2010

Privacy en identiteit in slimme omgevingen

Mireille Hildebrandt

Privacy en identiteit in slimme omgevingen

Mireille Hildebrandt[·]

Samenvatting

Omgevingen zijn slim omdat ze anticiperen op ons toekomstig gedrag. Op basis van een voortdurende opslag van data en de permanente analyse daarvan ontwikkelt de slimme omgeving kennis over onze voorkeuren, gewoonten, leefstijl, gezondheid, stemmingen en voornemens. Die kennis is statistisch van aard en de mate waarin toekomstig gedrag daadwerkelijk wordt voorzien hangt af van de juistheid, de relevantie en de compleetheid van de data. Tegelijk moeten we constateren dat wanneer de bewoner van een slimme omgeving op grond van die afgeleide kennis op een bepaalde manier wordt behandeld, de kans bestaat dat zij zich op den duur gaat gedragen naar wat van haar wordt verwacht. In de sociologie heet dat 'if men define a situation as real, it is real in its consequences';[1] hier kunnen we dat inzicht uitbreiden tot 'if machines define a situation as real, it is real in its consequences'.

In deze bijdrage zal ik mij richten op de vraag in hoeverre het feit dat omgevingen kennis over mij ontwikkelen en die kennis proactief toepassen een aantasting kan zijn van mijn privacy. Ik noem dit het 'inferentieprobleem' omdat meestal onzichtbaar is welke afgeleide kennis op mij wordt toegepast. Om te onderzoeken hoe dit zich verhoudt tot de privacy zal ik eerst ingaan op wat hier bedoeld wordt met slimme omgevingen en vervolgens de traditionele opvattingen van privacy bespreken. Ik zal daarna bepleiten dat privacy in het licht van slimme omgevingen het best kan worden opgevat als de bescherming van de vrijheid om onze identiteit zonder onredelijke beperkingen te kunnen ontwikkelen. Na een analyse van het Europeesrechtelijke kader van privacy en gegevensbescherming zal ik de lacunes en tekortkomingen hiervan analyseren met betrekking tot genoemd 'inferentieprobleem' en oplossingsrichtingen duiden voor een legitieme privacy verwachting die is gebaseerd op een effectief recht op adequate feedback, zoals bijvoorbeeld toegekend in art. 12 van de Richtlijn Gegevensbescherming. Tenslotte bepreek ik waarom dat transparantierecht, wil het een 'effective remedy' zijn, articulatie behoeft in de ICT infrastructuur van slimme omgevingen.

1 De slimme omgeving: subliminale beïnvloeding

Voordat we op zoek gaan naar een adequaat privacy begrip in het tijdperk van slimme omgevingen, gaan we eerst wat dieper in op wat we hier onder slimme omgevingen moeten verstaan. Ik ga er daarbij vanuit dat de lezer kennis heeft genomen van de heldere bespreking van de 'basics' van Ambient Intelligence door Bibi van den Berg,

---

[·] De auteur is universitair hoofddocent Rechtstheorie aan de Erasmus School of Law, Erasmus Universiteit Rotterdam en senior onderzoeker bij het Centre for Law Science Technology and Society aan de Vrije Universiteit Brussel. Van 2004-2009 coördineerde zij een Europees onderzoeksproject over profiling (als onderdeel van het FIDIS project, zie www.fidis.net). In 2008 verscheen *Profiling the European Citizen*, dat zij samen met Serge Gutwirth redigeerde. Zie verder http://works.bepress.com/mireille_hildebrandt/.

[1] W.I. Thomas en D. S. Thomas, *The Child in America*. New York: Knopf 1928.

eerder in dit nummer. Ambient Intelligence betekent in Nederlandse vertaling '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 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.[2] 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.[3] 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, bestellingen te doen om voorraden op peil te houden. Allerlei preventieve gezondheidsbevorderende maatregelingen kunnen in worden geprogrammeerd, waarbij vrijwel permanente meting van bloedwaarden, hartritme, temperatuur en transpiratie op den duur 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 is op complexe software programma's die op basis van computer algoritmes 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.[4] 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.[5] 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'. 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

---

[2] E. Aarts, S. Marzano (eds.), *The new everyday. Views on ambient intelligence*, Rotterdam: 010 2003; Information Society Technology Advisory Group (ISTAG), *Scenarios for ambient intelligence in 2010*, Brussels 2001, available at: http://www.cordis.lu/ist/istag-reports.htm.

[3] D.J. Hand et al., *Principles of data mining,* Cambridge, Mass.: MIT Press 2001.

[4] D.J. Hand, *Information generation: how data rule our world*, Oxford: Oneworld 2007.

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

'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.[6] 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'?

In deze bijdrage zal ik eerst ingaan op traditionele begripsvorming rond privacy, namelijk privacy als sociale terugtrekking en privacy als informationele zelfbeschikking, en vervolgens bespreken dat en hoe privacy in het tijdperk van slimme omgevingen beter kan worden opgevat als bescherming van de vorming van persoonlijke identiteit. Tot slot ga ik in op de nood aan juridische en technische instrumenten om door data-analyse gestuurde omgevingen doorzichtiger te maken.

