

Lustrumcongres - Nederlands Juristen Comité voor de Mensenrechten (NJCM)

"16 Miljoen BN'ers - Bescherming van persoonsgegevens in het digitale tijdperk"

Den Haag, 8 oktober 2009

Peter Hustinx

Europees Toezichthouder voor gegevensbescherming

Dames en heren,

Ik wil beginnen met het NJCM geluk te wensen met zijn verjaardag; 35 jaar is een beetje tussen jeugd en vergevorderde volwassenheid in. Maar het is een goed moment en ik moet bekennen dat ik een groot deel van die groei van het NJCM heb meegemaakt. Ik heb het vanochtend nog gecontroleerd, ik heb de elfde jaargang van het *NJCM-Bulletin* in mijn kast aangetroffen, kennelijk daarvoor had ik dat nog niet allemaal zo scherp op mijn radar staan, maar nu heel duidelijk. In de tweede plaats wil ik de organisatoren geluk wensen met de keuze van dit thema, want zoals het verloop van deze ochtend al laat zien het gaat over heel erg veel. Dit is niet een thema waar een strikt juridisch betoog toereikend is. Het gaat over een structureel onderwerp in onze samenleving. Daarbij rijst soms ook de vraag: wat is eigenlijk het probleem? Ik wil daar in het verloop van mijn opmerkingen wat over zeggen, maar ik wil beginnen met twee kanttekeningen bij de titel van het congres, want dat geeft me de ingang tot de kern van de zaak.

Het onderwerp van het congres

De titel zegt: 'bescherming van persoonsgegevens in het digitale tijdperk'. Mijn eerste punt daarbij is dat het natuurlijk niet alleen gaat om de bescherming van persoonsgegevens, maar vooral om de bescherming van de mensen op wie die persoonsgegevens betrekking hebben. Het begrip persoonsgegeven is alleen maar een *trigger*, een grensafbakening. Vanaf dat moment begint het stelsel van waarborgen te werken. En het is eigenlijk een *misnomer*, die zijn oorsprong kent in Duitsland en vanaf het eerste moment heeft men die term *Datenschutz*, *data protection*, gegevensbescherming overgenomen. Maar als u gaat naar de vroegste

stukken en ook de toelichting bij het Verdrag van de Raad van Europa leest, dan vindt u daar dat dit een grondrecht is dat raakvlakken heeft met antidiscriminatie en ook met free speech. Het altijd maar gemonitord worden bij het uitoefenen van free speech is bedreigend. Het is eigenlijk een ontwikkeld begrip voor het recht op *fair play* in een informatiesamenleving en van een hele grote structurele betekenis. Dat is het eerste punt.

Het tweede is '16 miljoen Bekende Nederlanders'. Betekent dit dat die 16 miljoen bekende Nederlanders - doordat ze op de een of andere manier bekend zijn - ook hun privacy verloren hebben? Nee, het vraagstuk is: wat betekent nou dat concept van privacy of bescherming van persoonsgegevens, zoals we dat vandaag behandelen, in een samenleving waar we allemaal op de een of andere manier bij heel veel anderen bekend zijn? Niet in de zin van, alles is van ons bekend en volstrekt publiek. Maar het kenmerk van onze samenleving is wel dat ie steeds meer berust op gegevensverwerking. We rekenen voortdurend af, we meten en we kunnen niet meer functioneren zonder die realiteit. De vraag is: wat is de betekenis van dit onderwerp in die samenleving?

Ik zou tegen die achtergrond een paar opmerkingen willen maken over wat er zoal aan de hand is op het terrein van de regels en de beginselen, internationaal gezien, welke trends er zich aftekenen, en ik wil aan het einde iets zeggen over de vraag 'en wat is er nou zo erg aan als het niet gebeurt?'. Want in de media of de politiek rijst soms de vraag: wat is nou eigenlijk het probleem, kun je een ramp noemen? Ik denk - als ik daar nou een tipje van mag geven - dat wij in toenemende mate rampen om ons heen zien gebeuren. Die zijn al gedocumenteerd in een aantal landen om ons heen. Engeland telt systematisch *data breaches* in alle sectoren en dat zijn er al zo'n 300 per jaar. In Duitsland zijn ook rampen gebeurd en in Frankrijk ook al een paar. En het zou me verbazen als het in Nederland niet ook al gebeurd was.

