Tweede Kamer der Staten-Generaal

1/2

Vergaderjaar 2012–2013

32 761 Verwerking en bescherming persoonsgegevens

A/ Nr. 45

VERSLAG VAN EEN INTERPARLEMENTAIRE CONFERENTIE

Vastgesteld op 7 november 2012

Op dinsdag 9 en woensdag 10 oktober 2012 vond een interparlementaire commissievergadering plaats in het Europees Parlement te Brussel over de herziening van Europese wetgeving ter bescherming van persoonsgegevens. De Eerste Kamer werd vertegenwoordigd door senator Ter Horst (PvdA), lid van de vaste commissie voor Immigratie & Asiel/JBZ-Raad. Namens de vaste Kamercommissie voor Veiligheid en Justitie van de Tweede Kamer nam het lid Gesthuizen (SP) deel. De conferentie had de vorm van een gemeenschappelijke vergadering van vertegenwoordigers van nationale parlementen uit 19 lidstaten en de commissie voor burgerlijke vrijheden, justitie en binnenlandse zaken (LIBE) van het Europees Parlement. Tevens namen maatschappelijke actoren deel aan de conferentie. Gedurende acht sessies, verdeeld over twee dagen, werd gedebatteerd over de verschillende aspecten van de nieuwe verordening voor gegevensbescherming in het algemeen en de nieuwe richtlijn voor bescherming van gegevens bij gebruik door politie en justitie.[1] De Europese Commissie, ook vertegenwoordigd bij deze bijeenkomst, heeft de voorstellen voor deze nieuwe regelgeving op 25 januari van dit jaar gepubliceerd.

Dag 1: dinsdag 9 oktober 2012

Opening door Martin Schulz, voorzitter van het Europees Parlement

De ochtendsessie wordt geopend door de voorzitter van het Europees Parlement, Martin Schulz. Deze opent met de mededeling dat het onderwerp van de conferentie één van de belangrijkste dossiers van het Europees Parlement is voor de huidige termijn tot 2014. Hij memoreert de tijd dat gegevensbescherming enkel techneuten interesseerde en stelt dat het nu iedereen raakt: van sociale media tot online bankieren, van verzekeringen afsluiten en vliegtickets kopen tot boodschappen doen. Schulz was in 1995, toen de huidige Richtlijn bescherming persoonsgegevens (Richtlijn 95/46/EG) werd opgesteld, lid van de behandelde commissie. Hij vertelt dat terwijl technologische vooruitgang de mogelijkheden om gegevens te gebruiken en op te slaan enorm heeft vergroot, het gebruik van gegevens over internet enorm is toegenomen en de interactie

[1] COM(2012)11 en COM(2012)10. Zie ook de dossiers **E120003** en **E120004** op www.europapoort.nl

kst-32761-45
ISSN 0921 - 7371
's-Gravenhage 2012

tussen mensen anders is geworden, de verwarring over de juiste omgang met gegevens niet is veranderd sinds 1995. Schulz somt in zijn openingsspeech de belangrijkste aandachtspunten van het Europees Parlement ten aanzien van de nieuwe regelgeving op:

- gegevensbescherming is een fundamenteel recht (waar de Europese Unie trots op mag zijn, aldus Schulz);
- de onafhankelijkheid van nationale toezichthouders;
- de gedelegeerde bevoegdheden zijn niet alleen technisch van aard. Het Europees Parlement zal hier scherp op toezien, ook als dat tot gevolg heeft dat het als hinderlijk wordt ervaren;
- het vertrouwen van burgers in de bescherming van persoonsgegevens is zeer laag;
- de bescherming van kinderen tegen de uitwassen van vrij internet. Vanwege laag risicobewustzijn is onderwijs op dit gebied van belang en
- omgang van gegevens door ordehandhavende instellingen.

Schulz grapt dat de pijlers van de Europese Unie nog lijken te bestaan buiten de muren van het Europees Parlement, terwijl deze formeel zijn afgeschaft met het Verdrag van Lissabon. Hij memoreert het geval van Schengenwetgeving waar het EP, door de behandeling van een aantal dossiers te blokkeren, heeft laten zien dat het de intergouvernementele manier van handelen door de ministers uit de lidstaten niet meer accepteert. Dit zou ook op dit gebied tot de mogelijkheden behoren, omdat de twee rapporteurs, waar het de ambitie om een hoog beschermingsniveau te bereiken betreft, het gehele Europees Parlement achter zich hebben. Het doel is volgens Schulz het bereiken van een sterk raamwerk voor gegevensbescherming ten behoeve van de interne markt. Mensen zullen enkel gebruik maken van de interne markt indien er sprake is van vertrouwen in de digitale economie en ze kunnen vertrouwen op de overheid bij het beschermen van hun rechten. Schulz benadrukt ten slotte het belang van samenwerking tussen het Europees Parlement en de nationale parlementen zodat het werk op beide niveaus complementair aan elkaar kan zijn.

Session I – The reform of the EU Data Protection Framework – Building trust in a digital and global world

De eerste sessie wordt voorgezeten door Europarlementariër **Juan Fernando López Aguilar** (S&D), tevens voorzitter van de LIBE-commissie. Hij opent de sessie met de korte opmerking dat tegenwoordig veel bedrijven gegevensverwerking als kern van hun *business model* hebben en dat gegevensverwerking en gegevensuitwisseling in toenemende mate van belang zijn voor opsporingsinstellingen. Hij stelt dat het Europees Parlement de doelstellingen van de nieuwe voorstellen ondersteunt en geeft zicht op de planning van de behandeling: de ontwerprapporten zullen naar verwachting in december 2012 in de LIBE-commissie worden gepresenteerd en een oriënterende stemming, waarna de rapporteurs kunnen onderhandelen met de Raad, wordt in het voorjaar van 2013 verwacht. López Aguilar sluit af met de mededeling dat de bijdragen van nationale parlementen mee worden genomen in de discussie in het Europees Parlement.

De eerste spreker van de eerste sessie is **Ionas Nicolaou**, voorzitter van de commissie voor Juridische Zaken van het Cypriotische parlement. Ook hij benadrukt het belang van de herziening van de wetgeving als antwoord op het enorme verschil tussen begin jaren '90 en nu. Nicolaou noemt de grote commerciële belangen bij gegevensverwerking en benadrukt het belang om vertrouwen in de bescherming van persoonsgegevens te versterken. De verschillen tussen lidstaten veroorzaken een

gebrek hieraan en het wetgevend kader moet een balans vinden tussen het recht op bescherming van persoonsgegevens enerzijds en de interne markt anderzijds. Verder stelt Nicolaou dat administratieve lasten moeten worden verminderd, met name voor het midden- en kleinbedrijf (MKB). In zijn speech somt hij vele aspecten uit de herziene voorstellen op, als inleiding voor de verdere discussie. In het bijzonder noemt hij het belang van bescherming van kinderen en de uitwisseling van gegevens met derde landen op basis van bilaterale overeenkomsten. Ten slotte roept Nicolaou op tot intensieve samenwerking tussen nationale parlementen, het Europees Parlement en de lidstaten om bezorgdheid over de herziene voorstellen te overwinnen.

De tweede Cypriotische spreker is de minister van Justitie, **Loucas Louca**. Hij noemt gegevensbescherming één van de belangrijkste uitdagingen van het Cypriotische voorzitterschap. Er wordt veel aandacht besteed aan het consulteren van belanghebbenden en het creëren van een degelijke basis voor het lerse voorzitterschap vanaf januari 2013. Louca spreekt zijn waardering uit voor de interparlementaire conferentie en beschouwt deze als een belangrijke ontwikkeling in het kader van het Verdrag van Lissabon waarin het Europees Parlement en de nationale parlementen een grotere rol hebben gekregen. Louca noemt verder een aantal aspecten van de ontwerpverordening waar zijn aandacht naar uitgaat, zoals het recht om vergeten te worden, de *one-stop shop* waardoor burgers en bedrijven zich slechts tot één toezichthouder hoeven te wenden (toezichthoudende autoriteit = de toezichthouder in het land waar een bedrijf zijn belangrijkste vestiging heeft; artikel 51, tweede lid), uniforme normen voor boetes, *privacy by design* en de verplichting om *privacy impact assessments* te houden. Hij benadrukt het belang dat de regelgeving technologische ontwikkelingen niet moet tegenhouden en geen obstakels moet creëren voor gewone mensen. Met betrekking tot de ontwerprichtlijn stelt hij dat deze verbeterde samenwerking van diensten in de lidstaten tot gevolg moet hebben en haalt aan dat Europol, Eurojust en inlichtingendiensten zijn uitgezonderd van de werking van de richtlijn. Louca gaat kort in op de lopende onderhandelingen in de Raadswerkgroep DAPIX, die nog zes keer bijeen zal komen in het najaar, en tevens op de besprekingen tijdens de informele JBZ-Raad van afgelopen zomer. Hij toont zich bewust van de problemen met en twijfels bij de bepalingen en zegt te streven naar een evenwichtig compromis met het Europees Parlement als belangrijkste partner. Volgens Louca is het zaak te komen tot een deugdelijk juridisch instrument dat gegevens van burgers beschermt, mensenrechten versterkt, economische groei stimuleert en welvaart voor burgers brengt.

Hierna is het woord aan **Françoise Le Bail**, directeur-generaal van het Directoraat-Generaal voor Justitie van de Europese Commissie. Zij spreekt haar waardering uit voor de samenwerking met nationale parlementen en zegt toe de bijdragen van de verschillende lidstaten in ogenschouw te nemen. Le Bail zet uiteen wat de belangrijkste intentie was van de Europese Commissie bij het voorstellen van de nieuwe regelgeving. Het betreft een intentie die wordt uitgedrukt door de titel van de bijeenkomst: vertrouwen creëren. Hiertoe is allereerst het versterken van individuele rechten van belang, bijvoorbeeld door het recht om vergeten te worden, het recht op dataportabliteit en het recht op informatie. Deze maatregelen worden noodzakelijk geacht om vertrouwen te creëren. Le Bail stelt dat het creëren van vertrouwen een *business case* is, omdat het ontbreken van vertrouwen het aankopen van goederen of diensten op internet door consumenten belemmert. Het tweede uitgangspunt is het simplificeren van het regelgevend kader in de Europese Unie. De verschillende wijzen van implementatie van de huidige regelgeving in de lidstaten zorgen er bijvoorbeeld voor dat bedrijven bij 27 verschillende toezichthouders

moeten zijn. Le Bail stelt dat de keuze voor een verordening, die rechtstreeks toepasselijk zal zijn in de lidstaten, het gevolg is van deze ambitie. Daarnaast is het idee van de *one-stop shop* van belang om de lasten van bedrijven en burgers te verlichten, net zoals de uitzondering voor het MKB, dat daardoor minder administratieve lasten heeft, met uitzondering van bedrijven waarvan de belangrijkste activiteit dataverwerking is.

Het derde uitgangspunt is dat de wetgeving bestand moet zijn tegen technologische ontwikkelingen in de toekomst. Dit is het voornaamste doel van de gedelegeerde handelingen, die op diverse plaatsen in de voorstellen voorkomen. Via deze weg kan de regelgeving op detailniveau, onder toezicht van het Europees Parlement en de Raad, nader worden uitgewerkt door experts. Volgens Le Bail geeft dit de noodzakelijke flexibiliteit om de regelgeving *future-proof* te kunnen noemen. Met betrekking tot de ontwerprichtlijn geeft Le Bail aan dat deze in meerdere opzichten een verbetering betreft ten opzichte van het kaderbesluit uit 2008 (2008/977/JBZ). Allereerst wordt toezicht voorgesteld door de Europese Commissie en het Hof van Justitie. Daarnaast betreft het voorstel een uitbreiding naar binnenlandse verwerking van gegevens door politie en justitie omdat het lastig is om onderscheid te maken tussen gegevens die over de grens worden uitgewisseld of enkel binnen een lidstaat. Le Bail benadrukt dat de ontwerprichtlijn ziet op het beschermen van gegevens door ordehandhavende instellingen met voldoende aandacht voor de specifieke vereisten van deze sector. Ten slotte geeft Le Bail aan dat de Commissie graag met betrokkenen wil samenwerken om de vraagtekens die nog leven weg te nemen.

