Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2010–2011

31 051 Evaluatie Wet bescherming persoonsgegevens

B

VERSLAG VAN EEN EXPERTMEETING

Vastgesteld 10 maart 2011

De vaste commissies voor de JBZ-Raad[1], Binnenlandse Zaken en de Hoge Colleges van Staat/Algemene Zaken en Huis der Koningin[2], Justitie[3], Onderwijs, Cultuur en Wetenschap[4] en Volksgezondheid, Welzijn en Sport/Jeugd en Gezin[5] hebben op maandag 21 februari 2011 gesprekken gevoerd over **de rol van de overheid bij digitale dataverwerking**. Van deze gesprekken brengen de commissies bijgaand stenografisch verslag uit.

kst-31051-B
ISSN 0921 - 7371
's-Gravenhage 2011

Aanvang 16.00 uur

Gesprek met:
- **Corien Prins, Wetenschappelijke Raad voor het Regeringsbeleid;**
- **Geert Munnichs en Jan Staman, Rathenau-instituut;**
- **Jacob Kohnstamm, voorzitter College bescherming persoonsgegevens CBP;**
- **Peter Hustinx van de European Data Protection Supervisor (EDPS);**
- **Thomas Meijer en Thomas Wijsman, Algemene Rekenkamer (mw. Van Schoten was wegens ziekte verhinderd).**

Voorzitter: Van de Beeten
Griffier: Van Dooren

Aanwezige leden: Van de Beeten, Dupuis, Duthler, Franken, Hamel, Ten Horn, Slagter-Roukema, Strik en Tan.

De **voorzitter**: Ik heet iedereen van harte welkom bij deze expertmeeting van de Eerste Kamer over de rol van de overheid bij digitale dataverwerking en data-uitwisseling. Ik heet in het bijzonder de sprekers achter de regeringstafel welkom. Ik hoop dat zij zich daar comfortabel bij voelen. Ook heet ik de collega's en de ambtenaren van diverse departementen welkom. De publieke belangstelling voor deze bijeenkomst is aanzienlijk. We hebben een vol programma. De bedoeling is dat we veel informatie krijgen van de experts. We zullen daartoe nog veel vragen stellen. De leden en de experts in de zaal die eventueel een bijdrage willen leveren kunnen daartoe gebruikmaken van de interruptiemicrofoons die midden in de zaal staan.
De Eerste Kamer beschikt tegenwoordig over maar liefst vijf camera's. Vroeger had zij er maar één. Toen was het nog saai in deze Kamer. Het wordt hier steeds opwindender, dus moeten meer camera's het beeld vastleggen. De sprekers hoeven zich daarover geen zorgen te maken; het gaat allemaal volautomatisch. Als zij op een bepaalde knop drukken, komen ze meteen in beeld. Deze bijeenkomst wordt via internet live uitgezonden. Door deze bijeenkomst kunt u dus ook nog wereldberoemd worden in dit land.
De sprekers is gevraagd om een inleiding te houden van niet langer dan tien minuten. Ik zal daaraan strikt de hand houden. Ik hoop dat dit allemaal goed gaat lukken. We zullen schorsen om ongeveer 18.00 uur. Van de griffie moet ik niet mededelen dat er voor de mensen in het publiek geen broodjes zullen zijn. Deze broodjes zijn er alleen maar voor de experts, de leden en de ambtenaren. Helaas hebben wij voor de gewone Nederlanders die vandaag aanwezig zijn geen soep en broodjes gereserveerd. Zij zullen ervoor moeten zorgen dat zij elders wat te eten krijgen. We hopen om 20.00 uur af te ronden. Bij de vorige expertmeeting, in maart 2008, kon ik dat niet doen. Toen heb ik het overhandigen van de gebruikelijke fantasieloze cadeaus van de Eerste Kamer aan de sprekers overgelaten aan een collega van mij, de heer Franken. Dit keer zal ik dit zelf doen. Ik hoop de bijeenkomst in zijn geheel te kunnen bijwonen.
Ik vraag de sprekers om vanachter het spreekgestoelte het woord te voeren. Voor de heer Kohnstamm is dat niet ongewoon en ook de heer Munnichs heeft dit al eens gedaan, maar voor de anderen zal dit de eerste keer zijn. Dat is altijd een hele ervaring.