Privacy en bescherming van persoonsgegevens

Tegen die achtergrond, een paar opmerkingen. In de eerste plaats denk ik dat het belangrijk is dat we conceptuele zuiverheid betrachten. Dat is een groot woord. Maar in de afgelopen 35 jaar, de periode waarin het NJCM bestaat, is er in Europa op brede schaal samengewerkt aan het kader voor privacy en bescherming persoonsgegevens op basis van een onderscheid tussen deze twee concepten. Het recht op privacy, het recht op eerbiediging van de persoonlijke levenssfeer, is namelijk naar zijn aard en ook in onze Grondwet een afweerrecht waarop geen inbreuk is toegestaan, tenzij op bepaalde voorwaarden. En de reikwijdte daarvan is onzeker en vatbaar voor ontwikkeling, maar natuurlijk niet alles is privacy. Dat is een kernpunt.

Daarnaast heeft men het concept van de bescherming van persoonsgegevens geponeerd en ontwikkeld als een stelsel van waarborgen dat altijd van toepassing is zodra je die drempel over bent van verwerking van persoonsgegevens. En dan gaat het om alle informatie die impact kan hebben op een identificeerbaar individu. Je kunt natuurlijk heel goed in het licht van de techniek argumenteren, en ik heb dat een spreker vóór mij horen doen, dat profilering van groepen ook vraagt om bepaalde waarborgen. Ik zou zeggen dat zetten we op de agenda voor toevoegingen aan het bestaande stelsel.

Maar het onderscheid tussen privacy en bescherming persoonsgegevens is heel essentieel. En je ziet dat - dat is zo interessant - ook erkend worden in het Europees Handvest van de Grondrechten dat in Nice aanvaard is en dat met het Verdrag van Lissabon bindende kracht zal krijgen voor alle Europese instellingen, maar ook op het nationale vlak wanneer er Europees recht wordt uitgevoerd. En u weet, dat is nogal vaak het geval. Dus dat onderscheid wat je vindt in artikel 7 en 8 van het Europees Handvest voor de Grondrechten lijkt mij een structureel kenmerk van groot belang en ik benadruk in allerlei situaties dat we ze allebei nodig hebben in onderling verband.

Als ik nu kijk naar de Nederlandse Grondwet, dan is daar in de jaren tachtig op een heel welkome manier een expliciete erkenning van het recht op eerbiediging van de persoonlijke levenssfeer met nog allerlei andere artikelen bijgekomen. En we zien daar dan toch een vrij zwakke verwijzing in een instructie aan de wetgever om regels te stellen over de verwerking van persoonsgegevens ter eerbiediging van de persoonlijke levenssfeer. Ik denk dat dit wat te eng is, een veel te beperkt perspectief is. Het zou dan ook tijd zijn om eens goed na te denken over een expliciete opneming van het recht op bescherming van persoonsgegevens in onze Grondwet.

Inmiddels is er op dat onderscheid tussen privacy en bescherming van persoonsgegevens - zoals u dat vindt in het Verdrag van de Raad van Europa, uitgewerkt in een EG-richtlijn in 1995 - een heel stelsel van regels ontstaan dat in toenemende mate horizontale doorwerking krijgt. De richtlijn was ervoor om de nationale activiteiten op dit punt te harmoniseren, om te zorgen dat er vanuit het perspectief van de interne markt een zogenaamd *level playing field* zou zijn. Maar al gauw is in de uitvoeringspraktijk en in de jurisprudentie erkend dat het iets is wat horizontaal werkt. Ook in heel veel lidstaten is die Richtlijn 95/46 breed uitgevoerd, ook voor politie, justitie en allerlei andere terreinen. Alleen door de structuur van de Europese Unie gaat dat een beetje moeizaam op Europees niveau. Er is in de derde pijler eind 2008 een kaderbesluit tot stand gekomen, dat in Nederland al grotendeels geïmplementeerd is in de

wetgeving die we hebben, de Wet bescherming persoonsgegevens, de Wet politiegegevens en de Wet justitiële gegevens.

Binnen die regels is er een praktijk waarbij op steeds grotere schaal in de diepte en in de breedte informatieverkeer dominant wordt. In de discussie over het beleid in de Europese Unie op het terrein van de politie- en justitiesamenwerking is dit een hoofdthema. Daarbij is ook de vraag aan de orde hoe we uitwisselingsstructuren kunnen bouwen waarin privacy en gegevensbescherming vanaf het eerste begin worden meegenomen. Het concept 'privacy by design' is binnen die discussie een werkelijk belangrijk thema. Er wordt gewerkt aan een informatiemodel, een architectuur van samenwerking, waarin we op dat punt meer vertrouwen kunnen hebben. Ik kom op het woord vertrouwen terug.