In reactie op deze drie bijdragen van de eerste sessie vragen meerdere deelnemers vanuit de nationale parlementen het woord. Opvallend is dat in een zeer groot aantal interventies scherpe kritiek doorklinkt op het grote aantal gedelegeerde handelingen dat de Europese Commissie volgens de voorstellen mag vaststellen. Verder klinkt er vanuit de zaal zowel lof als kritiek. Vanuit het Spaanse parlement benadrukt **Meritxell Batet Lamana** dat bepalingen omtrent de verantwoordelijkheid van zoekmachines (o.a. artikel 17 over het recht om gegevens te laten wissen) duidelijker moeten worden uitgewerkt. Zoekmachines zijn niet slechts tussenpersonen maar hebben verantwoordelijkheid wat betreft het beschermen van intellectueel eigendom en privacy van burgers en bedrijven. Namens de Italiaanse senaat spreekt **Laura Allegrini**. Deze senaat is voorstander van de herziening, maar ziet een bedreiging in gezamenlijke standaarden als daarmee bestaande nationale wetgeving overboord gaat en daarmee nationale beschermingsmaatregelen met een hoger beschermingsniveau. Ze uit twijfels bij de subsidiariteit van de voorstellen. Le Bail verwijst in haar antwoord naar artikel 8 van het Handvest van de grondrechten, dat een gelijk niveau van bescherming van persoonsgegevens vraagt. Vanuit de Italiaanse senaat klinkt tevens kritiek op de eventuele gevolgen van de *one-stop shop*, namelijk dat burgers niet bij de eigen nationale toezichthouder terecht kunnen. In reactie hierop geeft Le Bail aan dat burgers zich nog steeds kunnen wenden tot hun eigen nationale toezichthouder, die dan de verantwoordelijkheid heeft om met andere toezichthouders in contact te treden. Vanuit de Poolse Sejm reageren **Ryszard Kalisz** en **Andrzej Gałaśewski**. Eerstgenoemde meent dat er nog veel lacunes zijn in de voorstellen, bijvoorbeeld om misbruik van persoonsgegevens door niet-democratische regimes te voorkomen. Ook formuleert bij kritiek op onprecieze formuleringen in de verordening, bijvoorbeeld met het oog op het recht om vergeten te worden en de plicht om derde partijen te informeren. Volgens Kalisz is de definitie van «derde partijen» onvoldoende uitgewerkt om te voldoen in een tijd waarin links binnen een fractie van een seconde zijn gelegd. Gałaśewski vertelt dat de Sejm een

consultatie heeft georganiseerd onder parlementariërs, bedrijven en experts, waaruit steun voor het idee van een *one-stop shop* bleek. Hij benadrukt dat de ontwerpverordening onvoldoende bescherming biedt voor gevoelige gegevens, bijvoorbeeld gezondheidsgegevens.

Vervolgens krijgt **Sharon Gesthuizen** namens de Tweede Kamer het woord en ze vraagt Le Bail waarom er is gekozen voor de lijn om MKB's uit te zonderen op basis van het aantal werknemers, terwijl kleine bedrijven ook te maken kunnen hebben met gegevensverwerking van vele personen. Le Bail geeft aan dat het criterium van 250 fte de breed gesteunde Europese definitie voor een MKB betreft. Voor het MKB geldt dat bepaalde verplichtingen uit de verordening niet gelden, maar dat ze wel aan de uitgangspunten ervan moeten voldoen. Dat kleine bedrijven soms zeer gevoelige gegevens verwerken, wordt volgens Le Bail in de ontwerpverordening ten volle erkend. Ten slotte krijgt de Cypriotische Europarlementariër **Kyriacos Triantaphyllides** (GUE-NGL) het woord en hij stelt dat in het Europees Parlement op dit moment behoefte is aan een helder wettelijk kader met één instrument. Hij betreurt het dan ook dat er sprake is van twee instrumenten, een verordening en een richtlijn. Op zijn vraag waarom de Raad heeft gekozen voor een aparte behandeling van beide instrumenten krijgt hij het nietszeggende antwoord dat de ontwerprichtlijn en de ontwerpverordening twee maatregelen zijn die in tandem worden behandeld.

Session II – Harmonised and strengthened data protection rights and principles for an interconnected world

De tweede sessie van de conferentie wordt voorgezeten door de rapporteur van de ontwerpverordening, de Duitse Europarlementariër **Jan Philipp Albrecht** (EGP-EVA). Hij geeft snel het woord aan de eerste spreker terwijl hij aangeeft dat hij als rapporteur voldoende ruimte heeft om zich te uit te laten over de nieuwe regelgeving.

Marietta Karamanli, vicevoorzitter van de commissie voor Europese Zaken van de Franse Assemblée Nationale, benadrukt dat de verordening directe werking zal hebben in de lidstaten en daardoor meer gevolgen heeft op het niveau van de lidstaten dan een richtlijn. Ze spreekt de hoop uit dat de verordening het niveau van bescherming verhoogt en de privacy van burgers beter beschermt. De Assemblée heeft een aantal kanttekeningen en de spreker somt de verschillende onderwerpen op. Allereerst bijvoorbeeld bij het recht om vergeten te worden, met name met betrekking tot gegevens die kinderen online hebben gezet, welk artikel nadere uitwerking behoeft. Tevens moet de tekst over de verantwoordelijkheid van bedrijven voor de gegevens die ze gebruiken worden verduidelijkt. Het doel van de verordening is dat het recht van het individu wordt verbeterd en deze rechten moeten gegarandeerd worden. Ze benadrukt verder het belang van heldere en begrijpelijke communicatie tussen het individu en de gegevensverwerker en het belang van expliciete toestemming. In de voorstellen worden de verwerkers en de voor de verwerking verantwoordelijken verantwoordelijk gesteld voor het garanderen van de rechten van burgers en de verordening voorziet in sancties als zij daar niet aan voldoen. Hiertoe is het belangrijk om te identificeren wie er allemaal gegevens bezitten, aldus Karamanli. De Assemblée ondersteunt de voorgestelde procedures en mechanismen voor individuen om de uitoefening van hun recht te kunnen afdwingen en hecht waarde aan onderwijs aan burgers om verstandig met gegevens te leren omgaan. Dat de Assemblée belang hecht aan handhaving van de regelgeving blijkt uit de oproep voor nauwere samenwerking tussen nationale toezichthouders, onderwijl de onafhankelijkheid behoudend, en identificatie van dataverwerkers en hun hoofdkantoren om klachten te

kunnen afhandelen. Karamanli stelt een pilot voor om te testen of het voorgestelde systeem voor toezichthouders effectief werkt in het geval van klachten van individuele burgers wier gegevens zich ook in meerdere landen kunnen bevinden. Twee belangrijke zwakheden zijn verder de grote hoeveelheid gedelegeerde bevoegdheden en de uitzondering van Europol en andere EU-instellingen. Karamanli sluit af door te stellen dat de nieuwe voorstellen vooruitgang betekenen op een groot aantal punten, maar dat er nog substantiële verbeteringen nodig zijn waar de Europese Commissie verder aan moet werken.

Als tweede neemt **Gerrit Hornung** van de Universiteit van Passau[1] het woord. Hij acht de voorstellen een waardevolle verbetering van de bestaande wetgeving, maar heeft desalniettemin een aantal kritiekpunten, waarbij hij zich concentreert op de nieuwe rechten van burgers. Allereerst spitst zijn kritiek zich toe op de bepaling over «profiling» (artikel 20 van de ontwerpverordening). Die beperkt alleen de mogelijkheden voor maatregelen op basis van profiling, terwijl ook profiling zélf zou moeten worden gereguleerd. Een volgend aandachtpunt betreft het gebruik van zogenaamde keurmerken om een hoog niveau van gegevensbescherming aan te duiden. Hornung hecht waarde aan democratische vaststelling van procedures en bevoegdheden bij het gebruik en handhaven van een dergelijk «gegevensbeschermingskeurmerk». Hij haalt hierbij een voorbeeld aan waarbij het Duitse parlement geen overeenstemming kon bereiken over de nadere uitwerking van een «gegevensbeschermingskeurmerk». Dit brengt Hornung tot de mening dat dit niet via gedelegeerde bevoegdheden aan de Commissie moet worden overgelaten.

Hornung bestempelt vervolgens het consistentiemechanisme voor de handhaving van de regelgeving (Hoofdstuk VII, Afdeling 2 van de ontwerpverordening), waarin de nationale toezichthouders zoals het hoort volledig onafhankelijk zijn, maar de Europese Commissie zichzelf op Europees niveau het laatste woord heeft gegeven, als hogelijk inconsistent en stelt dat dit moet worden aangepast. Het recht op dataportabiliteit is volgens Hornung een stap vooruit, maar heeft pas het gewenste effect als digitale dienstverleners beter samenwerken (interoperabiliteit). Over het recht om vergeten te worden is Hornung terughoudend en hij wijst op de problematische verhouding tussen een Europees «recht om vergeten te worden» en nationale bepalingen omtrent vrijheid van meningsuiting en persvrijheid, waarvoor de nieuwe voorstellen geen oplossing bieden. Verder noemt Hornung het belang van een juridische basis voor het verwerken van gegevens, en hij stelt dat eventuele uitzonderingen hierop reeds in de regelgeving moeten worden opgenomen in plaats van later te beslissen of een juridische basis nodig is of niet voor bepaalde gegevens.

Hornung benadrukt ook de onduidelijkheid van bepalingen omtrent het verwerken van gegevens voor publieke autoriteiten, bijvoorbeeld als dit noodzakelijk is voor het vervullen van een «taak van algemeen belang» of een «taak die deel uitmaakt van de uitoefening van het openbaar gezag». In deze context wijst hij op de discussie die momenteel in Duitsland word gevoerd over nationale basisregistraties en bijvoorbeeld de toegang van private partijen tot deze databases. Ten slotte benadrukt hij, zoals meerdere sprekers, dat de ruime delegatie van bevoegdheden aan de Europese Commissie, die niet slechts niet-essentiële onderdelen van de voorstellen betreft zoals het Verdrag voorschrijft, niet te verantwoorden is.

Na deze kritische beschouwing krijgt **Jean Gonie**, director of privacy bij Microsoft Europe, het woord. Hij stelt dat iedereen op zoek is naar vertrouwen en vertrouwelijkheid, met name met het oog op de actuele en toekomstige ontwikkelingen. Met betrekking tot de nieuwe regelgeving

[1] http://www.europarl.europa.eu/document/activities/cont/201210/20121008ATT53088/20121008ATT53088EN.pdf

heeft Microsoft allereerst behoefte aan een helder pakket aan grondbeginselen. Microsoft is, net zoals een groot aantal andere bedrijven, een voorstander van maximale harmonisatie. Een belangrijk onderdeel hiervan is het principe van de *one-stop shop*, waarbij duidelijk moet zijn wat is bedoeld met de «belangrijkste vestiging» in artikel 51, tweede lid, van de ontwerpverordening. Verder zijn bedrijven vaak zowel verwerkers (*processor*) als voor de verwerking verantwoordelijken (*controller*) en dit is voor Microsoft aanleiding om te vragen om een betere definitie hiervan. Gonie slaat vervolgens alarm met betrekking tot de voorgestelde boetes voor nalatigheid (artikel 79 van de ontwerpverordening), omdat hierbij geen opzet in het spel is en onduidelijk is wat «nalatigheid» precies inhoudt. Hij plaatst een kanttekening bij de gedelegeerde handelingen op het gebied van boetes, omdat bedrijven behoefte hebben aan voorspelbaarheid en duidelijkheid over wat ze wel en niet mogen doen. Een belangrijk aandachtspunt van Microsoft is dat naast boetes ook goed gedrag moet worden beloond, bijvoorbeeld door certificaten en krachtige gedragscodes. Rechten voor burgers zijn goed, maar bedrijven moeten ook rechten hebben en gestimuleerd worden om zich goed te gedragen, aldus Gonie. Ten slotte benoemt Gonie het onderwerp transparantie. Dit is van groot belang om vertrouwen te genereren. Het kan niet worden opgelegd, maar wel worden aangemoedigd. Er is behoefte aan nadere uitwerking hiervan in de regelgeving.

