RECHT OP PERSOONSGEGEVENS ALS ZELFBESCHIKKINGSRECHT

'Personal data is the new oil of the internet and the new currency of the digital world'
Eurocommissaris Meglana Kuneva in een speech van 31 maart 2009

Door Egbert Dommering*
Verschenen in: J.E.J. Prins (red.) *16 miljoen BN'ers? Bescherming van persoonsgegevens in het digitale tijdperk*, Leiden: Stichting NJCM-Boekerij (47) 2010, p. 83-99.

1. De informatiesamenleving is een controle samenleving

Persoonsgegevens zijn in de 21e eeuw een belangrijke grondstof geworden.[1] Mensen produceren niet alleen artistieke werken, uitvindingen en kennis, maar in toenemende mate informatie over zich zelf: wie zij zijn, waar zij zijn, wat hun wensen zijn en wat zij doen. De informatiesamenleving is immers in de 21e eeuw niet alleen de *kennissamenleving* die in de 20e eeuw is gevormd, maar ook en vooral de *informatie-over-mensen-samenleving*. Via persoonsgegevens worden we door de overheid, instellingen van welzijn en commerciële organisaties aangestuurd en gecontroleerd.
Dit is een culminatiepunt van een ontwikkeling die inzette met de vorming van de nationale staat met zijn bestuur en politie die gretig opzoek gingen naar gegevens over de staatsburgers. De Amerikaanse politicoloog James Scott heeft in zijn boek uit 1998 *Seeing like a State* laten zien dat deze staten er altijd op gericht zijn geweest om van de staatsburger een *leesbare eenheid* te maken.[2] En dat zijn we dus als staatsburger in de 21e eeuw: leesbaar. Leesbaar op biologisch niveau, in onze bewegingen, in onze transacties, in onze communicatiehandelingen. Overal en altijd. Is het individu dan in de toekomst een speelbal van organisaties en instellingen die macht over hem uitoefenen? Formeel niet. Wij kennen immers regels die de privacy beschermen. Hoe zat het daar ook weer mee?

2. Ontwikkeling van het privacyrecht: EVRM

De Amerikaanse boulevardpers zorgde aan het het eind van de 19e eeuw in de Verenigde Staten voor het eerste privacyconcept: *the right to be let alone*. De periode 1850-1890 (de tijd van 'krantenmagnaten' Joseph Pulitzer en Ronald Hearst) werd gekenmerkt door een omstuimige groei van de massakranten, waarvan de kleinere oplagen behaalden van 800.000 en de grotere van 8 miljoen lezers. Zij vormden een nieuwe industrie die begerig was naar 'verhalen' uit het privéleven. [3] De informatietechnologie die hierbij centraal stond was de met telelenzen de privésfeer binnendringende fotografie en afluisterapparatuur. Schending van privacy werd daardoor een nieuw maatschappelijk fenomeen. In reactie op deze ontwikkeling formuleerden de

---

* Hoogleraar Informatierecht aan de Universiteit van Amsterdam, advocaat bij Brinkhof Amsterdam
[1] Een rudimentaire versie van dit artikel verscheen in *Mediaforum* 2009-11/12.
[2] James C. Scott *Seeing like a state, How certain schemes to improve the Human Condition Have Failed*, New Haven and London: Yale University Press 1998. Zie ook E.J. Dommering, *Gevangen in de waarneming*, Amsterdam: Otto Cramwinckel 2008.
[3] Daniel J. Solove & Paul M. Schwartz, *Privacy, Information and Technology*, Wolter Kluwer Law & Business 2009 (second edition), p. 11, hierna: Solove & Schwartz.

rechtsgeleerden Warren en Brandeis het nieuwe recht om alleen gelaten te worden. Zij situeerden dat recht tussen het recht van intellectuele eigendom en het materiële eigendomsrecht in. In de opsomming van de kenmerken van dat recht, die zij gaven, zien wij nog dat het ging om de reactie op de pers: 1. Het privacyrecht verhindert niet publicatie over kwesties van algemeen belang, 2. Publicaties over privé aangelegenheden die het publieke debat raken zijn toegestaan als het om publieke figuren gaat (zo stond het er nog niet, maar was het wel bedoeld. Letterlijk schreven zij: 'publication is made under circumstances which would render it a privileged communication according to the law of slander and libel'), 3. Het recht van privacy houdt op als het betrokken individu zelf de feiten publiceert of daaraan toestemming verleent, 4. De waarheid van de gepubliceerde feiten ontneemt daaraan niet de schending van het privé karakter; het gaat dus om de onthulling zelf. 5. Gebrek aan boos opzet ('malice') is evenmin een verweer. [4] Het Amerikaanse recht had moeite het als een recht te construeren, omdat de Amendments op de Constitution geen duidelijk privacyrecht kennen. Het ontwikkelde zich in de praktijk als een specifieke onrechtmatigedaadsactie die kon slagen als aan de volgende voorwaarden was voldaan: a. intrusion upon seclusion (het binnendringen in een sfeer van afzondering, b.public disclosure of private facts (onthulling van privé feiten; de kern van wat Warren en Brandeis het nieuwe recht noemden; de vraag werd nu wat zijn 'privé feiten', een vraag die bij de ontwikkeling van dataprotectie weer actueel werd), c false light (de gepubliceerde feiten zetten iemand in een 'vals daglicht'), d. appropriation (toeëigening; dit concept ging met name bij de ontwikkeling van een commercieel 'right of publicty'een rol spelen) .
Dat recht om alleen gelaten te worden erkennen we inmiddels wereldwijd. In Europa is het te vinden in artikel 8 van het Europese Verdrag voor de Rechten van de Mens (EVRM). Het Europese Hof voor de Rechten van de Mens (EHRM) heeft dat recht verder ontwikkeld tot een zelfbeschikkingsrecht, waarbij het ook de bescherming van persoonsgegevens ging betrekken. De zaak S. and Marper/VK uit 2008 betreffende de opslag van DNA gegevens kan als een piketpaaltje in het uitdijende zelfbeschikkingsrecht worden gezien:[5]

The Court recalls that the concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person. It can therefore embrace multiple aspects of the person's physical and social identity. Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8. Beyond a person's name, his or her private and family life may include other means of personal identification and of linking to a family. Information about the person's health is an important element of private life The Court furthermore considers that an individual's ethnic identity must be regarded as another such element (see in particular Article 6 of the Data Protection Convention quoted in paragraph 41 above, which lists personal data revealing racial origin as a special category of data along with other sensitive information about an individual). Article 8 protects in addition *a right to personal development, and the right to establish and develop relationships with other human beings and the outside world The concept of private life moreover includes elements relating to a person's right to their image. The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8.*(cursivering van mij EJD)

In een beslissing van het EHRM van 15 januari 2009 in de zaak Reklos en Davourlis[6] geeft het Hof een kortere samenvatting, en werkt het dit recht verder uit voor 'the right to one's image' (portretrecht)

Uit de gegeven opsomming valt op te maken dat het Hof vooral aan een beschikkingsrecht over gegevens denkt die werkelijk op het privéleven ('data relating to private life') betrekking hebben. Contextuele informatie zou er daarom buiten kunnen vallen, omdat die 'do not relate tot private

[4] 'The Right of Privacy', in: 4 *Harvard Law Review*, p. 193 (1890), opgenomen in: Solove & Schwartz (zie noot 3), p. 13-23.
[5] EHRM 4 december 2008, appl. 30562/04, *NJ* 2009, 410 m.nt E.A. Alkema.
[6] EHRM 15 januari 2009, appl. 1234/05, *AMI* 2009-5, nr. 18, *NJ* 2009, 524 m.nt. E.J. Dommering.

life', maar hoever dat gaat is onduidelijk.[7] Dit lijkt ruimer dan de 'gevoelige gegevens' (zoals sekse, ras en levensovertuiging) die we uit de Wbp kennen, zeker als het gaat om omschrijvingen 'the right to develop relationships with (…) the outside world' en het 'means of identification'. In dit artikel wil ik de opvatting verdedigen dat die omschrijvingen een ruime opvatting impliceren, en alle persoonsgegevens omvatten, niet alleen gevoelige gegevens. De nieuwste informatietechnologie die onbeperkt verzamelen van alle mogelijke gegevens met betrekking tot de persoon en zijn gedragingen naar plaats, tijd en soort mogelijk maakt, waarop steeds slimmere bewerkingen kunnen worden uitgevoerd ('datamining'), maakt dat het onderscheid in toenemende mate achterhaald is. Uit iemands uitwendige gedragingen naar tijd en plaats, kunnen door analyse gevoelige gegevens worden afgeleid.