2 Traditionele opvattingen van privacy

2.1 Mentale en fysieke terugtrekking

In een overtuigend betoog stelt Stalder dat de traditionele Westerse opvatting van privacy in zekere zin een bijproduct is van de opkomst van de drukpers.[7] 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 Ricoeur en Lévy 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.[8] Het schrift en de drukpers vormen aldus de kiem van een pluriforme samenleving

---

[6] Een belangrijk onderscheid waar ik in deze bijdrage niet nader op in kan gaan is dat tussen distributieve en non-distributieve profielen, zie daarover A. Vedder, KDD: The challenge to individualism, *Ethics and Information Technology* 1999-1, p. 275-281.

[7] F. Stalder, The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy, (7) *Sociological Research Online* 2002-2: beschikbaar via http://www.socresonline.org.uk/7/2/stalder.html. Cf. W. Ong, *Orality and Literacy: The Technologizing of the Word,* London New York: Methuen 1982. Zie ook E. Eisenstein, *The Printing Revolution in Early Modern Europe*, Cambridge New York: Cambridge University Press 2005.

[8] P. Ricœur, en J. B. Thompson, *Hermeneutics and the human sciences : essays on language, action, and interpretation* Cambridge New York Paris: Cambridge University Press 1981. P. Lévy, *Les technologies de l'intelligence. L'avenir de la pensée à l'ère informatique,* Paris: La Découverte 1990.

waarin de betekenis van bijvoorbeeld een wettekst niet makkelijk gemonopoliseerd kan worden. 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).[9]

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. Daarom 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 privacy begrip daar wel op georiënteerd, bijvoorbeeld waar art. 8 EVRM het grondrecht omschrijft als een recht op niet-inmenging in het privé-leven, 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 doorheen private, sociale en publieke ruimtes: we werken 's avonds laat thuis op de huis pc, versturen privé mails 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. Anderzijds is onze behoefte aan privacy juist in publieke contexten groot:[10] 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 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 toenemende profileringstechnologie.[11]

2.2 Het soevereine zelf: controle en autonomie

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 ziet 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 left 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.[12] Het ging daarbij om een onrechtmatige daadsactie; pas

---

[9] P. Ariès and G. Duby (eds.), *A History of Private Life. V Riddles of Identity in Modern Times*, Boston: Harvard University Press 1991.

[10] H. Nissenbaum, Towards an Approach to Privacy in Public: The Challenges of Information Technology, (7) *Ethics and Behavior* 1997-3, p. 207-219.

[11] L. Lessig, *Code and other laws of cyberspace*, New York: Basic Books 1999, p. 155.

[12] S. D. Warren, L. D. Brandeis, The Right to Privacy, (4) *Harvard Law Review* 1890-5, p. 193-220.

veel later wordt datzelfde recht met succes ingeroepen tegen de overheid in het kader van constitutionele bescherming, waartoe een grondrecht op bescherming van de privacy in de Constitutie werd ingelezen.[13]

In het verlengde van deze benadering stelt Westin in 1967 dat privacy het recht is om zelf te bepalen wie toegang heeft tot welke informatie over zichzelf.[14] 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.[15] Met name Duitsland gaat voorop in het eisen van een vergaande informationele autonomie, die wordt afgeleid uit het grondrecht op menselijke waardigheid.

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 autonomie legt grote nadruk op zelfbeschikking en keuzevrijheid en maakt van toestemming, instemming of overeenstemming ('consent') een van de belangrijkste dogma's van het privacy debat.[16] 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.[17] 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.[18] 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

---

[13] Brandeis' dissenting opinion in *Olmstead v US*, 277 US 438, 478 (1928); het Supreme Court 'ging om' in 1967 in *Katz v US*, 389 US 347, 350 (1967).

[14] A. Westin, *Privacy and Freedom*, New York: Atheneum 1967.

[15] Cf. A. Rouvroy 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, p. 45-76. P.M. Schwartz, Internet Privacy and the State, (32) *Connecticut Law Review* 2000, p. 815-859. G. Hornung and Ch. Schnabel, Data protection in Germany I: The Population census decision and the right to informational self-determination, (25) *Computer Law & Security Report* 2009-1, p. 84-88.

[16] Waarbij ook gewezen kan worden op de zogenaamde 'decisional privacy' in de VS, waar de Supreme Court bijvoorbeeld het recht op abortus baseerde in Roe v. Wade, 410 U.S. 113 (1973).

[17] M. Hildebrandt, Recht en markt: met falen en opstaan, in: *Het binnenste buiten. Liber amicorum ter gelegenheid van het emeritaat van prof. dr. Aernaout H.J. Schmidt, hoogleer Recht en Informatica te Leiden*, L. Mommers et al. (red.), Leiden: Meijers-Instituut 2010, p. 275-289.

