 2002; Nissenbaum 1997). Anderzijds is onze behoefte aan privacy juist in publieke contexten groot: de anonimiteit van de grote stad biedt een vorm van vrijheid die ontbreekt in een dorpse omgeving waar sociale controle zegeviert. Een slimme omgeving zou een terugkeer naar de nieuwsgierige buurgemeenschap kunnen inluiden, met als verschil dat de alwetende slimme buren geen gezicht hebben en niet alleen anoniem maar zelfs onpersoonlijk zijn. Ook (Lessig 1999: 155) beschrijft de samenhang tussen urbanisatie, toenemende mobiliteit en het ontstaan van een nieuw type vrijheid aan het eind van de middeleeuwen, die gedijt bij een zekere mate van anonimiteit in het sociale verkeer. Hij waarschuwt voor het verlies van die vrijheid als gevolg van toenemend gebruik van profileringstechnologie.

Met de komst van de fotografie en de massamedia aan het eind van de 19e eeuw en in de loop van de 20e eeuw ontstaat een nieuwe behoefte aan privacy, die niet zozeer een terugtrekking betreft maar eerder toeziet op een vorm van controle op informatie over de eigen persoon. De beroemde uitspraak van Warren and Brandeis uit 1890 dat burgers jegens elkaar een 'right to be let alone' kunnen inroepen had betrekking op de wens van publieke figuren om controle te houden over welke informatie door de roddelpers over hen werd verspreid (Warren and Brandeis 1890). In het verlengde van deze benadering stelt (Westin 1967) dat privacy het recht is om zelf te bepalen wie toegang heeft tot welke informatie over zichzelf. Met de opkomst van de informatiemaatschappij lijkt die opvatting aan belang te winnen; informationele zelfbeschikking wordt in veel literatuur gezien als de grondslag van zowel het privacyrecht van art. 8 EVRM als van het recht op gegevensbescherming van Richtlijn 95/46/EG (Rouvroy and Poullet 2009). Met name Duitsland gaat voorop in het eisen van een vergaande informationele autonomie, die wordt afgeleid uit het grondrecht op menselijke waardigheid (Hornung and Schnabel 2009).

Daarmee lijkt een nieuwe opvatting van privacy aan de orde, die naast privacy als isolatie of terugtrekking een eigen rol is gaan spelen. Privacy als zelfbeschikking legt grote nadruk op keuzevrijheid en maakt van toestemming, instemming of overeenstemming ('consent') een van de belangrijkste dogma's van het privacy debat. Daarmee dreigt privacy langs twee kanten een onmogelijk te realiseren waarde, belang of recht te worden. Enerzijds komt de bescherming van de privacy