Globalisering en renovatie

Natuurlijk is het huidige stelsel van regels tot zekere hoogte een gedateerd stelsel. Het vindt zijn oorsprong in de jaren '70 - '80, en is uitgewerkt in een richtlijn uit 1995. De Europese Commissie heeft inmiddels de stoute schoenen aangetrokken en eerder dit jaar een openbare raadpleging georganiseerd. Ik zie dat ook als het begin van een proces. We zullen waarschijnlijk de komende twee jaar steeds meer nadenken over de vraag 'hoe verder?'. Ik zou denken, als ik vandaag de discussie hoor, ik zet mijn kaarten op renovatie en ik zou met name transparantie willen inbouwen in die renovatiestrategie.

Maar dat proces is niet alleen Europees. Wat er de laatste jaren ontstaan is, is dat er eigenlijk over de hele wereld, want we praten hier ook over globalisering, ontdekt wordt dat er een grote overlap is tussen de verschillende aanpakken. Er zijn verschillen. Duidelijk. Maar de OECD (*Organisation for Economic Co-operation and Development*, red.), voor een groot deel van de ontwikkelde wereld, de Asia Pacific Region met interessante, nieuwe spelers zoals China en India praten, gelooft u het of niet, ook over dit thema. En OECD staat op het punt om zijn richtlijnen uit de jaren '80 ook te vernieuwen. Het is een buitengewoon relevant thema. De gedachte dat dit thema aan het verdwijnen is, wordt eigenlijk nergens gedeeld.

Ik verwacht dat over een maand in Madrid, op de jaarlijkse conferentie van *Data Protection and Privacy Commissioners*, een belangrijke tekst wordt aangenomen, het ontwerp van internationale standaarden, waarin collega's uit alle landen zich kunnen vinden, en waarin je invloed zult zien vanuit het Europese denken, Noord Amerika en de rest van de wereld.

Meer effectiviteit als hoofdzaak

Ik noem u dit als achtergrond om u aan te geven dat wat wij vandaag hier bespreken niet alleen een Nederlandse discussie is, en niet alleen in de EU, het speelt in de hele wereld. Wat zal er in het kader van die creativiteit en die renovatie gebeuren? Het allerbelangrijkste is denk ik: we hebben meer effectiviteit nodig. We hebben meer doorwerking nodig. Meer praktische toepassing, meer *compliance*. Meer effectiviteit, dat zal het hoofdpunt zijn. En ik zie daar drie belangrijke aanknopingspunten.

Het eerste is: wie is verantwoordelijk voor wat er gebeurt in gegevensverzameling, vastlegging, beheer enz.? Die verantwoordelijkheid, is mijn ervaring, wordt structureel veronachtzaamd en veel te laag ingestoken. Er wordt onderschat wat het inhoudt om verantwoordelijk te zijn voor zo een complexe werkelijkheid. We hebben vandaag al een aantal voorbeelden gehoord. Dat verklaart ook dat niemand zich verantwoordelijk voelt. Dus ik denk dat we die verantwoordelijkheid moeten onderstrepen en aanscherpen. Dat betekent internationaal dat de discussie gaat over *responsibility*, *accountability* en *liability*. En we zullen daar vermoedelijk een sterke aanscherping zien van de verantwoordelijkheid van wat in Nederland verantwoordelijken heet, en internationaal wordt aangeduid als *controllers*, die niet alleen verplicht zullen zijn regels na te leven, maar die ook verplicht zullen zijn vooraf te demonstreren dat zij alles gedaan hebben wat nodig is om naleving te verzekeren.

Dat is een belangrijke stap voorwaarts, want dat zal ertoe leiden dat dingen als *impact assessments*, periodieke audits, certificering, allerlei activiteiten die wij tot de *assurance* rekenen op allerlei andere terreinen, als het gaat om geld en milieu, ook in de wereld van de gegevensbescherming een steeds grotere rol gaan spelen. Dat zal ertoe leiden, dat mensen die verantwoordelijk zijn binnen organisaties, vanaf de top tot aan het feitelijke werkniveau aan eisen zullen moeten voldoen, die maken dat die regels worden nageleefd.