3. Dataprotectierecht als aparte Europese tak.

In de periode dat het EHRM het in artikel 8 van het EVRM beschermde privacyrecht begon uit te bouwen, heeft er in Europa een andere, parallelle ontwikkeling plaats gevonden. De informatietechnologie die hier de sleutel vormt is de computer, van meet af aan een potentiële databank waarin persoonsgegevens kunnen worden opgeslagen en gecombineerd. Het Duitse Constitutionele Hof erkende begin jaren tachtig van de vorige eeuw een op de menselijke waardigheid gebaseerd '*recht op informationele zelfbestemming*'. Het Hof stelde: 'Iedereen die er niet zeker van kan zijn dat gegevens over maatschappelijk afwijkend gedrag voor langere tijd worden geregistreerd en kunnen worden gebruikt op een manier waarvan hij niets weet, zal proberen om dat gedrag niet te vertonen. Dat is in strijd met de elementaire functie van zelfbeschikking in een democratische samenleving waarin de burgers de mogelijkheid moeten hebben om deel te nemen aan het maatschappelijke en politieke leven zonder risico te lopen op een voor hem ondoorzichtige manier te worden geregistreerd.'[8] Dat is een omschrijving die dichtbij de omschrijving van het EHRM komt om *betrekkingen met de 'buitenwereld'* te ontwikkelen, al benadrukt de Duitse rechter dat het gaat om een *democratisch* zelfbeschikkingsrecht. Kort daarvoor had de Raad van Europa een verdrag voor dataprotectie vastgesteld. In Nederland leidde de ophef rond de volkstelling van 1971 tot de instelling van de Commissie Koopmans. Deze commissie legde de grondslag voor de Wet Persoonsregistratie, de voorloper van de Wet Bescherming Persoonsgegevens.
Dat recht van informationele zelfbeschikking (zoals we het met een germanisme zijn blijven noemen) gaat over beperking van macht, aanvankelijk alleen die van de overheid, later ook die van commerciële en 'welzijn' machten. Dit zelfbeschikkingsrecht heeft vervolgens een zelfstandige ontwikkeling doorgemaakt waarin het element van controle op macht steeds meer verschoof in de richting van beginselen van behoorlijke machtsuitoefening, en waarbij het aspect van een zelfbeschikkings*recht* geheel op de achtergrond raakte. Een voorbeeld daarvan is het proefschrift van Peter Blok *Het recht op privacy* waarin het recht wordt teruggebracht tot *beginselen van behoorlijk gegevens beheer.*[9]De inzet op controle van macht heeft ook gemaakt dat wij het persoonsgegevens zijn gaan regelen in publiekrechtelijke regels. Mensen – datasubjecten - krijgen volgens die regels bepaalde bevoegdheden, degenen die persoonsgegevens verzamelen moeten zich aan bepaalde beperkingen houden en er is een toezichthoudende instantie (een College *bescherming* persoonsgegevens) die preventief (vooraf) en repressief (achteraf) toeziet op naleving van die regels. De kern van die bevoegdheden en plichten ziet er als volgt uit: persoonsgegevens moeten alleen worden afgegeven en mogen alleen worden verwerkt voor een bepaald en gerechtvaardigd doel (*doelbindingsbeginsel*), het datasubject moet inzicht hebben in (en heeft daarom een inzagerecht) welke gegevens er over hem zijn opgeslagen en verwerkt (*transparantiebeginsel*), er

[7] Zie de Decision inzake Smith, EHRM 4 januari 2007, *NJ* 2007, 475. Zie ook mijn noot bij de arresten van HR 29 juni 2007, (inzake Dexia en HBU), *NJ* 2007, nrs. 638 en 639.
[8] BVerfGH 15 december 1983, *NJW* 1984, p. 419.
[9] P.H. Blok *Het Recht op privacy*: Den Haag: Boom Juridische Uitgevers 2002.

mogen niet meer gegevens worden bewerkt en bewaard dan voor het gerechtvaardigde doel nodig is (*proportionaliteitsbeginsel*), en de kwaliteit en juistheid van de gegevens moeten zijn gewaarborgd en kunnen door het datasubject worden afgedwongen (*kwaliteitsbeginsel*).

Het gegevensbeschermingsrecht kreeg door deze parallelle ontwikkeling een aparte plaats. Een culminatiepunt is het Charter of Fundamental Rights of the European Union van 7 december 2000 dat per 1 december 2009 is geïncorporeerd middels artikel 6 van het EU verdrag. Het Charter definieert in de artikelen 7 en 8 het 'respect for private life' en 'the right to protection of personal data' als twee afzonderlijke rechten. De regels en het toezicht kregen vorm in de ons nu bekende dataprotectiewetten en de richtlijnen die de EG daarover opstelde. Het hele beschermingsregime scoorde goed op macroniveau, Europees en wereldwijd, waarbij vooral het doelbindingsbeginsel een machtig wapen bleek. De gegevens die binnen organisaties werden verzameld, mochten niet voor andere doeleinden worden gebruikt en niet zomaar met andere organisaties worden gedeeld. Dat leidde tot een afgedwongen herinrichting van de interne bedrijfsvoering waardoor de verwezenlijking van het doelbindingsvoorschrift werd gewaarborgd. Het preventieve toezicht dat de Colleges bescherming persoonsgegevens uitoefenden, bleek effectief, hoewel er ook veel klachten zijn over een tekort aan collectieve handhaving. De Europese Gemeenschap wist zijn beschermingsregime zelfs buiten Europa te exporteren, via *safe harbour agreements*. Alleen als de persoonsgegevens in een 'veilige haven' terecht komen - een bedrijf dat de beginselen van het Europese beschermingsregime toepast - mogen ze buiten de EG worden geëxporteerd.[10]

4. Dataprotectierecht zonder burgers

Op individueel niveau werkte deze aanpak minder. Opslag en verwerking van je persoonsgegevens is voor de meeste burgers te diffuus en abstract om je over op te winden. Dat de Duitse Bezettingsautoriteit het Amsterdamse bevolkingsregister misbruikte om razzia's te houden op Joodse burgers, was weggezakt in de geschiedenis. Daar denkt de consument die airmiles spaart niet aan. Maar er ging meer fout met het ideaal van de informationele zelfbeschikking. Laten we daar eens naar kijken.

