NJCM/ICJ

Verslag NJCM-lustrumcongres '16 Miljoen BN'ers? Bescherming van Persoonsgegevens in het Digitale Tijdperk'

Op donderdag 8 oktober jl. vierde het NJCM in Pulchri Studio te Den Haag zijn 35-jarig bestaan met het lustrumcongres '16 Miljoen BN'ers? Bescherming van Persoonsgegevens in het Digitale Tijdperk'.

Door de immer voortschrijdende technische ontwikkelingen krijgt de overheid op steeds meer terreinen grip op complexe maatschappelijke en sociale vraagstukken. Zo kennen we tegenwoordig onder meer de OV-chipkaart, het 'digitaal rechercheren' in cyberspace, het openbaar cameratoezicht om strafbare feiten op te sporen of te voorkomen, een Verwijsindex voor risicojongeren, het Elektronisch Patiënten-dossier en het biometrisch paspoort inclusief 'vingerafdrukken-databank'.

De verwerking van en omgang met particuliere persoonsgegevens kan echter op gespannen voet (komen te) staan met de naleving van mensenrechten, in het bijzonder het recht op de persoonlijke levenssfeer. Enerzijds beschermt de overheid in toenemende mate individuen met behulp van informatie-technologie, anderzijds kunnen de door haar gecreëerde digitale identiteiten een eigen leven gaan leiden. Deze ontwikkelingen raken zo nauw aan onze meest fundamentele rechten, dat ook de recentelijk geïnstalleerde Staatscommissie Grondwet zich in haar onderzoek zal buigen over grondrechten in het digitale tijdperk.

Het NJCM heeft tijdens dit lustrumcongres na willen gaan of de overheid klaar is voor de bescher-ming van persoonsgegevens in de 21ste eeuw. Tijdens de workshops werden de mensenrechtelijke grenzen en knelpunten van overheidsoptreden geanalyseerd. Deze grenzen en knelpunten zullen een rol gaan spelen in de toekomstige activiteiten van het NJCM.

Het verslag hieronder is een uitwerking van de bandopnamen op 8 oktober 2009.

Ochtendgedeelte

Quirine Eijkman
Voorzitter NJCM

Welkom bij het lustrumcongres van het Nederlands Juristen Comité voor de Mensenrechten, het NJCM. Mijn naam is Quirine Eijkman. Ik ben de huidige voorzitter. Graag, voordat ik begin, wil ik iedereen vragen om zijn mobiele telefoon uit te zetten.

Geachte NJCM'ers en wellicht toekomstige leden van het NJCM, sprekers, Jenny Goldschmidt, onze *Commissioner* van onze moederorganisatie de International Commission of Jurists (ICJ), voorzitter en leden van de Staatscommissie voor herziening van de Grondwet, en wellicht andere 'Bekende Nederlanders'.

Al 35 jaar streeft het NJCM, een van de voornaamste mensenrechtenorganisaties, naar het bevorderen en naleven van mensenrechten in het Nederlandse beleid en wetgeving. De afgelopen 35 jaar is de vorm soms gewijzigd, maar de inhoud niet. Als nationale sectie van de ICJ volgen wij nieuwe ontwikkelingen op het gebied van mensenrechten en signaleren wij mogelijke inbreuken op mensenrechten in ons kleine polderland. Zo ook met dit lustrumcongres; '16 miljoen BN'ers?'. Voor diegenen die geen RTL-Boulevard kijken is dit misschien een term die niet zo bekend is, maar een 'Bekende Nederlander' is iets wat we allemaal willen zijn, althans, als ik de crècheleidsters van mijn dochter goed begrijp.

Het NJCM is zich er terdege van bewust dat databescherming op Europees en nationaal niveau reeds sterk gereguleerd is. Desalniettemin zijn wij van mening dat dit debat een nieuw impuls nodig heeft.

De mogelijkheden tot het opslaan van gegevens door de overheid en het faciliteren van de burger lijken onbegrensd. Databanken beginnen op steeds meer gebieden een rol te spelen. Het opslaan van digitale persoonsgegevens, zoals bijvoorbeeld in het Elektronisch Patiënten-dossier (EPD), moet niet op zichzelf worden gezien. De gevolgen voor mensenrechten moeten integraal worden bekeken. De overheid speelt als gebruiker en hoeder van persoonsgegevens een cruciale rol. Informatiekoppeling moet breder worden benaderd dan alleen vanuit het oogpunt van efficiëntie.

Ook de mogelijke inbreuken op de persoonlijke levenssfeer spelen een rol. In dit kader zijn wat ons betreft belangrijke punten: wie is die overheid nou eigenlijk? Wie draagt er binnen de overheid de verantwoordelijkheid voor de veiligheid en het beheer van persoonsgegevens? Met welk doel worden persoonsgegevens opgeslagen en kun je bezwaar maken – niet alleen bij de instantie die het opslaat, maar ook tegen de koppeling – wanneer je als burger niet eens weet waar al je persoonlijke gegevens zijn opgeslagen? Grondrechten dienen toegespitst te worden op een samenleving die anders functioneert dan in het verleden.

Dit zijn slechts een paar gedachten voordat ik het woord geef aan Corien Prins, onze dagvoorzitter. We zijn zeer vereerd dat Corien Prins, lid van de Wetenschappelijke Raad voor het Regeringsbeleid en als Hoogleraar verbonden aan het Tilburg Institute for Law, Technology and Society, de dag voorzit. Wij denken dat met haar expertise niemand in Nederland zo goed als zij in staat zal zijn om dit congres te leiden.

Corien Prins – Dagvoorzitter
Hoogleraar recht en informatisering, Universiteit van Tilburg
Lid Wetenschappelijke Raad voor het Regeringsbeleid (WRR)

Dank. Ik ga mijn best doen. Dan kunt u aan het eind van de dag beoordelen of ik er inderdaad een mooi congres van heb gemaakt, maar dit ligt aan ons allemaal, denk ik. Er is alle ruimte voor debat en discussie, dus participeer en doe vandaag vooral graag mee. We hebben een aantal uitmuntende sprekers, zowel vanmorgen als vanmiddag, dus het wordt wat mij betreft een spannende dag met zeker een aantal prikkelende lezingen. Ik heb slechts kort de tijd om u een kleine aftrap te geven voor vandaag.

Als je kijkt naar de titel: 'BN'ers?', een 'Bekende Nederlander'. Dat betekent eigenlijk: bekende Nederlanders moeten sowieso meer bereid zijn hun privacy op te geven. Dus als wij 16 miljoen bekende Nederlanders hebben, dan gaan wij er sowieso ook vanuit dat al die bekende Nederlanders meer privacy opgeven dan die gewone Nederlander. U bent er in ieder geval één van. Ik wil u twee sheets tonen. (…)

Allereerst het decor van vandaag. Het decor wat betreft de omgang met persoonsgegevens, het belang van de discussie voor vandaag, het belang van deze conferentie. Daarom ben ik ook heel blij dat het NJCM besloten heeft het lustrumcongres daar op te zetten. Dus allereerst dit: u zult vandaag een aantal presentaties krijgen waarin aandacht wordt besteed aan de gigantisch grote hoeveelheden gegevens die over ons worden opgeslagen. En dan moet u vooral weten, het gaat niet alleen over naam-, adres-, woonplaatsgegevens van u. Het gaat steeds meer over gegevens die iets over u als persoon zeggen. Biometrie op het paspoort, een bekend voorbeeld van de afgelopen tijd, zegt iets over ons als persoon in de zin van unieke lichaamskenmerken. Steeds meer gegevens worden aan elkaar gekoppeld, we worden getypeerd, gestereotypeerd en soms gediscrimineerd op basis van profielen die zowel bij de overheid als in het bedrijfsleven gebruikt worden om efficiënt en heel specifiek diensten en producten aan te leveren. Wij zijn met zijn allen – want allemaal zijn wij werkzaam bij enige organisatie – bezig een niet in omvang (capaciteit is geen probleem) en zeker ook niet in tijd beperkt, systeemgeheugen te creëren. Een systeemgeheugen dat zichzelf vooralsnog niet corrigeert. Een databank zal niet tegen zichzelf zeggen 'dit gegeven is onjuist', 'dit gegeven is verouderd', 'eruit!'. Een mens, een politieagent op de hoek van de straat, ergens houdt het hier op. Onze geheugencapaciteit is beperkt. Het geheugen van computersystemen, van grootschalige databases, is dat niet. Kortom, wij creëren met elkaar een samenleving waarin wij een gigantische hoeveelheid gegevens aan het opslaan zijn.

Wat u vandaag ook zult horen is dat de wereld niet meer zo simpel is in de zin van: de overheid verzamelt uw gegevens, het bedrijfsleven verwerkt of verzamelt uw gegevens. Als u kijkt naar het Elektronisch Patiëntendossier of naar gegevensgebruik in de jeugdzorg, dan ziet u dat er sprake is van een toenemende complexiteit van actoren, van vervlechting van publieke en private samenwerkingsverbanden bij het gebruik van gegevens. Het is dus niet meer zo simpel te zeggen: hier ligt de verantwoordelijkheid bij de overheid, daar ligt de verantwoordelijkheid bij het bedrijfsleven en zo richten wij ons verantwoordelijkheidssysteem in.

Als ik kijk naar een aantal beleidsstukken in ieder geval, de discussie soms hier in Den Haag, dan moet ik constateren dat er een blindelings en zeker soms ook naïef vertrouwen is in de technologie en de uitkomsten van technologie. Weten wij zeker dat biometrie op het paspoort unieke identificatie van u bewerkstelligt? Weten wij zeker hoe die technologie precies in elkaar zit? En, weten wij eigenlijk wel hoe kwetsbaar we ons maken als samenleving, en de individuele burger, met de inzet van die technologie? Zijn wij niet te naïef door te stellen 'ik heb niets te verbergen'?

Een tendens die vandaag ook aan de orde komt, meneer Hustinx is te midden van ons: Europa en met name de Verenigde Staten sturen in een belangrijk aantal gevallen alle initiatieven die hier op ons afkomen. Biometrie op het paspoort, dataretentie, het bewaren van uw bel-, surf- en emailgedrag, de opzet van databanken, gegevensuitwisseling. Het is niet meer de nationale context en de discussie kan daarom ook niet alleen gevoerd worden binnen de

nationale context. Het is absoluut ook een grensoverschrijdende discussie geworden. Wederom maakt dat het complexer.

De eerste spreker straks is Alex Brenninkmeijer, de Nationale ombudsman, en hij zal u laten zien hoe burgers op nieuwe manieren kwetsbaar worden en zijn geworden de afgelopen tijd ten gevolge van het verwerken van persoonsgegevens en de inzet van technologie. Een van mijn medewerkers bij de WRR noemt dat 'onzichtbare zichtbaarheid'. Wij zijn als burgers zeer zichtbaar geworden voor bedrijven en overheid, maar voor ons is de wereld daarachter, de aan elkaar gekoppelde ketens en de wijze waarop onze informatie verwerkt wordt, uitermate onzichtbaar, ongrijpbaar en daarmee worden wij kwetsbaar. We weten niet meer waar we moeten aankloppen om te zeggen dat een bepaald gegeven niet juist is. En, als je kijkt naar al die initiatieven die op ons afkomen, dan vraag ik me af of er nog wel zoiets is als een *effective remedy*. Hebben wij, op verschillende niveaus in dat hele samenspel van allerlei actoren, nog wel inzicht hoe precies de lijntjes lopen, wie precies de actoren zijn, wie waarvoor verantwoordelijk is? We benaderen nog steeds alles vanuit een individueel initiatief. We denken onvoldoende na over de consequenties, ook met het oog op *effective remedy* van het totaal, de combinatie, de paraplu. Wie is er verantwoordelijk voor het parapluutje over alles wat we aan het bouwen zijn? Kortom, voor u een aantal elementen van het decor voor vandaag.