De heer **Munnichs**: Voorzitter. Hartelijk dank voor de gelegenheid om ons rapport over databases te mogen toelichten. Daar zijn wij zeer mee vereerd. De titel van ons rapport is «Ontwerp van databases. Een pleidooi voor structureel toezicht». Deze titel is meteen ook onze belangrijkste

boodschap. Op de slide is de omslag van het boekje te zien dat eind vorig jaar is verschenen. Als het goed is, hebben alle Eerste Kamerleden daarvan een exemplaar ontvangen.
In de studie hebben wij zes digitale datasystemen onderzocht: de ov-chipkaart samen met de kilometerheffing, het elektronisch patiëntendossier, het kinddossier, klantenprofielen op internet, het Schengeninformatiesysteem en de gemeentelijke basisadministratie. We hebben hierbij vooral naar het ontwerp en de architectuur van deze systemen gekeken. We hebben dus gekeken naar het technisch ontwerp. Wordt er gebruikgemaakt van versleuteling? Worden gegevens centraal of decentraal opgeslagen? Ook hebben we gekeken naar het functioneren van de systemen in een bredere context. Hoe zit het bijvoorbeeld met het inzagerecht van de burger? Tevens hebben we de vraag gesteld hoe het ontwerp samenhangt met de doelen die je aan zo'n systeem kunt stellen, welke risico's aan een bepaald ontwerp verbonden zijn en de gevolgen daar weer van voor personen waarover gegevens worden verzameld. De bedoeling van dit alles is niet om ons in zes afzonderlijke politieke discussies te mengen, maar om lessen te trekken voor de wijze waarop een doordachte omgang met databases er zou kunnen uitzien.
De eerste bevinding is dat beveiliging een heet hangijzer is en blijft. Zie bijvoorbeeld het gemak waarmee de ov-chipkaart valt te kraken, tegenwoordig ook door niet-experts. Maar ook het landelijk elektronisch patiëntendossier lijkt kwetsbaar door de honderdduizenden UZI-passen die in omloop komen, in combinatie met het gebrekkige risicobewustzijn in de medische sector en de constructie dat controle op onbevoegde toegang achteraf plaatsvindt. In beide gevallen hadden zwaardere technische maatregelen kunnen leiden tot een betere beveiliging door te kiezen voor een zwaardere chip in de ov-chipkaart of voor een decentrale opslag van medische gegevens, waarbij de patiënt de toegang beheert. In beide gevallen heb je het dan meteen al over ontwerpkeuze. Ik geloof dat de keuze voor de huidige Mifare-chip in de ov-chipkaart mede is ingegeven door de lage kosten ervan. Dat is één aspect.
Daarnaast vormen fouten in registraties een serieus probleem, bijvoorbeeld als gevolg van verschrijvingen, verouderde data, identiteitsdiefstal of problemen met de interpretatie van data. Zo kan het elektronisch kinddossier ertoe leiden dat kinderen door een samenloop van omstandigheden ten onrechte als risicokind worden aangemerkt. Voor het gebruik van klantenprofielen op internet geldt iets dergelijks. Profilering is vooralsnog een grof instrument. Er wordt een virtuele identiteit gecreëerd op basis waarvan de klant in een bepaald profiel past. Dat hoeft echter niet overeen te stemmen met de werkelijkheid. Maar je kunt er wel degelijk nadeel van ondervinden. Je zult maar ten onrechte als wanbetaler te boek staan, bijvoorbeeld omdat je in een «slecht» postcodegebied woont en ooit een akkefietje hebt gehad rond een betaling.
Een belangrijk aandachtspunt hierbij is de rechtspositie van de burger. Het wettelijk inzage- en correctierecht blijkt in meerdere gevallen toch vooral een papieren recht dat zich moeilijk laat effectueren. Fouten in registraties zijn dan door jou als burger moeilijk te herstellen. Bij de ov-chipkaart, het Schengeninformatiesysteem, klantenprofielen en mogelijk ook bij het elektronisch kinddossier vormt dat een probleem. Het ontwerp van databases lijkt over het algemeen primair toegesneden op de behoefte van de opdrachtgever, terwijl de belangen van de burger een ondergeschikte rol lijken te spelen. Dat raakt aan een meer fundamentele vraag: versterkt het systeem de afhankelijkheid van de burger of juist diens digitale autonomie? Bij krantenprofielen zie je bijvoorbeeld duidelijk dat er een asymmetrie ontstaat tussen de informatiepositie die bedrijven opbouwen en de informatie die je hebt als klant. Vaak heb je er niet eens weet van wat voor gegevens over jou worden verzameld, laat staat wat daar vervolgens mee wordt gedaan.