vrijwel geheel op de schouders van individuele burgers te liggen, die zonder veel zicht op de consequenties van het delen van informatie als een soeverein over hun gegevens moeten waken. Juist vanwege het ontbreken van informatie over wat de gevolgen zijn van gegevensuitwisseling lijkt marktfalen hier onvermijdbaar: de keuzes die consumenten, burgers of gebruikers maken zijn gebaseerd op een gebrek aan kennis (London Economics 2010). Anderzijds is het beeld van een individu die als soeverein over het eigen handelen regeert problematisch in een wereld waar alles lijkt te draaien om connectiviteit en interdependentie. Vaak wordt in het kader van de informationele zelfbeschikking gepleit voor het vestigen van een soort eigendomsrecht op persoonsgegevens, zodat mensen handel kunnen gaan drijven met hun data (Schwartz 2000).[v] Dat pleidooi gaat echter voorbij aan het feit dat data de facto allang functioneren als grondstof voor de economie en als wisselgeld voor de consument; een eigendomsrecht is daarvoor niet nodig. Bovendien schept het de illusie van een in zichzelf besloten individu dat naar eigen inzicht op grond van rationele afwegingen of naar eigen willekeur over het uitwisselen van gegevens kan beslissen. Het methodologisch individualisme dat aan deze opvatting van privacy als controle en autonomie ten grondslag ligt slaat de plank mis. Persoonsgegevens zijn per definitie relationeel: wij hebben een naam zodat anderen naar ons kunnen verwijzen als we er niet zijn. In die zin is mijn naam niet (alleen) van mij, maar juist van anderen die mij aan willen spreken, over mij willen spreken of hun aanspraken jegens mij een 'adres' willen geven (van de verkoper tot de belastingdienst). De vraag welke gegevens wanneer door wie worden vastgelegd gaat niet alleen degene aan op wie ze in eerste instantie betrekking hebben, maar juist degenen die iets met mij te maken (willen) hebben. Tegelijkertijd begint een specifiek soort relationele gegevens een steeds prominentere rol te spelen dankzij online sociale netwerken, namelijk gegevens zoals de structuur van het relatienetwerk dat ik online heb ontwikkeld of de foto's, verhaaltjes en documenten die ik op mijn netwerk plaats, waarin ik samen met anderen verschijn. Van wie is dat relatienetwerk? Van mij of ook van degenen met wie ik verbonden ben? Wie kan beschikken over de foto waarop ik samen met een aantal collega's aan de dis zit tijdens een conferentie in Verwegistan: moet ik eerst toestemming vragen aan alle disgenoten voor ik de foto op Facebook zet? En wie mag zulk materiaal van mijn account afhalen als het haar behaagt haar toestemming in te trekken? Ben ik daartoe verplicht, of moeten we daarover onderhandelen (Gurses and Berendt 2010)?

Privacy en identiteitsvorming[vi]

Het privacybegrip van de tijd van de drukpers en dat van de eeuw van de massamedia bieden geen adequate bescherming in tijden van proactieve, slimme omgevingen. Beide begrippen, sociale terugtrekking en informationele zelfbeschikking, verhouden zich tot medemensen, terwijl in geval van anticiperende omgevingen nood is aan een privacybegrip dat zich verhoudt tot de computationele infrastructuur die omgevingsintelligentie mogelijk maakt.

Om handen en voeten te geven aan een relationeel privacybegrip dat kritische potentie heeft in slimme omgevingen volgen we de werkdefinitie van (Agre and Rotenberg 2001: 7):

> Het recht op privacy is de vrijheid van onredelijke beperking op de constructie van de eigen identiteit.

Met deze definitie slaan zij zes vliegen in een klap. Om te beginnen gaat deze definitie ervan uit dat identiteit geen rustig bezit is, maar het vluchtige resultaat van een dynamisch proces. Ten tweede bevestigt ze de negatieve vrijheid (de vrijheid van) als kern van de privacy, waarbij ten derde niet iedere beperking een inbreuk is, maar alleen de onredelijke. Die beperking heeft – ten vierde – betrekking op de positieve vrijheid (de vrijheid om), waardoor het vrijheidsbegrip perspectief krijgt en niet gelijk komt te staan met de vrijheid om zich willekeurig te gedragen. Ten vijfde wordt het verband gelegd met de ontwikkeling van de eigen identiteit, die kennelijk – het zesde punt – tot stand komt in wisselwerking met anderen. Daarmee is het belang van context gegeven; wie we zijn wordt mede bepaald door de context waarbinnen we ons bewegen. Als de context ons de mogelijkheid ontneemt te doorzien hoe we worden geanticipeerd staat de vrijheid om de eigen identiteit te ontwikkelen op het spel. Slimme omgevingen anticiperen hun gebruikers. Omdat dit grotendeels zou gebeuren zonder bewuste input van hun bewoners ligt subliminale beïnvloeding voor de hand, die uit kan monden in gerichte manipulatie. Daarmee lijkt een onredelijke inperking van de eigen identiteitsvorming in zicht te komen.

De relatie tussen privacy en het vormgeven aan de eigen identiteit bevestigt dat identiteit geen statisch gegeven is, maar iets dat zich eigenlijk aan iedere vorm van

substantivering onttrekt. Identiteit in de zin van zelfbewustzijn is geen 'ding' maar het vluchtige resultaat van een dynamisch proces van identiteitsvorming. Het geeft aan dat we onszelf in de loop van ons leven als dezelfde (identieke) persoon ervaren, ondanks het feit dat diezelfde persoon zich voortdurend ontwikkelt en daarmee gaandeweg iemand anders wordt (ook dat is een ervaringsfeit). Identiteit in deze zin lijkt een blinde vlek, een punt dat wegspringt zodra we het in beeld willen brengen. De Franse filosoof (Ricoeur 1992) spreekt in dit verband van *ipse*-identiteit.