En dan, wat mij betreft, de opdracht voor morgen: ik zou graag de discussie vandaag willen voeren over veel meer dan alleen individuele gegevens en meer dus dan de Wet bescherming persoonsgegevens (Wbp). Het gaat niet langer over uw individuele gegevens. Het gaat over u als type mens. Het gaat over veel meer dan de simpele gegevens, het gaat ook over lichaamskenmerken. Het gaat over autonomie, het gaat over vrijheid. Kortom, veel meer dan alleen de naam en het adres. Fundamentele belangen staan op het spel. Hoe willen wij onze samenleving inrichten, zeker met het oog op de toekomst? Ik heb daarom nu maar even BN vertaald met '16 miljoen Brave Nederlanders'. Als wij allemaal geobserveerd worden, als wij allemaal in hokjes geplaatst worden, hoe voelt u zich dan? Als ik in de trein zit terug richting Brabant en er staat constant een camera op mij gericht, dan gedraag ik me toch echt op een andere manier, dan wanneer ik daar onbespied zou zitten. En dat is nog een simpel voorbeeld, want dan zie ik tenminste nog dat die camera op mij gericht is. Maar in heel veel gevallen weten wij niet eens dat we geobserveerd worden.

Wat mij betreft is de discussie en de agenda voor vandaag, en de opdracht voor morgen, een noodzaak tot een heroriëntatie. Wat mij betreft is het de opdracht privacy tot meer te maken dan alleen maar een mythe. Ik heb zo het idee dat wij langzaam alleen maar met een mythe aan het werken zijn. Privacy komt in alle beleidstukken, in alle discussies, natuurlijk op tafel. Natuurlijk staat het op de agenda bij verschillende organisaties. Maar hoe vaak wordt privacy serieus doordacht als in 'wat is de waarde die wij daaraan hechten?'. Wat is de relatie tussen privacy en kwetsbaarheid van onze samenleving? Laten wij met zijn allen eens nadenken over wat ik even noem het 'handelingsvermogen van privacy'. Hoe kunnen wij dat concept, dat fundamentele recht, dat grondrecht, zodanig vorm en invulling geven dat het daadwerkelijk in staat is, als concept, als belang, als recht, te hándelen, een bepaald verwerkingsgedrag van organisaties áf te dwingen, te reguleren? Hoe maken we het weer tot een serieus belang en concept? Wat mij betreft is dat de opdracht van vandaag en de uitdaging voor morgen.

Alex Brenninkmeijer
Nationale ombudsman

Dames en heren, als ombudsman wil ik graag het NJCM van harte gelukwensen met dit lustrum. Ik denk dat we trots kunnen zijn op de bijdrage die het NJCM levert aan de grondrechtendiscussie in Nederland. Ik wens het NJCM heel veel goeds toe in de toekomst.

Mijn bijdrage gaat over het thema '16 miljoen BN'ers', maar dan in verbinding met wat ik noem 'de onbekende overheid'. Dat zal het thema van mijn bijdrage zijn. Daar zit ook mijn grote zorg; de onbekende overheid tegenover de bekende Nederlander. Mijn stelling luidt dat we met de Wet bescherming persoonsgegevens en met bijvoorbeeld de rol van het College bescherming persoonsgegevens er nog niet zijn. De wet en het college vormen wel belangrijke waarborgen, maar er zijn nog belangrijke hiaten in de bescherming van de persoonlijke levenssfeer van burgers. Ik wilde die hiaten hier blootleggen.

Mijn invalshoek is ook bepaald door mijn persoonlijke ervaringen als ombudsman in een aantal zaken die betrekking hebben op bekende Nederlanders. Nederlanders die ernstig in de problemen kwamen vanwege het feit dat er zoveel over hen bekend was en wellicht ten onrechte. Dan heb ik het natuurlijk over zaken van identiteitsfraude. Zaken van identiteitsfraude geven goed weer wat er mis kan gaan.

De belangrijkste vraag is: wat kunnen wij daar van leren? U heeft in de media wellicht gelezen over de problemen van de heer Kowsoleea. Hij werd geconfronteerd met iemand die gedurende jaren in staat was om zijn criminele identiteit te plakken op die van meneer Kowsoleea. In onze zeer intensieve discussies met Justitie over alle databestanden die er waren, bleek het tot op de laatste dag uiterst moeilijk te zijn om dat te ontwarren. Je zou nog steeds kunnen twijfelen wie het nu wel of niet is. Hoe integer zijn de systemen?

Een tweede zaak die wij behandeld hebben en die ik ook erg boeiend vond – maar wel erg triest – was van een jongeman wiens identiteitskaart vóór uitgifte door de gemeente was gestolen. Iemand had zijn identiteit overgenomen en allerlei problemen voor deze persoon veroorzaakt. Waarom neem ik deze twee zaken als aanknopingspunt? Dat komt omdat ik zag welke impact dit had op het leven van die mensen. Het is niet een technische kwestie, maar een kwestie die veel meer ingrijpt in hun persoonlijke levens. Mensen kunnen daardoor zelfs in ernstige psychische problemen raken. Het is niet een oppervlakkige kwestie. Bij de afwikkeling van dit soort zaken vraag ik mij af hoe je in dit soort zaken tot een redelijke uitkomst moet komen. Er wordt gedaan alsof betrokkene zwak in zijn schoenen staat. In een van de casus zei de burgemeester dat de andere personen waarvan de identiteitskaart ook was gestolen niet in de problemen waren gekomen. Maar deze meneer wel. Als je kijkt naar wat hem is overkomen dan was dat buitengewoon triest. Wat komt er naar voren in deze zaken?

In de eerste plaats: dit soort problemen ervaar je pas wanneer je geconfronteerd wordt met de gevolgen. Er is al heel veel gebeurd, er zit informatie in allerlei systemen, gekoppeld en uitgewisseld, er zijn fouten gemaakt en je merkt het pas aan de gevolgen. Dan is het te laat.

Het tweede punt is de geweldige complexiteit van de zaken. In de zaak van de heer Kowsoleea ontstond een ongelooflijk heftig debat met de minister van Justitie, omdat de minister zei dat de ombudsman niet de juiste gegevens heeft gebruikt. Dàt was nou juist onderdeel van het probleem.

Bij complexiteit horen onbedoelde effecten; de systemen zijn goed uitgedacht, de mensen die er werken doen het goed, maar toch gebeuren er rare dingen die niet verklaarbaar zijn. Het valt mij op dat niemand verantwoordelijk is. De heer Kowsoleea bijvoorbeeld sprak de Staat der Nederlanden aan. Dan heb je een redelijke partij te pakken, zou je zo zeggen. De landsadvocaat verwees naar de politiekorpsen. Het is een ernstig probleem als je tot een oplossing wil komen. Niemand is verantwoordelijk voor de ketenproblemen. De achtergrond van dit soort zaken is intrigerend. Juist de ontwikkeling van datasystemen zet de ketenproblemen op de agenda. Die zijn naar hun aard complex. Door ketens te vormen denkt men de problemen op te lossen, maar men heeft onvoldoende oog voor het feit dat daardoor juist de problemen ontstaan.

Wat verder opvalt in deze zaak is dat de informatie overal en nergens is. Je weet niet waar je het moet vinden, vooral ook in de tijd gezien. Het gaat er niet om of ik op dit moment een bepaald feit in een bepaalde database vind, maar de vraag is ook hoe dat er een jaar geleden uitzag of langer geleden. De historie van de informatie is minstens zo belangrijk. De traditionele aanpak – het juridische handwerk – schiet tekort. We moeten een paar stappen verder zetten om tot een oplossing te komen. Rechtsbescherming en toegang tot de rechter schieten te kort. Het gaat om oplossingen die werken en die de praktische problemen oplossen.

Wat is de probleemstelling? Dan kom ik tot twee invalshoeken.

De eerste invalshoek is – zoals ook gezegd door Corien Prins – dat de Wet bescherming persoonsgegevens werkt per organisatie, per bestuursorgaan enz. Het gaat om de verantwoordelijke voor de verwerking van gegevens. Het privacyprobleem gaat daar echter dwars doorheen. Dat betekent dat de Wet bescherming persoonsgegevens iets raakt wat maar een facet is van het probleem. Het gaat om het geheel, de hele keten, het complex waarin data zijn verwerkt, opgeslagen en gekoppeld.

De omslag die nodig is, is dat het niet primair gaat om de zorg voor het opslaan en verwerken van data. Het gaat erom dat we erkennen dat burgers een virtuele identiteit aan het opbouwen zijn en dat die virtuele identiteit niet ergens te lokaliseren is. Als er iets gebeurt met iemand, kan het zijn dat hij in het Schengen Informatie Systeem (SIS) terechtkomt. Dat betekent dat hij een Europees land niet meer kan binnenkomen. Wie bepaalt of die melding in het SIS plaatsvindt? En weet je het eigenlijk wel? Of is het zo dat je bij de grens komt en het ineens te horen krijgt? Dat zijn de vragen.

De virtuele identiteit is heel reëel. Er zijn vele systemen en vele soorten gegevens. Als je uitgaat van de systemen die dus bijdragen aan de virtuele identiteit dan is het inherent dat dit soort systemen fout zijn. Als je aan grote organisaties vraagt – zoals het UWV – hoeveel procent van hun data fout is dan hoor je 5%. Maar als je het percentage optelt van de Belastingdienst, het UWV en alle andere diensten dan is dat zeer substantieel. Je kunt natuurlijk zeggen dat het vroeger bij de kaartsystemen om hetzelfde percentage ging. Dat hoort nu eenmaal bij systemen. Maar het verschil is dat het nu ook nog eens gekoppeld wordt. Er zitten geheugeneffecten in. Gegevens uit 2004 kunnen nu betekenis hebben en de fouten lopen door in de tijd.

De koppeling van gegevens leidt ertoe dat je betrouwbaarheid kunt creëren. Voor een paspoort bijvoorbeeld zijn de naam, handtekening, burgerservicenummer en daaraan toegevoegd de vingerafdruk nodig. Op het eerste gezicht lijkt het tot een grotere betrouwbaarheid van

die gegevens te leiden. Maar dat is paradoxaal. Want de keerzijde is dat als je zoveel precieze gegevens met betrekking tot één bepaalde identiteit moet opslaan en er verkeerde koppelingen plaatsvinden of fouten worden gemaakt, dan zijn de gevolgen veel ernstiger. Naarmate de identiteit van de burger steeds preciezer, scherper en aan meer kanten wordt vastgelegd in systemen wordt het risico voor burgers ook veel groter.

Eén ding is zeker: er is geen systematisch beheer van systemen. Er zijn allemaal deelsystemen die in eigen beheer zijn en een eigen logica hebben. Er is geen 'big product' voor alle systemen. Dat betekent dus dat het geheel een wat chaotische, eigen dynamiek heeft. Ik wil daaraan toevoegen het probleem van de onmatige overheid. Langzamerhand ontstaat er een discussie over wat de overheid allemaal wil en doet. Het blijkt dat de overheid ongeremd is in zijn ambities. Daarmee ook ongeremd is in zijn honger naar informatie en het opslaan van informatie. Nederland is kampioen 'tappen'. Waarom? Is daar een verklaring voor? Waarom is Nederland nou kampioen 'tappen'? De onmatige overheid. In het verlengde daarvan noem ik de consequenties, ook de internationale consequenties van terrorismebestrijding. Wat er in die wereld gebeurt, is eigenlijk een weg van meer en meer. Dan komt de vraag op: kan het ook minder? Hebben we het allemaal nodig? En hoe zit het met het beheer van die gegevens en de integriteit van die gegevens? Kan er ook wat weggegooid worden? Dat zijn essentiële vragen die spelen rondom dit onderwerp.

