

Privacy als het zelfbeschikkingsrecht van de 21e eeuw

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)

Egbert Dommering*

Persoonsgegevens zijn in de 21e eeuw een belangrijke grondstof geworden. 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 politiek 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. 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?

De Amerikaanse boulevardpers zorgde aan het eind van de 19e eeuw in de Verenigde Staten voor het eerste privacyconcept: *the right to be let alone*. De informatietechnologie die hierbij centraal stond was de met teledoziers de privé-sfeer binnendringende fotografie en af luisterapparatuur. De Amerikaanse rechtgeleerden Warren en Brandeis die dat recht om alleen te worden gelaten in 1890 formuleerden, gebruikten het voorbeeld van de op het toilet gefluisterde mededeling die door af luisterapparatuur van de daken wordt geschreeuwd.

Dat recht om alleen gelaten te worden erkennen we inmiddels wereldwijd. In Europa is het te vinden in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM). Het Europees Hof voor de Rechten van de Mens (EHRM) heeft dat recht verder ontwikkeld. Een mijlpaal is de beslissing begin deze eeuw in de zaak van prinses Caroline van Monaco, die al jaren in een verbitterde strijd met de boulevardpers verwickeld was. Het Hof oordeelde dat ook al ben je bekend en daardoor een gewilde prooi voor roddelbladen, je niet hoeft te tolereren dat je overal in de openbare ruimte wordt gefotografeerd en afgeluisterd.

Op het gebied van persoonsgegevens nam Europa het voortouw. 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 informatiele 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.' Hier gaat het dus niet om de gefluisterde mededeling die tegen de wil van de fluisteraar in de openbaarheid wordt gebracht, maar om de geheime af luisteraar die gegevens over openbaar gedrag van een ander in het geniep vastlegt en doorfluistert. 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 informatiele 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. Over dat recht wil ik het hier hebben.

De inzet op controle van macht heeft gemaakt dat wij het zelfbeschikkingsrecht 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 toezicht houdende instantie (een College *bescherming* persoonsgegevens) die preventief (vooraf) en repressief (achteraf) toeziet op naleving van die regels.

De kern van dat zelfbeschikkingsrecht 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 inzage recht) welke gegevens er over hem zijn opgeslagen en verwerkt (*transparantiebeginsel*), er mogen niet meer gegevens worden bewerkt en bewaard dan voor het gerechtvaardigde doel nodig is (*proportionaliteitsbeginsel*), en de kwaliteit en

* Prof. mr. E. J. Dommering is hoogleraar informatierecht aan de Universiteit van Amsterdam (IViR) en advocaat te Amsterdam (Brinkhof).

juistheid van de gegevens moeten zijn gewaarborgd en kunnen door het datasubject worden afgedwongen (*kwaliteitsbeginsel*). Het zelfbeschikkingsrecht werd in 1983 in artikel 10 van onze Grondwet opgenomen: het vormde een welkome aanvulling op eerder geformuleerde rechten op bescherming tegen machts-uitoefening. Ook in de jaren tachtig begon het EHRM artikel 8 EVRM uit te leggen als een recht op zelfbeschikking over je persoonsgegevens.

De regels en het toezicht kregen vorm in de ons nu bekende dataproductiewetten 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 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 bijzonder effectief. 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.

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 Bezettingssautoriteit het Amsterdamse bevolkingsregister misbruikte om razzia's te houden op joodse burgers, was weggezaakt in de geschiedenis. Daar denkt de consument die Air Miles spaart niet aan. Maar er ging meer fout met het ideaal van de informatieve 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 beleidsfeer. 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.

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, 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.

Collectieve belangenbehartiging door de Colleges bescherming persoonsgegevens is tegenwoordig een illusie. Door de omvang en complexiteit van het gegevensverkeer en -opslag kunnen zij zich niet meer bezighouden met de individuele burger. Zij hebben zich teruggetrokken op hun kerntaken, waarin nog slechts plaats is voor een selectief vervolgingsbeleid als daarbij een voldoende algemeen belang is betrokken.

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.

Het veiligheidsdenken is een politiek probleem dat de burger niet kan oplossen. Dat zullen politici moeten doen, en zolang die in de kramp van een deels door hen zelf gevoede terreurangst leven, zullen ze dat niet doen. Maar kan de burger misschien meer macht uitoefenen op het microniveau? Laten we daarvoor nog eens kijken naar dat informatieve zelfbeschikkingsrecht.

We hebben dat recht in Europa geformuleerd als een grondrecht dat ons privé-leven beschermt tegen inmenging van de staat en anderen, en als een zeggenschapsrecht om de macht van de staat en anderen over ons privé-leven te beperken. Maar privacy heeft ook trekken gemeen met economisch zelfbeschikkingsrecht, zonder het meteen op een lijn te stellen met eigendomsrecht.

Dat economische aspect van privacy wordt erkend in het portretrecht. Een portret, onze 'buitenkant', is een persoonsgegeven dat wij als privé-persoon buiten de privé-sfeer (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 advertentiecampaignede) wordt gebruikt. Een portret is een (sterk) persoonsgegeven. Waarom zouden andere persoonsgegevens (ons adres en onze tot de persoon herleidbare gedragingen) wel vogelvrij zijn?

Zijn persoonsgegevens om te vormen tot het ‘digitale geld’ waar de geciteerde Eurocommissaris het over had?

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. 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 voor 90% op gebaseerd. Uit de overal in databanken verzamelde persoonsgegevens zijn weer nieuwe zelfstandige producten te ontwikkelen, omdat die verzamelingen waardevolle markt-informatie 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? Het lijken mij legitieme vragen. Ik pleit daarom voor het organiseren van een markt van persoonsgegevens. Eenvoudig is dat niet.

Voorop moet worden gesteld dat dit een markt met beperkingen is. Gevoelige persoonsgegevens zijn niet verhandelbaar, tenzij met uitdrukkelijke toestemming van het datasubject. 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 afspele van een muzieknummer of het maken van een kopie) is er in toenemende mate op gebaseerd. De markt zal verder met technische en juridische middelen moeten worden georganiseerd. 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.

De pc’s van de gebruikers zullen van een gewaarmerkte ‘ont-cookings’-cookie voorzien moeten worden, die websites voor het plaatsen van cookies verwijst naar de tussenpersoon die de belangen van de gebruiker behartigt. Daar kunnen ze tegen betaling toestemming krijgen voor het plaatsen van cookies overeenkomstig het gedeponeerde profiel, waarna de pc voor dat doel door de 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 lijkt het me allemaal niet. Ook prijsvorming zal wel niet zonder problemen gaan, maar scheidt ook nieuwe mogelijkheden, omdat de markt

transpanter 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 gericht tegen betaling prijsgeven. Prijsstelling reguleert de markt, omdat een *data-miner* beter over zijn persoonsgegevens verzamelpolitiek 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 worden. Als we een vergelijking maken met het klassieke massacommunicatiemodel lijkt het zelfs niet onwaarschijnlijk dat het die kant op zou kunnen gaan. In dat model 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.

Waar het om gaat is dat er voor de toegang tot het publiek wordt betaald. 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. Waar het om draait is dat er ook in dit model voor de aansluiting op het publiek betaald zou moeten 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. De transparantie krijgt de gebruiker doordat hij telkens een overzicht van zijn tussenpersoon heeft welke cookies door wie op zijn of haar pc zijn geplaatst. 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.

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 wie weet, gaat in een ook voor 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.