Om aanspreekbaar te zijn voor andere personen en organisaties moet desondanks een stabiele identificatie mogelijk zijn. Het recht kent dan ook juridische instrumenten om mensen of organisaties te identificeren als verantwoordelijk voor de gevolgen van hun handelen, met name door het toekennen van rechtssubjectiviteit.[1] In dat verband is identiteit het aanspreekpunt voor de toekenning van rechten en plichten. Ricoeur zou in dat verband spreken van een *idem*-identiteit omdat het niet gaat om de mens van vlees en bloed maar om de formele identiteit als juridisch aanknopingspunt. De identiteit die mensen ervaren als de kern van hun persoon wordt echter door het recht afgeschermd, bijvoorbeeld door het toekennen van het recht op privacy. Met de Nederlandse rechtsfilosoof (Glastra van Loon 1980) kunnen we zeggen dat persoonlijke identiteit onderbepaald is (dynamisch, meervoudig, altijd in de maak). Het recht bevestigt en beschermt die onbepaaldheid door mensen een vrije ruimte te bieden waarin zij ongestoord kunnen handelen zonder daarover voortdurend verantwoording af te hoeven leggen. Tegelijk biedt het recht een instrumentarium om in specifieke gevallen tot aansprakelijkheid te kunnen besluiten en schadevergoeding of straf op te leggen.

Identiteit speelt dus een dubbele rol in het recht; enerzijds pint het mensen (en andere rechtspersonen) vast door ze verantwoordelijk te houden voor wat ze in het verleden hebben gedaan, anderzijds biedt het de kans om binnen bepaalde grenzen een eigen plan te trekken. Om daadwerkelijk de eigen identiteit te ontwikkelen moet echter wel helder zijn hoe bepaalde handelingen door het recht worden verstaan. Ik moet een beeld hebben van de legitieme verwachtingen die anderen van mij hebben, om mijn handelen daar op af te kunnen stemmen. Kennistheoretisch zou je dat kunnen uitleggen door te zeggen dat ik, om mijn eigen handelen te kunnen begrijpen,

[1] Alleen rechtssubjecten zijn drager van rechten en plichten. De wet bepaalt dat naast natuurlijke personen ook bepaalde organisaties (vereniging, stichting, NV, BV, de Staat, de provincie, de gemeente, etc.) rechtspersoon zijn.

moet weten hoe anderen mijn handelen gaan 'lezen'.[vii] Die dubbele anticipatie is kenmerkend voor de omgang tussen mensen: om te weten wie ik ben moet ik weten hoe anderen mij begrijpen. Niet alleen om mij aan te passen aan het beeld dat anderen van mij hebben, maar evenzeer om mij daartegen te kunnen verzetten.

Dit is ook de reden waarom ik mij anders verhoud tot een stoel, een auto of een zwembad, dan tot een vriend, een collega of een organisatie. In het eerste geval verwacht ik niet dat deze artefacten betekenis toekennen aan mijn handelen en zich naar aanleiding daarvan anders gaan gedragen. In het tweede geval verwacht ik dat wel. Maar anders dan stoelen, auto's en zwembaden blijken slimme omgevingen mijn handelen wel te anticiperen – net zoals overigens mijn hond of de mug die ik probeer te vangen. Het probleem van slimme omgevingen is, dat zij mij wel anticiperen en hun 'gedrag' daarop aanpassen, maar dat dit voor mij niet zichtbaar is. De anticipatie is eenzijdig. De omgeving interpreteert mijn handelen op basis van computationele patronen waarmee mijn gedrag overeenkomt, en neemt vervolgens een aantal beslissingen, zonder mij daar verder mee lastig te vallen. Omdat ik niet kan achterhalen hoe mijn handelen wordt geïnterpreteerd en wordt voorzien, kan ik mij daartegen niet verzetten. De kans is groot dat de omgeving mijn identiteit in vergaande mate gaat vormen zonder dat ik mij daar bewust van ben.