Nou kom ik met een tweede invalshoek die meer van filosofische aard is en die ik heel erg belangrijk vind. Dan sluit ik een beetje aan bij de woorden die Corien Prins in haar inleiding zei, namelijk privacy als mythe. Wat is privacy nou eigenlijk? Wat ik vanuit meer beschouwende zin naast privacy wil stellen, is bescherming van het eigendomsrecht. Hoe gaan wij om met eigendom en de bescherming van eigendomsrecht? En de integriteit van het lichaam, het fysieke lichaam. Hoe gaan we daar mee om? Plaats daar dan naast de virtuele persoon en de bescherming van die virtuele identiteit van iedere burger waar steeds meer over bekend wordt en de burger die steeds meer geëxploiteerd wordt. Bijvoorbeeld in het private dat er handel is in identiteiten van burgers. Dat moet ons te denken geven. Wat zijn de gevolgstappen en wat zijn de effecten van de commerciële waarde van identiteiten wanneer we zien dat overheid en de private sector steeds meer met elkaar verweven raken. We kunnen wel zeggen dat de Grondwet staat voor de bescherming van grondrechten enz., maar is dat ook zo als je in publiek/private verbanden terecht komt?

Wat in ieder geval opvalt, is dat de bescherming van de privacy in de publieke discussie erg zwak wordt door de gemakkelijke uitruil met veiligheid. In het debat is heel gemakkelijk die veiligheid naar boven te brengen. Wat ook opvalt is dat ten aanzien van privacy de *waiver* – het prijsgeven van het recht – zo omvangrijk kan zijn. Ten aanzien van de integriteit van het lichaam is het niet mogelijk om in die mate het recht prijs te geven. Dat is heel beperkt. Direct zijn bijvoorbeeld de strafrechtelijke consequenties duidelijk. Ook bij het beperken of prijsgeven van het eigendomsrecht stellen burgers zich veelal veel restrictiever op. Bij privacy is het zo dat er talloze momenten zijn waarop er iets met iemands gegevens gebeurt. Vaak weet de burger echter niet wat de consequenties hiervan zijn. Dus mijn beeld is zorgwekkend en ik plaats op de agenda de vraag: 'Wat moeten we de burger bieden, gegeven het feit dat er zich een virtuele identiteit ontwikkelt, gegeven het feit dat die virtuele identiteit concrete en actuele problemen voor burgers kan veroorzaken zonder dat er een oplossing is?' Ik ga

u niet vertellen dat ik daar zonder meer een oplossing voor heb. Ik wil wel een bepaalde denkrichting aan u voorleggen.

Als we een oplossing willen vinden dan kun je aan de ene kant denken aan het juridische instrumentarium. Maar naar mijn mening schiet dat juridische instrumentarium tekort. Als we kijken hoe de zaken bij ons verlopen zijn, dan bleek ook dat als de betrokken personen alleen gebruik zouden hebben gemaakt van hun juridische instrumentarium dat hen haast verpletterd had. Dat betekent dat er een toegang moet zijn tot veel eenvoudiger middelen. Je moet denken aan een interventie. Wij hebben gemerkt dat het essentieel is om relevante partijen bij elkaar te halen om een gemeenschappelijk *commitment* te creëren om tot een oplossing te komen. Er moet een loket zijn waar iemand terecht kan. Achter dat loket moet ook iets zitten dat daadwerkelijk de grote schoonmaak kan veroorzaken in de gevallen waarin dat nodig is. Je moet nadenken over hoe een en ander in elkaar zit. Deze inzet die noodzakelijk is voor de bescherming van de privacy van mensen die te maken krijgen met problemen moet er in ieder geval toe bijdragen dat die onbekende overheid beter te benaderen is. Dat is iets waar ik met alle energie verder over wil nadenken en aan wil bijdragen in de discussie. Ik wens u een goede dag toe.

Bert-Jaap Koops
Hoogleraar regulering van technologie, Tilburg Institute for Law, Technology and Society, UvT

Dames en heren, goedemorgen. Ik ben hier gevraagd om vanuit de wetenschap een verhaal te houden over dataprotectie. Dat doe ik graag, maar misschien iets anders dan u zou verwachten. Na alle problemen die geschetst zijn, verwacht u wellicht een zeer genuanceerd verhaal met mogelijke oplossingsrichtingen die wij in kunnen gaan en de consequenties, de slagingskans van die oplossingsrichtingen. Maar, eerlijk gezegd, dat verhaal kent u allemaal. Dat is preken voor de eigen parochie. Dat verhaal heeft u al vaker gehoord, dat verhaal moet heel vaak verteld worden, maar ik denk niet hier, maar vooral voor mensen die hier niet in de zaal zitten.

Ik ga iets anders doen. Ik ga de problemen die geschetst zijn nog wat erger maken en vervolgens aangeven wat we eraan kunnen doen. En ik dacht, als ik hier vanuit de wetenschap iets moet doen, dan heb ik Popper uit de kast gehaald en wat zegt Popper? 'Je moet een hypothese formuleren.' Dus ik ga vandaag een hypothese formuleren. Uw taak vandaag is om die hypothese te weerleggen, te falsificeren als bewijs van wat we wél zouden moeten doen. Ik ga de advocaat van de duivel spelen, en zoals het past bij advocaten ga ik overdrijven en een eenzijdig beeld schetsen. Ik wil u vriendelijk verzoeken om dat in het achterhoofd te houden, anders ga ik de pauze niet overleven, denk ik.

U kent allemaal dataprotectie, dus ik hoef dit niet te schetsen. Dataprotectie is een prachtig bouwwerk, gefundeerd in de grondrechten. Het is een belangrijk grondrecht, in verdragen vastgelegd, in onze Grondwet. Uitgewerkt in Europese richtlijnen, in de Wet bescherming persoonsgegevens en gebaseerd op een aantal dragende pijlers, de fundamenten, waarvan ik een aantal heb genoemd, niet allemaal, maar die voor mijn verhaal vooral van belang zullen zijn: doelspecificatie, doelbinding, en data-minimalisatie.

We moeten zo min mogelijk gegevens verwerken, en verwerking is alleen mogelijk als het noodzakelijk is voor een bepaald doel en niet voor andere doelen. De wet is opgehangen aan begrippen als 'identificeerbaarheid', 'naam adres woonplaats', 'herleidbaar tot een natuurlijk persoon', en de verantwoordelijke die het aanspreekpunt is voor de rechten en plichten.

Het probleem. We hebben al een deel geschetst en ik ga u kort even meenemen naar evaluaties van de wet. Als hommage aan de dagvoorzitter, maar ook omdat het nog steeds relevant is, begin ik met de evaluatie van de Wet persoonsregistraties (Wpr) uit 1995. De sociaal-wetenschappelijke evaluatie, die aangaf dat de Wpr een ingewikkeld en in geringe mate bruikbaar regelsysteem was dat het doel maar in beperkte mate bereikte. In diverse opzichten werd de wet niet nageleefd en waar de wet wel werd nageleefd kwam dit niet door de wet maar door allerlei andere dingen. Dat is op zich prettig, maar geeft wel aan dat de wet vaak het doel miste.

En dat is mede relevant omdat, als we kijken naar de evaluatie van de Wbp, die net gedaan is, we precies dezelfde dingen kunnen constateren. De eerste fase, literatuuronderzoek, gaf aan dat het een bijzonder complex regelsysteem is dat soms neigt naar overregulering, dat er een gebrek is aan bekendheid met de rechten en plichten uit de wet, en de vertaalslag naar de werkvloer moeilijk is. Materiële normen worden maar beperkt ingevuld op de werkvloer. En de tweede fase zegt in de algemeen overkoepelende conclusie dat de doelstellingen nog niet ten volle worden gerealiseerd en, als u het rapport goed leest, zult u zien dat dat een wat eufemistische benadering is. Zeer vriendelijk geformuleerd voor het feit dat de doelstellingen eigenlijk helemaal niet worden gerealiseerd en dat het nog niet tamelijk optimistisch is.

Dan hebben we de Commissie Brouwer, een rapport van begin dit jaar, 'Gewoon doen', waarop lang is gewacht en waarin staat dat je maar gewoon moet doen met die persoonsgegevens. Je moet afwegingen maken. Helaas zegt het rapport niet helemaal hoe je dat dan moet doen, en daar ging het nou juist om. Dus dat weten we nog steeds niet.

Kortom, tussenconclusie: we hebben een complex kader dat weinig richting geeft, dat onbekend is op de werkvloer of heel moeilijk te vertalen is naar concrete afwegingen en beslissingen voor omgang met persoonsgegevens op de werkvloer.

Maar dat is nog niet alles. Want wat in die evaluaties wat onderbelicht is, maar wat vanochtend ook al is uiteengezet, is de rol van technologie. We leven in databankenland. Bart Schermer heeft een rapport geschreven waarin hij uitrekende dat de gemiddelde burger in 250 à 500 databanken staat, maar vooral ook, dat die databanken steeds meer gekoppeld worden, gecentraliseerd, fysiek of virtueel. En dat het aantal doeleinden waarvoor die gegevens worden gebruikt en het aantal partijen dat daar toegang toe heeft stijgt. Kortom: doelbinding wordt moeilijker.

Dat heeft mede te maken met het maatschappelijke, sociale en politieke klimaat van risicobeheersing en wat ik maar even noem 'preventivisering'; de dringende behoefte om, zoveel mogelijk, alle rampen te voorkomen. En dat doen we vooral door zoveel mogelijk gegevens op te slaan, want je weet maar nooit waar ze goed voor zijn en als ze dan toch opgeslagen liggen, is het ook wel handig om ze te kunnen gebruiken voor allerlei doeleinden in de toekomst.

Daar komt nog bij, ook al genoemd in de inleiding, *datamining* en profilering, waarbij het niet zozeer gaat om de identificeerbaarheid van personen, maar om het gebruik voor herkenning

van personen als een bepaald type persoon of als dezelfde persoon die je de vorige keer tegenkwam. Je weet niet of het Jantje of Pietje is, maar je weet wel dat hij dezelfde dingen deed. En daar kan je dan allemaal leuke dingen mee gaan doen, met die profielen. En dan gaan het niet zozeer om de kwetsbaarheden van de Wbp, maar om intransparantie en manipulatie van betrokkenen en allerlei andere dingen. Beslissingen worden steeds meer genomen op basis van die virtuele identiteiten, digitale personen die leven in die databanken in plaats van de persoon die voor het loket staat. Door databanken die steeds meer 'gedecontextualiseerd' raken zijn de rechten die we hebben steeds moeilijker uit te oefenen.

En ik wil u, ter illustratie, het verzoek dat ik onlangs aan Amazon stuurde, alhoewel onlangs, het is alweer drie maanden geleden, voorlezen om aan te geven wat het betekent als je de Wbp in zo'n situatie wil uitoefenen:

> 'Beste Amazon.co.uk, kunt u mij informeren op basis waarvan u mij 'Maurice' van E.M. Forster. en Giovanni's room van James Baldwin heeft aangeraden? Ik vraag dat vanwege artikel 35 van de Wbp. Heeft uw suggestie misschien iets te maken met het feit dat ik drie weken geleden bij u The lost *language of cranes* van David Leavitt heb gekocht? Dat had ik toen dan wel graag willen horen van u, op basis van artikel 33 Wbp, wat u met mijn gegevens ging doen. Heeft u mij misschien door dat boek van David Leavitt geprofileerd als iemand die geïnteresseerd is in homoseksualiteit? Dat is een gevoelig persoonsgegeven, zie artikel 16 van de Wbp. Kunt u daarom alstublieft deze data verwijderen, omdat het onrechtmatig is voor u om deze data te verwerken. Zie wederom artikel 16 Wbp. En de verwerking ervan is bovendien niet nodig voor het doel dat ik bij u boeken koop, zie artikel 36 lid 1 van de Wbp. En wilt u mij een schriftelijke bevestiging sturen dat u inderdaad mijn gevoelige gegevens heeft verwijderd, zie artikel 36 lid 2 van de Wbp. Alvast dank.'