[18] Voor een heldere uiteenzetting van de pros en cons van eigendomsrechten op persoonsgegevens zie C. Prins, When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter? (3) *SCRIPT-ed* 2006-4, p. 270-303.

eigendomsrecht is daarvoor niet nodig. Bovendien schept het de illusie van een in zichzelf besloten individu die 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.[19] 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?[20]

3 Privacy en identiteit[21]

3.1 Tweeledige vrijheid

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 best de werkdefinitie van Agre & Rotenberg:[22]

---

[19] Waarbij met name de welvaartstaat een bijzonder belang heeft om zijn burgers te kunnen adresseren in verband met de aanspraken die deze hebben op zaken als stemrecht, sociale voorzieningen, subsidies en gezondheidszorg. Zie ook J.C. Scott, *Seeing Like a State. How Certain Schemes to Improve the Human Condition Have Failed*, New Haven London: Yale University Press 1998, en J. Torpey, *The Invention of the Passport. Surveillance, Citizenship and the State,* Cambridge: Cambridge University Press 2000.

[20] Over dit type relationele gegevens en de manier waarop conflicten rond hun gebruik opgelost kunnen worden zie S. Gurses en 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*, E. Ferrari en F. Bonchi (eds.), Florida: Chapman and Hall (in druk).

[21] Zie meer uitgebreid: M. Hildebrandt, Profiling and the identity of the European citizen, in: M. Hildebrandt and S. Gutwirth (eds.), *Profiling the European citizen. Cross-discplinary perspectives*, Dordrecht: Springer 2008, p. 303-326.

> 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 beinvloeding voor de hand, die uit kan monden in gerichte manipulatie.[23] Daarmee lijkt een onredelijke inperking van de eigen identiteitsvorming in zicht te komen.

3.2 Identiteit: aanspreekpunt en blinde vlek

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 zelf-bewustzijn 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).[24] Identiteit in deze zin lijkt een blinde vlek, een punt dat wegspringt zodra we het in beeld willen brengen. De Franse filosoof Ricoeur 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. In dat verband is identiteit het aanspreekpunt voor de toekenning van rechten en plichten. Ricoeur zou in dat verband spreken van een *idem*-identiteit. 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 kunnen we zeggen dat persoonlijke identiteit onderbepaald is (dynamisch,

---

[22] P.E. Agre en M. Rotenberg (eds.), *Technology and Privacy: The New Landscape,* Cambridge, Massachusetts: MIT 2001, p. 7 [mijn vertaling].

[23] Een voorbode daarvan zien we in 'behavioural advertising'. Zie daarover de klacht ingediend bij de Federal Trade Commission in de VS door o.a. het Center for Digital Democracy: http://democraticmedia.org/files/u1/20100407-FTCfiling.pdf.

[24] Cf. P. Ricoeur, *Soi-même comme un autre*, Paris: Seuil 1990. Ricoeur onderscheidt tussen 'zichzelf' (*ipse*) en 'hetzelfde' (*idem*) als onderscheiden maar verweven aspecten van menselijke identiteit.

meervoudig, altijd in de maak).[25] 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.[26] Tegelijk biedt het recht een instrumentarium om in specifieke gevallen tot aansprakelijkheid te kunnen besluiten en schadevergoeding of straf op te leggen.

3.3 Identiteit en dubbele anticipatie: het 'inferentieprobleem'

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, moet weten hoe anderen mijn handelen gaan verstaan.[27] Die dubbele anticipatie is kenmerkend voor de omgang tussen mensen: om te weten wie ik ben moet ik weten hoe anderen mij zien. 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. 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

---

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

[26] Cf. J. Habermas, *Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats*, Frankfurt am Main: Suhrkamp 1994.

[27] Deze dubbele anticipatie staat in de systeemtheorie bekend als 'double contingency', zie N. Luhmann, *Social Systems,* Stanford: Stanford University Press 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 D. Dennett, Intentional Systems Theory, in: *Oxford Handbook of the Philosophy or Mind*, Oxford University Press 2009**,** p. 339-350.

gedachteloos; ook de dubbele anticipatie die kenmerkend 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.[28] Voor zover het echter onduidelijk is hoe anderen ons 'verstaan' kunnen we daar niet op inspelen en gedragen we ons in een soort luchtledig, in dit geval wellicht bijgestuurd door de subliminale interventies van de slimme omgeving. Dit is inmiddels aangeduid als het 'inferentieprobleem'.[29] 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.