Door het - na 9/11 ook in Europa om zich heen grijpende - *veiligheidsdenken* kwamen doelbinding en proportionaliteit onder grote druk te staan. Overheden wilden steeds meer gegevens opslaan. Symbolisch daarvoor is de dataretentierichtlijn (de 'bewaarplicht'), die een vergaande *beperking* inhoudt op de doelbinding en proportionaliteit van de telecommunicatie-privacyrichtlijn. Laatstgenoemde richtlijn vestigt het hoofdbeginsel dat verkeersgegevens van elektronische communicaties (waar en met wie is wanneer gecommuniceerd?) slechts voor een beperkte periode mogen worden opgeslagen, en alleen voor zover nodig voor de dienstverlening (denk bijvoorbeeld aan facturen). De dataretentierichtlijn gaat dwars door dat proportionele doelbeginsel heen door te bepalen dat verkeersgegevens minimaal zes maanden en maximaal twee jaar moeten worden opgeslagen om als basis te kunnen dienen voor strafrechtelijk onderzoek. Voor Nederland is het rapport *Gewoon Doen* van de Commissie Brouwer van begin 2009 voortaan het 'richtinggevend kader' voor de privacybescherming in de publieke beleidssfeer. De commissie had als opdracht het recht op privacy en veiligheid met elkaar te verzoenen. Het rapport zet echter de bijl aan het kernbeginsel van het privacyrecht, de doelbinding, die slechts in concreet af te wegen gevallen mag wijken voor belangen van een andere orde. Het rapport formuleert als hoofdbeginsel zonder nadere concrete belangenafweging: *'indien noodzakelijk voor de veiligheid, moet je delen.'* Dat is niet een 'verzoening' van privacy en veiligheid (de taak van de Commissie), maar een onderschikking van privacy aan veiligheid. De Minister van Justitie heeft het rapport van de

[10] Voor een analyse , zie A.L. Newman *Protectors of Privacy, Regulating Personal Data in the Global Economy*, Ithaca and London: Cornell University Press 2008.

Commissie aangegrepen om de evaluatie van de Wbp om te turnen tot een veiligheidsexercitie. De brief aan de Kamer over die evaluatie bevat 28 pagina's, waarvan de helft gaat over 'veiligheid'. In dit verband spreekt de brief ook over een 'nieuwe benadering van persoonsgegevens'.[11]

Daarnaast ging het fout omdat transparantie en kwaliteitsbeginsel in toenemende mate een illusie bleken te zijn. De enige die echt transparant (en leesbaar) werd, is de burger zelf. De ondoorzichtigheid van de techniek en hoeveelheid digitale sporen die we achterlaten, in combinatie met de complexiteit van de problematiek, maken controle op opslag, kwaliteit en verwerking van persoonsgegevens vrijwel onmogelijk. Ze komen terecht in talloze databanken waarvan de identiteit en locatie niet zijn te traceren. Belangenbehartiging ten behoeve van individuele burgers door de Colleges bescherming persoonsgegevens is tegenwoordig een illusie. Door de omvang en complexiteit van het gegevensverkeer en -opslag kunnen zij zich daar niet meer mee bezighouden. Zij hebben zich teruggetrokken op hun kerntaken, waarin nog slechts plaats is voor een selectief vervolgingsbeleid als daarbij een voldoende algemeen belang is betrokken. Als de tekenen niet bedriegen zal de preventieve controle in de nieuwe privacy richtlijn verdwijnen en vervangen worden door een papieren muur van accountantsverklaringen dat een organisatie werkt volgens regels van 'behoorlijk gegevensbeheer'.

Staat de burger machteloos? Is hij de uitleesbare chip, het herkenbare DNA profiel, de wolk elektronische communicaties, die tevreden kiest, winkelt en reist, maar een vaag gevoel van onbehagen met zich meedraagt? Een onderzoek uitgevoerd in opdracht van het College Bescherming Persoonsgegevens (*Niets te verbergen en toch bang* januari 2009) concludeert dat burgers enerzijds gemakkelijk persoonsgegevens verstrekken, maar anderzijds blijven zitten met een vaag angstgevoel dat die gegevens verkeerd gebruikt kunnen worden. Of, zoals de aan het hoofd van dit artikel geciteerde Eurocommissaris Meglana Kuneva het in haar speech van maart 2009 zei: De mensen in de leeftijd van 15-25 jaar zijn de heavy users van het internet, maar zij vertrouwen dat zelfde internet voor geen cent; het is alsof ze hun dorst blijven lessen uit een kraan waarvan zij weten dat er licht vergiftigd water uit komt. En dat vage gevoel van onbehagen bestaat al heel lang en ook in de Verenigde Staten dat geen recht op dataprotectie kent.[12]

5. Terug naar de burger: Informationele privacy als ideëel-economisch zelfbeschikkingsrecht

We hebben dat recht in Europa geformuleerd als een grondrecht dat ons privéleven beschermt tegen inmenging van de staat en anderen, en als een zeggenschapsrecht om de macht van de staat en anderen over ons privéleven te beperken. Maar privacy is ook een economisch zelfbeschikkingsrecht, zonder het meteen op een lijn te stellen met eigendomsrecht op stoffelijke goederen. Het heeft dit ideëel-economische dubbelaspect gemeen met het auteursrecht dat immers uiteen valt in economische gefundeerde exploitatierechten en moreel gefundeerde persoonlijkheidsrechten. Dit dubbelaspect heeft in de literatuur nog weinig de aandacht getrokken, hoewel het al in het geciteerde artikel uit 1890 van Warren en Brandeis is te onderkennen, die het identificeren met wat wij nu in het auteursrecht het belangrijkste 'droit

---

[11] Brief van de Minister van Justitie van 3 november 2009, Kabinetsstandpunt advies Commissie Brouwer-Korf en evaluatie van de Wet bescherming persoonsgegevens, Kamerstukken II 2009-2010, 31051, nr. 5.

[12] Dat was al zo toen de *direct marketing* werd uitgevonden, zie Joseph Turow, *Niche Envy, Marketing Discrimination in the Digital Age*, Cambridge-Massachusetts: MIT Press 2006. Voor een in 2009 gepubliceerd onderzoek dat dezelfde gevoelens van onbehagen bij de Amerikaanse burger blootlegt, zie Joseph Turow e.a., *Americans reject Tailored Advertising and three Activities that enable it,* in 2009 gepubliceerd en geraadpleegd op http://ssrn.com/abstract=1478214.

moral' noemen: 'het droit de publication', het recht om zelf te beslissen of je een door jou gemaakt 'werk' wilt publiceren.Vooral in de Amerikaanse literatuur is over privacy als economisch recht veel gediscussieerd, maar niet over dit dubbel aspect.[13] Dat dubbelaspect zit trouwens ook in het recht van vrije meningsuiting dat immers uiteenvalt in het morele vrijheidsaspect en het economische door het auteursrecht beschermde eigendomsaspect, en misschien ook nog wel in andere fundamentele rechten, maar dat laat ik verder daar.

Het voordeel van de fundering van relationeel en informationeel privacyrecht als aspecten van hetzelfde recht is dat kan worden voorkomen dat er een proliferatie van rechten optreedt en de onderlinge samenhang beter kan worden begrepen. Die proliferatie zien we niet alleen in het EU Charter, maar ook in het Amerikaanse recht waar een afzonderlijk economische 'right of publicity' bestaat[14] of het al oudere in het Engelse recht bestaande 'right of reputation', waar de 'law of diffamation' op is gebouwd.[15] Dat laatste speelde het EHRM parten in de tamelijk duistere uitspraak in de zaak Karakó.[16] Die eenheid van het privacyrecht zou ik als volgt willen construeren. [17]

Met *relationele* privacy doelen we op de persoonlijke *levenssfeer*. Bij *informationele* privacy gaat het om het zelfbeschikkingsrecht met betrekking tot de informatie die over het individu in omloop is. Deze twee privacyrechten hebben, zoals gezegd, meer met elkaar te maken dan wij op het eerste gezicht in die tweedeling onderkennen, en wellicht is het jongere informationele recht zelfs het kernrecht en het relationele recht daarvan een speciaal geval. Warren en Brandeis reageerden op de informatietechnologie die het mogelijk maakte intieme feiten vast te leggen en verder te verspreiden. Die informatietechnologie maakt het nu mogelijke alle interne en externe gedragingen van individuen vast te leggen. In beide gevallen gaat het vooral om het vastleggen en doorgeven: dus de 'informationele' kant. Het speciale geval is het *fysiek* met rust laten. Het is de kring rond de persoon (niet noodzakelijk in een afgescheiden ruimte zoals in het Amerikaanse recht bij 'invasion upon seclusion'wordt aangenomen) die de afstand tussen het individu en de wereld rondom hem markeert. Overschrijding van de omtrek van die cirkel is iemand 'niet met rust laten', al gauw 'geen afstand bewaren', of, nog dichter bij: een aantasting van lichamelijke integriteit. Gaat het om informatie die tot de persoonlijke levenssfeer behoort, zoals al of niet intieme biografische feiten, identificerende kenmerken (persoonsgegevens) en vertrouwelijke communicaties dan loopt er een vloeiende lijn van de relationele sfeer naar de informationele zelfbeschikking. Dat komt omdat wij een informationele 'binnenkant' en een informationele 'buitenkant' hebben. Dit wordt treffend geïllustreerd door het portretrecht. Een portret van de binnenkant kan een (intensieve) waarneming en/of een afbeelding van de persoon in een intieme situatie zijn (naakt in de badkamer, het 'herdersuurtje', zoals Advocaat-generaal Leijten het in zijn