Ik wacht nog steeds op antwoord.

Kortom, we hebben niet alleen te maken met complexe datasystemen en wetgeving, maar met dataminimalisatie die haaks staat op de huidige praktijk en zeker op de praktijk van morgen. Doelbinding is steeds moeilijker vol te houden en naar mijn mening onrealistisch en onmogelijk in de toekomst. De aanknopingspunten van de Wbp zijn steeds minder te hanteren en steeds minder relevant voor waar het om gaat en het hele stelsel valt nauwelijks te handhaven. Kortom, als we kijken naar wat deze conclusies zeggen over de staat van het bouwwerk van dataprotectie, dan zal het duidelijk zijn: het is een ruïne.

Wat gaan we daar aan doen? Wel, er zijn twee mogelijkheden: de klassieke, orthodoxe, voor de hand liggende oplossing. De oplossing die u allemaal nastreeft is het bouwwerk renoveren. Zorgen dat er weer een mooie nieuwe tempel ontstaat. Door te simplificeren waar het mogelijk is en door de vage, complexe begrippen te verhelderen. Door meer voorlichting te geven aan betrokkenen en dataverwerkers. Door meer te handhaven. Door strenger te handhaven. Door te zorgen dat we toch contextuele integriteit kunnen hanteren in die databankwereld. En dat alles gaan we vooral doen door technologie in te zetten als oplossing; de u wel bekende *privacy enhancing technologies* en de iets minder bekende maar de even relevante *transparancy enhancing technologies*.

Daar gaat u vandaag ongetwijfeld veel over praten. Wat zijn de mogelijkheden hiervan? Hoe kunnen we dit gaan doen? Dat moet u ook vooral doen, maar ik denk dat het een achter-

hoedegevecht is. Ik denk dat het niet gaat werken, want het is meer van hetzelfde. Het zal over vijftien jaar waarschijnlijk leiden tot hetzelfde type conclusies dat we nu al trekken en dat we vijftien jaar geleden ook al trokken over de wet.

Er is een andere oplossing voorhanden die ik u graag wil voorhouden: laten we het bouwwerk afbreken en er iets heel nieuws voor in de plaats zetten. En dat gaan we doen door twee strategieën te hanteren.

De eerste is datamaximalisatie. Ook wel bekend als de hooiberg, die gebaseerd is op het feit dat als je iets te verbergen hebt, stop er dan vooral een hooiberg omheen. Ter illustratie het voorbeeld van, wat u misschien zes, zeven jaar geleden heeft meegekregen, *Jam Echelon day*, een activistische campagne om mensen een programmaatje te laten gebruiken dat ervoor zorgde dat automatisch bij elk bericht dat je op een bepaalde dag verstuurde, elk emailbericht, een onderschrift kwam met vijftig willekeurig gekozen woorden die allerlei rode alarmbellen deden afgaan bij de NSA (National Security Agency, red.). Als iedereen in elk bericht dit soort woorden gaat noemen dan is het zoeken op woorden volstrekt zinloos geworden. Dan gaat er natuurlijk weer andere *dataprofiling* gebruikt worden, maar daar kunnen we vervolgens onze onderschriften weer op aanpassen. En zo kunnen we, in strijd, ervoor zorgen dat het systeem nog steeds wordt platgelegd.

Dit past bij wat we op internet steeds meer zien: 'digitaal exhibitionisme'. Er worden steeds meer persoonsgegevens, de gekste dingen, van alles en nog wat, op internet gezet. Informatie, maar ook desinformatie, als overlevingsstrategie. Je kunt niet anders als je mee wilt komen, maar ook wel als levensstijl. Zeker bij de jongere generaties, denk ik, dat je dit ziet, maar ook wel bij de wat oudere generaties. Activiteiten in web 2.0, gebruik van *webcams*, professionele amateurs die met zijn allen dingen doen die vroeger alleen bedrijven of overheden deden. Nieuwe vormen van economie waarbij je gratis distribueert op grote schaal in ruil voor wat persoonsgegevens. Allerlei andere ontwikkelingen die een heel andere kijk op de wereld hebben. Je geeft gewoon al je gegevens prijs en dat maakt niet uit want iedereen doet dat. En het is dus helemaal niet erg dat je nu op Hyves dingen zegt die later tijdens je sollicitatiegesprek tegen je gebruikt kunnen worden, want je werkgever heeft dat zelf ook gedaan en dat kun je dus tijdens dat sollicitatiegesprek ook aan de orde stellen.

Dat is echter alleen mogelijk met een tweede deel van die strategie. Het is niet erg als wij als 16 miljoen BN'ers allemaal bekend zijn, zolang er maar goede waarborgen zijn voor foutencorrectie en toezicht. Dat heeft te maken met de tweede pijler, de strategie van de 'glazen samenleving'. We leven al in een glazen samenleving. En dat moeten we dus vooral gaan gebruiken. We moeten terugkijken. Ik ben erg onder de indruk van het werk van David Brin 'The transparant society', waar ik een citaat uit heb genomen: 'We may not be able to eliminate the intrusive glare shining on citizens of the next century'. Het licht van Big Brother, van allerlei kleine *brothers* en *soft sisters*, 'but the glare just might be rendered harmless through the application of more light, aimed at the other direction'. Met andere woorden: we moeten vooral terugkijken, collectief. Als we zorgen dat dat glas transparant is aan twee kanten, en dat Big Brother of Kafka of wie dat dan ook is die ons in de gaten houdt, evenzeer in de gaten wordt gehouden. Dan hebben we maximale transparantie als garantie voor *accountability*. Want dan kunnen we met zijn alle ervoor zorgen dat die mensen geen gekke dingen doen.

Goed, als we dat naast elkaar moeten zetten, dat verwacht u natuurlijk van mij, dan is dat wat lastig, want het is heel moeilijk om in te schatten hoeveel dat allemaal kost, hoe lang

het gaat duren, enzovoorts. Hier kan je natuurlijk niet meer mee aankomen in het huidige tijdperk; van het kabinet moeten we alles uitrekenen tot aan twee cijfers achter de komma. Dus ik heb een consultant ingehuurd, die heeft in zijn glazen bol gekeken en een grove berekening gemaakt. U ziet, de tweede strategie werkt op alle fronten beter.

Tijd voor een conclusie. Dataprotectie was best een leuk grondrecht. Het was geen slecht idee in de jaren '70, maar het was eigenlijk al achterhaald voordat het goed en wel was ingevoerd. In plaats van te streven naar dataprotectie 2.0, het renoveren van dat bouwwerk van dataprotectie, kunnen we veel beter een andere strategie hanteren. Niet proberen de geest terug in de fles te stoppen, die er al minstens vijftien jaar uit is, maar streven naar datamaximalisatie. Laten we ons gewoon vrolijk maken om *function creep* en *mission creep* en wat voor *creeps* er nog allemaal in databankland rondlopen.

Ja, we worden overal bekeken. We worden overal op beoordeeld, maar dat is niet erg als iedereen ziet *hoe* we worden beoordeeld. Als we allemaal meekijken dan zal iemand die ons onfatsoenlijk of onbehoorlijk of onterecht durft te behandelen genadeloos worden afgestraft, omdat het direct wordt opgemerkt door ons allemaal. Door meneer Brenninkmeijer, door meneer De Koning, door mevrouw Prins, door u allemaal en door allerlei mensen op straat. Door maximale transparantie te creëren, kunnen we nieuwe *checks and balances* inbouwen in de glazen samenleving waar we gewoon al in zitten.

Bart de Koning
Redacteur HP/De Tijd, auteur 'Alles onder controle: de overheid houdt u in de gaten'

Goedemorgen, dames en heren. Ik wil beginnen met een eenvoudig filmpje. Het is van het programma CQC van Veronica en het spreekt eigenlijk voor zich. [Televisiefragment waarin een CQC-reporter de vingerafdrukken van enkele Nederlandse ministers afhandig probeert te maken, *red*.] Hartelijk dank aan Veronica voor het gebruik van dit fragment en dan hebben we hier nog even een bonus [een slide, *red*]: dit is het paspoort van Ernst Hirsch Ballin, dat heeft hij zelf een paar jaar geleden aan het ANP gegeven als nieuwsfoto. En dat staat ook zo op internet en daar komen we zo nog even op terug.

Mij is gevraagd om iets te vertellen over privacy en media. En dan ligt het natuurlijk voor de hand om bijvoorbeeld een filmpje te laten zien van Wesley en Yolanthe die staan te zoenen in een parkeergarage en dat wordt dan uitgezonden door RTL-Boulevard. Of Willem-Alexander die een kort geding aanspant omdat hij op vakantie niet gefotografeerd wil worden. Maar dat is de *directe* invloed die media kan hebben op privacy.

Waar ik het over wil hebben is de *indirecte* invloed. De invloed die media hebben op beleid. Er is natuurlijk sinds '11 september' een enorme stortvloed aan maatregelen over ons uitgestort: preventief fouilleren, identiteitsplicht, databanken, camera's en noem het maar op. En de Nederlandse media hebben daarbij een nogal aanjagende functie gehad. Ik vond dat in het algemeen wel mooi. Een heel mooi voorbeeld daarvan is dat een tijd geleden in Gouda een buschauffeur op zijn gezicht is geslagen en dan haalt de Telegraaf de chocoladeletters uit de zetbak en dan wordt het 'Oorlog in Gouda'. En dan wordt de VVD helemaal hysterisch, 'het land staat in brand' en dan moeten er 'keiharde maatregelen' komen. Er worden in Nederland

namelijk nooit meer normale maatregelen genomen, maar alleen nog maar 'keiharde maatregelen'. En die trend werkt natuurlijk nogal aanjagend ,want politici worden opgejaagd door die media.

Maar er is ook nog een andere trend, dat journalisten ook slachtoffers van de media tegenkomen en daar ook veel aandacht aan besteden. Berucht voorbeeld is natuurlijk de Schiedammer parkmoord en de Puttense moordzaak. Maar er zijn wel meer van die zaken. Wat ik bijvoorbeeld persoonlijk heel vermakelijk vond was dat de Telegraaf door de AIVD geschaduwd is en ook werd afgeluisterd en dat er huiszoekingen zijn gedaan, omdat de Telegraaf bij uitstek de krant is geweest die de afgelopen jaren in commentaar na commentaar heeft geroepen dat er keiharde maatregelen genomen moesten worden en meer macht voor de overheid, weg met de linkse rechters en weg met de linkse advocaten. Die kregen even een koekje van eigen deeg. Ik heb me daar wel over geamuseerd.

Ik heb nu vrij sterk de indruk dat van die twee trends de kritische trend aan het winnen is. We zitten nu op een soort omslagpunt. Toen ik mijn boek twee jaar geleden zat te schrijven was het grote probleem: hoe moet je nou aan Nederlanders duidelijk maken dat privacy belangrijk is? Ik ben nog bij Bert-Jaap Koops geweest en gevraagd: heb je nou een *knock-out* argument voor me en dat had hij niet. Want het is allemaal 'wie niets te verbergen heeft'… etcetera. Toen kreeg ik een cadeautje van Donner. Zijn voorlichters hadden ingebroken op de computer van het gemeenschappelijk persbureau en gekeken wat voor artikelen er aankwamen over Donner. En dat heeft een enorme omslag veroorzaakt bij journalisten, want allemaal collega's die tot dan toe zeiden 'man wat loop je toch te zeuren met allemaal complottheorieën' werden ineens heel boos en ik heb sindsdien eigenlijk nooit meer het argument gehoord van journalisten van 'ik heb niets te verbergen'. Ze beseften allemaal opeens van: 'Ho! Gaat dat zó ver?'.

