

**Toespraak van mr. M.W. McLaggan t.g.v. het congres van de Vereniging Privacy
Recht op 24 maart 2011. Gesproken woord geldt.**

Dames en heren,

Er was eens een koning in India, en die veroordeelde een man tot de galg. Toen de koning zijn oordeel had uitgesproken, zei de veroordeelde: "U bent een wijs man, Majesteit. U bent nieuwsgierig naar alles wat uw onderdanen doen. U heeft respect voor goeroe's, slangenbezweerders en fakirs. Toen ik nog een jongen was, heeft mijn grootvader me geleerd hoe ik een wit paard kan laten vliegen. En omdat er niemand anders is in dit koninkrijk die weet hoe dit moet, moet u mijn leven sparen."

De koning liet onmiddellijk een wit paard komen.

"Ik heb twee jaar nodig om het paard te leren vliegen," zei de man. "OK, u krijgt twee jaar," antwoordde de koning, enigszins argwanend. "Maar als het paard niet leert vliegen, wordt u alsnog opgehangen." Dolgelukkig ging de man met het paard op weg naar huis. Toen hij thuiskwam, vond hij zijn hele familie in tranen. "Ben je gek geworden?" huilden ze, "sinds wanneer heeft iemand in dit huis ooit geweten hoe een paard te leren vliegen?"

"Maak je geen zorgen," antwoordde hij. "De koning is oud en kan de komende twee jaar doodgaan. En ook het paard kan de komende twee jaar sterven, en dan heb ik opnieuw twee jaar om een ander paard te leren vliegen. Zelfs als alles precies zo blijft als het nu is, dan heb ik twee jaar gewonnen. Maar vergeet vooral niet dat niemand ooit nog heeft geprobeerd om een paard te laten vliegen, en het zou best kunnen dat het paard vleugels krijgt".

Dit congres is gewijd aan de toekomst van privacyrecht. Er zijn wellicht onder u mensen die ervan uitgaan dat er niets verandert, dat de wet wordt afgeschaft, of de toezichthouder, of beide. Maar het is ook mogelijk dat het paard vleugels krijgt of dat u het paard leert vliegen.

Als toezichthouder is het CBP betrokken bij de evaluatie van de bestaande wetgeving, ook op Europees niveau, via de Artikel 29-werkgroep.¹ Daar wil ik het vandaag niet zozeer over hebben. Vandaag wil ik de ervaringen delen van de toezichthouder met een aantal materiële beginselen die voortvloeien uit de EU-richtlijn. Een selectie van een paar principes die het fundament vormen van privacywetgeving en waarvan de invulling beïnvloed is en wordt door technologische ontwikkelingen.

Hoe houdbaar zijn deze principes in het informatietijdperk en wat betekent dit voor de werkwijze en rol van het CBP als toezichthouder? Het gaat om de begrippen persoonsgegevens, transparantie, toestemming en doelbinding, toegespitst op derdenverstrekking.

Persoonsgegevens

Een belangrijk begrip dat raakt aan de reikwijdte en doelmatigheid van de wet is de definitie van het begrip persoonsgegevens. De wetgever heeft bij de invoering van de Wet bescherming persoonsgegevens bewust geanticipeerd op nieuwe technologische ontwikkelingen. In de wetsgeschiedenis is herhaaldelijk onderstreept dat de invulling van het begrip gelijke tred dient te houden met de voortschrijdende informatietechnologie.

Een gegeven dat op een bepaald moment nog "redelijkerwijs niet identificeerbaar" is omdat identificatie een disproportionele aanwending van geld en middelen zou vergen, en daarom niet als persoonsgegeven kan worden aangemerkt, kan met voortschrijdende informatietechnologie tot een persoonsgegeven worden omdat de identificatie dan gemakkelijk is geworden. Het omslagpunt zal afhangen van de beoordeling van de mogelijkheden van de techniek in het concrete geval.²

¹ Brief CBP aan de leden van de Eerste Kamer, 12 november 2010, met bijlage "The Future of Privacy – Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data" van de artikel 29-werkgroep van 1 december 2009. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

² Kamerstukken II, 25 892, nr. 9, blz 1-2.