De volgende spreker van de tweede sessie is **Nuria Rodriguez** van BEUC, de Europese koepel van 34 nationale consumentenorganisaties. Volgens BEUC zijn de nieuwe voorstellen een grote verbetering ten opzichte van wat er nu is, voor zowel burgers als bedrijven. Het is een enorme uitdaging om te zorgen dat het recht op gegevensbescherming niet wordt geschonden omdat het in toenemende mate winstgevend is om gegevens te verwerken. Een zorg van BEUC is het gebrek aan transparante informatievoorziening door bedrijven aan burgers over het verzamelen, verwerken en soms zelf commercialiseren van hun gegevens. Deze informatie is vaak dermate ontoegankelijk dat burgers vertrouwen op *default settings*. BEUC hecht waarde aan de nieuwe bepalingen die duidelijkheid en begrijpelijkheid van informatie vragen en is tevens blij met de mogelijkheid voor consumenten om juridische stappen te ondernemen als inbreuk wordt gemaakt op het recht op gegevensbescherming. Rodriguez spreekt namens BEUC steun uit voor het uitgangspunt achter het recht om vergeten te worden, maar benadrukt dat de voorstellen onvoldoende zijn uitgewerkt vanwege de mogelijke strijdigheid met vrijheid van meningsuiting: de uitwerking in de praktijk kan niet tot gevolg hebben dat communicatie wordt gefilterd. Ze verwelkomt verder het recht op dataportabiliteit, wat een oplossing is voor de meldingen die zij ontvangt dat digitale dienstverleners vaak eigenaarschap van persoonsgegevens claimen. BEUC stelt verder dat de bepalingen rondom profiling beter moeten worden ontwikkeld. Er bestaat onder consumenten veel angst en een groot gebrek aan kennis over de voor- en nadelen ervan. Daarom moeten de voorstellen worden aangevuld met de plicht om duidelijke informatie te geven over de technieken die gebruikt worden en de gevolgen ervan voor de betrokkenen. Ten slotte is er vanuit BEUC veel steun voor de voorgestelde brede meldplicht, met heldere richtlijnen over notificeren en voldoende mogelijkheden voor het claimen van schadevergoeding.

Ten slotte spreekt **Simon Davies**, hoogleraar aan de London School of Economics, over het *multi stakeholder assessment* dat hij heeft uitgevoerd en nog steeds uitvoert in opdracht van de rapporteurs uit het Europees Parlement. Davies vertelt dat bij in de zomer gesprekken heeft gevoerd met 2000–3000 individuen, via sociale netwerken en sociale evenementen, om te horen wat er leeft onder het brede publiek. Hieruit

komen verontrustende resultaten. Om met het positieve te beginnen vertelt Davies dat de principes achter de nieuwe regelgeving breed worden ondersteund, zelfs door sceptici. Een tweede positief resultaat is dat de infrastructuur voor gegevensbescherming overweldigend wordt ondersteund door het publiek. Echter, over de afzonderlijke onderdelen van de nieuwe regelgeving is geen overeenstemming onder de geraadpleegde mensen. Ten eerste betreft de regelgeving met name de private sector, terwijl het grootste gedeelte van de gesprekken over de publieke sector ging, waarbij de respondenten de overheid wantrouwen vanwege de opkomst van de *surveillance state* (de overheid als Big Brother). Ten tweede is er een breed gedeelde opvatting over het onvermogen en zelfs falen van overheidsinstellingen waar het gegevensbescherming betreft. Deze opvatting is niet universeel en leeft minder in grote delen van Duitsland, sommige Scandinavische landen en Frankrijk, maar er bestaat cynisme over de kracht van de rechtsstaat op dit gebied.

Davies stelt dat er een wetmatigheid lijkt te zijn dat waar burgers vragen om strakke definities, bedrijven het tegenovergestelde willen en vice versa. Dit is zichtbaar op alle gebieden van de nieuwe regelgeving en volgens Davies moet daarom worden gezocht naar het punt waarop burgers en bedrijven het meest tot elkaar komen, hoe moeilijk dat ook is. Uit de gesprekken heeft Davies 28 punten geïdentificeerd waarop gelijkgezind behoefte is aan bindende definities en meer transparantie. Bovenaan de lijst staan de nationale toezichthouders – hun kracht, standvastigheid, consistentie en technische kennis. Bij het bespreken van allerlei maatregelen op detailniveau, zoals *privacy by design*, komt steeds het cynisme naar voren dat laat zien dat mensen behoefte hebben aan bewijs voordat ze vertrouwen krijgen in de overheid. De belangrijkste boodschap uit het onderzoek is volgens Davies dat de grote hoeveelheid gedelegeerde bevoegdheden in de voorstellen dit wantrouwen voedt.

In reactie op de presentaties door het panel vragen parlementariërs uit Duitsland en Polen het woord. Zij gaan onder meer in op het gegeven dat de Europese instellingen niet onder de voorstellen vallen (wat de Duitse parlementariër **Gerold Reichenbach** onacceptabel acht) en de verwerking van gegevens van kinderen. In een discussie tussen **Ryszard Kalisz** van de Poolse Sejm en de eerder genoemde Hornung komt het geografisch toepassingsgebied van de verordening ter sprake (artikel 3). Kalisz vraagt wat dienstverlening van buiten de Europese Unie aan EU-burgers en het beschermen van EU-burgers uit derde landen precies inhouden, met het oog op de vele immigranten vanuit het oosten in Polen. Hij vermoedt dat het moeilijk wordt voor burgers van buiten de EU om hun rechten uit te oefenen en voorziet dat Europese toezichthouders geconfronteerd gaan worden met extra kosten. Hornung antwoordt onder meer dat de betekenis van het «aanbieden van goederen of diensten aan EU-burgers» en het «observeren van gedrag van iemand die in de EU verblijft» problematisch is (artikel 3, tweede lid). **Meritxell Batet Lamana** uit namens het Spaanse parlement zorgen over de gevolgen van de *one-stop shop*. Dit mag niet tot gevolg hebben dat de toezichthouder waar je je als burger toe moet wenden verder af komt te staan van de burgers, vooral niet als er sprake is van een nationale toezichthouder van hoge kwaliteit met goede bevoegdheden zoals in Spanje. Rodriguez ontkracht deze angst dat burgers naar een andere dan de nationale toezichthouder zouden moeten, maar stelt dat er moet worden geleerd van ervaringen van consumentbeschermingsautoriteiten en dat zeker moet worden gesteld dat burgers het recht hebben om zich tot hun eigen toezichthouder te wenden.

Verder vragen de Europarlementariërs **Birgit Sippel** (DE, S&D), **Timothy Kirkhope** (UK, ECR) en **Sarah Ludford** (UK, ALDE) nog het woord. Sippel stelt onder verwijzing naar de aanbeveling van de Raad van Europa[1] vragen over profiling en het nut van het belonen van goed gedrag van bedrijven, Kirkhope schetst op aansprekende wijze dat we bewegen naar een wereld waarin de helft van de mensen zijn tijd spendeert aan het afgeven van gegevens en de andere helft aan het verwerken van deze gegevens, terwijl Ludford betoogt dat de Europese Commissie blind is voor het feit dat profiling zélf een probleem is.

Opening door de vicepresident van de Europese Commissie, Viviane Reding

De middagsessie wordt geopend door de vicepresident van de Europese Commissie, **Viviane Reding**. Als Eurocommissaris voor Justitie, Fundamentele Rechten en Burgerschap is zij verantwoordelijk voor de voorstellen. Reding benadrukt dat het kerndoel van de voorgestelde richtlijn en de verordening is om in een gedigitaliseerde wereld het vertrouwen van burgers in de bescherming van hun privacy op te bouwen. Op dit moment is dit vertrouwen volgens haar tanende. De perceptie is dat technologie leidt tot schending van de privacy. Bovendien leidt de huidige fragmentatie van gegevensbescherming tot onnodige kosten voor het bedrijfsleven. Dit beperkt de concurrentiekracht van de gemeenschappelijke markt. De algemene verordening gegevensbescherming maakt een einde aan de huidige fragmentatie van gegevensbescherming in de Europese Unie. Daarom is ook gekozen voor een verordening, en niet voor een richtlijn.

Vervolgens vertelt de Commissaris dat er bewust voor gekozen is om geen onderscheid te maken tussen het verwerken van data in de publieke en de private sector. Dit onderscheid is namelijk vaak helemaal niet helder te maken. De nieuwe regelgeving laat uiteraard wel differentiatie ten behoeve van de uitvoering van publieke taken toe en identificeert een aantal sectoren waarbinnen een andere benadering toegestaan is, zolang de volgende, voor eenieder geldende basisprincipes in acht worden genomen: doelbeperking, dataminimalisatie, de bepalingen voor de rechten van het gegevenssubject en *privacy by design*. Lidstaten, en derhalve ook nationale parlementen, blijven dus een rol spelen, aldus de Commissaris, bijvoorbeeld bij de afweging tussen vrijheid van meningsuiting en gegevensbescherming.

Hierna vertelt de Commissaris dat zij gekozen heeft voor het gebruik van gedelegeerde handelingen, zodat het pakket van maatregelen technologisch neutraal en daarmee toekomstbestendig kan worden gemaakt. Ze stelt dat het Verdrag van Lissabon haar de mogelijkheid geeft om hier gebruik van te maken. Reding geeft echter wel aan dat zij graag in discussie gaat met parlementariërs om te kijken welke van de gedelegeerde handelingen belangrijk zijn en voor welke een andere oplossing gevonden kan worden. Zij benadrukt dat alternatieven, zoals een sectorspecifieke aanpak of gedragscodes, opnieuw zullen leiden tot fragmentatie. Tevens vertelt de Commissaris dat er geen overkoepelende Europese autoriteit voor gegevensbescherming wordt opgericht. Dit is een bewuste keuze en *peer review* tussen nationale toezichthouders is volgens Reding een goed alternatief. Zij stelt dat de Europese Commissie alleen in uiterste gevallen zal interveniëren in het kader van de conformiteitstoetsing (Hoofdstuk VII, Afdeling 2 van de ontwerpverordening), bijvoorbeeld als een nationale autoriteit niet tot een beslissing kan komen.

De richtlijn heeft zowel betrekking op de uitwisseling van informatie binnen de landsgrenzen als over de landsgrenzen heen. Voordat infor-

[1] Zie Recommendation CM/Rec(2010)13.

matie wordt verzameld kunnen politie en justitie namelijk niet voorzien of de gegevens uitgewisseld gaan worden met derde landen en het aanleggen van twee databanken is inefficiënt. Tot slot benadrukt de Commissaris dat lidstaten verplicht zijn eventuele bilaterale overeenkomsten met andere lidstaten in overeenstemming te brengen met de richtlijn (artikel 60). De lidstaten hebben hier 5 jaar de tijd voor. In het belang van de nationale veiligheid mag informatie zonder beperking direct uitgewisseld worden met derde landen. De Commissaris verwacht dat de onderhandelingen over het pakket van maatregelen mogelijk in juli, onder het Ierse voorzitterschap, kunnen worden afgerond. Daarbij benadrukt zij dat zij de verordening en de richtlijn wil behandelen als één pakket.