Daarom ben ik ook zo blij met dat filmpje van Veronica, dat staat sinds vorige week op YouTube. Dit speelt in Duitsland al jaren. Daar hebben *hackers* de vingerafdrukken van Schäuble gejat, de toenmalige minister van Binnenlandse Zaken, en dat als duimpje meegestuurd met een tijdschrift zodat iedereen zich voor kon doen als Schäuble. En die man is daar heel boos over geworden, waarmee meteen het punt gemaakt was van ja, zie je, het is dus heel erg als je je vingerafdrukken kwijt bent.

Ik hoorde vorige week hoe de vingerafdrukken nu worden opgeslagen in Nederland, de grote centrale boevendatabank die ons wordt beloofd door Binnenlandse Zaken; die is er nog niet want ze hebben de systeemspecificaties nog niet rond. Het wordt nu opgeslagen op de servers van gemeenten. Dat betekent dat er nu vingerafdrukken op veertien stadsdeel-servers staan. Nou, ik weet hoe lek die dingen zijn want McKinsey heeft dat vorig jaar doorgelicht en het is echt een drama, het is een soort Noord/Zuidlijn, maar dan op ICT-gebied. Dus dat is hartstikke lek, er komt ook steeds meer aandacht voor en dat vind ik heel aardig.

Wat je ook ziet aan Hirsch Ballin, zijn bonnetjes zijn een poosje geleden openbaar gemaakt. De sukkels op zijn departement dachten dat ze het onleesbaar hadden gemaakt, maar bij GeenStijl hadden ze binnen dertig minuten de versleuteling eraf. Creditcardgegevens op straat, vervaldatum op straat, van Klink ook. De volgende dag moesten die creditcards ingetrokken worden. Uiterst vermakelijk. Guusje ter Horst had natuurlijk ook iets heel vervelends, toen het bekend werd dat ze twee harinkjes gedeclareerd had. Daar heb ik ook erg om moeten

lachen, omdat de Raad van Europa, in de jaren '70 toen politici privacy nog belangrijk vonden, heeft gezegd dat privacy ook het recht op bescherming is dat er onbetekenende en gênante details geheim blijven. Nou, dit is zo'n onbetekenend en gênant detail, dat je met zo'n ministersalaris twee harinkjes gaat declareren. Dat heeft gewoon heel veel publicitaire schade opgeleverd.

Een ander mooi voorbeeld is Ton Hooijmaijers, de VVD'er die _ 100.000.000 heeft zoekgemaakt op IJsland. Die kreeg als nabrander nog even dat zijn bonnetjes in de provincie Noord-Holland bekend werden en daar zat een klein postje op. Hij was op zakenreis in China geweest en had op de hotelkamer PayTV bekeken en dat ook gedeclareerd. Nou, we weten allemaal dat als je op je hotelkamer moet gaan betalen voor programma's wat voor programma's dat dan zijn. Dat is weer zo'n onbetekenend, maar gênant detail. Dat een VVD'er, toch de partij van de belastingbetaler, van de hardwerkende Nederlander, zich op mijn kosten ligt te amuseren op een hotelkamer. En het aardige is dat dit vooral affaires zijn die de politici raken die zelf het hardst op privacy inhakken. CDA'ers en PvdA'ers en VVD'ers lopen voorop in die strijd en roepen voortdurend: 'wie niets te verbergen heeft, hoeft nergens bang voor te zijn!'. En je ziet, dat ze zelf nu geconfronteerd worden, in de media, met de gevolgen van totale openbaarheid. Dit is dus het terugkijken naar Big Brother. Dat is een trend die eigenlijk al dagelijks waarneembaar is.

Ik ben een fan van GeenStijl, niet omdat ik het met ze eens ben, maar omdat je daar goed *feeling* kan houden over hoe grote delen van Nederland daarover denken. Dat is vaak anders dan ik, maar je moet er toch contact mee houden. Daar staan heel veel filmpjes op van agenten die in de berm staan te plassen, agenten die verkeerd geparkeerd staan omdat ze een kroketje aan het eten zijn. Een paar maanden geleden een prachtig filmpje met een motoragent in Maarssen, die had ruzie, met wat ze dan noemen een 'scooter mocro', dat is een Marokkaan op een scooter, en hij kreeg hem niet te pakken. En die agent werd helemaal gek. Dit was gefilmd vanaf een balkon. Hij deed zijn leren jas uit, zijn steekvest ging uit, zijn koppel ging op de grond en hij stond er zo van: 'Kom maar, kom maar, kom maar!' En dat is gefilmd en uitgezonden, en die agent heeft een berisping gekregen., stond twee weken geleden in de krant, schriftelijk van de korpsleiding; die konden natuurlijk niet anders, want het was een totale afgang.

Je ziet dus: de overheid wordt gecontroleerd door burgers, die ook een cameraatje pakken en zeggen 'hé, wat ben jij daar bezig?'. In die zin ben ik redelijk optimistisch. Ik spreek veel op bijeenkomsten over privacy, en dat zijn allemaal hele sombere mensen, die zeggen 'het gaat helemaal fout', maar het is helemaal niet zo moeilijk om terug te duwen en dat heeft ook best snel effect.

GeenStijl had onlangs ook weer zo'n prachtige kop: 'deze zomer komt de gemeente-Gestapo naar u toe'. Dat ging over huiszoekingen in Den Haag. Ik weet niet of u het weet, maar in Den Haag worden in de krachtwijken systematisch woningen doorzocht door teams van de gemeente waarbij er dan een aantal ambtenaren binnenkomen en die doorlopen alles – woonkamer, slaapkamer – en kijken of er niet geknoeid is met de elektriciteitsmeter, of er niet mensen illegaal wonen, ze kijken even naar de stapeltjes post die daar liggen. Dat is heel heftig. Dat is al jaren gaande. Vrijwel geen klachten, gek genoeg, totdat ze ineens iemand aantroffen die niet open wilde doen. Die werd heel boos en heeft staan schelden, 'Flikker maar op!' en dan

druk ik me nog netjes uit. Die man kreeg een brief van de gemeente: 'U dient mee te werken met dit onderzoek. Zo niet, dan gaat de burgemeester een machtiging tot binnentreden tekenen.' Die man heeft dat doorgestuurd aan GeenStijl en die hebben er een stukje van gemaakt. Grote rel, zowel Rita Verdonk als GroenLinks boos. En Rop Gonggrijp. Een hele interessante coalitie van mensen die echt woedend werden van 'wat is dit? Fascisme? Gestapo-praktijken? Ik ga naar Duitsland, daar heb je nog wel fatsoenlijke politici.'

Heel interessant. Ik ben daar een verhaal van gaan maken. Ik ben naar Den Haag gegaan, ik heb meegelopen met die pandbrigade en het blijkt dus dat de gemeente zijn excuses heeft aangeboden aan deze man. Sterker nog, de procedures zijn aangepast. De ambtenaren mogen dit soort brieven niet meer versturen. Het gaat nu eerst via de juristen. En die denken wel drie keer na want de wethouder krijgt op zijn donder en daar heeft hij geen zin in. En zo zie je, dat als je een beetje terug duwt, je wel degelijk resultaten kunt bereiken.

Het meest saillante hieraan was dat de man die boos werd een huiseigenaar was, een blanke Nederlandse autochtoon. Die had een hypotheek en die dacht 'wat is dit voor een gedonder?' En die honderdduizend mensen die open hebben gedaan, dat waren huurwoningen en ik denk het grootste deel allochtoon. Mensen die voor een deel ook afhankelijk waren van de staat. Dat bevestigt voor mij een trend. Ik heb ook een beetje Popper gelezen, en ik ga nu aan inductie doen. Ik ga een aantal voorbeelden noemen. Dat is niet hetzelfde als een theorie vormen, maar ik doe het toch.

Een trend die ik al een paar jaar langer zie. Ik heb me wel eens afgevraagd, waarom maken Nederlanders zich nou niet zo boos over die uitholling van die privacy? Dat heeft voor een deel te maken met historische dingen, in Duitsland zijn er in het verleden bepaalde 'dingetjes' gebeurd waardoor ze terughoudend zijn geworden met staatsmacht. In Nederland zijn we wat naïever. Maar wat er *ook* gebeurt, is dat heel veel van die agressie van de staat zich niet richt op, zegmaar, 'ons soort mensen' zoals we hier bij elkaar zitten, die richt zich niet op de blanke middenklasse, of op de elite, die richt zich op de gekleurde onderklasse.

Dat viel me een paar jaar geleden op toen een vriend van mij terugkwam uit Suriname en die had een hele leuke vakantie gehad, alleen de terugreis was een hel geweest want hij had zich vanaf het opstijgen de hele tijd kwaad zitten maken, 'Straks krijg ik die 100% controle. Dan staat er zo'n marechaussee met een grote snor en een rubber handschoen.' En – hij is net zo bezig met privacy als ik – 'ik pik het niet, ik ben een Nederlander, ik laat me niet fouilleren, en ze gaan al helemaal niet met die rubber handschoen…' Dus die vriend kwam helemaal opgefokt bij de *gate* aan met zijn vriendin, zo van 'we gaan er tegenaan', maar hij kon zó doorlopen. En de rest van het vliegtuig kon achter aansluiten in de rij. Het enige wat er nog ontbrak was het bordje 'slechts voor blanken'. Want dat was wat er aan de hand was: 'Nederlanders, die hoeven we niet te controleren.'

Sindsdien ben ik daar op gaan letten. En het valt me gewoon op, dat preventief fouilleren is eigenlijk alleen maar, wat ze dan in krachtwijken noemen, een 'patserproject'. Mensen die dan in te dure auto's rondrijden, dat doen ze alleen maar in Zuidoost. Ze gaan niet bij het concertgebouw mensen uit hun dikke Mercedes trekken, zo van 'waar hebt u die mee verdiend?' Want nummer drie is een advocaat en dan heb je een probleem. Ja, u lacht er nou om, maar ik vind het… dat verhaal van Kowsoleea heeft vijftien jaar geduurd, die nachtmerrie.

Er is nog zo'n voorbeeld. Dat is Peter Tabbers, die is ook slachtoffer geworden van identiteitsfraude. Daarover zijn stukken verschenen in het NRC een paar jaar terug. Zowel Fred Teeven als Sophie in 't Veld hebben zich met zijn zaak bemoeid, vanuit het Nederlandse Parlement en vanuit het Europees Parlement en het heeft een jaar geduurd voordat hij bij Europol uit die database was; hij kon Nederland niet uit. Dat heeft dan maar een jaar geduurd. Ik kan dat niet bewijzen, maar ik denk dat dat er dan iets mee te maken heeft dat hij 'de ideale Nederlandse schoonzoon' is en gewoon bij een groot Nederlands bedrijf werkt en dan krijg je wel rugdekking. Maar je zult maar een rare achternaam hebben en je zal vooral maar Ahmed heten en een rare achternaam hebben en op zo'n lijst staan, dan kom je er gewoon niet meer vanaf.