Bij die herleidbaarheid is van groot belang dat dergelijke gegevens niet *voor een ieder* herleidbaar hoeven te zijn. Uit de memorie van toelichting volgt dat gekeken moet worden naar alle middelen die redelijkerwijs door de verantwoordelijke dan wel enig ander persoon zijn in te zetten om een persoon te identificeren. Het criterium is dus dat het volstaat dat de verantwoordelijke de gegevens zonder onevenredige inspanning kan verbinden aan een natuurlijk persoon. Om te beoordelen of die inspanning disproportioneel is, heeft de wetgever bepaald dat de specifieke mogelijkheden van die verantwoordelijke zwaar moeten meewegen:

*Uitgegaan moet worden van een redelijk toegeruste verantwoordelijke. In concrete gevallen moet echter wel rekening worden gehouden met bijzondere expertise, technische faciliteiten en dergelijke van de verantwoordelijke.*³

In de dagelijkse realiteit spelen nummers steeds vaker een rol, in plaats van namen. De ordeningsstructuren zijn niet meer fysiek; we raken op andere manieren verbonden met technologie. Onze internetmobieltjes zenden voortdurend unieke nummers uit, waarmee we feilloos kunnen worden onderscheiden van elke andere passant. Dankzij die unieke nummers kunnen we gevolgd worden, geïnformeerd worden, verleid tot een aankoop, of juist bewust uitgesloten van een aanbieding. Op grond van analyse van ons eigen gedrag en het gedrag van anderen die in hetzelfde hokje zijn beland, kunnen uitgebreide voorspellingen worden gedaan over onze toekomstige wensen en verlangens. Zodanig uitgebreid dat je zelf geen zoekopdrachten meer hoeft in te voeren in een zoekmachine. *“Google will just know”* aldus voormalig Google-topman Eric Schmidt begin februari tijdens een toespraak in Davos.⁴

³ Kamerstukken II, nr. 3, 25 892, blz. 48-49.

⁴ Google's Eric Schmidt predicts the future of computing - and he plans to be involved, Telegraph, 5 februari 2011, URL: <http://www.telegraph.co.uk/technology/google/8303847/Googles-Eric-Schmidt-predicts-the-future-of-computing-and-he-plans-to-be-involved.html>

Het gaat hier om een maatschappelijke context waarin technologisch goed toegeruste verantwoordelijken individuen herkennen en in kaart kunnen brengen met behulp van unieke nummers. Dat dit technologisch mogelijk is geworden, is in abstracte zin voorzien door de wetgever, en heeft consequenties voor de invulling van de definitie.

Transparantie

Op grond van de algemene dataproductierichtlijn (95/46/EG) dienen partijen die persoonsgegevens verwerken personen te informeren over het bestaan en de doeleinden van de verwerking.

De informatieplicht vloeit voort uit de gedachte dat transparantie een ieder in de gelegenheid stelt om na te gaan wie gegevens over hem vastlegt, en waarom. Een geïnformeerde burger kan zijn rechten uitoefenen als hij constateert dat een verwerking onrechtmatig is, zoals vragen om inzage, correctie of verwijdering. Een geïnformeerde burger weet van tevoren welke specifieke handelingen het bedrijf wil verrichten met zijn gegevens. En hij weet dat hij opnieuw wordt geïnformeerd als het bedrijf andere dingen wil doen met zijn persoonsgegevens. En als dat hem niet zint, stapt hij over naar een andere dienstverlener.

Transparantie is daarmee lang gezien als de belangrijkste waarborg voor de bescherming van het recht van betrokkenen op bescherming van hun persoonlijke levenssfeer en hun persoonsgegevens. Dat was zo ten tijde van de Wet persoonsregistraties, toen er nog een overzichtelijk aantal databanken was – enorme kamers voorzien van ponskaartmachines. Dat bleef zo toen de Europese richtlijn, en later de Wet bescherming persoonsgegevens tot stand kwamen. De Registratiekamer schreef in haar advies over de Wbp in 1997 ervan overtuigd te zijn: *“dat deze wet zal leiden tot een grotere zichtbaarheid van het gegevensverkeer voor de betrokken personen. en een scherpere afbakening van bevoegd en onbevoegd gebruik in relatie tot het doel waarvoor de gegevens verkregen zijn. Ook zullen betrokkenen op basis van de nieuwe regeling beter in staat zijn voor hun belangen op te komen.”*⁵

⁵ Registratiekamer, z1996-00562, Advies Wbp, februari 1997.