In reactie op het betoog van Reding wordt gediscussieerd over de noodzaak om in de richtlijn ook een bepaling op te nemen over de verwerking van informatie binnen de landsgrenzen en of dit niet in strijd is met het subsidiariteitsbeginsel (de Zweedse Riksdagen meent dat dit het geval is). Verder wordt er nogmaals benadrukt dat de richtlijn en de verordening niet los van elkaar behandeld kunnen worden. Verder wordt er besproken of de richtlijn niet leidt tot een *race-to-the-bottom*. Gedurende de discussie wordt nogmaals benadrukt dat de verordening een einde moet maken aan de huidige fragmentatie van verschillende nationale regimes voor gegevensbescherming. Er is echter wel gekozen voor een richtlijn op het terrein van politie en justitie, omdat hier sprake is van nationale «gevoeligheden» en bevoegdheden, en omdat justitieel onderzoek vraagt om maatwerk op nationaal niveau, aldus Reding. Tevens wordt er gediscussieerd over de voorwaarden voor toestemming voor de verwerking van gegevens en de wijze waarop dit in de praktijk uitgewerkt kan worden (ontwerpverordening artikel 7). Verder wordt in de discussie ingegaan op de relatie tussen het uitwisselen van passagiersgegevens met de Verenigde Staten en het pakket aan maatregelen. Reding merkt in dit verband nog op dat er nog altijd onderhandelingen gaande zijn met de Verenigde Staten over een overkoepelend verdrag voor de bescherming van persoonsgegevens.[1]

Session III – Data protection and law enforcement challenges

De sessie wordt geopend door de Griekse Europarlementariër **Dimitrios Droutsas** (S&D), de rapporteur voor de ontwerprichtlijn. Hij benadrukt het belang van gelijke gegevensbescherming in alle sectoren, dus ook op het gebied van rechtshandhaving. Om deze reden benadrukt hij tevens dat het Europees Parlement zowel de ontwerpverordening als de ontwerprichtlijn als pakket behandelt.

Vervolgens krijgt **Lord Hannay** (Crossbench) het woord, namens het Britse House of Lords en in zijn hoedanigheid van voorzitter van de EU Home Affairs commissie. Hij vertelt dat het pakket aan maatregelen grote belangstelling heeft van belanghebbenden in Groot-Brittannië. Lord Hannay stelt dat zijn commissie, vanuit een pragmatisch oogpunt, het verdedigbaar vindt dat er onderscheid is gemaakt tussen een richtlijn en een verordening. De ontwerprichtlijn geeft de flexibiliteit aan de lidstaten om de regels af te stemmen op de nationale context. Tevens is de ontwerprichtlijn, anders dan sommige EU-landen lijken te menen, een verbetering ten opzichte van het huidige kaderbesluit. Ten eerste is de ontwerprichtlijn strikter dan het thans geldende kaderbesluit uit 2008. Het valt echter wel op dat de ontwerprichtlijn minder strikt is dan de verordening, met name met betrekking tot de rechten van het individu. Door deze inconsistentie ontstaan er ongewild risico's. Ten tweede is Lord Hannay blij dat er in de ontwerprichtlijn regels zijn opgesteld voor de binnenlandse verwerking van gegevens door politiediensten. Hij is het

[1] Zie dossier **E100035** op www.europapoort.nl voor het ontwerpmandaat voor onderhandelingen over een overeenkomst EU-VS inzake bescherming persoonsgegevens bij doorgifte en verwerking daarvan met het oog op het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten, waaronder terrorisme, in het kader van de politiële en justitiële samenwerking.

met Commissaris Reding eens dat er geen verschil is tussen de uitwisseling van gegevens binnen een lidstaat en tussen diensten van verschillende lidstaten. Hier neemt het House of Lords een andere positie in dan de Britse regering. Tot slot merkt Lord Hannay op dat het wellicht beter zou zijn als de ontwerprichtlijn ook van toepassing is op instanties als Europol en Eurojust, en op de informatie-uitwisseling in het kader het Verdrag van Prüm of het Prüm-besluit. Daarvoor geldt nu steeds een eigen regime van gegevensbescherming. De huidige hervorming biedt juist een kans om het gefragmenteerde landschap te uniformeren.

Diana Alonso Blas is hoofd van de gegevensbeschermingsdienst binnen Eurojust en gaat in haar presentatie in op het raamwerk voor gegevensbescherming waarbinnen Eurojust opereert. Zij benadrukt dat zij blij is met de ontwerprichtlijn. De reikwijdte van de vorige richtlijn en het kaderbesluit uit 2008 vindt zij te beperkt. Vanwege de specifieke taken van Eurojust valt dit agentschap onder specifieke regelgeving, met name het Eurojust-besluit. Het raamwerk waarbinnen Eurojust opereert voldoet aan alle eisen die gesteld worden in de ontwerprichtlijn en is daarnaast toegesneden op de taken die Eurojust uitvoert. In sommige gevallen zijn de regels voor Eurojust zelfs gedetailleerder en bieden zij meer bescherming dan de ontwerprichtlijn. De spreker verklaart dat dit komt vanwege de interne expertise, de efficiëntie waarmee toezichthouders werken, de hoge frequentie van audits, de grote transparantie en de bindende beslissingen van de Raad van Toezicht. Alonso Blas raadt aan niet te repareren wat niet kapot is.

Na de vorige presentatie volgt een duopresentatie door **Daniel Drewer**, gegevensbeschermingsfunctionaris, en **Marnix Auman** van de operationele afdeling, beiden werkzaam voor Europol. Samen lichten zij het privacyraamwerk van Europol toe. Drewer vertelt dat de verwerking van gegevens één van de kernactiviteiten is van Europol. Vervolgens benadrukt hij dat de regels die Europol hanteert gebaseerd zijn op de algemene principes van gegevensbescherming. Daarnaast zijn ze toegespitst op het specifieke veld waarbinnen Europol opereert, de rechtshandhaving. De regels zijn, net als bij Eurojust, meegenomen in de bouw van de systemen, wat hij *privacy by design* noemt. Verder zijn er specifieke regels voor de verwerking van de gegevens van verschillende soorten gegevenssubjecten (zoals getuigen, slachtoffers en verdachten), i.e. wanneer informatie verwerkt mag worden en hoelang deze mag worden bewaard. Drie elementen spelen bij deze overwegingen een belangrijke rol: nauwkeurigheid, relevantie en proportionaliteit. Bovendien zijn er ook speciale regels voor de omgang met verzoeken van burgers. Europol krijgt ongeveer 600 van dit soort verzoeken per jaar en burgers krijgen, voor zover mogelijk, precies te horen wat voor informatie Europol heeft over hen. Drewer vertelt verder over de waarborgen die zijn ingebouwd als het gaat om de uitwisseling van informatie met derde landen. Zo benadrukt hij dat Europol alleen informatie mag uitwisselen op basis van een operationele overeenkomst en dat deze pas gesloten wordt na een volledige inspectie van het raamwerk voor gegevensbescherming van het derde land. Tot slot vertelt Drewer dat Europol onder een onafhankelijke gegevensbeschermingsautoriteit (de JSB – Joint Supervisory Body) valt. Deze bestaat uit leden van de 27 toezichthouders van de verschillende lidstaten. Er is volgens de spreker sprake van een goed systeem, en de wijziging daarvan moet dan ook goed worden overdacht.

Hierna krijgt **Els de Busser** het woord. Zij werkt voor het Max-Planck Institute for International Criminal Law in Freiburg. Zij gebruikt haar presentatie om in te gaan op een, wat haar betreft, fundamenteel principe in het raamwerk van gegevensbescherming, het doelbindingsbeginsel (artikel 4 sub b en c van de ontwerprichtlijn). Dit beginsel zou bij elke

vorm van gegevensverzameling, zoals passagiers- en bankgegevens, van toepassing moeten zijn. In een strafrechtelijk onderzoek kan er gebruik worden gemaakt van gegevens die verzameld zijn met drie verschillende doelen: het originele doel (strafrechtelijk onderzoek), een ander doel (niet-strafrechtelijk), maar hier wel mee verenigbaar en ten slotte een ander doel (niet-strafrechtelijk), maar hier niet mee verenigbaar. Vervolgens stelt zij dat de drie criteria uit de ontwerprichtlijn ten aanzien van het eerste doel aangescherpt moeten worden. Aan de criteria van artikel 4 sub c, te weten «adequaat, ter zake dienend en niet excessief», moet gegevensminimalisatie worden toegevoegd. Tevens moet «ter zake dienend» worden toegespitst door te expliciteren dat het gaat om een specifiek gegevenssubject en specifiek onderzoek. Vervolgens stelt De Busser dat de ontwerprichtlijn aangegrepen moet worden om een definitie te ontwikkelen en vast te leggen voor het tweede en het derde doel. Volgens De Busser moet aan de volgende drie criteria worden voldaan om van verenigbaarheid te spreken: er is sprake van functionele gelijkwaardigheid, het gebruik is voorzienbaar voor het gegevenssubject en het gegeven mag alleen gebruikt worden in een specifieke situatie. Als deze definitie wordt vastgelegd, dan is het gemakkelijk een definitie voor het derde doel te ontwikkelen. Tot slot benadrukt zij dat het verschil tussen bevestigde en onbevestigde gegevens verder uitgewerkt moet worden in de richtlijn, evenals verschillende categorieën van gegevenssubjecten.

Als laatste spreker van de sessie komt **Anna Fielder** van Privacy International aan het woord. Zij benadrukt dat het erg belangrijk is dat de Europese Unie de wetgeving rond gegevensbescherming verandert. In haar presentatie gaat ze in op twee elementen van de ontwerprichtlijn, de reikwijdte en de inhoud, in verhouding tot de ontwerpverordening. Fielder juicht toe dat de richtlijn zich zowel op de binnenlandse aangelegenheden als op de activiteiten over de grens richt. Ze benadrukt dat ze liever één verordening voor alle gevallen van gegevensverwerking had gezien. Een aparte richtlijn voor politie en justitie zal, net als met de huidige richtlijn bescherming persoonsgegevens uit 1995, leiden tot een gefragmenteerd systeem en dat is fnuikend voor zowel het wederzijdse vertrouwen tussen de lidstaten als voor de rechten van de burgers. Dit klemt temeer omdat gegevens die verzameld worden voor commerciële doeleinden steeds vaker gebruikt worden voor strafrechtelijk onderzoek. Vervolgens benadrukt Fielder dat de politie veel gegevens van individuen beheert. In veel gevallen gaat het ook om gegevens van onschuldige burgers, zoals slachtoffers en getuigen. Fielder is daarom verwonderd over het feit dat de ontwerprichtlijn veel minder ambitieus is dan de ontwerpverordening. Het gegevenssubject heeft minder rechten, de beheerder heeft vagere verplichtingen, de regels betreffende de uitwisseling van gegevens zijn onduidelijk en de toezichthouders hebben minder macht. Tot slot wordt in de richtlijn geen aandacht besteed aan de verschillende gegevenssubjecten en kinderen worden in het geheel niet genoemd.

Na de presentatie van de panelleden ontstaat er een discussie over de gevolgen die het onderscheid tussen de richtlijn en de verordening heeft voor de rechten van de burger. Meerdere sprekers benadrukken dat het doelbindingsbeginsel van groot belang is en dat er nogmaals goed gekeken moet worden of de richtlijn niet aangescherpt dient te worden. Tevens wordt er ingegaan op de spanning die er bestaat tussen het mogelijk maken van strafrechtelijk onderzoek en het beschermen van de individuele privacy. Hierbij wordt benadrukt dat vertrouwen in de Europese instituties en in de rechtsstaat essentieel is voor de bescherming van de privacy. Europol en Eurojust benadrukken beide dat privacy een voorwaarde is voor het goed functioneren van hun instanties.

Session IV – Data controllers and processors in the private and employment sector

Moderators bij deze sessie zijn de Europarlementariërs **Sean Kelly** (EVP; rapporteur van de commissie Industrie, onderzoek en energie) en **Nadja Hirsch** (ALDE; rapporteur van de commissie Werkgelegenheid en sociale zaken). Eerstgenoemde licht toe dat het voor de sector van groot belang is dat er duidelijkheid bestaat over de begrippen «controller» («voor de verwerking verantwoordelijke») en «processor» («verwerker») in artikel 4 van de ontwerpverordening. Dit in verband met de primaire verantwoordelijkheid en aansprakelijkheid van de «controller». Hirsch verwijst naar artikel 82 van de ontwerpverordening, waarin is geregeld dat de lidstaten bij wet specifieke voorschriften kunnen vaststellen voor de verwerking van persoonsgegevens in het kader van de arbeidsverhouding. Voor deze voorschriften zouden volgens haar bepaalde Europese minimumstandaarden moeten gelden, bijvoorbeeld geen camera's in kleedruimtes en voldoende autonomie voor de functionaris voor gegevensbescherming. Werknemers hebben immers een zwakkere positie dan werkgevers.