Een laatste aandachtspunt betreft de doelmatigheid van databases. Doen ze wat ze moeten doen? De ambities zijn vaak hoog. Het elektronisch kinddossier moet kindermishandeling voorkomen, maar het gebruik van risicoprofielen in de jeugdgezondheidszorg dreigt te leiden tot onwerkbaar grote aantallen mogelijke risicokinderen. Er worden enorme hoeveelheden gegevens gegenereerd die het zicht belemmeren op de echte probleemgevallen. Daarmee dreigt het zijn doel voorbij te schieten. Het Schengeninformatiesysteem dreigt te bezwijken onder aanhoudende technisch-organisatorische problemen die mede voortkomen uit de veelheid aan politieke doelen die het systeem moet dienen, onder meer drastische uitbreiding van het aantal lidstaten. Te hoge ambities kunnen omslaan in hun tegendeel. Het principe «select before you collect», ook aangewezen door de commissie-Brouwer-Korf, verdient dan ook meer aanbeveling. Dat betekent ook reflectie op het eigenlijke doel dat een database moet dienen.
Ik kom aan mijn conclusies. Uit onze studie komt naar voren dat digitale datasystemen niet risicovrij zijn. Dat is niet te wijten aan toevallige fouten of slordigheden. Als je de verschillende casestudy's op een rijtje zet, tekent zich een patroon af van vaak te weinig aandacht voor de risico's die samenhangen met ontwerpkeuzes. Vooral de burger wordt het kind van de rekening.
Kan het ook anders? Ja. De casestudy over de kilometerheffing laat zien dat de dikke variant van de kilometerheffing, die bedacht is onder het bewind van Eurlings, een privacyvriendelijk ontwerp is waarbij alleen de automobilist direct toegang krijgt tot zijn gegevens en de exploitant alleen versleutelde data, met als extra voordeel dat de automobilist bewijsmateriaal tot zijn beschikking heeft als hij een verkeerde rekening krijgt opgestuurd, in tegenstelling tot bijvoorbeeld bij de ov-chipkaart. ICT kan dus ook de positie van de burger versterken, maar dat vereist dan wel dat bepaalde keuzes worden gemaakt in de ontwerpfase.
Op grond van het bovenstaande komen wij tot de volgende aanbevelingen voor het ontwerp van databases:
– maak zo veel mogelijk gebruik van technische maatregelen om gegevens te beschermen;
– versterk de positie van de burger;
– faciliteer het inzage- en correctierecht en bouw opnieuw die rechten zo veel mogelijk in het systeem in;
– houd het simpel, kies een welomschreven doel en beperk de gegevensverzameling tot de voor dat doel noodzakelijke gegevens.

Deze aspecten hangen overigens nauw samen en kunnen ook strijdig met elkaar zijn. Zo kan inzage door een burger in zijn gegevens of het kunnen delen van gegevens met andere instanties op gespannen voet staan met de wensen op het gebied van beveiliging.
Iedere ontwerpkeuze heeft zijn voor- en nadelen. Die behoeven afweging en reflectie. Een doordacht ontwerp veronderstelt kennis van technische mogelijkheden en beperkingen, kennis van alternatieve ontwerpkeuzes en reflectie op de doeleinden. Vanwege het groeiende belang van digitalisering pleiten wij dan ook voor structureel toezicht op de keuzes die worden gemaakt in de ontwerpfase van grote digitale informatiesystemen. Dat kan bijvoorbeeld in de vorm van een ICT-autoriteit.

Mevrouw **Slagter-Roukema** (SP): Je sprak over structureel toezicht in de ontwerpfase en toen noemde je een ICT-autoriteit. Nu is mijn ervaring vanuit het epd dat juist een van de dingen die daarin fout zijn gegaan, is dat het heel erg ICT-driven is geweest en dat te weinig gekeken is waarvoor het nodig zou zijn, als je kijkt naar ondersteuning van het zorgproces. Op welke manier denk jij dat eventueel de inhoudelijke kennis kan worden ingebouwd in de zin van «waarvoor het systeem bedoeld is en wie ervoor moet werken»?

De heer **Munnichs**: Wij pleiten primair voor het structurele toezicht. Hoe je dat precies gaat vormgeven is natuurlijk een tweede. In onze studie staat nog: roep een ICT-autoriteit in het leven. Wij zijn er ook nog niet uit hoe je dat nu precies inhoud en vorm geeft.