Het tweede aanknopingspunt: hoe staat het met de rechten van ons allemaal? Ik denk dat deze niet wezenlijk uitgebreid zullen worden, maar dat er wel geïnvesteerd zal worden in mogelijkheden om ze eenvoudiger af te dwingen. Ook daar dus meer effectiviteit. Dat heeft ook te maken met gemakkelijke toegang tot de rechter, alternatieve geschillenoplossing. Niet inzetten op klachtenbehandeling door een toezichthouder, die daar geen tijd voor heeft.

Het derde aanknopingspunt is de zojuist bedoelde toezichthouder. De noodzaak van een onafhankelijke toezichthouder wordt ook uitdrukkelijk genoemd in het Handvest van de Europese Grondrechten en in het Verdrag van Lissabon. Ik denk dat die de mogelijkheid moet krijgen om strategisch en veel selectiever te opereren om zich te richten op die onderwerpen

waar de risico's en de bedreigingen, zowel individueel als maatschappelijk, het grootst zijn. De toezichthouder zal handhavingsbevoegdheden moeten hebben die adequaat zijn, waarbij men bijvoorbeeld zou kunnen eisen dat een organisatie die geen adequate voorzieningen heeft getroffen die alsnog treft, maar ook stevige rechtstreekse sancties zou kunnen opleggen.

Ik zie dus dat het CBP - de Nederlandse toezichthouder - zich op dit moment in de eerste fase bevindt van een robuuste handhaver. En door die verantwoordelijkheid onder woorden te brengen en aan te scherpen zal de effectiviteit van het stelsel toenemen. Dat geldt ook voor de overheid. Ik denk dat bij de overheid die verantwoordelijkheid ook sterk onderschat wordt, zowel in het beleid als in de uitvoering. Als de verantwoordelijkheden worden aangescherpt, en de toezichthouder goed en strategisch selectief te werk kan gaan, dan kan er met een systematische aanpak wel degelijk het een en ander gebeuren.

Daarbij speelt technologie als oplossing ook een grote rol. En ik denk dat het concept van 'privacy by design' dat in allerlei opzichten ook mogelijk maakt. Natuurlijk is het een onderwerp dat in de politiek moeilijk hanteerbaar is. Ik herinner mij uit het verleden, dat men dat daarom het liefst ontweek, en dat is nog steeds zo. Het is technisch en daar wil men niet verantwoordelijk voor zijn. Maar, wanneer je dit vertaalt in een aantal hele simpele eisen, zoals de noodzaak van een *privacy impact assessment* vooraf, dan is het ook politiek gezien verrassend eenvoudig: mag ik die *assessment* zien, is die er geweest, wat was de conclusie? En dat kan met kamervragen en debatten heel makkelijk geregeld worden. Op die eenvoudige manier kan verantwoordelijkheid worden geactiveerd en ook worden afgelegd.

De ernst van het probleem

Is dit nou allemaal zo erg? Ik zou denken dat, als wij allemaal om ons heen kijken, en zien dat in het Verenigd Koninkrijk per jaar 300 of meer grote veiligheidslekken, *data breaches*, ontstaan, waaronder een aantal gepubliceerd gevallen: 25 miljoen belastingbetalers zomaar kwijt, een disk met alle kinderbijslagontvangers zomaar kwijt, er toch wel wat aan de hand is. Als dat op grote schaal gebeurt, dan is dat funest voor het vertrouwen in de samenleving.

Als wij dat soort incidenten analyseren, dan is in de meeste gevallen de diagnose dat de verantwoordelijke organisaties hun verantwoordelijkheid schromelijk onderschat hebben. Dat het niet zelden *sheer stupidity* is wat er gebeurd is. Dan waren er bijvoorbeeld niet de meest elementaire regels en instructies. Niemand voelde zich verantwoordelijk. Als dat zo is in het Verenigd Koninkrijk, als dat zo is in Duitsland, en als dat zo is in veel andere lidstaten, dan

denk ik dat het een structureel probleem is van de samenleving waarin we zitten en waar we in toenemende mate in verzeild zullen raken.

En dat is erg. Niet alleen vanuit het individuele perspectief, dat is een maatschappelijk vraagstuk van de eerste orde. En zet u nou eens tegen die achtergrond een project zoals het Elektronisch Patiënten Dossier.

Is het erg als wij een netwerk krijgen van gegevensuitwisseling, van medische gegevens, dat mogelijk niet zo solide is? Dat lijkt me erg. Dat is niet alleen heel onprettig voor de patiënten, het is ook funest voor de gezondheidszorg. Als wij alleen maar een beveiliging kunnen krijgen - techniek kan alles mogelijk maken, en het kan helemaal gespecificeerd worden - die zo ingewikkeld is dat de doktoren er de voorkeur aan geven om deze maar niet in te stellen 's morgens, en het de hele dag open laten staan, omdat het sneller werkt, dan leidt dat ertoe dat men accepteert dat er suboptimaal gewerkt wordt en dan zijn wij dus bezig een van de kernpunten van de gezondheidszorg uit te hollen.