Vanaf het moment dat je er op gaat letten kom je erachter dat er een soort nare, niet al te subtiele tweedeling aan het ontstaan is. De Volkskrant had een tijd geleden een verhaal over een parkeerplaats in Noord-Brabant waar dan kennelijk overlast was van homo's die van alles met elkaar aan het uitspoken waren. Toen was de politie daar mensen staande gaan houden en had even alle namen staan registreren van alle homo's die daar waren. Grote rel. Binnen twee dagen bood de korpschef zijn excuses aan: 'Nee, in Nederland gaan wij natuurlijk niet homo's preventief registreren.' Nou, prima, probleem opgelost.

Maar in Amsterdam zijn wij wel bezig met het preventief registreren van Marokkanen. En dat gebeurt onder verantwoordelijkheid van Job Cohen. Als jij een Marokkaan bent op een scooter kan je aangehouden worden en wordt jouw naam preventief geregistreerd. En omdat Cohen ook wel door heeft dat dat een beetje raar is, worden er voor de vorm ook nog 500 makelaars in Oud-Zuid van hun scootertjes afgehaald en wordt ook even hun naam opgeschreven. Maar iedereen weet: daar gaat het niet om. Ze zoeken naar die Marokkanen. Ik vind dat heftig.

Nu gebeurt dat onder leiding van Job Cohen en dat vind ik een fatsoenlijke man. Ik geloof niet dat hij daar nou rare plannen mee heeft. Maar Eberhard van der Laan maakte een tijdje geleden de terechte opmerking van 'Ja, dat etnisch registreren doen wij allemaal met de beste bedoelingen, maar wat nou als straks Geert Wilders 30 zetels heeft? Willen wij als PvdA eigenlijk nog wel meewerken aan het optuigen van dit apparaat? Nu zit daar Job Cohen die het nog wel goed bedoelt met die databank, maar straks zit daar een meneer die vindt dat Marokkanen door hun knieschijven geschoten moeten worden.'

En dan, met een druk op de knop, dan staan de vlaggetjes op de kaart op de laptop van de politie. En, ik moet eerlijk zeggen, als je dan nog even naar de rol van de media kijkt, dan hebben wij daar natuurlijk ook een kwalijke rol in gespeeld. Job Cohen is vaak genoeg afgeschilderd als softe theedrinker en hij wordt daar ook in zekere zin toe opgejaagd. Hij heeft niet veel ruimte om een genuanceerd betoog te houden als er schietpartijen zijn. Dan moet er preventief gefouilleerd worden, dan moeten die keiharde maatregelen er komen. Maar ik vind het zelf, en dat verwacht je misschien niet uit de mond van iemand die bij HP/De Tijd werkt, ik vind op dit moment dat Job Cohen veel te rechts is. Wat mij betreft mag hij wel wat softer worden en wat meer thee gaan drinken en wat minder preventief registreren. Daar wilde ik het graag bij laten.

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.

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.

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 Bert-Jaap Koops wel 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.

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 Bert-Jaap hoor praten, 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.

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 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.

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.

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 Alex Brenninkmeijer dat thema heel 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 dooddoener 'Ach, niets te verbergen.' bewijzen we – en degenen die de dezelfde dooddoener 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.

Mensenrechtelijke knelpunten voor het NJCM en aanbevelingen voor de Staatscommissie Grondwet

's Middags vonden vier workshops plaats: 'ICT en wetgeving' door Marga Groothuis (Universiteit Leiden) en Paul de Hert (Vrije Universiteit Brussel & Universiteit van Tilburg), 'Wettelijke bescherming in de praktijk' door Evelien Brouwer (Universiteit Utrecht) en Egbert Dommering (Universiteit van Amsterdam), 'Verantwoordelijkheid van het openbaar bestuur' door Ot van Daalen (Bits of Freedom) en Jolien Schukking (Rechtbank Utrecht) en 'Invloed van Europa' door Herke Kranenborg (Bureau Europees Toezichthouder voor gegevensbescherming) en Paul van Sasse van Ysselt (ministerie van Binnenlandse Zaken en Koninkrijksrelaties).

De bedoeling in de workshops was om de mensenrechtelijke knelpunten te identificeren op het gebied van bescherming van persoonsgegevens waar het NJCM de komende jaren mee aan de slag kan. Daarnaast werd de deelnemers van de workshops gevraagd om aanbevelingen te formuleren voor de Staatscommissie Grondwet ten aanzien van grondrechten en databescherming in het digitale tijdperk.

Paul de Hert – Workshop 'ICT en Wetgeving'

Goedendag allemaal. Wij hadden de leukste workshop van alle vier, we kwamen ook allemaal tot een breed gedragen consensus. Dus er was heel veel wijsheid, en ook de diversiteit met mannen en vrouwen, jonger en ouder, zat allemaal goed.

De knelpunten. Ondanks mijzelf was *het* knelpunt het Engelse 'problem of pace'. Dus het verschil tussen de technologische turbulentie en de wetgever, die daar dan maar op moet reageren, schijnbaar. Het gevoel was, tot mijn grote spijt, dat het recht daar veel te weinig tegen in kan brengen. Ik moet het signaleren als voorzitter, maar met een kleine dissent: ik geloof in algemene beginselen van het recht dus ik denk dat wij wel wat te zeggen hebben tegen die technologische turbulentie. Maar, vanuit het perspectief van de wetgever was dat het probleem.

- Knelpunt 1: de technologische turbulentie, 'problem of pace'. De technologie holt en de wetgever moet er achteraan.
- Knelpunt 2: afdwingbaarheid van transparantie en controlerecht. Dus de 'law in the books' komt niet naar voren in de praktijk of wordt niet beleefd.
- Knelpunt 3: een behoefte aan anonimiteit van communicatie, die moet opboksen tegen eisen en belangen als die van de opsporing.
- Knelpunt 4: het onderscheid tussen privacy en bescherming van persoonsgegevens niet voor iedereen duidelijk was. Dat bleek toch een knelpunt.

De aanbevelingen zijn niet noodzakelijk aansluitend op de knelpunten, zo werken wij niet, we zijn veel intelligenter. Een eerste aanbeveling valt uit het niets en gaat over Duitse rechtspraak van het *Bundesverfassungsgericht* die computersystemen beschermt. Dus naar aanleiding van Duitse wetgeving om politie toe te laten computers te hacken en door te zoeken heeft de *Bundesverfassungsgericht* interessante jurisprudentie ontwikkeld met een nieuw grondrecht op bescherming van computersystemen, de integriteit ervan. En onderzoek naar het nut en waarde van zo'n grondrecht is onze eerste aanbeveling. Dus die commissie moet gaan werken. Het is recente jurisprudentie, het is in het Duits dus het is hard werk, maar ze moeten het doen.

De tweede aanbeveling is het idee van *privacy by design*. We moeten op het niveau van de wetgeving rekening gaan houden met die 'ontwerpers'. Zij richten al het kwaad aan door slechte privacy producten te maken en het voorstel is dus concreet: vul de Wbp aan met een nieuw hoofdstuk dat zich richt tot de ontwerpers. Geef een juridisch kader aan die gedachte en bouw ook, en dat voeg ik er dan aan toe, meer juridische elementen rond de notie van veiligheid. Het juridisch kader om veilig te werken en om privacy-vriendelijk te werken is bijna onbestaand. Dat zit allemaal in de sfeer van *policies* en weet ik waar allemaal, maar niet in de sfeer van het recht.

Ten derde, aansluitend, vul de Wbp met materiële normen aan. En in het algemeen, elke wetgeving die er komt moet keuzes bevatten van het parlement, dus het parlement mag die niet doorschuiven, zoals het Europees Parlement wel heeft gedaan met de biometrie in het paspoort. Het is eigenlijk de keuze tussen centraal en decentraal, doorschuiven naar de lidstaten, wat aan Nederland heeft toegelaten om de slechtste keuze te maken. Dat mag niet gebeuren. Het probleem doorschuiven naar lagere niveaus in de keten, doorschuiven naar de ministers, is geen grondrechtelijk respectueuze aanpak. De wetgever moet de essentiële keuze zelf maken

en moet zich dan ook op het terrein van die technologie wagen en durven de beschikbare keuzes op een rij te zetten.

Concreter en terug naar de Grondwet is het herijken van artikel 13. Er moet een volwaardig grondrecht komen op de bescherming van alle communicatie, ook de digitale, met de focus op het middelen aspect. De mensen verwachten bescherming wanneer ze bepaalde communicatiemiddelen gebruiken, die suggereren dat er geheimhouding kan gebeuren.

En, herbekijk de Grondwet in het licht van het Europees Handvest dat met het Verdrag van Lissabon bindend zal worden en werk een mooie bepaling uit rond de bescherming van persoonsgegevens en hijs zoveel mogelijk principes in de Grondwet. Doelbinding, minimalisatie, eerlijkheid, werk die uit, besteed ook aandacht aan de *dataprotection* plichten voor de overheid. Laat niet gebeuren wat nu gebeurd is in de Grondwet, dat er voor de overheid eigenlijk maar één ding in staat: dat ze een wet nodig hebben om persoonsgegevens te verwerken. Er moeten meer grondwettelijke ijkpunten komen voor de overheid, die als een van de grote bedreigende actoren wordt gezien.

En dan de laatste aanbeveling, en daarover was de consensus het grootst: als er dan turbulentie is en als de wetgever en grondwetgever niet alles kunnen, kijk dan vooral naar het misbruik, naar wat er kan fout gaan op het terrein en zorg voor *effective remedies*, maar wérkelijk effectief. Daar staan we nu nog nergens. Dus een benadering van het consumentenrecht bijvoorbeeld, zou hier kunnen helpen. Wees genereuzer in uw herstel van individuele privacykrenkingen, denk aan de menselijke bewijslast. Ga niet op zoek naar concrete schade en tel die op een apothekersschaaltje op, maar geef gewoon toe als overheid dat je gefaald hebt en voorzie een serieus budget aan remediëring en kosteloosstelling voor opgelopen schade.

Dat zijn de aanbevelingen en knelpunten uit onze workshop.

Egbert Dommering – Workshop 'Wettelijke bescherming in de praktijk'

Het hoofdpunt dat wij besproken hebben en dat ook als punt 1 staat vermeld is 'privacy als zelfbeschikkingsrecht'. Zo is het eigenlijk ook als het gaat om dataprotectie. Het EHRM heeft dat recht in recente uitspraken steeds sterker zo geformuleerd. En dat heeft twee kanten. Het heeft natuurlijk de kant van het morele zelfbeschikkingsrecht, maar als het gaat over zelfbeschikking en de persoon dan is er ook altijd een economische component. Dat is iets minder ingewikkeld dan dat Brenninkmeijer vanochtend zei, we kennen dat natuurlijk al uit het portretrecht, persoonsgegeven bij uitstek. Dat betekent dus dat je ook dat zelfbeschikkingsrecht moet uitbouwen, niet alleen met publiekrechtelijke toezichtinstrumenten, maar ook met privaatrechtelijke middelen.

Dat kan allerlei consequenties hebben. Ten eerste, in geschillen over of je wel juist in het bestand staat. Dan heb je natuurlijk allerlei inzage- en correctierechten, maar voordat je daar een keer aan toe bent is de tijd alweer verstreken. Het is misschien beter om voorop te stellen dat niet de persoon moet bewijzen dat hij degene is die hij is, maar dat het systeem moet bewijzen dat de gegevens over een persoon in het systeem juist zijn. Dat betekent ook, en dat is een oude gedachte die weer bovenkomt, dat gegevens in beginsel in eigen beheer moeten zijn, dus het digitale kluisje waarover je zelf kan beschikken. Bijvoorbeeld, het patiëntendossier en zo zijn er nog veel meer dossiers waarover je in beginsel zelf beslist.