---

[13] Zie Daniel J. Solove, *The Digital person. Technology and privacy in the information age*. New York/London: The New York University Press, hoofdstuk 5. Zie ook de verschillende artikelen, opgenomen in Solove & Schwartz (zie noot 3) in hoofdstuk 1C 'Perspectives on Privacy' en de opvattingen besproken bij Corien Prins, 'Property and Privacy: European Perspectives and the Commodification of our Identity', in: Lucie Guibault & P. Bernt Hugenholtz (eds.),*The Future of the Public Domain, Identifying the Commons in Information Law* Den Haag/Londen/New York: Kluwer Law International 2006, p. 223, in het bijzonder p. 231.

[14] Zie Bas Pinckaers, 'Het Amerikaanse Right of Publicity', in: D.J. Visser (red.), *Commercieel Portretrecht, 't Schaep met de 5 pooten',* Amstelveen: De Lex 2009, p. 203-213.

[15] In de Angelsaksisch e literatuur woedt nog steeds een debat over de grondslag van dit recht:, zie Paul Mitchell, book review van Dario Milo *Defamation and Human Rights*, Oxford: Oxford University Press 2008, in: [2009] 2 Journal of Media Law, p. 289.

[16] EHRM 28 april 2009, appl. 39311/05, *NJ* 2009, 522, m.nt. E.J. Dommering.

[17] Het navolgende bouwt voort op E.J. Dommering, 'Van Ja zuster, nee zuster" naar "Discodans": de lange weg naar commerciële informationele privacy,' in: D.J.G. Visser (red.), Commercieel portretrecht. 't Schaep met de 5 pooten', p. 259-273 en mijn noot bij de zaak Reklos en Tirion/Sauaerbreij (Hof Amsterdam 14 april 2009) in: AMI 2009/5, nr. 18 en 19, p. 196-198.

conclusie bij de het Bespiede Bijstandsmoeder arrest nog noemde[18]). Een afbeelding van de buitenkant gaat om iemands openbare *persona* in een maatschappelijke situatie: een consument winkelend gadegeslagen door een bewakingscamera, een politicus door de pers waargenomen en gefotografeerd op het spreekgestoelte. In onze openbare democratische en consumentistische verzorgingsstaat, maakt het individu immers in toenemende mate deel van de 'publieke sfeer.'[19] Ook biografische feiten en identificerende kenmerken kunnen tot de binnenkant behoren (de wetenschap van het plegen van een niet ontdekt misdrijf, de geheime keuze in het stemhokje, de slechts door deelnemers aan een gesprek waargenomen communicatie), maar zij hebben dikwijls een buitenkant (een proces-verbaal van politie van een gepleegd strafbaar feit, de op een opiniepagina beleden politieke overtuiging, het luid in de trein gevoerde telefoongesprek).[20]

Een bijzonder aspect van de informationele buitenkant is iemands *reputatie* of *eer en goede naam*. Dit is de uit de Romeinse tijd en de Middeleeuwen stemmende *fama* die kan worden *gediffameerd*. Reputatie is van oudsher een belangrijke waarde die nuttig en noodzakelijk is voor deelname aan het maatschappelijke - en het rechtsverkeer. Verlies of beschadiging van die waarde kan ernstige morele (gevoelens van spijt en schaamte) en economische (afwijzing bij sollicitaties) consequenties hebben.[21] Het is een onderdeel van de informationele privacy, omdat het gaat over de informatie die over iemand in omloop is en waar iemand dus iets over te zeggen wil en moet hebben. Bovendien bepaalt het individu zelf welke informatie hij van binnen naar buiten wil brengen om die reputatie te voeden. Het feit dat 'eer en goede naam' ouder is dan ons hedendaagse privacyrecht is geen reden om het thans niet te zien als onderdeel van het concept privacy (en als informationele privacy: het gaat om negatieve of positieve informatie *over* iemand, mede in het licht van onthulde geheime 'binnenkant' feiten).

De waarneming van de binnenkant heeft steeds een *relationeel* aspect, omdat deze waarneming niet mogelijk is zonder (al of niet met behulp van technische hulpmiddelen) in de persoonlijke *levenssfeer* binnen te dringen. Dat geldt ook voor het vastleggen en verwerken van persoonsgegevens bij in beginsel *geheime elektronische transacties* en *elektronische communicaties* . De

---

[18] HR 9 januari 1987, *NJ* 1987, 928, zie de conclusie van de AG onder punt 45:'De advocaat van eiser is van mening, dat daartoe bijv. gesteld had moeten worden, dat die waarnemingen waren gedaan met gebruikmaking van technische hulpmiddelen, zoals verrekijker, fototoestel, afluisterapparaat e.d. Ik kan niet inzien dat zulke zaken beslissend zijn. Sommige mensen zien beter zonder verrekijker dan andere met. Waar het m.i. op aankomt is binnentreden in de privé-sfeer van een ander op een wijze waarmede de ander in redelijkheid geen rekening hoeft te houden. *Gaat het over een herdersuurtje dan zal de daarbij vaak begeerde privacy geschonden zijn als iemand met een apparaat dit beeld in zich opneemt en naar zich toetrekt, terwijl dit met het blote oog niet mogelijk zou zijn.* Maar als het er nu om gaat vast te stellen of iemand een min of meer duurzame relatie onderhoudt, dan helpt zo'n apparaat maar heel weinig. Het enkele feit, dat de constante observator vaststelt dat daar voor dat huis altijd diezelfde auto staat, die door X bestuurd wordt, zulk met het oog op het vaststellen voor zo'n relatie is dan veel belangrijker en grijpt veel dieper in de persoonlijke levenssfeer in. Het is niet de waarneming die ieder ander ook kan doen, maar het is de volgehouden observatie met een bepaald doel die een bepaalde wijze oplevert van schending van privacy.'

[19] Volgens A. Etzoni, zijn we zelfs alleen maar 'community'. Hij is daarom tegen privacy, zie Solove & Schwartz (noot 3), p. 59.

[20] Let wel de 'buitenkant' kan ook betrekking hebben op 'gevoelige gegevens', zoals de ras of sekse kenmerken van een portret. Ook kunnen valselijk gevoelige kenmerken worden toegevoegd, bijvoorbeeld door bij iemand die een baard heeft en een hoofddeksel draagt, baard en hoofddeksel zo suggestief af te beelden, dat hij een radicale moslim lijkt. Er zijn veel 'false light' portretten door verkeerde context.

[21] Verlies van *fama* had in de Middeleeuwen dikwijls noodlottige gevolgen voor volwaardige deelname aan het rechtsverkeer, zie Thelma Fenster & Daniel Lord Small (eds.), *Fama. The politics of talk & reputation in Medieval Europe*, Ithaca/London: Cornell University Press 2003. Het verlies van de eer van de familie speelde ook een grote rol in het *Ancien Régime*, waar de familie een familielid dat de reputatie van de familie besmeurde met hulp van het openbare gezag door middel van een *lettre de cachet* uit het openbare leven kon laten verwijderen en in de Bastille laten opbergen, zie Arlette Fage, 'Familles, L'honneur et le secret', in: Philippe Ariès en Georges Duby (red), *Histoire de la vie privé, De la Renaissance aux Lumières,* tôme 3, p. 581-618, Parijs: Éditions du Seuil, 1986.

waarneming van de buitenkant *kan* een *relationeel* aspect krijgen door de intensiteit ervan, bijvoorbeeld door opdringerige paparazzi die je met camera's met telelenzen overal volgen, of het belastende kruisverhoor van de verbalisant die je de bekentenis probeert te ontwringen.