Als eerste spreekt **Stephan Mayer** (CSU), lid van de Duitse Bundestag. Hij is kritisch over de ontwerpverordening.[1] Deze zoekt naar evenwicht tussen de betrokken belangen (van consumenten en ondernemingen), maar slaagt daar niet altijd in. Minder bureaucratie voor ondernemingen klinkt mooi, maar gelet op de verplichtingen van de artikelen 14, 15 en 32 lijkt het er niet op dat dat gaat lukken. Die artikelen zorgen juist voor meer kosten en rompslomp. De vrijheid van ondernemerschap is ook vastgelegd in het Handvest van de grondrechten van de Europese Unie (artikel 16) en deze dient te worden gerespecteerd. Midden- en kleinbedrijf zullen grote moeite hebben met het artikel over de melding van inbreuken binnen 24 uur (artikel 31) en naar de mening van de spreker zit er weinig logica achter het criterium van meer of minder dan 250 werknemers voor het wel of niet van toepassing zijn van een verplichting. In Duitsland is de bescherming van persoonsgegevens volgens de spreker goed geregeld. Artikel 6 van de ontwerpverordening lijkt geen basis te bieden voor cao's of bedrijfsovereenkomsten als juridische grondslag voor gegevensverwerking en dat betreurt Mayer. De voorwaarden voor het geven van toestemming zijn niet realistisch. Het aantal gedelegeerde handelingen in de ontwerpverordening is te hoog en in strijd met artikel 290 van het EU-werkingsverdrag. De rol van de Europese Commissie in het kader van de conformiteitsprocedure (Hoofdstuk VII, Afdeling 2) is dubieus. Deze ondergraaft de onafhankelijkheid van de nationale toezichthouders. De spreker raadt aan om de tijd te nemen om alle onvolkomenheden weg te werken.

Vervolgens komt **Erika Mann** aan het woord, managing director van Facebook. Facebook gelooft in de mogelijkheid van het combineren van goede privacybescherming met een bloeiende digitale sector. Facebook is wel kritisch over nieuwe administratieve lasten, zoals de documentatieplicht van artikel 28 van de ontwerpverordening. We staan volgens Mann nog maar aan het begin van de ontwikkeling van de internetsector. Nieuwe modellen en innovatieve ideeën moeten niet onnodig lijden onder lasten die nieuwe Europese wetgeving meebrengt. Veel van de meest succesvolle IT-bedrijven zijn Europees en ook van groot belang voor de Europese economie. Facebook draagt ook bij aan deze economie, zowel in geld als in arbeidsplaatsen. Het bedrijf is voorstander van het *one-stop shop* systeem. Dit maakt de zaken minder complex en zorgt voor betere gegevensbescherming, maar het vereist wel goede samenwerking tussen nationale toezichthouders. De positie van de leidende toezichthouder zou bedreigd kunnen worden door de voorgestelde conformiteitsprocedure (Hoofdstuk VII, Afdeling 2). Facebook is gevestigd in Ierland en werkt

[1] De Duitse Bundes*rat* heeft overigens een subsidiariteitsbezwaar gemaakt.

nauw samen met de Ierse autoriteit voor gegevensbescherming. Het bedrijf is onlangs aan een audit onderworpen. Conclusie: Facebook respecteert Europese en nationale beginselen van gegevensbeschermingsrecht. Aanbevelingen van de toezichthouder worden opgevolgd. Facebook is groot voorstander van *privacy by design*, maar is van mening dat *privacy by default* niet goed past bij een sociale netwerksite. Mensen die daar komen willen juist gegevens delen. Uiteraard kunnen privacy settings wel aangepast worden, met simpele tools.

De volgende spreker is **Alexander Dix**, commissaris voor gegevensbescherming en vrijheid van informatie voor Berlijn. In zijn betoog levert hij zeer gedetailleerde kritiek op de ontwerpverordening. Enkele hoogtepunten uit zijn toespraak:

- Harmonisatie is een lofwaardig doel, maar mag niet leiden tot een lager niveau van gegevensbescherming. In de geldende richtlijn uit 1995 is dat met zoveel woorden vermeld. Dit zou ook in de voorgestelde verordening het geval moeten zijn, anders dreigt een *race to the bottom*.
- Dit vraagt om meer flexibiliteit voor lidstaten. Artikel 82 van de ontwerpverordening, over gegevensverwerking in het kader van de arbeidsverhouding, is te beperkt en te vaag.
- De bepalingen met als criterium of een bedrijf meer of minder dan 250 medewerkers heeft, zijn zonder ratio. Een staalbedrijf met 250 werknemers moet nu een functionaris voor gegevensbescherming hebben, een huisartsenpraktijk met 5 medewerkers niet, terwijl hier gevoelige gegevens worden verwerkt. Gelet op de aard van de gegevensbescherming is dat zeer onlogisch.
- Artikel 19, tweede lid, over het bezwaar maken tegen gegevensverwerking voor direct marketing, kan geschrapt worden. Direct marketing dient altijd gebaseerd te zijn op toestemming van de betrokkene.
- De Europese Commissie heeft een te dominante rol in het voorstel. Dat geldt zowel voor de vele gedelegeerde handelingen als voor haar rol in de conformiteitsprocedure. Wat het laatste punt betreft constateert de spreker zelfs strijd met de jurisprudentie van het Hof van Justitie over onafhankelijkheid van toezichthouders.
- Het systeem van *one-stop shop* kan alleen werken als de leidende toezichthouder (*lead authority*) voldoende wordt gesteund door de andere nationale toezichthouders.

Het verhaal van **Armin Duttine** van het Europees Economisch en Sociaal Comité komt mede door een haperende PowerPoint presentatie niet geheel uit de verf. De spreker acht het onder meer onzinnig om de grens in enkele bepalingen bij 250 medewerkers te leggen. Het merendeel van de bedrijven (90% van de bedrijven in Spanje, aldus een interventie vanuit de zaal) valt daardoor buiten het bereik van de verordening.

Zo moeizaam als de presentatie van Duttine verloopt, zo soepel gaat die van **Frederik Borgesius** van het Amsterdamse Instituut voor Informatierecht. In zijn heldere betoog maakt hij twee punten, te weten dat de definitie van «persoonsgegevens» in artikel 4 breder zou moeten worden getrokken en dat het artikel over het geven van toestemming voor verwerking (artikel 7) juist prima is en niet teveel meer moet worden aangepast. Met betrekking tot het eerste punt pleit Borgesius ervoor in artikel 4 sub 1 van de ontwerpverordening niet alleen te spreken over een persoon die kan worden geïdentificeerd, maar tevens van een persoon die «eruit kan worden gepikt» («singled out»). Een naam is namelijk vaak niet nodig om een zeer gedetailleerd profiel van iemand te kunnen opstellen, bijvoorbeeld op basis van iemands surfgedrag (voorkeur websites e.d.) of iemands reisroute (peilen locatie mobiele telefoon). Dergelijke «anonieme profielen» dienen binnen het bereik van de verordening te worden

gebracht door het aanpassen van de definitie van «persoonsgegevens».[1] Daarmee wil de spreker overigens niet zeggen dat dergelijke profielen verboden moeten worden, wel dat ze gereguleerd dienen te worden. Borgesius roept ten slotte op het artikel over het geven van toestemming voor verwerking van persoonsgegevens, waarin staat dat stilzwijgen nooit kan worden gelijkgesteld aan actieve instemming, sterk is geformuleerd en moet worden behouden.

Na de bijdragen van de sprekers volgen interventies vanuit de zaal van Duitse, Poolse en Spaanse parlementariërs en van Birgit Sippel van het Europees Parlement (S&D). In hun bijdragen valt onder meer te beluisteren dat Europa op het vlak van de gegevensverwerking in de arbeidsverhouding minimumregels kan stellen en dat deze voor de werknemer (de zwakke partij) gunstigere nationale normen niet mogen verlagen of wegdrukken.

Dag 2: woensdag 10 oktober 2012

Session V – Implementation of Data Protection law. Ensuring consistency and efficiency

De tweede dag begint met een sessie over handhaving van de regelgeving over de bescherming van persoonsgegevens. Moderator is de Europarlementariër **Marielle Gallo** (EVP; rapporteur van de commissie Juridische zaken). Zij benadrukt onder meer het belang van daadwerkelijk onafhankelijke toezichthouders voor gegevensbescherming die over voldoende middelen beschikken om de gestelde regels ook echt te handhaven, die goed met elkaar samenwerken en die effectieve, proportionele sancties kunnen opleggen.

De eerste spreker is **Peter Eriksson** (Groenen), voorzitter van de commissie voor constitutionele zaken van de Zweedse Riksdagen. Hij heeft bezwaren tegen de keuze voor een verordening, die ook veel te gedetailleerd is. Liever had hij een herziening van de richtlijn uit 1995 gezien. Harmonisatie door middel van een verordening kan namelijk contraproductief werken en tot een te laag niveau van gegevensbescherming leiden. Strengere nationale regels, die meer bescherming bieden, worden dan immers onmogelijk. Eriksson meent dat de ontwerpverordening te weinig aandacht besteedt aan openbaarheid van documenten en vrijheid van expressie, belangrijke principes van de Zweedse Grondwet. Hij is niet te spreken over de kwantitatieve aanpak van de Europese Commissie, waarbij het aantal werknemers binnen een bedrijf als uitgangspunt wordt genomen in plaats van de aard van de verwerkte gegevens (triviaal of gevoelig). Een kwalitatieve aanpak is te prefereren. Eriksson is verder bang voor meer bureaucratie en administratieve lasten, en dus hogere kosten, door toedoen van de verordening. Het *one-stop shop* systeem leidt tot geringere kosten voor sommige bedrijven, maar tot hogere voor vele andere. In teveel bepalingen krijgt de Europese Commissie de bevoegdheid gedelegeerde handelingen vast te stellen. Zij dreigt daardoor een wetgevend lichaam te worden, wat niet de bedoeling van de Europese verdragen is. De spreker constateert strijd met het subsidiariteitsbeginsel en het Zweedse parlement heeft ook een subsidiariteitsbezwaar gemaakt.[2] De Zweedse toezichthouder voor gegevensbescherming functioneert goed en bemoeienis van de Europese Commissie in het kader van de conformiteitsprocedure is ongewenst.

Europees Toezichthouder voor Gegevensbescherming **Peter Hustinx** is de volgende spreker. Hij beschouwt het voorgestelde pakket als een grote stap voorwaarts, noodzakelijk en welkom, maar wel met de nodige zwakten. De ontwerprichtlijn gegevensverwerking politie en justitie biedt

[1] Vgl. in dit verband de vragen van de Eerste Kamerfractie van de PvdA over het uitbreiden van de definitie van «persoonsgegevens» naar aanleiding van opmerkingen van de organisatie Bits of Freedom, die een soortgelijk betoog hield als Borgesius. De regering geeft in reactie aan het niet verstandig te vinden een toch al moeilijk te hanteren begrip verder uit te breiden met «een categorie die zich bijzonder moeilijk laat afgrenzen». Dit zou volgens de regering kunnen leiden tot interpretatieproblemen. Zie Kamerstukken I 2011/12, 33 169, C, p. 21.