4 Privacy en gegevensbescherming in slimme omgevingen

4.1 Het juridisch kader vanuit Europees perspectief

Privacy en gegevensbescherming vallen niet samen. Enerzijds is er een doel-middel verhouding tussen beide, voor zover gegevensbescherming een middel is om privacy te beschermen. Anderzijds omvat het recht op privacy zowel meer als minder dan gegevensbescherming. Privacy omvat naast een recht op gegevensbescherming bijvoorbeeld ook het meer algemene recht op bescherming van de persoonlijke levenssfeer, sinds 1950 gecodificeerd in art. 8 van het Europese Verdrag van de Rechten van de Mens (EVRM). Dit omvat bescherming van het privé- en familieleven, het huisrecht en het recht op vertrouwelijkheid van privé correspondentie. Het klassieke privacy recht lijkt daarmee vooral gericht op sociale terugtrekking binnen een duidelijk als zodanig herkenbaar privé domein. Gegevensbescherming bevat een meer specifiek juridisch regime voor de omgang met persoonsgegevens, waarmee niet alleen informationele zelfbeschikking wordt beoogd maar tegelijk ook het bevorderen van de vrije uitwisseling van informatie. Sinds 2002 zijn beide rechten als afzonderlijke fundamentele rechten opgenomen in het Handvest van de grondrechten van de Europese Unie (art. 7 en 8).

Het recht op gegevensbescherming is sinds 1995 gecodificeerd in de Richtlijn Gegevensbescherming (D 95/47/EC) en omvat meer precies een nadere uitwerking van wat sinds de jaren '70 bekend staat als de 'fair information principles'. Deze beginselen kunnen worden samengevat als: data minimalisering (geen onnodige verzameling en opslag van persoonsgegevens), data kwaliteit (gegevens moeten correct, complete en up-to-date zijn), doel-specificiteit (het doel waarvoor gegevens worden verwerkt moet zijn gespecificeerd en zij mogen uitsluitend voor dat doel worden gebruikt), doelbeperking (het ontsluiten van gegevens voor andere doelen is

---

[28] R.R. Hassin et al., *The new unconscious,* New York: Oxford University Press 2005.

[29] C. Dwyer, The inference problem and pervasive computing, in *Proceedings of Internet Research 10.0*, Milwaukee, WI, October 7-11 October 2009, beschikbaar via http://csis.pace.edu/~dwyer/research/DwyerAoIR2009v2.pdf.

verboden tenzij met toestemming van de persoon op wie zij betrekking hebben, dan wel op grond van de wet), het transparantiebeginsel (personen moeten op de hoogte zijn van de verwerking van hun persoonsgegevens, alsmede van het doel en van de identiteit van degene in wiens opdracht zij worden verwerkt), het individuele participatie beginsel (het recht om de eigen persoonsgegevens te verwijderen, te verbeteren of aan te passen) en tenslotte de verantwoordelijkheid (degene die opdracht geeft tot gegevensverwerking is aansprakelijk voor het naleven van de verplichtingen inzake de andere beginselen). Naast deze richtlijn zijn ook nog van belang de onlangs aangepaste e-Privacy richtlijn (D 2002/58/EC), waarin bijvoorbeeld een opt-in verplichting is opgenomen ten aanzien van het plaatsen van cookies op computers van eindgebruikers om het 'tracken and tracen' van surf-gedrag te legitimeren, en de Richtlijn Data Retentie (D 2006/24/EC), die een verplichting oplegt aan de aanbieders van openbare elektronische communicatie*diensten* en -*netwerken* om verkeersgegevens voor een bepaalde duur vast te leggen met het oog op mogelijke opsporingsbelangen. Hoewel de Richtlijn Gegevensbescherming toepasselijkheid in het kader van de strafvordering in de publieke veiligheid uitsluit, is inmiddels het Kaderbesluit 2008/977/JHA in werking getreden waarin een vergelijkbaar regiem van toepassing wordt verklaard op de gegevensverwerking in de sfeer van politionele en justitiële samenwerking in strafzaken. Daarbij zijn enerzijds een aantal strafrechtelijke beginselen toegevoegd (met name legaliteit, proportionaliteit en subsidiariteit) en anderzijds zijn voorbehouden gemaakt ten aanzien van bijvoorbeeld de mededelingsplichten.

4.2 Tekorten van het juridisch kader bij de realisering van Ambient Intelligence[30]

Het probleem met de huidige regelgeving is in de eerste plaats dat handhaving een hachelijke zo niet onmogelijke zaak wordt als we overgaan naar 'ubiquitous, subliminal, real time adaptive computing'. Hoe zou technisch achterhaald kunnen worden of data controllers de rechten van de gebruikers respecteren en hoe kan effectief worden gecontroleerd of ze zich aan hun verplichtingen houden? Het is een illusie dat de duizelingwekkende hoeveelheid gegevens die onder voortduring moeten worden verwerkt om de menselijke gebruiker een stap voor te blijven gecontroleerd gaan worden; noch de individuele gebruiker noch de autoriteit gegevensbescherming kan narekenen welke gegevens hoe door wie worden opgeslagen, doorverkocht, samengevoegd en doorzocht. Het meest pregnante probleem is het hierboven gesignalieerde 'inferentieprobleem', dat onstaat doordat uit die gegevens profielen worden afgeleid waarmee gebruikers worden gecategoriseerd, zonder dat zij zicht hebben op die categorisering, laat staan op potentiële consequenties. Technisch is het op dit moment niet mogelijk om gebruikers via intuïtieve interfaces real-time feedback te geven over hoe de slimme omgeving hun gedragingen interpreteert.