Het haakje tussen het relationele en het informationele privacyrecht als een ideëel-economisch zelfbeschikkingsrecht over een persoonsgegeven, wordt gevormd door het portretrecht dat over het algemeen in het domein van het auteursrecht wordt behandeld, omdat het in verband wordt gebracht met de rechten van de fotograaf.[22] In de geciteerde Rekloszaak noemde het EHRM het portret 'one of the essential components of personel development and presupposes the right to control the use of that image.' Een portret, onze 'buitenkant', is een persoonsgegeven dat wij als privépersoon buiten de privésfeer (het familiefotoalbum) liefst geheim (anoniem) willen houden. Dat lukt vaak niet omdat er steeds meer foto's van ons als 'een plaatje' bij het nieuws worden gepubliceerd. De buitenkant is daarnaast nodig als pasfoto voor identificatie. Maar dat portret heeft ook een economische kant. Beroemde artiesten zien hun portret als een even grote 'asset' als hun performance. Ze vragen voor het gebruik daarvan geld, net zoals ze geld vragen voor hun optreden. Dat economische belang van het portret wordt overal in het recht erkend. Ook de anonieme burger heeft portretrecht. Hij hoeft niet goed te vinden dat zijn portret zonder zijn toestemming voor een commercieel doel (bijvoorbeeld een advertentiecampagne) wordt gebruikt.

Een portret is een (sterk) persoonsgegeven. Waarom zouden andere persoonsgegevens (ons adres en onze tot de persoon herleidbare gedragingen) wel vogelvrij zijn? Is mijn PC niet een extensie van mijn privé levenssfeer en het instrument om vorm te geven aan relaties tot de buitenwereld? Zijn persoonsgegevens om te vormen tot het 'digitale geld' waar de geciteerde Eurocommissaris het over had?

6. Nadere fundering van het economisch zelfbeschikkingsrecht: het geheim.

In Nederland is naar aanleiding van het Valkenhorstarrest [23]een soort juridisch stuivertje verwisselen gespeeld, namelijk of het privacyrecht niet eigenlijk moet worden afgeleid uit een *algemeen persoonlijkheidsrecht*, een opvatting die ontleend is aan de Duitse doctrine en die door de Advocaat-Generaal Koopmans in zijn conclusie bij het Valkenhorstarrest naar voren is gebracht.[24] Het bezwaar van het persoonlijkheidsrecht als grondslag is dat het zo algemeen is dat het als grondslag kan dienen voor ieder grondrecht. *Toestemming, doelbinding, inzage-* en *correctierecht,* die we uit het dataprotectierecht kennen zijn welbeschouwd bevoegdheden die zich gemakkelijk laten vertalen als economische privaatrechtelijke zeggenschapsrechten. De basis is de toestemming. In vergelijking tot het recht van intellectuele eigendom kun je deze privaatrechtelijke bevoegdheden zien als *licenties*: er wordt niet zozeer een stukje eigendom overgedragen als wel een gebruiksrecht voor een bepaald doel verstrekt met de mogelijkheid te controleren of de licentie wel juist wordt uitgevoerd.[25] Het is misschien wel mogelijk om een stuk eigendomsrecht over te dragen (bijvoorbeeld het explotatierecht van een portretrecht, winningsrechten voor een archief en dergelijke), maar in het algemeen zal het toch gaan om

[22] Zie reeds K.C. Laudon, 'Markets and Privacy', geciteerd bij Corien Prins, 'Property and Privacy: European Perspectives and the Commodification of our Identity', in: Lucie Guibault & P. Bernt Hugenholtz (eds.),*The Future of the Public Domain, Identifying the Commons in Information Law* Den Haag/Londen/New York: Kluwer Law International 2006, p. 223 (noot 3 op pagina 224).
[23]HR 15 april 1994, *NJ* 1994, 608, opgenomen met een noot van Corette Ploem in: T.E. van Dijk e.a. (red.), *Uitsprakenbundel, Wet Bescherming Persoonsgegevens* 35.2. (p. 504 e.v.). De fundering van privacy in het algemeen persoonlijkheidsrecht is ook terug te vinden in de zaak Parool/Van Gasteren, HR 6 januari 1995, *NJ* 1995, 422.
[24] A.J. Nieuwenhuis, *Tussen Privacy en Persoonlijkheidsrecht*, Nijmegen: Ars Aequi Libri 2001, p. 179 en 188. Hierover ook Britta van Beers, *Persoon en lichaam in het recht*, Boom Juridische Uitgevers 2009, p, 130 e.v.
[25] Vgl. Lawrence Lessig in *Code and Other Laws of Cyberspace*, en Richard Murphy, geciteerd bij Solove & Schwartz (noot 3), p. 437.

persoonlijke gebruikslicenties. Dit past ook in de opvatting van de Amerikaanse gangmaker van de discussie over het economische privacyrecht, Richard Posner, die begin jaren tachtig over dit onderwerp begon te publiceren.[26] Hij fundeert het economische privacy recht vooral op het *geheim*, het economische belang dat het individu er bij heeft om feiten over hem zelf af te schermen van de wereld. Het gaat om een geheim, omdat buiten de rechten van intellectuele eigendom informatie alleen 'exclusief' geëxploiteerd kan worden als zij geheim kan worden gehouden. Er bevindt zich in de privésfeer wel informatie die vatbaar is voor auteursrecht (dagboeken, brieven, niet gepubliceerde manuscripten), maar heel veel informatie is dat niet (dat hadden Warren en Brandeis ook al gezien; zij schrijven: 'A man records in a letter to his son, or in his diary that he did not dine with his wife on a certain day. No one in whose hands those papers fall could publish them to the world. Even if possession of the had been obtained rightfully …What is the thing protected? Surely, not the intellectual act of recording the fact that the husband did not dine with his wife, but the fact itself.'). [27] Het is dus vergelijkbaar met het bedrijfsgeheim dat wij in Europa beschermen door middel van contractuele constructies of via de maatschappelijke zorgvuldigheidnorm (Het arrest Lindenbaum/Cohen dat bij ons aan de basis staat van de onrechtmatige daad als overtreding van een maatschappelijke zorgvuldigheidnorm ging over de diefstal van een bedrijfsgeheim!).