De vorming van persoonlijke identiteit is geen kwestie van een voortdurende bewust gewilde onderneming. Veel van ons handelen is geautomatiseerd en verloopt gedachteloos; ook de dubbele anticipatie die kenmerkend is voor menselijke interactie vindt voor een groot deel plaats op intuïtief niveau. Dat heeft de rechter er echter nooit van weerhouden om een verdachte die zijn moeder heeft gedood, de vraag voor te leggen of er redenen of oorzaken zijn die het strafbare feit kunnen rechtvaardigen of verontschuldigen. Het vermogen om achteraf redenen te geven voor het eigen handelen werpt zijn schaduw vooruit en maakt het mogelijk om vooral die handelingen te automatiseren die moreel of juridisch gerechtvaardigd zijn. Voor zover het echter onduidelijk is hoe anderen ons 'verstaan' kunnen we daar niet op inspelen en gedragen we ons in een soort vacuum, in dit geval wellicht bijgestuurd door de subliminale interventies van de slimme omgeving. Dit is inmiddels aangeduid als het 'inferentieprobleem' (Dwyer 2009). Daarmee wordt hier gedoeld op het feit dat het in slimme omgevingen lastig – zo niet onmogelijk – wordt om te voorzien

welke inferenties uit ons gedrag worden afgeleid en op basis van welke inferenties we proactief worden behandeld.

Privacy en gegevensbescherming na de computationele wending

Tegenover een stoel, een auto of een zwembad hoef ik mijn privacy niet te beschermen. Dit soort technologische artefacten treedt mij niet tegemoet op basis van een inschatting van mijn zwakke en sterke kanten en zal in die zin mijn identiteit niet mede bepalen. Indien slimme omgevingen de komende jaren daadwerkelijk gerealiseerd worden zal onze verhouding tot technologische artefacten fundamenteel veranderen. Wij zullen in zekere zin moeten leren om in te schatten hoe wij door de omgeving worden ingeschat, net zoals we gewend zijn in te schatten hoe onze vrienden, buren, werkgever, belastingdienst of zakenpartner ons inschatten. Zoals we onze identiteitsvorming in bepaalde contexten afschermen van andere mensen en organisaties, zullen we op enig moment geconfronteerd worden met de noodzaak om onze *ipse*-identiteit af te schermen van de slimme omgeving.

Enerzijds is dat natuurlijk mogelijk door onze *idem*-identiteit af te schermen, dat wil zeggen door zo min mogelijk persoonsgegevens te 'lekken' of te verschaffen. Bijvoorbeeld door 'unplugged' te blijven of door privacy enhancing technologies (PETs) in te zetten die de beginselen van data minimalisering en doelbeperking implementeren. Anderzijds zullen we slimmere manieren moeten vinden om onze *ipse*-identiteit af te schermen als we de voordelen van slimme omgevingen willen behouden. Het gebruikelijke privacyparadigma van controle en autonomie impliceert dat zoveel mogelijk persoonsgegevens verborgen moeten blijven (dataminimalisering) en dat gegevens uitsluitend gebruikt mogen worden voor tevoren vastgestelde doelen (doelspecificiteit en doelbeperking). Beide strategieën gaan in tegen de onvoorspelbaarheid die eigen is aan slimme omgevingen: het is tevoren niet bekend welke correlaties tussen welke gegevens tot nieuwe interventies gaan leiden. Eigenlijk is functiekruip een voorwaarde voor de productiviteit van zo'n omgeving (Massiello and Whitten 2010); fundamentele beginselen van gegevensbescherming, zoals doelspecificatie en doelbeperking, staan dan ook op gespannen voet met Omgevingsintelligentie. Voor zover we de voordelen van slimme omgevingen willen genieten op een manier die privacybestendig is, moeten we erachter komen hoe de

omgeving ons waarschijnlijk anticipeert en op basis daarvan besluiten waar, wanneer en hoe we welke gegevens gaan achterhouden. Dat is precies wat wij in het 'gewone' intermenselijke verkeer ook doen. Dat vraagt naast PETs om transparency enhancing tools (TETs), die het mogelijk maken zicht te krijgen op de onzichtbare hand van de slimme omgeving.