Inmiddels heeft het aantal databases en verwerkingen een veel grotere vlucht genomen dan in de jaren negentig werd voorzien. Het aantal en de soorten verwerkingen van persoonsgegevens, al dan niet in de vorm van koppelingen en afgeleide profielen, zijn volstrekt ondoorzichtig geworden, ondanks de beoogde grotere zichtbaarheid.

Neem bijvoorbeeld de marktpartijen die betrokken zijn bij het tonen van reclamebanners op websites, de display advertenties. Uit een recent overzicht van de Nederlandse markt, gemaakt door een van die marktpartijen⁶, blijkt dat er ten minste vijftien soorten bedrijven betrokken zijn bij deze handel, in rollen variërend van zogenaamde 'Yield Optimisers' tot aan 'Ad Exchanges' en 'Demand Side Platformen'. In elk van de vijftien rubrieken zijn talloze bedrijven vertegenwoordigd, van start-ups tot mondiale spelers met een wereldwijd bereik.

Het landschap waarvan we transparantie verwachten is dus volledig veranderd, van een overzichtelijk geheel van een paar grote databases beheerd door professionele partijen naar een kluwen van nationale en internationale bedrijven. Daarin spelen nieuwe soorten bedrijven een rol, die complexe diensten aanbieden. Feit is ook dat door het wegvallen van territoriale beperkingen een kleine start-up in een paar jaar tijd kan uitgroeien tot wereldwijde marktleider.

Het valt voor een gemiddelde burger nauwelijks nog te doorgronden welke partijen persoonsgegevens over hem verwerken, aan wie ze die persoonsgegevens verstrekken, en voor welke doeleinden. Uit onderzoek door de Engelse consumentenorganisatie *Which?* blijkt dat bijna driekwart van de Britten niet weet wat online behavioural advertising is.⁷

De tekst van sommige privacyverklaringen levert bepaald geen bijdrage aan het begrip van consumenten over de verwerkingen.

⁶ Improve Digital, schema's van de display advertising markt in Nederland en Europa, URL: <http://www.improvedigital.com/market-map-2010>

⁷ Onderzoek door het tijdschrift *Which?* in oktober 2010 onder 1.000 Engelse internetgebruikers. 74% van de ondervraagden had nog nooit gehoord van OBA (online behavioural advertising).

Herkent u de zinsnede: *Wij kunnen uw gegevens delen met derden om u betere diensten te kunnen aanbieden.*

of:

Wij slaan alle informatie op die u via onze website invoert of ons op enige andere wijze verstrekt. Ook informatie die wij uit andere bronnen ontvangen voegen wij toe aan de informatie over u.

De informatieplicht mag niet verworden tot een louter juridische verplichting, tot een procedurele formaliteit.

Dat is tegengesteld aan wat de wetgever nationaal en Europees heeft beoogd. Begrijpelijke informatie is een essentiële voorwaarde voor een op feitelijke informatie gebaseerde vrije keuze.

Naarmate de complexiteit van gegevensverwerkingen toeneemt, wordt het belangrijker dat informatie duidelijkheid biedt, juist ook over het bestaan van gegevensverwerkingen die je in werkelijkheid niet eens meer kunt opmerken.

Wat betekent deze ontwikkeling voor de wijze waarop het CBP als toezichthouder opereert? De toenemende complexiteit betekent dat we als toezichthouder hoge prioriteit geven aan de kwaliteit van de informatie als waarborg voor een behoorlijke gegevensverwerking. Dat betreft niet alleen een toets aan artikel 33 en 34 van de Wbp, maar ook de meer fundamentele toets of er wel een grondslag is voor de gegevensverwerking op grond van artikel 8 Wbp en of de gegevensverwerking daarmee behoorlijk en zorgvuldig is, conform artikel 6 Wbp. De kwaliteit van de informatie is daarmee ook een belangrijk element bij de beoordeling van de legitimiteit van een beroep op toestemming als grondslag.