Prijsgeven van het geheim van persoonsgegevens aan de openbaarheid betekent dat de informatie in het publieke domein is gekomen, maar niet onbeperkt: doelbinding beperkt de gebruiksmogelijkheden, inzage- en correctierecht waarborgen controle op het gebruik.
Het privacyrecht dat gebaseerd is op een door de rechthebbende zelf te clausuleren geheimhouding van zijn persoonsgegevens, is geen absoluut eigendomsrecht. Het is ook in een ander opzicht niet absoluut, omdat de samenleving allerlei aanspraken heeft op de persoon die het mogelijk maken van persoonsgegevens gebruik te maken ook zonder toestemming van de betrokkene. Wij maken, zoals gezegd, als democratische en consumerende burger immers ook deel uit van de publieke sfeer. De omvang van het geheim wordt dus niet alleen door het individu maar ook door de samenleving gedefinieerd: In de Wbp ligt middels algemene normen vast in welke gevallen persoonsgegevens mogen worden gebruikt en bewerkt zonder toestemming van de betrokkene. Je kunt dit ook zien als dwanglicenties, de figuur van het afgedwongen gebruik die we uit het IE recht kennen. Bovendien kan het publieke recht een 'morele ondergrens' aan verhandelbaarheid stellen, zoals dat bijvoorbeeld ook gebeurt bij de handel in menselijke organen. Zo zouden 'gevoelige gegevens' kunnen worden aangemerkt als 'zaken buiten de handel'. De exploitatie van persoonsgegevens is vergelijkbaar met die van een exploitatie van een auteursrechtelijk werk: opslag en verwerking is te vergelijken met 'verveelvoudiging', doorgeven en gebruiken met 'openbaarmaking'. Het 'doelbinding' beginsel moge een beperking van de macht van een ander zijn, het is ook een zeggenschapsrecht om de omvang en beperkingen van een 'licentie' te definiëren.[28] Maar hoe kan een buitenkant nu 'geheim' zijn, zal de lezer zich afvragen? Dat is inderdaad moeilijk, maar een voorbeeld moge dit verduidelijken. De verdachte die zijn gezicht bedekt bij het binnenkomst in het Paleis van Justitie doet een poging de buitenkant aan de openbaarheid te *onttrekken*. Andere voorbeelden zijn vermommingen en het gebruiken van aliassen in het elektronisch communicatieverkeer. *Anonimiteit* is een poging de buitenkant van de persoon geheim te houden.

---

[26] R. A. Posner, 'The Economics of privacy'(1981) 71 *The American Economic Review*, p. 405 e.v.; 'Privacy as secrecy', in: R.A. Posner, *The Economics of justice*, Massachusetts/London: Harvard University Press 1983, p. 231 e.v. Posner zag privacy als een belemmering voor het economische rechtsverkeer, reden waarom hij geen voorstander was van een eigen privacyrecht. Mijns inziens legt zijn analyse wel de juiste grondslag bloot van de economische-morele categorie waar het om gaat: het geheim.

[27] In: Solove & Schwartz (noot 3), p. 16.

[28] Vgl. Pamela Samuelson, 'Privacy as Intellectual Property', in: 52 Stanford Law Review, p. 1125 e.v. (2000). Zij ziet overigens problemen in de constructie van een eigendomsrecht in verband met allerlei vormen van marktfalen.

Mijn benadering wijkt dus af van die van Daniel Solove, die in een reeks publicaties geprobeerd heeft het privacyrecht te 'conceptualiseren'.[29] Zijn pluriforme privacy concept valt uiteen in vier categorieën: informatieverzameling, informatieverwerking, informatieverspreiding, en binnendringen in de privésfeer. Mijns inziens ziet hij over het hoofd dat het bij de eerste drie categorieën gaat om vermenigvuldiging en openbaarmaking van persoonsgegevens die tot de beschikkingsmacht van het individu behoren, net zoals de informatie in de binnenkant (invasion) tot die beschikkingsmacht behoort (de koningin beslist of zij haar familie bij haar thuis wil laten portretteren). De puur fysieke inbreuk zonder informatieverzameling is een speciaal geval. Misschien zou je dat moeten onderbrengen bij het recht op bescherming van lichamelijke integriteit en het huisrecht, overigens als een *middel* informatie over het individu te vergaren.

De overheid zal door blijven gaan met het aanleggen van steeds grotere en koppelbare bestanden van persoonsgegevens. Deze afgedwongen, in publiekrechtelijke regels verankerde verzameling en opslag van gegevens, is uiteindelijk het politieke probleem van een samenleving die in angst leeft. Dat valt buiten het bestek van dit artikel. Het valt onder het hoofdje 'beperkingen op het privacy recht in het algemeen belang', zo men wil de geoorloofdheid van de *dwanglicenties*. Hier gaat het er om de inhoud van het recht zelf te bepalen. De formulering van het recht op persoonsgegevens als een zelfbeschikkingrecht kan wel bijdragen om de proportionaliteit van de beperkingen en doelbeperking terug te krijgen in de discussie.

7. De technische organisatie van een markt van persoonsgegevens: een digitale kluis

Wie een beperkt verhandelbaar recht of een contractueel recht toestemming tot verhandeling te geven heeft, moet ook over een markt kunnen beschikken waar hij dat goed op kan verhandelen. Dat is bij persoonsgegevens natuurlijk erg ingewikkeld. Maar eerst een andere vraag: waarom zou een neutraal persoonsgegeven eigenlijk geld waard zijn? Sommige Amerikaanse auteurs zien hier een probleem om een markt te construeren.[30] Anderzijds is er binnen het recht van intellectuele eigendom een toenemende aandacht voor de 'commodification'van informatie: de economische waarde van feitenverzamelingen.[31]

Maar die verzamelde en geordende persoonsgegevens, vertegenwoordigen wel degelijk een economische waarde, die op de markt verhandeld wordt (zij vormen een groot deel van de goodwill van veel bedrijven). Op de markt van grondstoffen (dat is de markt van persoonsgegevens ten opzichte van die van derivaatmarkten van databestanden) worden zij voor niets gewonnen. Maar ook individuele persoonsgegevens zijn geld waard. Het bedrijf dat een cookie wil plaatsen, maakt economisch gebruik van de consument achter de PC. Waarom is dat eigenlijk gratis? Het bedrijf betaalt immers wel voor het vervoer van reclameboodschappen in collectieve elektronische media en voor het gebruik van mijn portret in een reclamecampagne in de massamedia. Het bedrijf zal misschien stellen dat het wel degelijk allerlei diensten in ruil hiervoor aan de consument levert. Blijft het feit dat dit soort 'barters' volkomen intransparant zijn. Bovendien draagt de consument in belangrijke mate bij aan de inhoud van de dienstverlening, omdat hij gratis recensies schrijft over bezochte hotels en restaurants of gelezen boeken etc., en doordat zijn geregistreerd aandachtsgedrag een gespecialiseerde en lucratievere dienstverlening mogelijk maakt (ontwikkeling van profielen). Het businessmodel van Google is er op gebaseerd. Uit de overal in databanken verzamelde persoonsgegevens zijn weer nieuwe zelfstandige producten te ontwikkelen, omdat die verzamelingen waardevolle marktinformatie

[29] Zie o.a. "'I've Got Nothing to Hide" and Other Misunderstandings of Privacy', in: *San Diego Law Review* 2007, p. 745-772 en in dat artikel vermelde eerdere publicaties.
[30] Samuelson, a.w. noot 28 en Daniel Solove, geciteerd in Solove & Schwartz, (zie noot 3), p. 438.
[31] Zie Nina Elkin-Koren & Neil Weinstock Nethanel (eds.), *The Commodification of Information*, Den Haag/Londen/New York: Kluwer Law International 2002 (Information Law Series).

bevatten. Waarom zou de consument als 'auteur' van die gegevens niet mee mogen delen in deze exploitatie, zoals hij dat wel doet bij exploitatie van auteursrechtelijke werken? En zou hem dat meer effectieve zeggenschap in termen van transparantie en controle kunnen verschaffen? [32]

Voorop moet worden gesteld dat dit een markt met beperkingen is. Gevoelige persoonsgegevens zijn niet verhandelbaar. Het gaat om de uitwendige gegevens die onze gedragingen aan bepaalde marktkennis of (gewenst of ongewenst) maatschappelijk gedrag koppelen, de dataprofielen waar het de hele marketing op internet en de 'behavioural advertising' (reclameboodschappen gericht op individueel consumentengedrag) om te doen is. Het vragen van een prijs voor persoonsgegevens is niet goed denkbaar zonder enige vorm van collectieve belangenbehartiging. Er moeten, om deze markt te organiseren, dus collectieve belangenbehartigers/tussenpersonen komen. Dat is niet nieuw. De exploitatie van intellectueel eigendom (waar het net als het gebruik van persoonsgegevens gaat om het afrekenen van grootschalige kleine exploitaties, zoals het afspelen van een muzieknummer of het maken van een kopie) is er in toenemende mate op gebaseerd.[33] De markt zal verder met technische en juridische middelen moeten worden georganiseerd, en dat niet zo gemakkelijk zijn, omdat er nog maar heel weinig economisch onderzoek naar dit soort markten is gedaan, laat staan dat gebouwd kan worden op sociale experimenten. Om misbruik te voorkomen zal een systeem moeten worden ontwikkeld voor kwaliteitsmaatstaven van de nieuwe tussenpersonen en zal er toezicht op hun gedragingen en organisatie moeten zijn. Dit kan binnen de aangepaste wetten tot bescherming van persoonsgegevens worden gerealiseerd. De Colleges bescherming persoonsgegevens kunnen het toezicht uitoefenen.