[2] Overigens ook tegen het voorstel voor een richtlijn gegevensverwerking door politie en justitie. Het Zweedse parlementslid Bohlin had daar de vorige dag al op gewezen.

bijvoorbeeld onvoldoende waarborgen. Als Europees Toezichthouder heeft hij dan ook een kritisch advies gepubliceerd, dat gelukkig weerklank vindt, onder meer bij de rapporteurs van het Europees Parlement. Onafhankelijkheid van toezichthouders is essentieel. De ontwerpverordening laat de lidstaten de keuze tussen benoeming van de leden van de toezichthoudende autoriteit door de regering of door het parlement, maar eigenlijk is parlementaire betrokkenheid bij de benoeming altijd gewenst. De regel dat er «passende middelen» beschikbaar moeten zijn voor de toezichthouders moet meer geobjectiveerd worden om een wassen neus te voorkomen. Voor wat betreft de sancties geldt dat flexibiliteit vereist is. Het moet niet alleen om strafsancties gaan, maar ook om *remedial sanctions*. Richtlijnen voor de toepassing van sancties zijn belangrijk, en het nog op te richten Europees Comité voor gegevensbescherming kan daarbij een rol spelen. De bepaling over «belangrijkste vestiging» en «leidende toezichthouder» (artikel 52, tweede lid van de ontwerpverordening) behoeft verduidelijking. De samenwerking met andere toezichthouders is essentieel, want de leidende toezichthouder kan niet buiten zijn eigen jurisdictie optreden. Hoofdstuk VII over samenwerking en conformiteit behoeft nadere bestudering, vooral wat betreft de conformiteitstoetsing. De rol van de Europese Commissie in deze procedure moet worden beperkt tot het geven van adviezen. Zij moet bijvoorbeeld zeker niet maatregelen van nationale toezichthouders kunnen schorsen. De ontwerpverordening is nu overduidelijk in strijd met de rechtspraak van het Hof van Justitie.

De Nederlander **Jacob Kohnstamm** is niet alleen voorzitter van het College Bescherming Persoonsgegevens, maar tevens van de Artikel 29 Werkgroep, het onafhankelijke advies- en overlegorgaan van Europese toezichthouders voor gegevensbescherming. Deze werkgroep wordt in de ontwerpverordening omgevormd tot het Europees Comité voor gegevensbescherming (artikel 64 e.v.). Kohnstamm wijst allereerst op de vervolgopinie die de Artikel 29 Werkgroep recentelijk heeft gepubliceerd. Vervolgens betoogt hij dat niet getornd moet worden aan de definities van «persoonsgegevens» en «uitdrukkelijke toestemming». Kohnstamm roept verder het Europees Parlement op beide voorstellen, voor de verordening en voor de richtlijn, als één pakket te blijven behandelen. Sancties zijn essentieel om het nieuwe kader te laten werken. De nationale toezichthouders verschillen van mening over (de uitwerking van) het conformiteitsmechanisme, hoewel Kohnstamm zich zelf aansluit bij het betoog van Hustinx. De kwestie van het budget voor toezichthouders is een zeer zwakke schakel van de voorstellen. Opname van een minimumomvang en andere objectieve criteria is noodzakelijk. De Artikel 29 Werkgroep heeft de bepalingen waarin sprake is van gedelegeerde handelingen tegen het licht gehouden. Dat leidde tot genuanceerde conclusies: in sommige gevallen zijn dergelijke handelingen onvermijdelijk, in andere gevallen zijn alternatieven denkbaar, zoals nadere uitwerking in de verordening zelf, in de overwegingen daarbij, in nationale wetgeving of in opinies van het Europees Comité voor gegevensbescherming.

De laatste spreker van deze sessie is **Mario Oetheimer** van het Fundamental Rights Agency uit Wenen. Dit EU-agentschap heeft, anders dan bijvoorbeeld de Artikel 29 Werkgroep of de Europese Toezichthouder voor Gegevensbescherming, de voorstellen bekeken in het licht van álle fundamentele rechten van het Handvest van de grondrechten. Het agentschap richt zich dus op meer dan alleen privacy en bescherming van persoonsgegevens. Oetheimer mist in de voorstellen de verwijzing naar alle betrokken grondrechten. Bij het aftappen van journalisten of het in beslag nemen van hun materiaal is bijvoorbeeld ook de vrijheid van meningsuiting en informatie in het geding. De voorstellen kunnen in dit opzicht beter.

Tijdens de discussie die volgde op de toespraken werden nog enkele interessante opmerkingen gemaakt. **Willem Debeuckelaere**, voorzitter van de Belgische Privacycommissie, hield een betoog voor één echte Europese toezichthouder voor gegevensbescherming die in alle EU-lidstaten toezicht kan uitoefenen en sancties kan opleggen.[1] In het licht van multinationals als Google en Swift achtte hij het onbegrijpelijk dat in de nieuwe voorstellen niet hiervoor gekozen is. Een Europese toezichthouder met tanden is veel beter dan het nu voorgestelde systeem met nationale toezichthouders, moeizame samenwerkingsprocedures en conformiteitstoetsingen waar ook de Europese Commissie zich mee bemoeit. Hustinx en Kohnstamm gaven daarop aan dat een *bottom-up* aanpak te verkiezen is. Er moet eerst sprake zijn van *empowerment* van de nationale toezichthouders. Zo'n aanpak kan werken, zoals is gebleken in Ierland (met Facebook), België (met Swift) en Frankrijk (met Google). Kohnstamm meende verder, in lijn met Eurocommissaris Reding de vorige dag, dat er geen sprake van kon zijn dat voor de overheid andere regels gelden dan voor de private sector. Natuurlijk kan rekening gehouden worden met de specifieke taken die de overheid heeft, maar de basisbeginselen en basisregels dienen hetzelfde te zijn voor alle actoren.[2]

Session VI – Police data sharing and access to private data bases

Moderator bij deze tweede sessie van de woensdag is de Britse Europarlementariër **Timothy Kirkhope** (ECR). Deze is ook rapporteur voor het voorstel voor een richtlijn betreffende het gebruik van persoonsgegevens van passagiers voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en zware criminaliteit (EU PNR).[3] Kirkhope vestigt de aandacht op twee vragen die in deze sessie aan de orde moeten komen: moet de richtlijn ook van toepassing zijn op puur interne verwerking van persoonsgegevens door politie en justitie en hoe kan het juiste evenwicht gevonden worden tussen de belangen van rechtshandhavingsinstanties en de bescherming van fundamentele rechten wanneer de genoemde instanties toegang wensen tot databanken die door bedrijven voor commerciële doeleinden zijn aangelegd?

De eerste spreker is **Konstantin von Notz** (Die Grünen) van de Duitse Bundestag. Het Duitse recht kent hoge standaarden voor gegevensbescherming, die zowel zijn vastgelegd in wetgeving als in de rechtspraak van het Bundesverfassungsgericht over bijvoorbeeld dataretentie.[4] Deze kunnen als inspiratiebron dienen voor het Europese recht, waar hoge standaarden ook noodzakelijk zijn. De spreker ziet harmonisatie ook als noodzakelijk en niet per definitie als een bedreiging voor hogere niveaus van gegevensbescherming. Er is sprake van een wirwar aan gegevensverzamelingen en databanken, bestreken door een baaierd aan onderling afwijkende regelgeving, maar uiteindelijk allemaal ergens met elkaar verbonden. Dit geheel, waartoe de spreker de uitwisseling tussen diensten in het kader van Prüm, PNR, dataretentie, het Visa Informatie Systeem en Frontex rekent, is volstrekt niet transparant. Daarom zijn hoge standaarden voor zowel interne als grensoverschrijdende gegevensverwerking nodig. Een nieuw Europees kader voor gegevensbescherming is dus nodig, maar Duitsland kan geen regels aanvaarden die gegevensuitwisselingen toestaan die tegen de eigen Grondwet en nationale wetgeving ingaan. Het is positief dat de ontwerprichtlijn zowel op interne als grensoverschrijdende gegevensverwerking van toepassing is. De ontwerprichtlijn is dan ook beter dan het kaderbesluit uit 2008. Er bestaat volgens de spreker zeker een bevoegdheid interne gegevensverwerking op Europees niveau te reguleren. Het gebruik van databanken die door bedrijven voor commerciële doeleinden zijn aangelegd voor rechtshandhaving is zeer problematisch. In Duitsland gelden voor profiling, datamining en toegang door politie en justitie tot privé communicatie

[1] De huidige Europese toezichthouder voor gegevensbescherming is ingesteld op basis van Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad van 18 december 2000 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens. Hij ziet toe op de verwerking van persoonsgegevens door EU-instellingen en kan in dat verband ook adviseren over nieuwe EU-voorstellen. Handhavende bevoegdheden jegens (organen van) lidstaten of de private sector heeft hij niet.

[2] Zie in dit verband de vragen van de Eerste Kamerfractie van de VVD over het al dan niet verplicht stellen van *privacy impact assessments* voor overheidsorganen, Kamerstukken I 2011/12, 33 169, C, p. 12.

[3] Zie dossier **E110005** op www.europapoort.nl

[4] Zie BVerfG 2 maart 2010 over implementatie van Richtlijn 2006/24/EG.

zware constitutionele voorwaarden. Het moet gaan om uitzonderlijke gevallen van concreet gevaar voor hoogwaardige belangen. Een algemene dreiging van terrorisme kan nooit de toegang tot persoonsgegevens rechtvaardigen. Deze beginselen zouden ook voor Europese regelgeving moeten gelden. De ontwerprichtlijn is op dit moment veel te zwak en onaanvaardbaar.

Frédéric Tardif van het Franse ministerie van Binnenlandse Zaken is de volgende spreker. Bij het voorkomen, bestrijden, opsporen en vervolgen van criminaliteit kan de politie gebruik maken van haar eigen gegevensverzamelingen, maar deze zijn niet volledig. Daarom is soms toegang tot door de private sector verzamelde gegevens nodig. Deze zijn uiteraard niet voor rechtshandhavingsdiensten verzameld, dus er gelden strenge voorwaarden voor toegang. Het gaat bijvoorbeeld om telecommunicatiegegevens, PNR e.d. Dergelijke gegevens kunnen een grote bijdrage leveren bij opsporing en vervolging. De toegang is in Frankrijk zowel juridisch als politiek strikt omkaderd. Bij de inkadering door de wet wordt gekeken naar de rang van de betrokken opsporingsambtenaar, de kwaliteit van het onderzoek en de betrokkenheid van een rechterlijke instantie. De politiek waakt tegen overmatige toegang tot gegevens.

Veel kritischer dan de vorige spreker is **Joe McNamee** van European Digital Rights (EDRI). Hij spreekt namens 32 digitale burgerrechtenorganisaties. De opslag van data is volgens hem steeds goedkoper geworden, zelfs zo goedkoop dat bedrijven niet eens meer hoeven na te denken over de vraag of ze data moeten gaan opslaan. De enorme opslag van gegevens brengt ook gevaren met zich mee. Dat geldt ook voor bepaalde voorgestelde wetgeving, zoals de Britse Draft Communications Data Bill (die waarschijnlijk verworpen wordt door het Britse parlement), die de staat veel te gemakkelijk toegang geeft tot door bedrijven opgeslagen informatie. McNamee stelt de vraag of deze informatie ook in de handen van een democratische staat wel veilig is. Het Verenigd Koninkrijk heeft geen goede reputatie op dit punt. Een databank creëert door haar enkele bestaan al een veiligheidsrisico. Gelet op de risico's, beschermen de nieuwe voorstellen ons voldoende? De ontwerpverordening laat volgens de spreker teveel ruimte voor nationale wetgeving over profiling. Dat kan tot fragmentatie in de Europese Unie leiden. McNamee roept rapporteur Albrecht op op dit punt ambitieuzer te zijn. Vervolgens heeft hij ook zware kritiek op de Richtlijn dataretentie uit 2006 (Richtlijn 2006/24/EG).[1] Dataretentie is een Europees probleem. De geldende richtlijn zou idealiter moeten worden ingetrokken. De spreker vindt ten slotte dat derde landen alleen onder strikte voorwaarden toegang tot gegevens moeten kunnen krijgen. De Amerikaanse Patriot Act en Foreign Intelligence Surveillance Amendment Act (FISA) voldoen in dit opzicht totaal niet in een democratische samenleving. Beide wetten zijn eenzijdig vastgesteld en de laatstgenoemde wet richt zich in potentie ook op politieke activiteiten. De Europese Commissie heeft dit probleem aanvankelijk onderkend en in de ontwerpverordening een artikel 42 opgenomen dat een *verdrag* tussen het derde land en de Europese Unie of een EU-lidstaat vereiste voor doorgifte.[2] Hij betreurt dat dit artikel door invloed van de Verenigde Staten is gesneuveld. Het hele wetgevingspakket bevat veel sterke punten, maar teveel zwakheden om zo aangenomen te worden.