Mevrouw **Slagter-Roukema** (SP): Misschien moet ik dan duidelijker vragen hoe de ICT-autoriteit eruitziet. Als jij «ICT-autoriteit» zegt, denk ik aan iemand die weet hoe ICT in elkaar zit, terwijl het natuurlijk wel veel breder zou moeten zijn.

De heer **Munnichs**: Wij hebben niet voor niets gezegd dat wij niet alleen naar een technisch ontwerp hebben gekeken, maar ook naar de bredere context waarin een systeem moet functioneren. Je moet altijd naar de bredere context kijken. Het gaat inderdaad om wat een ICT-systeem gaat doen met burgers en gegevens en hoe het functioneert in de samenleving. Ik ben het helemaal met u eens dat het niet alleen om ICT-kennis gaat. Ik wil echter vooral benadrukken dat je voldoende ICT-kennis in huis moet hebben om goed over dit soort systemen te kunnen oordelen. Het is dus meer de andere kant op.

De heer **Hamel** (PvdA): De discussie gaat vaak over de techniek en het gebruik van het systeem. Ik noem het voorbeeld van het elektronische patiëntendossier. Er gaat een wereld voor je open als je ontdekt wie er op welk moment een interpretatie van geeft. In hoeverre wordt dat gewogen? Wij hebben het vaak over «het systeem» en de mate waarin dat systeem veilig is. Uiteindelijk kan de wijze waarop het systeem zijn gegevens weergeeft of de wijze waarop die gegevens zijn verzameld, tot interpretatiefouten leiden. Dat kan in het systeem aanwezig zijn door de wijze waarop de gegevens worden verzameld. In hoeverre noemt u dat «context»? Of vindt u het een volgend hoofdstuk?

De heer **Munnichs**: Je moet je bezinnen op het eigenlijk doel van een epd. Het primaire doel is het terugbrengen van het aantal medische missers. Als een systeem een nieuw soort medische missers gaat produceren, moet je je nog eens goed afvragen hoe het systeem zinvol kan zijn. Het gaat om fundamentele vragen: wat moet het systeem eigenlijk doen en biedt ICT daar de beste manier voor? Dat moet onderdeel van de hele discussie zijn.

De heer **Hamel** (PvdA): Je ziet het ook bij andere vormen van gegevensverzameling. Het gaat om de wijze waarop wie wat gaat doen met die gegevens. Het gaat om de vraag in hoeverre helder is waarop die gegevens betrekking hebben.

De heer **Franken** (CDA): Voorzitter. De stukken die heer Munnichs produceert zijn altijd buitengewoon interessant en weldoorwrocht. Met dat compliment wil ik graag beginnen. Nu komt de kritiek, met name over de gedachtevorming. Zo'n ICT-autoriteit wordt weer een huis met een boom ervoor en een koperen plaat naast de deur en zoveel fte's. Dat interfereert weer met bevoegdheden van andere instituten. Je moet niet alleen de techniek beoordelen, maar ook politieke afwegingen maken. Je moet de mogelijkheden van het gebruik bezien. Wat schieten wij met zo'n autoriteit op? Wat het epd betreft zijn er volgens de heer Munnichs drie kwetsbare punten: er is alleen controle achteraf, er worden veel te veel gebruikspassen afgegeven waardoor misbruik dreigt, en het ICT-bewustzijn in de sector is niet groot genoeg. Kan zo'n autoriteit daar iets aan doen? Geldt dat niet voor ieder gebruik? Met een mes kun je iemand doodsteken, maar je hebt het ook nodig om je boterham te snijden. Het zijn praktische dingen waarvan je niet kunt zeggen dat je het allemaal tevoren moet regelen. Komen wij dan niet in een samenleving

terecht waarvoor geldt: het is verboden te leven, tenzij je voldoet aan de voorwaarden a t/m z?

De heer **Munnichs**: Ik wil niet beweren dat je alle problemen van tevoren kunt voorzien. Je kunt dus ook niet alles van tevoren bespreken. Bij het epd ben ik wel benieuwd naar een afweging tussen een decentrale opslag van gegevens en het huidige systeem. Voor zover ik weet, heeft zo'n discussie niet plaatsgevonden. Een ICT-autoriteit zou zo'n vraag kunnen opwerpen: moeten wij niet naar een heel andere architectuur van zo'n systeem toe?

De heer **Franken** (CDA): Bij het epd is er toch helemaal geen sprake van centrale opslag? De dokter houdt de gegevens in zijn eigen file.