Voor de technische organisatie kan teruggegrepen worden op de ideeën van de Commissie Snellen van 2001 over de Gemeentelijke Basisadministratie.[34] Deze Commissie lanceerde het (niet door de overheid overgenomen) voorstel van het 'digitale kluisje' waarin de burger al zijn persoonsgegevens opslaat en van waaruit hij 'de regie' voert over opslag en gebruik van zijn gegevens, die niet behoren tot de openbare bestanden die de overheid aanlegt. Die digitale kluis was geheel ingebed in de bestuurlijke keten, maar hier zou zij dus privaatrechtelijk in de markt moeten worden ingebouwd. We kunnen twee situaties onderscheiden, namelijk dat de zeggenschap van de eigenaar van de persoonsgegevens zich 'dicht bij' bevindt op de eigen PC, of dat deze (en dat zal steeds vaker het geval zijn) 'op afstand' zal zijn, op het web. In beide gevallen gaat het om beveiligde bestanden met persoonsgegevens die alleen met toestemming van de eigenaar voor gespecificeerde doeleinden op gespecificeerde tijdstippen kunnen worden gebruikt. Dat geldt ook voor de profielen die van de gebruiker worden gevormd op basis van zijn communicatiegedrag. Gaat het om de PC's van de gebruikers dan zullen deze bijvoorbeeld van een gewaarmerkt 'ontcookings'-cookie voorzien kunnen worden, die websites voor het plaatsen van cookies verwijst naar de tussenpersoon die de belangen van de gebruiker behartigt (het kluisje beheert). [35]Daar kunnen ze (tegen betaling) toestemming krijgen voor het plaatsen van cookies in overeenstemming met het gedeponeerde profiel, waarna de PC voor dat doel door de

[32] Zie Corien Prins, 'Property and Privacy: European Perspectives and the Commodification of our Identity', in: Lucie Guibault & P. Bernt Hugenholtz (eds.),*The Future of the Public Domain, Identifying the Commons in Information Law* Den Haag/Londen/New York: Kluwer Law International 2006, p. 223, die er op wijst dat in markt van tailor made producten en diensten deze informatie steeds meer waard wordt.

[33] Ik ga nu voorbij aan de crisis in het collectief beheer, maar dat heeft voor een deel met de gevestigde belangen binnen de wereld van het collectief beheer te maken.

[34] Uitgave van de Tijdelijke Adviescommissie GBA, Den Haag maart 2001. Daarover ook Henk Bos & Olf Kinkhorst, 'De burger aan de knoppen maar dan echt,'in: *Overheidsmanagement* 2001/7-8, p. 199-204.

[35] De Europese Data toezichthouder heeft in zijn Opinion van 18 maart 2010 (*Opinion on Promoting Trust in the Information Society by Fostering Data Projection and Privacy)* onder VIII bepleit dat als een vorm van *privacy by design*, websites zo moeten worden ingericht dat cookies niet zonder toestemming van de 'bezoeker' mogen worden geplaatst.

tussenpersoon op afstand wordt ontgrendeld met een melding aan de gebruiker. Daarbij kunnen ook de verdere gebruiksvoorwaarden van de persoonsgegevens (die de gebruiker vooraf heeft afgestemd met de tussenpersoon) worden gecontracteerd. Om dit op grote schaal te laten draaien is informatietechnologie noodzakelijk, maar onmogelijk is het allemaal niet. Ook prijsvorming zal wel niet zonder problemen gaan, maar schept ook nieuwe mogelijkheden, omdat het de markt transparanter maakt. Zoals de gebruiker nu niet weet wat hij door zijn gedrag aan wie prijs geeft, kan hij nu een gecalculeerd risico nemen en meer persoonsgegevens gerichter tegen betaling prijsgeven. Prijsstelling reguleert de markt, omdat een dataminer beter over zijn verzamelpolitiek inzake persoonsgegevens moet nadenken, aangezien het een kostenpost in zijn bedrijfsvoering wordt. Het grootste deel van spam is een economisch probleem, omdat een reclameboodschap tegen nul kosten kan worden verspreid. Al kost het de spammer maar een fractie van een cent om een boodschap op een individueel adres af te vuren, dan is het al niet meer interessant om dat te doen omdat er dan aan één miljoenste hit niet meer valt te verdienen.

Het kan ook een nieuwe dienstverlening voor Internet Service Providers, leveranciers of informatie bemiddelaars (zoals Google) worden. Google heeft met de dienst *Dashbord* al een stap in die richting gezet. Als we een vergelijking maken met het klassieke massacommunicatiemodel lijkt het zelfs niet onwaarschijnlijk dat het die kant op zou kunnen gaan. In dat massacommunicatiemodel wordt de distributeur (zeg de kabel) door de programma-aanbieders betaald voor het aanleveren van een ongesorteerd publiek (de kabelabonnees). De programma-aanbieders maken daar gesorteerd publiek van (opgesplitst naar programma), waarbij zij reclameboodschappen zoeken. Voor de combinatie van programma en reclameboodschap laten zij zich door de adverteerder betalen. Zelf proberen zij van het publiek betaling te krijgen voor de programma's die zij aanleveren. Het hangt van de verdere marktomstandigheden af hoe de prijsvorming in deze verschillende betaalmomenten verloopt. Het is ook denkbaar dat er een moment komt dat de door de programma-aanbieders aangeleverde informatie interessanter voor de distributeurs wordt om de aangeslotenen op het netwerk vast te houden dan de door de distributeur aangeleverde potentiële klanten voor de programmaleverancier. Dat is echter telkens een punt van onderhandeling in gewijzigde marktverhoudingen.

Je zou het 'soft opt-in' model dat voor e-mail geldt voor alle commercieel gebruik van persoonsgegevens kunnen hanteren, al zal dit velen te ver gaan. In ieder geval zal er transparantie moeten komen. In het nieuwe model levert de ISP individueel ongesorteerd publiek. De zoekmachine is de informatiemakelaar tussen individuele informatievraag en algemeen informatieaanbod die het publiek op individuele basis voorsorteert. Bedrijven als Facebook zijn makelaars in individuele relaties tussen gebruikers. Aan de hand van individueel gedrag van de gebruikers in deze makelaarsrelaties (het dataprofiel) verkopen deze bedrijven individuele reclameboodschappen. Hoe dit model er economisch aan de aanbodzijde verder uitziet, gaat het bestek van dit artikel te buiten. Essentieel is dat er ook in dit model voor de aansluiting op het publiek toestemming (tegen betaling) gevraagd moet worden, maar dat dit nu niet gebeurt.

Het bijkomende grote sociale voordeel van dit systeem is dat het transparantie en controle - die het publiekrechtelijke toezicht op microniveau niet meer kan bieden - terugbrengt bij de consument. Lessig: 'Property talk would give privacy rhetoric added support within American culture. If you could get people to see certain resource as property, then you are 90 percent to your protective goal.'[36] Dit geldt mijns inziens ook voor Europa. De transparantie krijgt de

[36] Lawrence Lessig in 'Privacy as Property', 69 *Social Research* p. 255 (2002), geciteerd bij Corien Prins, 'Property and Privacy: European Perspectives and the Commodification of our Identity', in: Lucie Guibault & P. Bernt Hugenholtz (eds.),*The Future of the Public Domain, Identifying the Commons in Information Law* Den Haag/Londen/New York: Kluwer Law International 2006, p. 227, noot 10.

gebruiker doordat hij telkens een overzicht van zijn tussenpersoon heeft van de verzamelingen persoonsgegevens en profielen die er over hem in omloop zijn. De tussenpersoon kan ook het gebruik blijven monitoren en eventueel als gemachtigde voor een klant of een groep van klanten optreden om bevoegdheden op grond van de privacy en telecommunicatiewetgeving uit te oefenen om de kwaliteit van de opslag en het gebruik in de gaten te houden.