---

[30] Zie W. Schreurs, M. Hildebrandt, E. Kindt and M. Vanfleteren, Cogitas ergo sum: The role of data protection law and non-discrimination law in group profiling in the private sphere, in *Profiling the european citizen: Cross-disciplinary perspectives*, Dordrecht: Springer (2008); P. De Hert, S. Gutwirth, A. Moscribroda, D. Wright and G. Gonzalez Fuster, Legal safeguards for privacy and data protection in ambient intelligence, (13) *Personal and Ubiquitous Computing* 2009, p. 435-44; A. Rouvroy, Privacy, data protection, and the unprecedented challenges of ambient intelligence, (2) *Studies in Ethics, Law, and Technology* 2008-1: Article 3.

Het tweede probleem is dat privacy vooralsnog wordt begrepen vanuit de dichotomie tussen privé en publiek. De traditionele opvatting is dat privacy met name bescherming biedt voor wat zich afspeelt in de privé-sfeer en dat burgers en consumenten geen privacy verwachten in de publieke ruimte. Een dergelijke dichotomie is vanuit feministische hoek al eerder aan de kaak gesteld vanwege de bescherming die het leek te bieden aan wandaden in de privé-sfeer, maar inmiddels is deze dichotomie om heel andere redenen onhoudbaar. Privé en publiek lopen enerzijds volledig en voortdurend door elkaar, doordat mensen een veelheid van private en publieke rollen spelen vanuit eenzelfde locatie, bijvoorbeeld wanneer zij van huis uit hun werkmail bijhouden of op kantoor privé-zaken regelen via internet. De toegenomen mobiele bereikbaarheid verstrekt die overlap. Veel contexten, zoals gezondheid, sociale zekerheid, sportevenementen, hebben bovendien een hybride karakter dat niet evident binnen het private dan wel publieke domein past. Nissenbaum beargumenteert dan ook dat we voor een goed begrip van privacy afmoeten van deze dichotomie en de domeinspecificiteit van een veelheid van contexten in kaart moeten brengen ten einde op een legitieme manier om te kunnen gaan met de verwachtingen van burgers, consumenten, werknemers, patiënten en reizigers ten aanzien van hun privacy.[31]

Het derde probleem betreft het feit dat de centrale uitgangspunten van de huidige Richtlijn Gegevensbescherming zich moeizaam verhouden tot de centrale uitgangspunten van Ambient Intelligence. In feite lijkt het regiem van de Richtlijn in rechtstreekse tegenspraak met alles waar slimme omgevingen voor staan. Het eerste problematische uitgangspunt is dat het cruciale object van bescherming van de Richtlijn het persoonsgegeven is, dat wordt gedefinieerd als een gegeven waarmee een persoon kan worden geïdentificeerd. Ambient Intelligence drijft op de mogelijkheid personen onder voortduring te herkennen ten einde zich aan hun – door middel van profileringstechnieken, data mining en machine learning berekende – voorkeuren aan te passen. Dat herkennen hoeft geen betrekking te hebben op naam en adres, zolang iemand maar als dezelfde persoon wordt terug-herkend (bijvoorbeeld aan de hand van haar biometrisch doorgerekende typegedrag). Daadwerkelijk slimme omgevingen kunnen van ieder triviaal gegeven op enig toekomstig moment een persoonsgegeven maken, hoewel niet voorzien kan worden welke gegevens te zijner tijd met welke profielen zullen 'matchen'. Dit verwijst weer naar het 'inferentieprobleem' en leidt ertoe dat het onderscheid tussen persoons- en andere gegevens dermate casuïstisch dat de rechtszekerheid – zowel voor het data subject als voor de data controller – ver is te zoeken.[32] De focus op persoonsgegevens leidt er bovendien toe dat veel tijd en moeite wordt gestoken in het anonimiseren van gegevens, met de – onjuiste - gedachte dat daarmee het privacy probleem zou worden opgelost. Zowel het feit dat de-anonymisering in een Ambient Intelligent omgeving technisch gezien steeds eenvoudiger wordt, als het feit dat de voorgenomen subliminale afstemming gemakkelijk plaats kan vinden zonder dat daadwerkelijke

---

[31] H.F. Nissenbaum, *Privacy in context : Technology, policy, and the integrity of social life*, Stanford: Stanford Law Books 2010. Over de 'reasonable expectation of privacy' in de VS zie A. Gruber, Garbage pails and puppy dog tails: Is that what *Katz* is made of? (41) *University of California David Law Review* 2008, p. 781-838, en in de EU De Hert and Gutwirth et al. supra noot 30, 438-439.