De heer **Munnichs**: Met «decentrale opslag» doel ik erop dat de patiënt de toegang tot zijn gegevens beheert. De patiënt heeft de sleutel. Je moet vooraf toestemming aan de patiënt vragen. Alleen dan kun je toegang tot de gegevens krijgen. Dat is een andere situatie dan bij de plannen voor het landelijke epd op dit moment, waarin er een landelijk schakelpunt is en waarin zorgverleners via een aantal procedures toegang tot de gegevens kunnen krijgen. Formeel hoort daar toestemming van de patiënt bij, maar dat is een procedure. Op het moment dat een zorgverlener aanvinkt dat hij toestemming heeft, heeft hij die stap gezet. Het kan achteraf gecontroleerd worden door dat login-systeem. Bij de Gesundheitskarte heeft de patiënt zelf de beschikking over zijn gegevens en kan hij uitmaken wie er wel en niet bij die gegevens kan. Dat is een ander systeem. Ik zeg niet dat het ene systeem beter is dan het andere. Het gaat er mij om dat dit soort vragen eigenlijk op tafel moet komen voordat je beslist tot een bepaald systeem.

Mevrouw **Ten Horn** (SP): Ik ben benieuwd of de heer Munnichs wat betreft de aspecten van betrouwbaarheid, beveiliging en toegankelijkheid een onderscheid heeft gevonden tussen de databases die commercieel zijn en de databases die van de overheid zijn.

De heer **Munnichs**: Nee, ik kan daar geen algemene dingen over zeggen. We hebben een spreiding gemaakt over zes verschillende systemen, waaronder ook commerciële. We hebben gewoon te weinig verschillende systemen bekeken om daar algemene uitspraken over te kunnen doen. Ik weet bijvoorbeeld dat er ten aanzien van de TomTom wel goed is nagedacht over het anonimiseren van de ritgeschiedenis. Dus er zijn ook voorbeelden bekend van commercieel gebruik waarbij wel goed is nagedacht over de architectuur.

Mevrouw **Tan** (PvdA): Ik probeer het toch nog een slagje scherper te krijgen waar het gaat om de reikwijdte van de ICT-autoriteit. Het ging zo-even al over de vraag met welk doel op een gegeven ogenblik een systeem wordt opgezet en wie dat dan bepaalt. Om bij het voorbeeld van het epd te blijven: het primaire doel was het voorkomen van missers. Vervolgens heeft het systeem zich in eerste instantie gericht op de instellingen, waarbij de patiënt of de burger een beetje vergeten is. Hoort het in de opvatting van de heer Munnichs tot de bevoegdheden van de ICT-autoriteit om die opzet te becommentariëren? Of is dat eigenlijk voorbehouden aan de politieke afweging van regering en parlement?

De heer **Munnichs**: Naar mijn idee zou zo'n toezicht in de ontwerpfase wettelijk verplicht moeten worden. Hoe de verhouding is tussen de oordeelsvorming door de toezichthouder en de politieke besluitvorming heb ik zo een-twee-drie niet scherp. Dat weet ik niet precies.

Mevrouw **Tan** (PvdA): Bij de beslissing om een systeem te ontwikkelen en daarbij vast te leggen wat het doel is en waarop het zich primair richt, houdt de heer Munnichs dus open dat zo'n ICT-autoriteit ook opzet en doel gaat toetsen alvorens te gaan kijken naar de uitwerking qua systeemontwikkeling?

De heer **Munnichs**: Misschien moet ik die doeltoetsing nog even toelichten. Het gaat mij er daarbij niet primair om dat het hele politieke debat door de ICT-autoriteit wordt gevoerd. Als je een systeem in het leven wilt roepen, heb je een lijstje met wensen waaraan zo'n systeem moet voldoen. Dat zijn, zeg maar, de politieke doelen. Die kunnen tot op zekere hoogte onverenigbaar met elkaar zijn. Maar in welke mate dat het geval is en welke risico's er aan de verschillende doelen zijn verbonden, heeft onder meer te maken met de mogelijkheden en beperkingen van het ICT-systeem. Dus de doelen en de middelen staan niet los van elkaar. Die moet je in onderlinge verhouding bekijken. Bij het elektronisch kinddossier kun je je afvragen of het gewenste doel om van ieder kind een risicoprofiel te maken verstandig is als je ziet waartoe dat leidt. Misschien moet je dat doel dan opnieuw gaan definiëren als je ziet dat het eigenlijk iets onmogelijks oplevert.