Let wel, ik bepleit niet dat dit in de plaats moet komen van publiekrechtelijk toezicht. Het is eerder 'en' 'en'. Ingewikkelde markten waarin op allerlei fronten misbruikrisico's dreigen vergen publiekrechtelijke regulering en toezicht.

8. De omkering van het perspectief: VRM of Vendor Relation Management

In de Verenigde Staten is aan de Universiteit van Harvard een zogenaamd 'Vendor Relation Management' systeem ontwikkeld als reactie op 'Customer Relation Management'. Voor VRM zijn beginselen ontwikkeld, ik citeer:[37]

1. Relationships are voluntary.
2. Customers are born free and independent of vendors.
3. Customers control their own data. They can share data selectively and control the terms of its use.
4. Customers are points of integration and origination for their own data.
5. Customers can assert their own terms of engagement and service.
6. Customers are free to express their demands and intentions outside any company's control.

These can all be summed up in the statement *Free customers are more valuable than captive ones*. In a broader way, the same should be true of individuals relating to organizations. With VRM, however, our primary focus is on customer relationships with vendors, or sellers.

VRM heeft een set instrumenten in ontwikkeling om de verschuiving van een op 'datamining' gebaseerd model waarin de consument het willoze object is, naar een door de consument aangestuurd 'data vending' concept. In dit artikel heb ik geprobeerd een juridische fundering aan een dergelijk concept te geven: gegevensbeheer als onderdeel van een moreel/commercieel privacy zelfbeschikkingsrecht.

Er zijn natuurlijk ook grote nadelen die niet alleen liggen in de complicaties bij de uitvoering. Een groot nadeel is het veiligheidsdenken. De beschikbaarheid van ontgrendelbare persoonsprofielen zal opsporings- en veiligheidsautoriteiten gretig maken om daar toegang toe te eisen. De misbruikrisico's zijn ook niet gering. Maar die zijn er in huidige model ook.

9. Conclusie

De artikelen 7 en 8 van het EU Charter markeren de tweesprong tussen privacy en dataprotectie. Tegelijk verwijst lid 1 derde volzin van artikel 6 van het EU Verdrag naar titel VII van het Charter. Daar staat in artikel 52 lid 3 dat de rechten en vrijheden van het Charter worden uitgelegd overeenkomstig de rechten en vrijheden van het EVRM. Artikel 6 lid 3 zegt bovendien dat EVRM rechten als rechtsbeginselen deel uitmaken van de EU. Dit is de weerslag van de *acquis communautaire* jurisprudentie van het HvJEG, dat langs deze omweg grondrechten is gaan toepassen binnen de oorspronkelijk als economische orde gedachte EU rechtsorde. Dat betekent mijns inziens dat de tweesprong van de artikelen 7 en 8 kan worden teruggebracht tot twee aspecten van hetzelfde zelfbeschikkingsrecht, zoals het door het EHRM op basis van artikel 8

[37] http://cyber.law.harvard.edu/projectvrm/Main_Page, geraadpleegd december 2009.

EVRM is ontwikkeld. De Europese Privacy richtlijn verzet zich er niet tegen dit zelfbeschikkingsrecht via privaatrecht uit te oefenen.[38]

In dit artikel heb ik geprobeerd te laten zien dat privacy en persoonsgegevens loten zijn van hetzelfde recht, namelijk het recht om controle uit te oefenen over de *binnenkant* van zijn privéleven, die zowel een fysieke als informationele begrenzing (het 'geheim') is van de buitenwereld, en de *buitenkant* van zijn privé leven (de publieke persona), die betrekking heeft op de informatie die over hem wordt verspreid. De binnen- en buitenkant vormen communicerende vaten. Daarom moet het individu over beide kanten een zelfbeschikkingsrecht kunnen uitoefenen.

In dit artikel heb ik geen onderscheid gemaakt tussen 'gevoelige' persoonsgegevens die wel onder het zelfbeschikkingsrecht zouden vallen en 'niet- gevoelige' gegevens die daar niet onder zouden vallen, omdat uit een oogpunt van zelfbeschikking dat onderscheid zinledig is. Wel is het zo dat de publieke sfeer steeds meer claims op het individu legt. Die claims moeten vanuit mijn optiek geconstrueerd worden als dwanglicenties. Een verder argument om het onderscheid niet te maken, is dat bij de voortschrijding van de techniek van de datamining van ieder 'ongevoelig' gegeven door analyse een 'gevoelig' gegeven valt te maken.

Het heeft geen zin om het privacyrecht uiteen te laten vallen in verschillende rechten, ook al hebben verschillende aspecten van het privacyrecht een eigen geschiedenis en ontwikkeling gekend. Het heeft dus geen zin om te spreken over, 'recht op reputatie', 'right of publicity', enzovoort. Misschien is het juister de informationele privacy als het kernrecht te omschrijven, en het relationele privacyrecht dat tegen de fysieke inbreuken op de privésfeer ziet onder te brengen bij recht op lichamelijke integriteit en huisrecht.

Zowel de binnen- als de buitenkant heeft een moreel en economisch aspect. Wie aan de binnenkant tegen zijn wil wordt waargenomen kan daarvan morele schade ondervinden. Het heeft ook economische waarde, bijvoorbeeld in de vorm van het nog niet gepubliceerde werk of (geheime) biografische feiten van beroemde personen. Aan de buitenkant hebben we het dubbelaspect leren kennen aan het portretrecht, dat om historische redenen binnen het auteursrecht is ontwikkeld, maar daar niet thuis hoort. Publicatie van een portret tegen zijn wil kan morele, maar ook economische schade vertegenwoordigen. Het portretrecht is een persoonsgegeven bij uitstek. Vanuit het portretrecht kunnen wij het dubbelaspect van alle persoonsgegevens herkennen en de noodzaak inzien om de beschikking over persoonsgegevens als een zelfbeschikkingsrecht te zien.

Het recht op beschikking over persoonsgegevens als zelfbeschikkingsrecht kan de burger terug brengen in het dataprotectierecht. Dat heeft zich boven zijn hoofd ontwikkeld tot een procedureel in publiek recht verankerd recht dat gaat over inrichting van administraties. Daar gaat het over responsability, accoutability, liability, privacy by design, en niet te vergeten een papieren muur van accoutantsverklaringen. Commercieel gezien kan het de omkering van het perspectief betekenen van een customer relation management naar een vendor relation management (VRM), waarin de consument centraal komt te staan.

De organisatie van een markt van persoonsgegevens als een markt van verhandelbare licenties, vergt techniek en organisatie en zal nooit in de plaats kunnen komen van publiekrechtelijk toezicht, er wel een welkome aanvulling op kunnen zijn. Wie weet, gaat in een ook voor

[38] Corien Prins, 'Property and Privacy: European Perspectives and the Commodification of our Identity', in: Lucie Guibault & P. Bernt Hugenholtz (eds.),*The Future of the Public Domain, Identifying the Commons in Information Law* Den Haag/Londen/New York: Kluwer Law International 2006, p. 242.

gebruikers transparante markt privacy op leefniveau weer leven, worden ze daardoor weerbaarder (consumentenbescherming!) en hoeft er geen oorlog uit te breken om dat voor elkaar te krijgen. Tegen de tijd dat we de Buma voor het auteursrecht kunnen afschaffen, kunnen we die voor persoonsgegevens oprichten.