Eric Töpfer, onderzoeker aan het Deutsches Institut für Menschenrechte, is de volgende spreker. Hij vindt dat de ontwerprichtlijn ook van toepassing moet zijn op puur interne verwerking van persoonsgegevens door politie en justitie. Gebruik en uitwisseling van dergelijke gegevens tussen de diverse diensten is enorm toegenomen sinds de eerste vormen van politiesamenwerking in de jaren zeventig. Miljoenen mensen zijn opgenomen in databanken. Dit vraagt om regels over bescherming van

[1] In Nederland geïmplementeerd door de Wet bewaarplicht telecommunicatiegegevens uit 2009 (Kamerstukken 31 145).

[2] «No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State.»

persoonsgegevens, die nu vaak nationaal worden vastgesteld, bijvoorbeeld als het gaat om opslagtermijnen, rechten van toegang en toezichthouders. De Europese regulering van de bescherming van persoonsgegevens die door politie en justitie worden verwerkt is te zwak. Er is in het kader van de Raad van Europa wel een Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data uit 1981 (ETS 108), maar dat verdrag loopt 30 jaar achter en is onvolledig. Ook het EU-kaderbesluit uit 2008 is onvoldoende. Dat de voorgestelde richtlijn ook op interne verwerking ziet, is toe te juichen en van strijd met het subsidiariteitsbeginsel is geen sprake. Wel moet er meer aandacht zijn voor de rechten van betrokkenen (Hoofdstuk III van de ontwerprichtlijn), met name het recht op toegang tot gegevens in databanken. Ten slotte moet er in de ontwerprichtlijn meer aandacht zijn voor publiek-private samenwerking, bijvoorbeeld samenwerking van de politie met particuliere beveiligingsbedrijven.

De sessie wordt afgesloten door de Pool **Wojciech Wiewiórowski**, inspecteur-generaal voor de bescherming van persoonsgegevens. Hij prent de zaal in dat alle aanwezigen «data subjects» zijn. Het gaat bij de op tafel liggende voorstellen niet alleen om criminelen en getuigen, maar vooral om gewone burgers. Overal worden data over ons verzameld door politie en justitie, bijvoorbeeld in het kader van PNR, de douane of de belasting. Vaak weten burgers niet of dat gebeurt en zelfs Wiewiórowski als toezichthouder weet niet wat er in de Europese Unie allemaal precies gebeurt. Toezichthouders hebben volgens hem geen idee wat er in andere EU-lidstaten door politie en justitie zoal wordt verzameld, en wat de standaarden voor gegevensbescherming daar zijn. Dat pleit allemaal voor Europese standaarden, die zowel op puur interne als grensoverschrijdende gegevensverwerking door politie en justitie van toepassing zijn. Natuurlijk hebben politie en justitie toegang tot gegevens nodig in het kader van hun zorg voor de veiligheid, maar wel binnen Europese grenzen. De spreker is ook groot voorstander van artikel 60 van de ontwerprichtlijn, dat lidstaten verplicht hun eerdere bilaterale verdragen over politiële en justitiële samenwerking in strafzaken indien nodig binnen vijf jaar na de inwerkingtreding van de richtlijn te herzien.

In de discussie die volgt op de presentatie worden nog enkele interessante opmerkingen gemaakt. Vanuit de Duitse Bundestag klinkt kritiek op de houding van de Verenigde Staten onder de Swift-overeenkomst[1], een Spaanse Europarlementariër betoogt dat de Verenigde Staten een totaal andere kijk op privacy hebben dan de Europese Unie, spreker Von Notz betreurt dat in de discussie over de voorstellen voor de verordening en de richtlijn geen aandacht is voor PNR en dataretentie, spreker McNamee hekelt de PNR-overeenkomst van de Europese Unie met de Verenigde Staten en Europarlementariër Baroness Ludford (ALDE) verdedigt haar keuze om vóór deze overeenkomst te stemmen, omdat anders totale chaos in de luchtvaartbranche zou ontstaan.

Session VII – Data Protection in the global context – (1st part) The transatlantic dimension

De eerste sessie over gegevensbescherming in mondiaal perspectief, met een vrijwel volledige Amerikaans panel, wordt voorgezeten door de Duitse Europarlementariër **Axel Voss** (EVP). Bij wijze van inleiding vraagt hij zich af hoe we effectieve standaardisering kunnen aanbrengen op het gebied van gegevensbescherming, zoals in het verkeer verkeersborden en rijbewijzen bestaan.

De eerste spreker van het panel is **Paul Nemitz** van DG Justitie van de Europese Commissie. Hij benadrukt in zijn speech de goede samen-

[1] Zie de dossiers **E100001** en **E100013** op www.europapoort.nl

werking met vertegenwoordigers van de Verenigde Staten en gaat gelijk in op de «deuren» waardoor gegevens over grenzen kunnen bewegen. Dit zijn *adequacy contracts*, *binding corporate rules* en uitzonderingen voor het MKB. Dat partijen buiten de Europese Unie de Europese benadering van gegevensbescherming ondersteunen blijkt volgens Nemitz uit de grote hoeveelheid bedrijven en organisaties die *adequacy contracts* hebben ondertekend. De Amerikaanse overheid handhaaft de naleving van deze contracten en legt boetes op, zoals bij Google en Facebook is gebeurd. Nemitz vervolgt door aan te geven dat de trends in de Verenigde Staten en de Europese Unie vergelijkbaar zijn, alhoewel het proces verschillend verloopt in de tijd. Interoperabiliteit is de kern van de benadering waar het uitwisseling van gegevens betreft. Volgens Nemitz is dit in de Verenigde Staten «laaghangend fruit» omdat de bedrijven die contracten hebben getekend met de Europese Unie welwillend zullen zijn om de regelgeving die gaat volgen uit de Blueprint van Obama's regering te implementeren. Het vertrouwensprobleem in de maatschappij leeft aan beide zijden van de Atlantische Oceaan. Nemitz zegt enthousiast dat de schoonheid van het onderwerp gegevensbescherming is dat er geen tegenstelling bestaat tussen economische groei en bescherming van persoonsgegevens, want ze zijn beide gebaat bij een hoog niveau van vertrouwen. Met betrekking tot de richtlijn geeft Nemitz aan dat effectieve samenwerking tussen de Verenigde Staten en de Europese Unie voor gedeelde doelstellingen zoals het bestrijden van terrorisme voor ogen wordt gehouden. Er leven conceptuele kwesties, zoals het belang dat EU-burgers die zich beschermd voelen door EU-regelgeving zich ook beschermd moeten voelen in de Verenigde Staten. Er is zodoende symmetrie nodig en een overeenstemmende aanpak. De gesprekken daarover zullen na de verkiezingen in de Verenigde Staten worden opgepakt. Nemitz rondt zijn speech af met een verwijzing naar het artikel over rechtsbescherming bij het uitwisselen van gegevens dat is verdwenen uit de eerste gelekte concepttekst.[1] Hij stelt dat de bepalingen zoals ze zijn voorgesteld in de definitieve tekst voldoende zijn vanwege de rechtsbescherming die hierin besloten zit.

De tweede spreker is **David Vladeck**, directeur van de US Federal Trade Commission (FTC), een onafhankelijk orgaan met bevoegdheden op het gebied van gegevensbescherming. Hij benadrukt het kritieke belang van een interoperabel wetgevend kader en is verheugd over de kans om inbreng te leveren in het Europese wetgevingsproces. Hij waardeert de Europese inbreng bij de Amerikaanse herziening van wetgeving op dit gebied (White House Privacy Blueprint). Er bestaan veel overeenkomsten tussen de twee herzieningsprocessen en er is steeds minder licht tussen verschillende systemen waar het *privacy by design*, betere keuzes voor consumenten, transparantie, toegankelijkheid van informatie en sectorale wetgeving betreft. Vladeck vervolgt met de stelling dat gedragscodes en wederzijdse erkenning zinvol zijn bij het uitwisselen van gegevens, maar dat deze niet worden genoemd in de verordening. Hij benadrukt vervolgens het belang van het bestaande US-EU Safe Harbor Framework[2], waardoor Amerikaanse bedrijven zich verbinden te voldoen aan de Europese beginselen voor gegevensbescherming, hetgeen wordt gecontroleerd met onafhankelijke audits door de FTC. Een kritiekpunt van Vladeck is dat de verordening uitgaat van samenwerking tussen adequate toezichthouders, en slechts beperkt ingaat op samenwerking met overheden in andere landen terwijl gegevensbescherming gebaat is bij internationale samenwerking. Ten slotte vraagt hij aandacht voor de positie van kinderen, van wie de gegevens bijvoorbeeld door apps worden verzameld zonder toestemming van ouders. Hier treden de Verenigde Staten tegen op, maar een mondiale aanpak door goed geëquipeerde toezichthouders is van belang.

[1] Zie noot 13.
[2] http://export.gov/safeharbor/eu/eg_main_018365.asp

De tweede spreker uit de Verenigde Staten, **Bruce Swartz**, Deputy Assistant Attorney General van het US Department of Justice[1] valt gelijk met de deur in huis. Hij spreekt over noodzakelijke samenwerking tussen ordehandhavende instellingen en gegevensuitwisseling om criminaliteit te bestrijden en stelt dat de noodzaak om gegevens internationaal uit te wisselen steeds groter wordt. Kort en goed vreest Swartz een dramatisch en negatief effect na de inwerkingtreding van de ontwerprichtlijn die internationale samenwerking zal verlammen en de wereld minder veilig maakt. Dit is volgens hem het onbedoelde gevolg van de richtlijn. Als Nemitz weer het woord krijgt geeft hij aan dat dit doemscenario waarin het sluiten van verdragen niet meer mogelijk is niet klopt, aangezien de bepalingen waar Swartz over spreekt ook al bestaan in het nu vigerende kaderbesluit uit 2008.

Concrete kritiekpunten van Swartz betreffen allereerst artikel 60, dat voorziet in herziening – indien nodig – van bilaterale rechtshandhavingsverdragen binnen vijf jaar. Volgens Swartz trekt deze bepaling niet alleen alle bestaande bilaterale verdragen, maar tevens multilaterale verdragen tussen de Verenigde Staten en de Europese Unie, verdragen in het kader van de Verenigde Naties en de Raad van Europa en samenwerking in het kader van Interpol in twijfel. Dit artikel moet worden gewijzigd of verwijderd, aldus Swartz. Zo niet, dan zijn de overheden jaren bezig met het heronderhandelen van verdragen in plaats van met het bestrijden van criminaliteit. Ten tweede bekritiseert Swartz de drietrapsraket van bescherming uit de richtlijn bij overdracht aan derde landen: *adequacy decision*, *appropriate safeguards* en *case-by-case derogation* (hoofdstuk V van de richtlijn). Verder waarschuwt hij voor de in zijn ogen ongewenste verschuiving van finale beslissingsbevoegdheid naar gegevensbeschermingsexperts in plaats van ordehandhavingsfunctionarissen. Aan het eind van de sessie gaat Swartz nog kort in op de uitgebreide juridische beschermingsmaatregelen die in de Verenigde Staten bestaan voordat er gegevens mogen worden verzameld, bijvoorbeeld een uitspraak van een rechter voordat e-mails en telefoongesprekken mogen worden ingezien en verzameld. Volgens Swartz is dit in veel lidstaten van de Europese Unie niet eens nodig. Ten slotte zegt hij dat de Verenigde Staten nooit het eigen systeem zullen opleggen aan de Europese Unie of anderen maar altijd zullen zoeken naar wederzijdse erkenning waarbij systemen naast elkaar kunnen blijven bestaan.