Mevrouw **Strik** (GroenLinks): Voorzitter. Deels heeft de heer Munnichs al antwoord gegeven op de vraag die ik wil stellen. Hij geeft terecht aan dat beperkt gegevens verwerkt moeten worden tot het doel waarvoor dat nodig is. Dan is de vraag pregnant of het doel precies genoeg is geformuleerd en of de techniek daarop vooruitloopt. In het SIS, dat ook door het Rathenau Instituut is onderzocht, zie je dat de systematiek en de techniek al vooruitlopen op mogelijke politieke besluitvorming om de doelen eventueel uit te breiden. Zo lees ik het tenminste. Vindt de heer Munnichs dat een goede zaak? Maakt dat niet dat er nog voordat de wetgever het doel heeft verruimd, misschien toch al wordt geanticipeerd door meer gegevens te verzamelen dan de wetgever uiteindelijk nodig heeft voor het bereiken van zijn doel? Kan er niet een duidelijke knip in worden gemaakt, zodat pas bekeken wordt welke gegevens nodig zijn op het moment dat er wetgeving is die dat doel duidelijk heeft gemaakt?

De heer **Munnichs**: Als ik het goed begrijp, spelen hier twee verschillende dingen. Ten eerste dat je in het systeem de mogelijkheid van verschillende functionaliteiten inbouwt. Bij SIS II is besloten om in het systeem in te bouwen dat er in de toekomst nog voor extra functionaliteiten kan worden gekozen, maar dat wil natuurlijk niet zeggen dat er meteen in het kader van die functionaliteiten gegevens worden verzameld. Dat hoeft niet. Daar zit voor mijn gevoel nog een knip in. Ten tweede is onze analyse van het SIS echter dat het systeem dan zo hopeloos ingewikkeld wordt, dat het bijna niet meer kan functioneren, onder meer door die functie-uitbreiding en deels door de gestage uitbreiding van het aantal landen. Maar je kunt er natuurlijk altijd voor kiezen om niet al die functionaliteiten te activeren, lijkt mij.

Mevrouw **Strik** (GroenLinks): Laat ik de vraag iets breder formuleren. Ziet u in de praktijk wel eens dat er meer gegevens worden verzameld dan het doel rechtvaardigt, misschien met het oog op eventuele wenselijkheid om het doel in de toekomst uit te breiden?

De heer **Munnichs**: Ik snap de vraag niet helemaal.

Mevrouw **Strik** (GroenLinks): U zegt: beperk de gegevens tot het doel. Waarom maakt u die opmerking? Ziet u in de praktijk dat er meer gegevens worden verzameld dan strikt noodzakelijk is voor het geldende doel?

De heer **Munnichs**: Dan gaat het over het principe van doelbinding en het verschijnsel van function creep, waarbij een systeem voor het ene doel wordt ingericht en vervolgens voor andere doeleinden wordt gebruikt. Dat is het klassieke idee van doelbinding. Alleen voegen wij daar de reflectie op het eigenlijke doel aan toe, waarbij je niet alleen vanuit het gegeven doel moet redeneren maar je ook kritisch naar dat doel moet kijken. Dat is in feite een extra slag. Function creep komt dagelijks voor op allerlei gebieden. ANPR is daar een voorbeeld van. Iets wordt de wereld ingestuurd om zware criminaliteit en terrorisme te bestrijden, maar het leidt er vooral toe dat mensen met openstaande parkeerboetes van de snelweg worden geplukt. Je kunt je afvragen of je dat moet willen.

De **voorzitter**: Dank u wel, mijnheer Munnichs. Ik verzoek de collega's om bij de volgende ronde iets meer terughoudendheid te betrachten, anders komen we met ons tijdschema in de knoop.
Dan geef ik nu graag het woord aan de heer Wijsman van de Algemene Rekenkamer. Mijnheer Wijsman, ik zie dat u uw glas water meeneemt. Dat had u niet hoeven doen, want de Kamerbewaarder zorgt ervoor dat u een vers glas krijgt.