Art. 12 (a) van de Richtlijn Gegevensbescherming kent Europese burgers het recht toe om 'mededeling' te verkrijgen 'van de logica die ten grondslag ligt aan de automatische verwerking van hem betreffende gegevens, in elk geval als het gaat om de geautomatiseerde besluiten als bedoeld in art. 15, lid 1' (D 95/46/EG). Precies in slimme omgevingen zou dit een voorwaarde kunnen zijn voor effectieve bescherming van de privacy. Als je niet weet wat de gevolgen zijn van het lekken of verstrekken van gegevens is toestemming of instemming een gevaarlijke fictie, omdat het de illusie van autonomie en controle in stand houdt. Als het recht op privacy toeziet op de vrijheid om de eigen identiteit zonder onredelijke beperkingen te ontwikkelen stelt de slimme omgeving ons voor bijzondere uitdagingen. Proactieve omgevingen oefenen in het kader van de gebruiksvriendelijkheid een subliminale invloed uit, die als zodanig onzichtbaar is. Daardoor wordt het bovendien een hachelijke zaak om vast te stellen welke beslissingen van de slimme infrastructuur moeten worden aangemerkt als een onredelijke beperking op die vrijheid. Dat kan immers pas worden vastgesteld als je weet waar zo'n beslissing op is gebaseerd en waar die uiteindelijk toe leidt.

Het probleem van art. 12 is dat het op dit moment technisch niet mogelijk is om het toegekende recht uit te oefenen en dat het juridisch moet worden afgewogen tegen het bedrijfsgeheim of de intellectuele rechten van het bedrijf dat de data-analyse doet verrichten (de data controller) (Van Dijk 2010). Wil dit transparantierecht effectieve bescherming bieden dan zal het juridisch scherper moeten worden geformuleerd en standaard (by default) in de slimme omgeving moeten worden ingebouwd. Daarmee komen we op een ander aspect van privacy en identiteit in slimme omgevingen, namelijk de constatering dat bescherming tegen de onwenselijke gevolgen van deze technologie niet effectief is als ze uitsluitend wordt gearticuleerd in de technologie van de drukpers. Het geschreven recht zal in een aantal gevallen moeten worden gecomplementeerd met recht dat – op initiatief van de democratische wetgeving – in de nieuwe ICT infrastructuur is ingeschreven. In het bijzonder wanneer het gaat om proactieve omgevingen zoals Ambient Intelligence, zal

het recht aanvulling moeten zoeken in wat wij in ander werk *Ambient Law* (Hildebrandt and Koops 2010) of *Legal Protection by Design* (Hildebrandt nog te verschijnen 2011) hebben genoemd. Het mag duidelijk zijn dat juridische bescherming *by design* vraagt om een her-denking en een ver-bouwing van de rechtsstaat op het niveau van de technische infrastructuur. Niet om op onzichtbare wijze de handhaving van rechtsregels technisch af te dwingen, hetgeen eerder een vorm van administratie of discipline zou zijn dan een vorm van recht. Wel om bewoners van slimme omgevingen inzicht te geven in de manier waarop ze worden 'gelezen', zodat ze hun handelen aan kunnen passen of zich tegen de 'lezing' van de omgeving kunnen verzetten. *Ambient Law* zou daarenboven kunnen inhouden dat het recht op privacy in een slimme omgeving wordt gearticuleerd in de technische mogelijkheid om delen van de omgeving 'uit te zetten'.