[32] Zie bijvoorbeeld de opinie van de art. 29 Werkgroep inzake het begrip 'persoonsgegeven' (Opinie 4/2007, WP136).

identificatie plaatsvindt, maken van anonymisering een schijnoplossing.[33] Dat knelt temeer nu het directe gevolg van anonymisering is dat de bescherming van de Richtlijn vervalt, nu geen sprake meer is van persoonsgegevens.
Het tweede problematische uitgangspunt is dat informationele zelfbeschikking de legitimering van de verwerking van persoonsgegevens zoekt in 'consent': toestemming of instemming. Dat gaat rechtstreeks in tegen het centrale paradigma van Ambient Intelligence, dat immers beoogt te voldoen aan de wensen van gebruikers zonder ze lastig te vallen met vragen over hun voorkeuren. Die voorkeuren worden afgeleid uit de manier waarop gebruikers zich gedragen en de suggestie is dat slimme omgevingen beter 'weten' welke voorkeuren zij hebben dan zij zelf kunnen bedenken. Het zou in dat verband de mijl op zeven zijn om de gebruiker steeds opnieuw te vragen of hij instemt met een bepaalde categorisering. Daarmee zou de 'gebruikerservaring' zoals dat in de betreffende tak van sport heet weer worden teruggebracht tot bewuste deliberatie in plaats van onbewuste aanpassing.[34]
Het derde centrale uitgangspunt dat onoverkomelijke problemen oproept is het beginsel dat het doel waarvoor gegevens worden verwerkt tevoren bekend moet zijn en dat gebruik voor een ander doel niet is toegestaan zonder de gebruiker om toestemming te vragen. De veronderstelling van de Richtlijn dat op het moment van het verzamelen van gegevens bekend is welk gebruik mogelijk in het verschiet ligt, lijkt bovendien nogal misplaatst in het kader van Ambient Intelligence. De gedachte achter slimme omgevingen en hun voorlopers is eerder dat steeds nieuwe verbanden zullen worden gevonden tussen verschillende typen gegevens, die aanleiding kunnen zijn tot nieuwe vormen van dienstverlening. Hier speelt wederom het 'inferentieprobleem'. Bij één van de voorlopers van slimme omgevingen, 'behavioural advertising', blijkt hoe dat in de praktijk werkt. Webstatistieken die het online gedrag van consumenten tot in de fijnste details weergeven maken het mogelijk voor adverteerders om hun reclame af te stemmen op de individuele voorkeuren van de gebruiker. Dat levert de betreffende website voldoende inkomen op om zijn diensten gratis aan te bieden: gratis 'content' als 'value-added service', zo genoemd omdat deze diensten voortkomen uit de inzet van gegevens die in een ander kader zijn 'gelekt' (met name websurfgedrag). In de aangepaste e-Privacyrichtlijn wordt daarop ingespeeld door te eisen dat consumenten vooraf instemmen met het plaatsen van 'cookies' (kleine databestanden) op hun computer, teneinde het 'gluren' naar hun websurfgedrag mogelijk te maken. De art. 29 Werkgroep heeft inmiddels al aangegeven dat het voortdurend vragen om een dergelijke opt-in natuurlijk ondoenlijk is en geadviseerd dat consumenten de mogelijkheid wordt geboden om in één keer toestemming geven voor een reeks van dergelijke inkijkmomenten.[35] Zo'n toestemming heeft echter weinig waarde als de gebruiker geen flauwe notie heeft waar het delen van haar gegevens uiteindelijk toe kan leiden. Daarmee is eigenlijk al duidelijk dat de centrale rol van toestemming, alsmede die van de doellimitering voor de gebruikers van slimme infrastructuren weinig substantie heeft; wie de geneugten

---

[33] Over deanonymisering zie P. Ohm, Broken promises of privacy: Responding to the surprising failure of anonymization, (57) UCLA Law Review 2010, p. 1701-77.

[34] M. Kuniavsky, *Observing the user experience a practitioner's guide to user research*, San Francisco: Morgan Kaufmann Publishers 2003.

[35] Opinie 2/2010 (WP171) inzake 'behavioural advertising' van 22 juni 2010. Daarbij formuleert de Werkgroep een aantal cruciale voorwaarden: (i) een tijdslimitering van de toestemming, (ii) de mogelijkheid de toestemming in te trekken en (iii) visuele instrumenten die tonen wanneer sprake is van het bespieden van websurfgedrag.

van proactieve omgevingen wil smaken zal geen keus hebben dan ruim bemeten toestemming te geven voor het aflezen en interpreteren van haar data.