De derde en laatste spreker van het trans-Atlantische panel is **Cameron F. Kerry**, General Counsel van het US Department of Commerce.[2] Hij vangt aan met de constatering dat in de Verenigde Staten en de Europese Unie gelijke principes ten grondslag liggen aan nieuwe privacyregelgeving. Met het oog op economische groei en de toenemende digitalisering is dit van groot belang, aldus Kerry. De eerder genoemde Blueprint van het Witte Huis heeft vier kernonderdelen, waaronder interoperabiliteit van het systeem ten behoeve van samenwerking met internationale partners. Ten aanzien van de richtlijn heeft hij vier opmerkingen. Allereerst is het principe van geschiktheid zodanig gedefinieerd dat het uitgaat van gelijke systemen terwijl binnen de Europese Unie al sprake is van verschillende systemen die ook nog eens geen van alle overeenkomen met het Amerikaanse systeem. Dit uitgangspunt biedt niet de flexibiliteit die nodig is voor samenwerking, zoals wel wordt geboden door de Safe Harbor. Vervolgens uit Kerry kritiek op de bepaling dat aanpassing aan technische ontwikkelingen bij de Europese Commissie is belegd en niet tot stand komt via een *multi stakeholder approach* om gelijke tred te houden met technologische ontwikkelingen, zoals in de Verenigde Staten. Ten slotte vraagt Kerry om aanpassing van de definitie van toestemming. Toestemming hoeft volgens hem niet altijd actief en expliciet te zijn.

[1] http://www.europarl.europa.eu/document/activities/cont/201210/20121019ATT54062/20121019ATT54062EN.pdf
[2] http://www.europarl.europa.eu/document/activities/cont/201210/20121015ATT53644/20121015ATT53644EN.pdf

Beslissend dient volgens hem te zijn het type gegevens waar het om gaat, de context en de gevoeligheid.

In reactie op dit Amerikaanse drietal vragen twee Europarlementariërs het woord. Birgit Sippel (S&D) waarschuwt dat hoe meer gegevens er verzameld worden, hoe groter de kans is op misbruik van deze gegevens. We hebben volgens haar duidelijke regels nodig en boetes voor hen die zich niet aan de regels houden. Vervolgens citeert ze uit een evaluatierapport over de Safe Harbor uit 2004 waarin problemen worden gesignaleerd. Ze vertelt dat de Duitse toezichthouder in 2010 opnieuw heeft bepaald dat er niet werd voldaan aan de afspraken en dat de Europese Unie en de Verenigde Staten niet in staat waren om naleving af te dwingen. In reactie hierop geeft Nemitz aan dat een nieuw rapport over de Safe Harbor aanstaande is en dat sinds 2004 de controles zijn geïntensiveerd. Vladeck weerspreekt de kritiek uit het rapport over Safe Harbor en stelt dat de Verenigde Staten de naleving ervan heel serieus nemen. Kerry ten slotte stelt dat de activiteit op het gebied van Safe Harbor zeer is toegenomen, net zoals samenwerking met DG Justitie van de Europese Commissie. Daarnaast zijn er plannen om de bevoegdheden van de FTC te vergroten op dit gebied. Europarlementariër Krisztina Morvai (NA) vraagt naar een nadere uitweiding over en de mogelijke gevolgen voor de toekomst van de Google-case. Vladeck vertelt wat de precieze aanklachten waren in de twee zaken tegen Google. Ten aanzien van de gevolgen zegt Vladeck dat het signaal aan Google – en aan anderen in de toekomst – duidelijk heeft gemaakt wat de FTC verwacht van bedrijven, namelijk duidelijke informatie verlenen en toestemming vragen, voldoen aan de eisen van Safe Harbor en een privacyprogramma ontwikkelen met openbare audits. Het opleggen van boetes is een ingewikkelde kwestie en er zal altijd kritiek zijn op de hoogte ervan.

Session VII – Data Protection in the global context – (2nd part) What standards for effective data protection

De laatste sessie, gemodereerd door vicevoorzitter van het Europees Parlement **Alexander Alvaro**, wordt geopend door **Marc Rotenberg**, president van het Electronic Privacy Information Center (EPIC). Rotenberg vertelt dat zijn organisatie, samen met 20 consumentenorganisaties in de Verenigde Staten, de hervorming van de privacywetgeving van de Europese Unie ondersteunt. Hij verwacht dat het ook voordelen oplevert voor consumenten over de hele wereld en in Amerika. Dat gebeurde in 1995 ook, toen de huidige richtlijn werd vastgesteld. Bovendien benadrukt hij dat de opslag van grote hoeveelheden gegevens in de *cloud* vraagt om andere dan de traditionele juridische waarborgen. Ook de wetgeving in de Verenigde Staten loopt op dit punt nog achter; de Electronic Communications Privacy Act dateert van 1986 en de Patriot Act heeft de toch al lage bescherming nog verder verlaagd. Met name de bescherming van gegevens van niet-Amerikaanse burgers laat nog te wensen over. Voor Amerikaanse consumenten is er wel vooruitgang geboekt, bijvoorbeeld in de vorm van de (overigens niet-bindende) Consumer Privacy Bill of Rights, vastgesteld door de regering-Obama (ook bekend als de White House Privacy Blueprint). Hierin is een aantal grondbeginselen vastgelegd dat belangrijk is voor de bescherming van de privacy van de consument. Daarnaast heeft de Federal Trade Commission belangrijke resultaten geboekt tegen de grote bedrijven die de privacy van consumenten schenden (Facebook and Google). Het thema van deze sessie is heel belangrijk, benadrukt Rotenberg. Alle landen zitten namelijk met dezelfde problemen. Hij heeft de indruk dat er overal ter wereld overeenstemming is over de oplossingen. Rotenberg noemt de volgende zes stellingen waar iedereen het volgens hem over eens is:

- wetten betreffende gegevensbescherming moeten scherper worden en deze wetten moeten vervolgens gehandhaafd worden;
- bedrijven moeten verantwoordelijk gehouden worden voor wat zij met informatie doen,
- grotere transparantie betreffende het verwerkingsproces van informatie is gewenst;
- beschermende technieken voor privacy (*Privacy Enhancing Technologies*/*privacy by design*) moeten ontwikkeld worden en vervolgens routinematig worden ingezet;
- speciale bescherming voor de gegevens van kinderen is vereist en
- individuen moeten de baas blijven over hun eigen gegevens, ook als deze elders berusten.

Na deze spreker krijgt **Casper Bowden**, een privacy advocaat die voorheen bij Microsoft werkte, het woord. Hij spreekt over de geheime toegang tot gegevens van Europese burgers door de Amerikaanse overheid in het kader van *cloud computing*. In 2008 is de Foreign Intelligence Surveillance Amendment Act (FISA) aangenomen. Volgens Bowden kunnen alle gegevens die Europese burgers opslaan in de *cloud* door deze wet onderworpen worden aan het toezicht van de Amerikaanse overheid, zonder de juridische bescherming die van toepassing is op Amerikaanse burgers. Bovendien stelt Bowden dat de Amerikaanse overheid via FISA internationale verdragen omzeilt. Bowden benadrukt dat het aanscherpen van de juridische bescherming alleen geen oplossing biedt. Verder stelt hij, in navolging van de eerder genoemde Willem Debeuckelaere, dat er een Europese autoriteit voor de gegevensbescherming moet komen die groot genoeg is om een juridische strijd aan te gaan met bedrijven als Microsoft. Een boete van 2% van de jaarlijkse wereldwijde omzet, zoals voorgesteld in artikel 79 van de ontwerpverordening, kan zeker effect hebben, maar het opleggen ervan leidt doorgaans tot lange procedures. Een toezichthouder moet dus voldoende geëquipeerd zijn om die procedures vol te houden. Tevens benadrukt de spreker het belang van goede ondersteuning van klokkenluiders.

Hierna krijgt **Alexander Seger** het woord. Als hoofd van de Divisie Gegevensbescherming en Internetcriminaliteit van de Raad voor Europa is hij betrokken bij de onderhandelingen over herziening van de Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data uit 1981 (ETS 108). Hij vertelt dat de onderhandelingen gestart zijn in maart 2010. Op 30 november 2012 zal het voorstel worden aangenomen in het raadgevend comité inzake de het verdrag voor de bescherming van personen in verband met automatische verwerking van persoonsgegevens, waarna het doorgestuurd wordt naar het comité van ministers. De verwachting is dat dit in de loop van 2013 de onderhandelingen afrondt. Seger benadrukt dat het van belang is dat de Europese Commissie tegen die tijd ook een mandaat heeft om te onderhandelen. Hiernaast benadrukt hij het belang van consistentie tussen de hervormingen in de Europese Unie en Conventie 108. Op dit moment is het belangrijkste punt van discussie de vrije uitwisseling van gegevens tussen de 27 EU-lidstaten en de andere landen in Europa. Hierna gaat hij kort in op twee verzoeken van de Raad van Europa aan de Europese Unie, te weten het verzoek dat zowel de richtlijn als de verordening verwijzen naar Conventie 108 en het verzoek dat de Raad van Europa en de Europese Unie samenwerken om tot een adequaat systeem van gegevensbescherming te komen ten aanzien van derde landen. Seger heeft tot slot nog drie opmerkingen ten aanzien van de richtlijn. Ten eerste valt het hem op dat de richtlijn op sommige punten minder bescherming biedt dan de verordening. Ten tweede moet er een oplossing worden gevonden voor wat hij noemt «het verlies van locatie». Tegenwoordig weten wijzelf en opsporingsdiensten niet meer waar onze gegevens fysiek zijn opgeslagen.

Daarom verliest wat hij noemt het «territoriumprincipe» zijn relevantie. Dat leidt niet tot een adequate bescherming van gegevens. Daarom moet hiervoor een alternatief worden gevonden. Ten derde benadrukt hij dat voorkomen moet worden dat gegevensbescherming in de weg staat van effectieve rechtshandhaving. Mogelijk verplaatst rechtshandhaving zich anders van het veld van het strafrecht naar het veld van nationale veiligheid, waar relatief lage waarborgen gelden voor o.a. gegevensbescherming.

Michael Donohue, senior beleidsanalist bij de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO), gaat in op drie elementen van gegevensbescherming: schaal, risico en interoperabiliteit. Hij benadrukt dat sinds het ontstaan van privacywetgeving de omvang van het belang van gegevens voor de economie en de samenleving is toegenomen. De context waarbinnen de wetgeving moet functioneren is dus sterk veranderd. Hierbij stelt hij dat tegenwoordig middelgrote en kleine bedrijven ook onder privacywetgeving vallen. Deze wetgeving moet wel werkbaar blijven voor het MKB. Ten tweede stelt Donohue dat privacybescherming risicogericht moet zijn. De vraag is dan in hoeverre bepaalde technieken, of het bezit van bepaalde gegevens door een bedrijf of overheid, een bedreiging vormen voor de individuele privacy. Tot slot benadrukt hij dat privacykaders naar elkaar toe schuiven vanwege interoperabiliteit. Alleen op deze manier kan de privacy gewaarborgd zijn, los van de plek waar de gegevens zich bevinden en de nationaliteit van het individu.

In reactie op de presentaties van de panelleden wordt er gediscussieerd over de achtergrond van de FISA-wet, sectie 1881a hiervan (Procedures for targeting certain persons outside the United States other than United States persons) en de grootte van het probleem dat zich hierdoor voordoet. Enkele sprekers maken nogmaals duidelijk dat de Amerikaanse overheid andere normen oplegt voor haar eigen burgers dan voor burgers met een andere nationaliteit. Tevens wordt er gesproken over de mogelijkheid dat de verschillende landen clausules in hun privacywetgeving van elkaar overnemen, maar dit wordt over het algemeen als te ambitieus gezien. Daarnaast wordt er ook kort ingegaan op de relatie tussen privacy en andere rechten zoals vrijheid van meningsuiting. Tot slot wordt nog gesproken over de problemen ten aanzien van interoperabiliteit.

Na deze laatste sessie betreden de rapporteurs **Albrecht** en **Droutsas** opnieuw het podium. Zij constateren dat er over het algemeen een positieve grondhouding bestaat ten opzichte van harmonisatie en dat de voorstellen «leven» in de nationale parlementen. Zij bedanken de aanwezigen voor hun nuttige en belangrijke bijdragen en beloven de opmerkingen van de nationale parlementen mee te nemen in hun rapporten.

De delegatie,
Ter Horst
Gesthuizen

De griffiers van de delegatie,
Dragstra
Vermeer