Een derde aspect is dat persoonsgegevens ook geld waard kunnen zijn. Naar mijn overtuiging worden persoonsgegevens het digitale geld van het internet. En dat kan dus betekenen dat je, net zoals dat met het auteursrecht gebeurt, je persoonsgegevens collectief beheert, dus dat je een soort privacy-Buma's krijgt.

Dat brengt me tot het tweede knelpunt: de falende toegang tot de rechter. Er zijn wel bemiddelingssituaties die werken, maar de algemene gevoelens in de praktijk in deze workshop was dat de toegang tot de rechter om allerlei redenen niet goed functioneert. Rechtsbijstand assuradeuren zijn geneigd om iemand die met een privacyklacht komt uit het bestand te verwijderen of op een zwarte lijst te zetten. De kosten zijn natuurlijk daardoor te hoog. De stappen die genomen moeten worden, allerlei dingen die te maken hebben met consumentachtige problematiek, die door het feit dat de vraagkant, de consumentenkant, niet georganiseerd is een belemmering voor de toegang tot de rechter is. Daar zou, vanuit een zelfbeschikkingsrechtgedachte, collectieve belangenbehartiging – naast wat de publiekrechtelijke toezichthouders doen – toch een stap voorwaarts zijn.

Nogmaals, we focussen, en dat viel me vanochtend ook al op, voortdurend op de publiekrechtelijk toezichthouding. We moeten meer bevoegdheden geven, hogere straffen opleggen, meer onderzoeksbevoegdheden geven. Helemaal vanuit het publiekrecht gedacht, omdat dat privacyrecht daar nu eenmaal vandaan komt.

Een derde knelpunt: het toezicht. Op zich moet je toezicht hebben, juist als het gaat om de structurele aanpak. Daar was men het in de workshop ook over eens. Dus een verbetering van de bevoegdheden.

Over de adviesfunctie van de toezichthouder zijn we het niet helemaal eens geworden, omdat daar natuurlijk ook speelt of het verplicht moet zijn, wat de betekenis daarvan moet zijn, of dat in één organisatie moet blijven? Daar waren we het eigenlijk niet zo over eens, dus daar doen we dan ook geen aanbeveling over.

Een belangrijk punt dat genoemd werd is concreter: het toenemende gebruik dat wordt gemaakt van de informatie die wordt verzameld door de veiligheidsdiensten in Nederland. En dat die op allerlei andere fronten worden ingezet. Dus de aanbeveling is dat daar een veel sterkere beperking van bevoegdheden in individuele gevallen moet zijn en dat er ook een betere concrete rechtsbescherming moet zijn met in individuele gevallen inzage in dossiers.

En dan bijna tenslotte de technische onbegrensdheid, *privacy by design*. Ik denk dat we de discussie in de eerste workshop, die de leukste workshop was die er is geweest heb ik begrepen, aanzienlijk hadden kunnen bekorten als we ze hadden kunnen uitleggen dat je natuurlijk nooit technische normen in de wet moet zetten, dat is echt het slechtste wat je kunt doen. Je moet natuurlijk wel, en dat heeft Hustinx vanochtend ook gezegd, streven naar privacy binnen *design*-protocollen en dergelijke. Met name ook omdat verdere invulling van een algemene zorgvuldigheidsnorm ook zin kan hebben als het gaat om aansprakelijkheidszaken en schadevergoedingsacties. Dat verbetert de bewijspositie van de consument bij grote data *breaches* en zou je er een collectieve actie voor kunnen starten. Dan heb je een betere uitgangspositie als je kunt aantonen dat gewoon de technische protocollen niet zijn gevolgd.

Een laatste punt, dat is alleen een knelpunt gebleven en geen aanbeveling: het probleem van de internationale gegevensstromen. Dat is eigenlijk helemaal niet aan de orde geweest vanochtend: het probleem van de rechtsmacht als het gaat over concerns, wereldwijde concerns, vooral als ze niet zijn gevestigd in de Europese Gemeenschap. Welke toezichthouder is daar

bevoegd en met name, hoe krijg je grip op de enorme druk en tendens naar zelfregulering. die natuurlijk vanuit die concerns uitgaat, de *binding corporate rules*? En ook, in verband daarmee de rechtsbescherming. Dus dat stond ook niet op de lijst, dit is erbij geschreven, punt 6: knelpunt, maar dat leidt niet tot punt 6 aanbeveling voor de Staatscommissie. Hoewel meneer Hustinx mij verzekerd heeft dat als wij de oplossing wisten, hij zich zeer aanbevolen hield.

Jolien Schukking – Workshop 'Verantwoordelijkheid van het openbaar bestuur'

Het was in deze workshop zeer interessant om te zien hoe aan de hand van het thema 'verantwoordelijkheid van het openbaar bestuur' tevens het onderwerp verantwoordelijkheid van de burger naar voren kwam. Niet alleen zijn er heel veel knelpunten gesignaleerd, er zijn ook kansen of voordelen genoemd hoe met het registeren van persoonsgegevens misschien juist de communicatie met of tussen burgers en overheid als een voordeel kan worden gezien. Genoemd werden bijvoorbeeld belastingformulieren, die voor een gedeelte al zijn ingevuld, wat het voor de burger makkelijker maakt om een aanvulling te geven en niet weer allerlei gegevens opnieuw te hoeven invoeren. We kwamen op basis van onze discussie tot een lange lijst van hele interessante punten, veel meer dan ik nu kan noemen. Die lijsten zijn bewaard en daar zal zeker nog wat mee gedaan worden. We hebben geprobeerd de punten die naar voren kwamen toch zodanig te koppelen dat ze ook weer terugkwamen in de aanbevelingen.

Als eerste werd een punt genoemd dat ook vanmorgen tijdens het plenaire gedeelte aan de orde kwam: de mogelijkheid of het gevaar van identiteitsfraude of -verwarring. Dat blijft natuurlijk een punt waar de overheid heel kritisch naar moet blijven kijken en veel aandacht aan moet besteden hoe dat voorkomen kan worden.

Als tweede mensenrechtelijke knelpunt hebben we samengevat als het ware onder de noemer 'onmatige overheid', 'Nanny State' of 'catch-all mentaliteit': de neiging van de overheid om alles te willen invoeren en koppelen zonder daarvan de consequenties van te voren goed in beeld te hebben.

Als derde knelpunt werd naar voren gebracht: de 'onzichtbare zichtbare overheid', dus het gebrek aan transparantie en voorlichting waardoor het draagvlak onder de samenleving en het verstrekken van gegevens afkalft. Het gebrek aan vertrouwen, waar vanochtend ook door de heer Hustinx over werd gesproken, zien we als een knelpunt.

Het vierde en vijfde knelpunt hebben allebei met 'onomkeerbaarheid' te maken. De ene in technische zin: alles wat technisch aan gegevens in systemen staat, alle datagegevens. Als daar een lek in komt is het niet te overzien wat de gevolgen zijn. De onomkeerbaarheid van de consequenties van een lek in de databestanden, technisch gezien.

En in de zin van het vijfde knelpunt: de onomkeerbaarheid van de juridische kant. De oneindigheid in bestaan van inbreukmakende bevoegdheden. Er kan een hele goede reden zijn geweest om opsporingsbevoegdheden in te voeren als er bijvoorbeeld een dreigingsgevaar is, maar moeten die regels dan ook altijd blijven bestaan?

Dat is kort samengevat de lange lijst van knelpunten.

Dan ga ik nu over naar de aanbevelingen. Deze zijn niet direct gekoppeld aan de knelpunten, ook omdat sommige aanbevelingen natuurlijk een waarde kunnen hebben voor meerdere

knelpunten. De eerste twee punten hebben een wat meer juridisch karakter, de anderen wat praktischer.

Als eerste is er gesuggereerd om met betrekking tot de wetgeving een soort privacy-effect-rapportage te introduceren. Een soort privacy-toets, die dan niet alleen betrekking heeft op het wetsvoorstel dat aan de orde is, maar dat juist in kaart brengt wat dit nieuwe wetsvoorstel in combinatie met reeds bestaande wetten voor effect heeft op de privacy.

Tweede punt, *sunset* regels: introduceer regels met een beperkte geldigheidsduur ofwel een hertoetsingmoment om te bezien of het bestaan van de inbreukmakende bevoegdheid nog wel noodzakelijk is.

Dan twee meer praktische punten. Ze kwamen vanmorgen ook al deels aan de orde. Het introduceren van een laagdrempelig loket waar burgers, die klachten of problemen hebben naar toe kunnen en hun problemen aan de orde kunnen stellen zonder van het kastje naar de muur te worden gestuurd. En dan is het de bedoeling dat achter dat loket de klacht wordt neergelegd bij de instantie waar die ook thuishoort.

Het vierde punt, dat ook meer van praktische aard is, is dat voorlichting heel belangrijk is in de communicatie met de burger. Maak kenbaar wat de bedoeling is van de wetgeving, wees daar volledig in. Dat maakt dat het draagvlak voor de regel groeit en het geeft aan de burgers aan waar ze aan toe zijn en tegelijkertijd, als iedereen weet wat de bedoeling is, wat de mogelijkheden zijn en wat de grenzen zijn. Dan biedt dat tegelijkertijd een waarborg tegen oneigenlijk gebruik van een dergelijke regeling.

Daaraan gekoppeld werd ook nog genoemd een meldplicht van blunders. Als per ongeluk gegevens op straat liggen, een plicht om dat meteen te melden zodat ook direct actie ondernomen kan worden.

En als vijfde, en dat heeft dan eigenlijk te maken met een zowel juridisch als technische punt, een invoer van een *audit*-plicht om zowel de integriteit van de technische systemen als de integriteit van het juridische systeem eens in de zoveel tijd door te lichten. En daaraan gekoppeld dan ook de aanbeveling meer gebruik te maken van *ethical hacking*.

Dat waren kort samengevat de knelpunten, kansen en voordelen en aanbevelingen, die tijdens de discussie in de workshop naar voren zijn gekomen.

Paul van Sasse van Ysselt – Workshop 'Invloed van Europa'

Het was niet de leukste werkgroep, dat kan al niet meer, maar het was wel erg leuk niettemin. Dat kwam mede omdat de discussie varieerde tussen inzichten over de pro's en contra's, de voor- en nadelen van de rechtsgang in een individueel geval, tot en met weidse vergezichten over waar we heen moeten met Europa en hoe Europa zich op dit moment ontwikkelt.

De invloed van Europa. We hebben eerst stilgestaan bij de vraag over welk Europa we het nu hebben. De Europese Unie, de Raad van Europa? Dat resulteerde al gauw in het gegeven dat we het al snel hebben over de EU als we het hebben over de relatie van Europa tot de bescherming van persoonsgegevens, waarbij ik direct aanteken het punt van verschil in standaardzetting. Standaardzetting is voornamelijk vanuit de Raad van Europa gekomen in het verleden, terwijl de handhaving van de standaarden zijn neergezet in de Raad van Europa en de Europese Unie zelf. Dus we hebben gekeken naar de standaardzetting en naleving van

die standaarden en de instituties die ook kunnen bijdragen aan de handhaving en de bevordering van de naleving van de bescherming van persoonsgegevens.

Rode draad daarbij was de vraag of Europa nou de beschermer van privacy is of inbreukmaker. Uiteraard allebei, maar belangrijk is toch dat, hoewel vaak in het publieke debat wordt gewezen met een vinger naar het boze Europa, maar dat in de werkgroep de Europese Unie ook zeker wordt gezien als een beschermende instantie. Uiteraard, vanwege de specifieke bepalingen in het Lissabon verdrag en het Europees Handvest van de grondrechten. Dus Europa omarmen of vrezen? Zo simpel ligt het niet. De voortreffelijke inleider overigens, die zeker eraan heeft bijgedragen dat de discussie werd gekanaliseerd, gaf ook aan dat dat per geval moet worden bekeken en beoordeeld. Maatstaven voor die beoordeling zijn de klassieke beginselen als doel, noodzaak, en controle achteraf. En dat zijn toch de punten die keer op keer worden gezien als waardevolle referentiebeginselen om de producten binnen Europa op te beoordelen.