4.3 Oplossingsrichtingen: de legitieme privacy-verwachting en art. 12 Richtlijn Gegevensbescherming

Zowel in de VS als in Europa lijkt de rechtspraak een uitweg te zoeken door aan te haken bij wat de 'redelijke verwachting van privacy' wordt genoemd. Het Amerikaanse Hooggerechtshof hanteert hierbij een dubbele test: (1) er moet sprake zijn van een daadwerkelijke verwachting (subjectieve test) en (2) deze verwachting moet maatschappelijk gezien redelijk zijn (objectieve test).[36] Bij de 'landmark case' uit 1967, Katz v. US, stelde Justice Harlan in zijn 'concurring opinion' dat 'an enclosed telephone booth is an area where, like a home, a person has a constitutionally protected reasonable expectation of privacy'. In California v. Greenwood (1988) werd beslist dat een politioneel onderzoek in buiten gezet vuilnis geen inbreuk is op de privacy, onder meer omdat wie informatie deelt met een derde geen legitieme privacy-verwachting meer kan hebben. In Kyllo v. US (2001) meent het Amerikaanse Hooggerechtshof dat het gebruik van een warmtebeeldkijker om de woning van een verdachte te scannen wel een privacy schending oplevert. Een probleem bij deze jurisprudentie is dat ze lijkt terug te grijpen op de dichotomie privaat-publiek, door steeds wanneer informatie is gedeeld met een derde partij te veronderstellen dat de informatie daarmee publiek is en dus niet meer beschermd wordt. Probleem met deze benadering is dat wanneer technische ontwikkelingen ertoe leiden dat gegevens gemakkelijker achterhaald kunnen worden, daarmee de subjectieve privacy-verwachting kan verdwijnen. Wanneer de tweede test pas aan de orde komt nadat een subjectieve verwachting is vastgesteld lijkt deze doctrine weinig of geen bescherming te bieden. Het Europese Hof voor de Rechten van de Mens (EHRM) heeft inmiddels ook de notie van een 'redelijke privacy-verwachting' geïntroduceerd.[37] Daarbij lijkt het Hof voorbij de traditionele privaat-publiek dichotomie te gaan door privacy bijvoorbeeld ook in werk-gerelateerde situaties te beschermen. Zo stelde het Hof in Copland v. the UK dat het monitoren van persoonlijke emails, telefoontjes en internetgebruik van werknemers een schending was van de redelijke verwachting van privacy. Die schending werd volgens het Hof overigens mede veroorzaakt doordat de betreffende werknemer niet op de hoogte was van deze vorm van toezicht. Zolang de redelijkheid van een subjectieve privacy-verwachting afhangt van de vraag of die maatschappelijk is aanvaard, lijkt het begrip 'redelijke verwachting van privacy' geen enkele bescherming te bieden tegen de oprukkende transparantie van individuele burgers. Die technologisch bemiddelde transparantie kan immers gemakkelijk leiden tot een lage privacy-verwachting. Beter is dan ook om te spreken van een 'legitieme privacy-verwachting' die een helder normatief perspectief veronderstelt op de waarde van privacy als onmisbaar element van een constitutionele democratie.

---

[36] 'Landmark cases' zijn: Katz v. U.S., 389 U.S. 347 (1967), California v. Greenwood, 486 U.S. 35 (1988), Kyllo v. U.S., 533 U.S. 27 (2001). In alle gevallen gaat het om inbreuken op het Vierde Amendement van de Amerikaanse Grondwet, waarin de huiszoeking is geregeld.

[37] EHRM, Niemitz v. Germany (23.11.1992), EHRM Halford v. the UK (27.03.1997), EHRM Copland v. the UK (3.4.2007).

Om te bepalen welke privacy-verwachtingen rechtens beschermd horen te worden als legitieme anticipaties moeten rechter en wetgever met name rekening gaan houden met wat hierboven is aangeduid als het 'inferentieprobleem'. Als gezegd hoef ik tegenover een stoel, een auto of een zwembad 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 (delen 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.[38] 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 privacy paradigma van controle en autonomie impliceert dat zoveel mogelijk persoonsgegevens verborgen moeten blijven en dat gegevens uitsluitend gebruikt mogen worden voor tevoren vastgestelde doelen. Die beide strategieën in tegen de onvoorspelbaarheid van slimme omgevingen: het is nu juist van te voren niet bekend welke correlaties tussen welke gegevens tot nieuwe oplossingen gaan leiden. Ten einde dit 'inferentieprobleem' aan te vatten is het interessanter om te ontdekken hoe de omgeving mij waarschijnlijk anticipeert en op basis daarvan te besluiten waar, wanneer en hoe ik welke gegevens ga minimaliseren. 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.[39]

Een legitieme privacy-verwachting vraagt in het licht van het 'inferentieprobleem' in de eerste plaats om *adequate feedback van hoe de omgeving ons interpreteert*. Een pertinent juridisch instrument daartoe vinden we in art. 12 (a) van de Richtlijn Gegevensbescherming die Europese burgers het recht toekent 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

---

[38] K.J. Dolinar, J. Porekar, et al., Design Patterns for a Systemic Privacy Protection, *IARIA International Journal of Advances in Security* (2) 2009 2/3, p. 267-287. Zie de aanbevelingen van de Europese Commissie inzake het gebruik van PETs COM/2007/228 en Economics rapport inzake PETs, en van de Art. 29 Werkgroep, *The Future of Privacy* (WP168), p. 27 en het in opdracht van de Europese Commissie geschreven rapport van London Economics, *Study on the economic benefits of privacy enhancing technologies* (PETs), July 2010.