Literatuur

Aarts, E. and S. Marzano (eds.), *The new everyday. Views on ambient intelligence.* Rotterdam: 010, 2003

Agre, P.E. and M. Rotenberg (eds.), *Technology and privacy: The new landscape.* Cambridge, Massachusetts: MIT, 2001

Ariès, P. and G. Duby, *A history of private life*. Cambridge, Mass.: Belknap Press of Harvard University Press, 1987

Custers, B. *The power of knowledge. Ethical, legal, and technological aspects of data mining and group profiling in epidemiology*. Nijmegen: Wolf Legal Publishers, 2004

Dennett, D. Intentional systems theory. In *Oxford handbook of the philosophy or mind*, Oxford: Oxford University Press, 2009, pp. 339-50

Dwyer, C. The inference problem and pervasive computing. In *Proceedings of internet research 10.0*. Milwaukee, WI, 2009

London Economics, L. Study on the economic benefits of privacy-enhancing technologies (PETs) - final report to the European Commission DG Justice, Freedom and Security. London: London Economics, 2010

Eisenstein, E. (2nd edn.), *The printing revolution in early modern europe*. Cambridge New York: Cambridge University Press, 2005

Gigerenzer, G. *Gut feelings : The intelligence of the unconscious*. New York: Viking, 2007

Glastra Van Loon, J.F. *De eenheid van het handelen. Opstellen over recht en filosofie*. Amsterdam: Boom, 1980

Greenfield, A. *Everyware. The dawning age of ubiquitous computing*. Berkeley: New Riders, 2006

Gurses, S. and B. Berendt, The social web and privacy: Practices, reciprocity and conflict detection in social networks. In *Privacy-aware knowledge discovery: Novel applications and new techniques*. Florida, USA: Chapman and Hall/CRC Data Mining and Knowledge Discovery book series, 2010

Gutwirth, S. *Privacy and the information age, translated by raf casert*. Lanham Boulder New York Oxford: Rowman & Littlefield, 2002
Hand, D.J. *Information generation. How data rule our world*. Oxford: Oneworld, 2007
Hand, D.J., H. Mannila and P. Smyth, *Principles of data mining Adaptive computation and machine learning*. Cambridge, Mass.: MIT Press, 2001
Hildebrandt, M. Profiling and the identity of european citizens. In *Profiling: Implications for democracy and rule of law*. Brussels, 2005 available at: www.fidis.net.
Hildebrandt, M. A vision of ambient law. In *Regulating technologies*. Oxford: Hart, 2008a
Hildebrandt, M. Profiling and the identity of the european citizen. In *Profiling the european citizen. Cross-discplinary perspectives*. Dordrecht: Springer, 2008b
Hildebrandt, M. Privacy en identiteit in slimme omgevingen. Computerrecht 2010a, pp. 172-82.
Hildebrandt, M. Recht en markt: Met falen en opstaan. In L. Mommers, H. Franken, H.J. Van den Herik, F.A.M. Klaauw-Koops, G.J. Zwenne (red.) *Het binnenste buiten. Liber Amicorum ter gelegenheid van het emeritaat van prof. Dr. Aernout H.J. Schmidt, hoogleraar Recht en Informatica te Leiden*, Leiden: Meijers-Instituut, 2010b, pp. 275-89
Hildebrandt, M. Legal protection by design. *Legisprudence* (nog te verschijnen) 2011a
Hildebrandt, M. The meaning and mining of legal texts. In D.M. Berry (ed.), *Understanding digital humanities: The computational turn and new technology*. London: Palgrave Macmillan, (nog te verschijnen) 2011b.
Hildebrandt, M. and B.J. Koops, The challenges of ambient law and legal protection in the profiling era. *Modern Law Review* 73 2010, pp. 428-60.
Hornung, G. and C. Schnabel, Data protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law & Security Reports* 2009, pp. 84-88.
ITU The internet of things. Geneva: International Telecommunications Union 2005
Lessig, L. *Code and other laws of cyberspace*. New York: Basic Books, 1999
Lévy, P. *Les technologies de l'intelligence. L'avenir de la pensée à l'ère informatique*. Paris: La Découverte, 1990
Luhmann, N. *Social systems*. Stanford: Stanford University Press, 1995
Massiello, B. and A. Whitten, Engineering privacy in a age of information abundance. In *Intelligent information privacy management*, AAAI 2010, pp. 119-24
Merton, R.K. The self-fulfilling prophecy. *The Antioch Review* (8) 1948, pp. 193-210.
Nissenbaum, H. Towards an approach to privacy in public: The challenges of information technology. *Ethics and Behavior* (7) 1997, pp. 207-19.
Office of Fair Trading (UK), Online targeting of advertising and prices, 2010 http://www.oft.gov.uk/shared_oft/business_leaflets/659703/OFT1231.pdf
Ong, W. *Orality and literacy: The technologizing of the word*. London/New York: Methuen, 1982
Prins, C. When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter? SCRIPT-ed (3) 2006, pp. 270-303.
Ricoeur, P. 1992. *Oneself as another*. Chicago: The University of Chicago Press, 1992
Ricœur, P. (translation J.B. Thompson), *Hermeneutics and the human sciences: Essays on language, action, and interpretation*. Cambridge: Cambridge University Press, 1981
Rouvroy, A. and Y. Poullet, The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy. In