Internet biedt ongekende mogelijkheden om heel uitgebreid te informeren, maar tegelijkertijd worden de beeldschermen kleiner en de aandachtsspanne korter. In dat spanningsveld kunnen bedrijven niet lichtvaardig concluderen dat de consument toch toestemming heeft gegeven, en dat het dus in orde is.

Doelbinding en derdenverstrekking

Nauw verwant aan transparantie en toestemming is het beginsel van doelbinding. De essentie van doelbinding is dat het grenzen stelt aan de toegestane gegevensverwerkingen. Doelbinding ziet zowel op het vaststellen en vastleggen van specifieke en gerechtvaardigde doeleinden bij verzameling, als op het toetsen van de verenigbaarheid van verdere verwerkingen aan die doeleinden. Je verzamelt gegevens voor een welbepaald doel, en het is in beginsel niet toegestaan om de gegevens voor een ander doel te gebruiken, tenzij je een beroep kunt doen op een van de uitzonderingen uit artikel 9 Wbp.

Bij direct marketing hoort derdenverstrekking vaak bij het doel van de verzameling. Nederlandse directmarketingbedrijven hebben in de vroege jaren negentig een rol gespeeld bij de totstandkoming van de algemene dataproductierichtlijn.⁸ Aan de specifieke grondslagen zoals toestemming of wettelijk voorschrift is aan de richtlijn een balansbepaling toegevoegd. Artikel 7 onder f maakt het mogelijk om een beroep te doen op een gerechtvaardigd belang om gegevens te verwerken, inclusief derdenverstrekking.

Daarbij zijn in de richtlijn wel grenzen bepaald. Conform de richtlijn, zoals vrijwel letterlijk vertaald in artikel 8 onder f van de Wbp, moet de verwerking noodzakelijk zijn en voldoen aan de vereisten van proportionaliteit en subsidiariteit. Daarnaast dient de verantwoordelijke zijn eigen belang nog eens apart af te wegen tegen het belang van betrokkenen bij de bescherming van hun persoonlijke levenssfeer.

⁸ De Nederlandse inbreng op de richtlijn is beschreven in D. Korff, Data protection law in practice in the European Union, Federation of European Direct Marketing (FEDIM), 1993.

Bovendien geldt bij toepassing van deze grondslag ook onverkort het bepaalde in artikel 9 Wbp. Naast de toets op het gerechtvaardigd belang moet de verenigbaarheidstoets worden doorlopen. Daarbij speelt transparantie opnieuw een fundamentele rol. In de eerste plaats is gerichte online marketing vrijwel onzichtbaar geworden voor mensen, in tegenstelling tot de papieren reclamefolders die op de deurmat vielen. En in de tweede plaats laat de praktijk zien dat internetbedrijven voortdurend gebruik maken van nieuwe mogelijkheden om persoonsgegevens te gelde te maken.

Met vooruitziende blik is de wetgever in de memorie van toelichting specifiek ingegaan op de risico's van heimelijke profilering.

*Wordt iemand geconfronteerd met een profiel van zijn persoon dat zonder zijn toestemming van hem is vervaardigd en voor commerciële doeleinden wordt aangewend, bij voorbeeld om hem te benaderen, dan is het niet onredelijk wanneer hij dit als een inbreuk op de persoonlijke levenssfeer ervaart. Van belang in laatstgenoemd geval is vooral dat de gegevens buiten de betrokkene om zijn verkregen en deze gegevens bovendien zijn verwerkt tot een specifiek voor die persoon geldend profiel zonder deze persoon daarbij op enigerlei wijze te betrekken. Onder die omstandigheden zal veel eerder van onverenigbaarheid sprake zijn.*⁹

Staat het principe van doelbinding daarmee in de weg aan innovatie? Nee, dat hoeft geenszins het geval te zijn. Doelbinding is geen statische toets. Het dient een vast onderdeel te zijn van de besluitvorming over nieuwe producten en diensten en nieuwe derdenverstrekkingen. Zodra een bedrijf kansen ziet in nieuwe verwerkingen van persoonsgegevens, dient het zich af te vragen of ze verenigbaar zijn met de oorspronkelijke doeleinden. Om niet te struikelen over verenigbaarheid, is het van belang om op voorhand de mogelijke negatieve gevolgen in kaart te brengen (bijvoorbeeld door een *privacy impact assessment*) en om technische waarborgen in te bouwen voor betrokkenen (zoals *privacy by default*). Als de toets toch negatief uitvalt, betekent dat nog steeds niet dat de verwerking niet is toegestaan. Het betekent dat het betreffende bedrijf toestemming moet vragen voor de nieuwe verwerking.