De heer **Wijsman**: Voorzitter. De Algemene Rekenkamer is onafhankelijk, dus ook de watervoorziening is onafhankelijk. Overigens ben ik mij helemaal niet bewust van camera's. Ik vraag me af of hier een mogelijk privacyprobleem ligt. Maar dit terzijde.
Ik wil de aanwezigen de komende kleine tien minuten graag uitleggen wat de Algemene Rekenkamer doet op het gebied van onderzoek naar ICT en informatiehuishouding. Zoals u weet, heeft de Algemene Rekenkamer de taak om de overheid te controleren. Bij het uitvoeren van die controlerende taak hebben wij de ambitie om bij te dragen aan de slagvaardigheid, de transparantie en het lerend vermogen van het openbaar bestuur. Van deze taak en ambitie – kort gezegd: onze missie – is onze strategie afgeleid in de huidige periode, van 2010 tot 2015. Wij hebben ons daarbij ook gebaseerd op het concept van good governance, van goed openbaar bestuur, van de Verenigde Naties.
De Verenigde Naties onderkennen acht kernprincipes van goed openbaar bestuur. Van vier van die principes is onze strategie afgeleid. Het zijn de volgende: het openbaar bestuur is transparant, legt publieke verantwoording af, is vraaggericht en is effectief en efficiënt. Deze vier principes vormen bij elkaar genomen twee pijlers van onze strategie. De ene pijler richt zich op beleid, de uitvoering van het beleid en de aansluiting daartussen. Wij noemen dat ook wel eens de kloof tussen beleid en uitvoering. De andere pijler is verantwoording en toezicht.
De kernprincipes die op de sheet vermeld staan, raken de democratische rechtsstaat. In feite zijn daarin de klassieke grondrechten weergegeven. Zij vormen echter niet het uitgangspunt voor onze strategie. Dat betekent niet dat wij deze onbelangrijk vinden; ze zijn alleen niet expliciet benoemd als richtinggevend voor ons onderzoek. Bij gelegenheid besteden wij daar wel degelijk aandacht aan. Ik verwijs even naar het rapport Financiering politieke partijen en naar ons lopende onderzoek naar het functioneren en presteren van de strafrechtketen. Dat is rechtstreeks relevant voor de rechtshandhaving en de rechtszekerheid.
Ik heb even bekeken wat wij de laatste tien jaar aan ICT-onderzoek hebben gedaan. In het algemeen noemen wij dat doelmatigheidsonderzoek. Wij moeten niet vergeten dat wij in het rechtmatigheidsonderzoek, dus in het onderzoek naar de financiële verantwoordingen, in het kader van de bedrijfsvoering stelselmatig aandacht besteden aan ICT. Ik heb in de sheets die ik hier laat zien, nog een aantal onderzoeken genoemd. Ik zal deze hier niet bespreken. Het is meer bedoeld om aan te geven welke type onderwerpen wij in de loop van de tijd hebben geraakt. Verschillende aanwezigen zullen vele van deze onderwerpen wel herkennen. Ik zie de

heer Kohnstamm al knikken. Wij hebben elkaar in een verder verleden al eens ontmoet in het kader van een van deze onderzoeken.
Ik zei net dat ik nog zou ingaan op onze bedrijfsvoeringsonderzoeken. Daarin besteden wij altijd aandacht aan informatiehuishouding en aan ICT. Er is een top drie samen te stellen van problemen, tekortkomingen, die je steeds weer ziet, soms bij dezelfde ministeries, soms variërend. Een ervan is ontoereikend autorisatiebeheer: wie mag wat doen met welke data? Wij komen dat het meest tegen bij de financiële systemen, misschien ook wel omdat wij er daar naar op zoek zijn. De heer Munnichs heeft al een aantal duidelijke voorbeelden gegeven van autorisatieproblemen die tot privacyproblemen leiden bij bijvoorbeeld het elektronisch patiëntendossier of het elektronisch kinddossier.
Een andere in de top drie is onvoldoende functiescheiding. Een van de voorbeelden die ik daarvan kan geven, is de visumverlening door ambassades in het buitenland. In een aantal gevallen is de behandelend ambtenaar ook de beschikkende ambtenaar. In dat geval is het wel heel erg gemakkelijk om een bekende, al dan niet met vreedzame of andere bedoelingen, een visum te verlenen en het land binnen te loodsen.
Wij constateren ook geregeld problemen met de beveiliging van informatie. Ik geef daar een voorbeeld van. In 2009 constateerden wij dat het ministerie van VWS geen inzicht had in de naleving van de Wet bescherming persoonsgegevens. In het rechtmatigheidsonderzoek waar wij nu mee bezig zijn, komt een ministerie naar voren dat ook nog niet eens weet in welke informatiesystemen persoonsgegevens verwerkt worden. Dat ministerie heeft dus geen volledig beeld van alle systemen. Ik kan op dit moment nog niet zeggen om welk ministerie het gaat, dat komt binnenkort.
Ik wil u graag meenemen in een aantal conclusies, niet zozeer uit een concreet onderzoek als wel door de oogharen heen kijkend naar aanleiding van meerdere onderzoeken. De eerste conclusie lijkt een dooddoener, maar het wordt nog wel eens vergeten: een goede informatievoorziening is cruciaal voor het functioneren en presteren van de overheid. Het gaat om de wijze waarop er met informatievoorziening en ICT wordt omgegaan. De heer Munnichs heeft daar al een aantal voorbeelden van gegeven en vanuit de Kamer is ook al gezegd: het is vaak ICT-gedreven. Ja, dat herkennen wij. Een voorbeeld van zo'n cruciale gebeurtenis hebben wij in ons rapport Informatiehuishouding bij het Rijk gegeven. Dat was een geval waarin de IB-Groep een beslissing had genomen over een student. Dat was een besluit met mogelijke precedentwerking. Een volgende student die zich wilde beroepen op het genomen besluit door de IB-Groep, verwees naar de e-mail, die hij zijn bezit had, waarin dat besluit vervat was. De IB-Groep kon die e-mail niet te voorschijn halen en moest dus bij gebrek aan eigen bewijs ongezien de tweede student ook het recht toekennen.
Een ander voorbeeld is het onderzoek van de commissie-Bakker naar de gebeurtenissen in Srebrenica. Deze commissie kon niet beschikken over het e-mailverkeer van Defensie en heeft ook de aanbeveling gedaan aan de overheid om het e-mailverkeer goed te gaan beheren. Een derde voorbeeld is niet iets wat mis is gegaan, maar waarmee wordt aangegeven waarom informatiehuishouding en omliggende ICT cruciaal zijn. Dat is de communicatie vanuit het Europees Hof voor de Rechten van de Mens over een besluit. Ik zal dat zo meteen toelichten.
De tweede algemene conclusie is dat ICT-projecten van de overheid vaak te ambitieus en te complex worden en daardoor nogal eens te laat worden opgeleverd en te veel geld kosten. Ze gaan ook niet snel in de lucht zonder dat alle functionaliteit gerealiseerd is. Eén van de eerste dingen die verdwijnt als een project in de problemen komt, is de aanvullende functionaliteit die dient voor de controleerbaarheid van het systeem en niet zelden ook voor een goede privacybescherming. Veel voorkomende oorzaken zijn politieke deadlines. Heel vaak wordt er een