S. Gutwirth, P. De Hert, Y. Poullet (eds.), *Reinventing data protection*. Dordrecht: Springer, 2009
Rusli, E.M. Yahoo is said to move toward personalized content. New York Times, 6th February 2011
Schwartz, P.M. Beyond lessig's *code* for internet privacy: Cyberspace filters, privacy-control and fair information practices. Wisconsin Law Review 2000, pp. 743-88.
Sculley, D. and B.M. Pasanek, Meaning and mining: The impact of implicit assumptions in data mining for the humanities. *Literary and Linguistic Computing* (23), 2008, pp. 409-24.
Stalder, F. The failure of privacy enhancing technologies (pets) and the voiding of privacy. *Sociological Research Online* (7), 2002, <http://www.socresonline.org.uk/7/2/stalder.html>.
Sunstein, C. *Republic.Com*. Princeton and Oxford: Princeton University Press, 2001
Van Den Berg, B. *The situated self: Identity in a world of ambient intelligence*. Nijmegen: Wolf Legal Publishers, 2010
Van Dijk, N. Auteursrecht in profielen. *Computerrecht* (2), 2010, pp. 53-61.
Vedder, A. Kdd: The challenge to individualism. *Ethics and Information Technology* (1) 1999, pp. 275-81.
Warren, S. and L.D. Brandeis, The right to privacy. *Harvard Law Review*, 1980, p. 193.
Westin, A. *Privacy and freedom*. New York: Atheneum, 1967
Wolpert, D.H. and W.G. Macready, No free lunch theorems for optimization. *IEEE Transactions on Evolutionary Computation* (1), 1997

---

[i] Deze tekst is een bewerkte versie van (Hildebrandt 2010a), zoals verschenen in de special issue van *Computerrecht* over Ambient Intelligence in 2010. Voor verdere uitwerking van de juridisch-technische implicaties zie aldaar.

[ii] Zie ook: art. 29 WP, Opinion 2/2010 on online behavioural advertising, 00909/10/EN, WP 171.

[iii] Zie http://www.pcmag.com/article2/0,2817,2376030,00.asp (geraadpleegd op 28 februari 2011).

[iv] Zie ook Ong (1982) en Eisenstein (2005).

[v] Voor een heldere uiteenzetting van de pros en cons van eigendomsrechten op persoonsgegevens zie Prins (2006). Ook Hildebrandt (2010b).

[vi] Meer uitgebreid: Hildebrandt (2008b).

[vii] Deze dubbele anticipatie staat in de systeemtheorie bekend als 'double contingency', zie Luhmann (1995). De dubbele anticipatie leidt er ook toe dat wij ten aanzien van anderen een zogenaamde 'intentional stance' innemen. Dat wil zeggen dat wij ervan uitgaan dat anderen kenbare redenen hebben voor hun handelen die ik kan achterhalen, waardoor ik mij anders tot hen zal verhouden dan wanneer ik geen idee heb waarom zij zich gedragen zoals ze zich gedragen, zie Dennett (2009).