⁹ Kamerstukken II, nr. 3, blz. 91.

Exemplarisch voor de wijze waarop het CBP omgaat met deze problematiek is het onderzoek dat het CBP in 2009 deed. Het ging om gegevensverwerkingen door een bedrijf dat verantwoordelijk was voor een aantal websites met uitgebreide vragenlijsten. Het CBP concludeerde dat het bedrijf de deelnemers onvoldoende informeerde over de verschillende doeleinden waarvoor de gegevens werden verzameld en verwerkt. Het bedrijf volstond ten onrechte met een verwijzing naar de algemene voorwaarden waarin 'zorgvuldig geselecteerde partners' waren vermeld aan wie -niet nader omschreven- gegevens konden worden verstrekt.

In de praktijk verzamelde het bedrijf ook gevoelige en bijzondere persoonsgegevens en gebruikte die om groepen betrokkenen te selecteren voor *hostmailings* ten behoeve van derde partijen. Ook bleek het bedrijf contactgegevens en kenmerken die afgeleid waren uit antwoorden op vragen via listbrokers aan derde partijen te verstrekken voor directmarketingdoeleinden. Deze derdenverstrekkingen waren niet uitdrukkelijk omschreven, laat staan dat klanten erover waren geïnformeerd.

Nadat het CBP in december 2009 zijn bevindingen publiceerde, zag het bedrijf zich gedwongen tot een ommekeer. Het bedrijf stuurde zijn klanten uitgebreide informatie en vroeg hen om gerichte toestemming voor de verschillende verwerkingen.¹⁰ Alle klanten die niet reageerden, werden uit de bestanden vernietigd.

Gelukkig biedt communicatietechnologie ook nieuwe oplossingen om persoonsgegevens te beschermen. Door goed na te denken over de risico's en door de behoefte van burgers centraal te stellen kunnen verantwoordelijken ook manieren verzinnen om hun klanten in één oogopslag te informeren. Een voorbeeld daarvan is de manier waarop een groot advertentienetwerk het mogelijk maakt om online, elk

¹⁰ CBP, 'CBP sluit onderzoek naar internetbedrijf Advance, Verstrekking gevoelige gegevens van internetters aan derden niet toegestaan', 18 december 2009, URL: http://www.cbpweb.nl/Pages/pb_20091218_advance_bevindingen.aspx en: CBP, '(Herstel) maatregelen internetbedrijf Advance leiden tot beëindiging vervolprocedure', 24 augustus 2010, URL: http://www.cbpweb.nl/Pages/einde_vervolprocedure_advance.aspx

moment van de dag, in te zien in welke belangstellingscategorieën iemand is ingedeeld, en zich daartegen met één muisklik te verzetten.

Conclusie

De wetgever heeft ervoor gekozen om met open normen te werken om het beschermingsniveau van de Wbp zoveel mogelijk technologie-onafhankelijk te maken. Deze wens keert terug in de huidige discussie rond de herziening van het Europese en Nederlandse wettelijk kader. Open normen krijgen invulling al naar gelang het voortschrijden van de technologie.

In het huidige informatietijdperk speelt transparantie een sleutelrol in het bereiken van het resultaat dat de wetgever voor ogen stond, te weten een verantwoord beschermingsniveau waar de burger aanspraak op kan maken.

Het is nu aan u, om uw cliënten bij te staan om hun verwerkingen transparant te maken. En als uw cliënt weigert, met een beroep op de onmogelijkheid, onzinnigheid of onduidelijkheid van de wet, kunt u altijd nog een wit paard van stal halen. Maar wilt u dat risico werkelijk lopen?