Psychiaters hebben mij laatst op een spreekbeurt verteld dat hun patiënten liever niet meer komen, want nu wordt hun diagnose behandel combinatie opgeschreven en dat is voor een psychiatrische patiënt op zichzelf al een extra probleem. Als het zo is dat patiënten niet meer vertrouwen in een goed beheer van de gegevens over de behandeling, denk ik dat dit heel erg is. Als ik lees in de krant dat heel veel weigeraars doktoren zijn, die de gezondheidszorg van binnenuit kennen, is dat een interessant gegeven. Dan hebben we dus een project dat niet solide genoeg is en waar we dus gedonder mee gaan krijgen. Ik denk dat dit heel erg is.

Dit is maar één voorbeeld: als we kinddossiers gaan opbouwen en daar een erg groot vertrouwen in hebben, dan is dat één probleem. Maar de consequenties van de praktijk van die kinddossiers laten mogelijk een zelfde defect en structurele problematiek zien als de patiënten dossiers. Ik spreek tentatief, maar u voelt wat ik wil zeggen.

Nederland is het enige land in Europa dat niet alleen biometrische kenmerken in het paspoort heeft staan, maar ook de gelegenheid heeft aangegrepen om één centrale database van biometrische kenmerken op te gaan bouwen. Dat is het perspectief.

Nou moet ik hier gezegd hebben dat de invoering in 2004 van biometrie als een vereiste, wat mij betreft, wat te vroeg is gekomen. Want, zo supersolide is het allemaal nog niet. En biometrie is naar zijn aard gebaseerd op waarschijnlijkheid, en er is dus ook een kans, en die ligt soms in de orde van 1-2%, dat het niet dezelfde persoon is. En daarom moet je daar heel zorgvuldig mee omgaan en allerlei strategieën daaromheen ontwikkelen. Dat is één probleem. Maar, wanneer je een kenmerk dat bedoeld is om identiteitsfraude tegen te gaan, en het ultieme wapen, opslaat in een centrale database in een omgeving waarin de overheid wellicht

structureel de kwaliteitseisen onderschat, dan kun je, vrees ik, de klok gelijk zetten op een rampzalige gebeurtenis.

En ik denk dus dat de staatssecretaris van Binnenlandse Zaken, die in de Eerste Kamer met dat vraagstuk is geconfronteerd door de oppositie en toen als enige antwoord gaf: ‘Als dat probleem zich voordoet, dan lossen we het op’, het misschien toch allemaal wat onderschat.

Vertrouwen en bezorgdheid

Ik denk dat het thema waar het hier vandaag om gaat in werkelijkheid is: hoe kunnen we het gebruik van ICT zo organiseren we dat we inderdaad vertrouwen kunnen hebben in de meest basale principes van onze samenleving in een omgeving waar alles op digitaal verkeer berust. Ik dacht dat ik in de opmerkingen van de Nationale Ombudsman dat thema duidelijk terug zag komen, waar er veel voorbeelden zijn van tekort schieten.

En door dus dit grote probleem, dat een structurele betekenis heeft, terug te brengen tot een doodoener ‘Ach, niets te verbergen.’ bewijzen we - en degenen die de dezelfde doodoener gebruiken, in de politiek en daarbuiten, dat ze er heel weinig van begrepen hebben. En dat vind ik zorgelijk. En ik kom dat verschijnsel niet zo tegen in andere landen. Dat is curieus. En dat is niet een kwestie van politieke correctheid. Ik denk dus dat Nederland daarin toch een beetje alleen loopt.

In de opinieonderzoeken die er regelmatig zijn, is het opvallend dat bezorgdheid onder de bevolking als een indicatie, in de EU gemiddeld 68% is, in landen als Duitsland en Oostenrijk is het tegen de 90%. In Engeland, niet naïef, tegen de 80%. In Nederland is het 32%. In vijf jaar tijd is de bezorgdheid weggezakt van rond de 50% tot 32%.

Ik denk dat de politiek, de media, maar ook ons hele maatschappelijk discours, daaraan debet zijn. En ik vind het dus buitengewoon gelukkig dat het NJCM dit thema stevig op de agenda heeft gezet.

Dank u wel.