[39] M. Hildebrandt (red.), *Behavioural Biometric Profiling and Transparency Enhancing Tools*, rapport D7.12 Future of Identity in the Information Society (FIDIS), Brussel 2009, beschikbaar via www.fidis.net.

als bedoeld in art. 15, lid 1'.[40] Precies in slimme omgevingen zou dit een voorwaarde kunnen zijn voor effectieve bescherming van de privacy, die ook een effectieve bijstelling van privacy-verwachtingen mogelijk maakt. Het probleem van art. 12 is echter dat het 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*).[41] Wil dit transparantierecht effectieve bescherming bieden dan zal het juridisch scherper moeten worden geformuleerd en *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. Om 'effective remedies' te verkrijgen zal het geschreven recht in een aantal gevallen moeten worden gecomplementeerd met recht dat – op initiatief van de democratische wetgever – in de nieuwe ICT infrastructuur wordt ingeschreven.[42] 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 hebben genoemd.[43]

5 Privacy als bron van vrijheid om de eigen identiteit te ontwikkelen

Gutwirth en De Hert hebben al eerder overtuigend aangetoond dat privacy een middel is burgers om af te schermen van de alziende blik van overheden of andere machtige organisaties, terwijl gegevensbescherming een middel is om transparantie te verkrijgen over gegevensverwerking.[44] Dit komt overeen met het uitgangspunt van de rechtsstaat: terwijl aan de burger een vrije ruimte toekomt om vorm te geven aan de eigen identiteit, hoort de overheid zich op transparante wijze van haar taak te kwijten. Transparantierechten zijn een middel om het tweeledige doel van de Richtlijn

---

[40] Zie tevens art. 7 van het Kaderbesluit 2008/977/JHA waar het nemen van geautomatiseerde beslissingen is toegestaan indien voldaan is aan het legaliteitsbeginsel. In dit geval is geen recht op informatie inzake 'the logic of processing' toegekend.

[41] Overweging 41 van de Preambule van de Richtlijn Gegevensbescherming stelt inzake dit transparantierecht: 'dat dit recht geen afbreuk mag doen aan het zakengeheim of aan de intellectuele eigendom en met name aan het auteursrecht dat de software beschermt; dat zulks er evenwel niet toe mag leiden dat de betrokkene alle informatie wordt geweigerd. Zie N. van Dijk, Auteursrecht in profielen, *Computerrecht,* 2010-2, p. 53-61.

[42] Het EHRM legt speciale nadruk op het feit dat de enkele opname van een geschreven regel in wetgeving of rechtspraak niet voldoende is om tot adequate verdragsrechtelijke bescherming te concluderen (de 'effective remedy' van art. 13 ECRM). In de context van het concrete geval moet die bescherming ook gerealiseerd kunnen worden. Op enig moment zal de afweging gemaakt moeten worden of, onder welke condities en op welke wijze bepaalde juridische bescherming afhankelijk is van het *ontwerp* van nieuwe informatie en communicatie infrastructuur.

[43] M. Hildebrandt, M. en B. J. Koops, The challenges of Ambient Law and legal protection in the profiling era, (73) *Modern Law Review,* 2010-3, p. 428-460.

[44] S. Gutwirth en P. De Hert, Regulating Profiling in a Democratic Constitutional State, in: *Profiling the European Citizen. Cross-Disciplinary Perspective*, M. Hildebrandt en S. Gutwirth (eds.), Dordrecht: Springer 2008, p. 271-302.

Gegevensbescherming te bereiken: enerzijds gaat het de Richtlijn om het wegnemen van hindernissen voor het vrije verkeer van informatie, anderzijds gaat het om de bescherming van de privacy. Bescherming van data is dan ook geen doel op zich. Het gaat erom de burger een positie toe te kennen van waaruit zij grenzen kan stellen aan de eigen doorzichtigheid, en zeker te stellen dat gedeelde informatie op een doorzichtige manier wordt verwerkt.

Slimme omgevingen staan of vallen met intensieve data analyse. Privacy activisten zouden er goed aan doen zich minder te richten op het zo volledig mogelijk anonymiseren en uitwissen van gegevenssporen en zich serieus te verdiepen in de computationele darmen van slimme omgevingen. De gevaren van statistische kennisclaims die zijn gebaseerd op onjuiste gegevens of op non-distributieve groepsprofielen moeten in kaart worden gebracht op een manier die uiteindelijk voor de betrokken burgers zichtbaar maakt hoe ze worden gecategoriseerd en welke consequenties dat kan hebben. De impact van subliminale, proactieve, autonoom functionerende slimme omgevingen op het vormen van onze persoonlijke identiteit is vele malen groter en subtieler dan die van individuele klantenprofielen. Patroonherkenning gaat veel verder dan bijeengeraapte digitale sporen. De persoonlijke identiteit die wordt beschermd door het recht op privacy is dan ook veel meer dan een verzameling attributen.