Als we kijken naar de normstelling, zijn er drie interessante punten aan bod geweest: zou er niet een verbod moeten komen op een soort kop op de Europese regelgeving waar je ziet dat een Europese regeling iets voorschrijft op een gegeven moment? Dan kan een nationaal parlement natuurlijk daarop verdergaan bij de implementatie. Die discussie heeft zich natuurlijk voorgedaan met betrekking tot de paspoorten en de vingerafdrukken en de vraag is: zou dat niet vanuit de Europese Unie verboden moeten worden? Er wordt een handreiking gedaan om het ene te regelen, en zou het daar dan niet bij moeten blijven? Daar was verder geen consensus over, maar het was wel een onderwerp van discussie.

Daarnaast ook het punt van de vraag of er niet juist meer Europa zou moeten zijn als er onduidelijkheid is over open normen? Ook op de werkvloer via de implementatie van Europese regelgeving, zoals in de Wbp. En zou dat niet moeten leiden tot meer richtsnoeren en dergelijke, eventuele *soft law*?

Als derde punt is aan de orde geweest de vraag, naar aanleiding van het enorme regelcomplex in Europa, of er niet een overkoepelend instrument zou moeten zijn? En de vraag of de plannen binnen de Europese Commissie, binnen Europa, zich niet ook al in die richting ontwikkelen met een mogelijke herziening van de Europese richtlijn uit 1995? Dat wat betreft normstelling.

Voor wat betreft de instituties, daar hebben we ook naar gekeken en dan komen we meer in de richting van aanbevelingen richting het NJCM. De weg naar Brussel, dat is toch wel een hele belangrijke beïnvloeding van de inhoud van Europese instrumenten en uiteindelijke ook de Nederlandse instrumenten. Dat betekent dat, bijvoorbeeld als je kijkt naar het Stockholm programma dat de komende tijd onderhandeld wordt – het meerjarenprogramma voor Justitie en Binnenlandse Zaken aangelegenheden binnen de Europese Unie – het belangrijk is om niet te wachten tot over tien jaar, als er een implementatiewet is die voortvloeit vanuit een richtlijn of instrument dat voortvloeit vanuit het Stockholm programma. Nee, dan zou nu al in een reactie op het concept-Stockholm programma invloed kunnen worden uitgeoefend. De vraag is waar dat dan te doen? Dat is natuurlijk op allerlei niveaus en via allerlei wegen: het Europees Parlement, de Tweede Kamer, of de Eerste Kamer, waarbij de interessante strategische signalering nog wel werd gedaan, en dat is natuurlijk een knelpunt. En soms is het strategisch wijzer

om de Tweede Kamer niet te belobbyen op een bepaald punt, omdat dat juist afbreuk zou kunnen doen aan het beschermende gehalte van Europese instrumenten die in de maak zijn.

Andere instellingen die benaderd zouden kunnen worden zijn ook meer recente instellingen zoals het EU-Grondrechtenagentschap dat ook activiteiten verricht op het terrein van de bescherming van persoonsgegevens in de meer dataverzamelende zin, die van nut kan zijn voor Europese lidstaten en instellingen. En bijvoorbeeld ook bij de Europese toezichthouder zelf. Daar is nu geen gestructureerd contact tussen NGO's en de werkzaamheden van de Europees Toezichthouder. Er wordt wel gebruik gemaakt van opinies en dergelijke en dat is het nadenken en het verder bekijken waard van meer structurele of effectievere invloed op een dergelijk toezichthoudend orgaan. Dan kom ik bij het laatste punt voor wat betreft de aanbevelingen en aandachtspunten ook richting het NJCM.

De Staatscommissie is ook aan de orde geweest en wat we de commissie zouden kunnen meegeven. Dat is in een korte tijd aan de orde geweest, maar er zijn drie heldere punten uit gekomen. In de eerste plaats wijziging van artikel 120 Gw, die nu onmogelijk maakt dat de rechter wetgeving in formele zin toetst aan de Grondwet. In de tweede plaats zou privacy meer gekoppeld moeten worden aan het recht op persoonlijke identiteit en als zodanig explicieter in de Grondwet moeten worden opgenomen. In de derde plaats, en als laatste, de aanbeveling om bescherming van persoonsgegevens nu een meer materiële invulling te geven dan enkel de opdracht aan de wetgever om dat verder uit te werken.

Dat was samengevat hetgeen dat zich in onze werkgroep heeft afgespeeld.

Corien Prins – Afsluitingsspeech

Dames en heren, wij gaan richting de borrel om het glas te heffen op de jarige. Over tien minuten wilde ik u uitnodigen hiernaast dat glas te gaan heffen. Ik wilde heel kort afronden. Ik ga geen herhaling van alles doen.

Ik heb krampachtig geprobeerd om mee te schrijven met al deze aanbevelingen en samenvattingen. Zoals gezegd geen herhalingen, maar er vallen mij toch wel een paar punten op en die licht ik, als conclusie voor u vandaag, voor u uit.

Effective remedies, falende toegang tot de rechter, laagdrempelig loket. Iets wat in ieder geval onze *keynote speaker*, de Nationaal ombudsman, tijdens zijn lezing ook aan ons meegaf en ik zie het in ieder geval in de aanbevelingen van een drietal werkgroepen terugkomen. Ik proef dat dat ook echt een opdracht is. Misschien niet zozeer specifiek voor de Staatscommissie, maar voor ons allemaal, werkzaam bij de departementen, de rechterlijke macht, de advocatuur, het bedrijfsleven.

Wat ik in ieder geval in mijn werkgroep heb geproefd is dat we in het begin allemaal onze stellingen innamen, de mensen van de departementen, er was iemand van Vrijbit bij ons, een advocaat, en uiteindelijk had ik aan het einde van tweeënhalf uur praten het gevoel dat wij met zijn allen een taak zien, ieder vanuit zijn eigen niveau, vanuit zijn eigen functie.

Mijn eerste punt, laagdrempelig, iets voor burgers realiseren, *effective remedies*. Toegang tot de rechter of andere mogelijkheden daartoe is absoluut, voor ons allemaal denk ik, een aandachtspunt.

Een tweede punt dat ik eruit haal: de realiteit is dat de technologie een heel belangrijke rol speelt in de problematiek die wij vandaag hebben besproken. Het observeren van mensen, opslaan van gegevens, verwerken van gegevens, grootschalige systemen, camera's etcetera, het is allemaal technologie. En of technologie het nu zelf doet of dat technologie een neutraal instrument is en de mensen het doen, de organisaties. Maar technologie speelt daar een rol en technologie is ook absoluut faciliterend in de oplossing en dat zou mijn tweede observatie zijn.

Ik heb een aantal keren gehoord, dat *privacy by design*, ik vat het maar even onder die brede noemer, en daar is natuurlijk van alles rond omheen te vertellen. *Privacy by design* benut de technologie. Vooral ook daar waar de technologie een dreiging is, is ze ook een kans. Laten we dat verder proberen te doordenken. In ieder geval ook voor mij een conclusie aan het einde van de dag.

Dan heb ik als laatste conclusie voor mijzelf genoteerd: de aandacht voor de materiële normen en de verantwoordelijkheid voor het zetten van die materiële normen. In ieder geval in de eerste samenvatting van Paul de Hert, werd expliciet gezegd: schuif dat als wetgever niet door. Niet alleen op het Europese niveau, maar ook hier, in Den Haag. Schuif het niet door naar een onderliggend niveau. Hou dat op je eigen bordje, ga de uitdaging aan. Dat wat betreft de materiële normen.

En richting de Staatscommissie: misschien is het ook wel eens tijd om op het niveau van de Grondwet veel explicieter te maken dat het tijd is voor meer dan alleen een algemene riedel, maar dat we handen en voeten moeten geven aan die materiële normen op het niveau van de Grondwet en dat we daarmee ook bij de wetgever meer expliciet de opdracht geven om het niet door te kunnen schuiven. Kortom, heb meer aandacht voor de materiële normen, ga die uitdaging aan in deze tijd en maak er dan wat van en laat privacy niet tot een mythe verworden.

Ik zou van alles en nog wat nog met u kunnen delen aan aantekeningen die ik van deze dag heb gemaakt. U heeft voor uzelf vanuit uw eigen perspectief ook heel veel aantekeningen kunnen maken, heel veel kunnen meepraten en meediscussiëren. Ik denk dat dat absoluut deels een succes van deze dag is geweest.

Ik wil het NJCM daarvoor bedanken en ik denk dat het een uitstekend platform is geweest met een aantal interessante lezingen, waarvan ik de sprekers namens de organisatoren wil bedanken. Niet allemaal zijn ze nog hier, maar in ieder geval heel erg bedankt. Ik wil ook de sprekers, voorzitters en inleiders van de verschillende werkgroepen van vanmiddag nog bedanken. En u allemaal.

Ik geef de voorzitter nog heel even het woord, laten we dan het glas heffen op de toekomst van privacy. Ik wil nog niet zover gaan als Bert-Jaap Koops, dat hij alles wil afschaffen, dat vind ik te veel een doemscenario. Ik heb zelf het idee dat we aan het eind van deze dag allemaal inspiratie hebben gekregen om weer stapjes te zetten in een andere richting, namelijk in de richting van opbouwen.

Quirine Eijkman – Afsluiting van het congres

Hartelijk dank, Corien Prins. Ik ga nu nogmaals afsluiten. Allereerst wil ik alle aanwezigen bedanken voor jullie actieve bijdrage. Ook wil ik hierbij oproepen dat, mocht je nog geen lid zijn van het NJCM, dat je dat natuurlijk vandaag kan worden. Kom straks even vragen hoe dat moet en ik licht je in. Je kan ook actief betrokken worden bij het NJCM, want we zijn altijd op zoek naar advocaten, rechters, ambtenaren, iedereen die mee wil denken om van het NJCM een platform te maken om mensenrechten na te leven in beleid en wetgeving.

In dit specifieke geval gaat het natuurlijk om digitale grondrechten. Wat gaat het NJCM nou doen met dit congres, want dat is natuurlijk ontzettend belangrijk. Ten eerste komt er een lustrumbundel. Die is in de maak. Alle sprekers vandaag en anderen gaan hun gedachten nog wat verder uitkristalliseren op papier en daar gaan we een bundel van maken. We hopen ook zeer concrete adviezen aan de Staatscommissie voor de herziening van de Grondwet mee te geven, maar ook voor de wat meer algemene discussie en om een naslagwerk te schrijven zodat mensen er ook op de lange termijn wat aan hebben.

Wat betreft de knelpunten, we hopen dat het de komende jaren centrale onderwerpen gaan worden binnen het beleid van het NJCM, niet alleen de risico's voor de inbreuk op fundamentele rechten, zoals privacy, de risico's op *ethnic profiling*, non-discriminatie. We denken ook zeker dat fundamentele rechten en mensenrechten een deel van de oplossing kunnen zijn, bijvoorbeeld als het recht op informatie wat explicieter wordt, *effective remedies*, waar vandaag al een paar keer over is gesproken, de waarborgen voor de vrijheid van meningsuiting en ga zo maar door.

Heel concreet: graag wil ik iedereen bedanken die hier vandaag heeft gesproken, de plenaire sprekers, de inleiders en voorzitters van de workshops en in het bijzonder dagvoorzitter Corien Prins.