wet aangenomen en dan moet de wet ingaan op 1 januari van het eerstkomende jaar. Maar ja, die systemen kunnen nu eenmaal niet zo snel worden gebouwd. Dan wordt het dus haastwerk. Heel vaak gaat een ministerie dan maar alvast aan de slag met het bouwen van een systeem, terwijl nog niet helemaal bekend is aan welke eisen het precies moet voldoen.
Een ander probleem dat we vaak zien, is dat de technologie wordt overschat. De redenering is heel vaak: ik heb een probleem – een beleidsprobleem, een bestuursprobleem, een organisatorisch probleem – en de ICT gaat dat voor mij oplossen. Dat is één van de redenen waarom ik persoonlijk niet zo heel veel zie in een ICT-autoriteit, want die zal eerder geneigd zijn om helemaal vanuit die ICT te redeneren. Het voorbeeld dat zojuist door de heer Munnichs gegeven is, kan hier ook als voorbeeld dienen: het elektronisch patiëntendossier of het elektronisch kinddossier. Het is niet helemaal duidelijk welke doelen het precies moet dienen laat staan dat al helemaal duidelijk is aan welke beveiligingseisen het dan moet voldoen.
Ik zal het met het oog op de tijd bij deze voorbeelden laten. Zit ik nog een beetje binnen de tijd?

De **voorzitter**: U zit vijftien seconden over de tien minuten.

De heer **Wijsman**: Dan zal ik het kort houden. Ik kom bij de gemeenschappelijke noemer bij de geschetste problemen, namelijk het feit dat er een probleem is met de informatiehuishouding van de overheid. Voor die informatiehuishouding hebben wij het beeld van een bloem gekozen. De bloem symboliseert de samenhang. De blaadjes hebben elk op zichzelf een bepaalde status, een bepaalde waarde, maar de bloem ontleent zijn belang aan de samenhang daartussen. Het belang zit in de fase van de informatie – informatie wordt gecreëerd, gebruikt, hergebruikt, bewaard, gearchiveerd en eventueel vernietigd – maar in het digitale tijdperk heeft informatie al die statussen tegelijkertijd. Informatie zit in een database en staat op een fileserver en blijft daar. Iedereen die van die data gebruikmaakt, doet dat met dezelfde data. Als je data creëert, moet je dus ook al weten hoe je daarmee omgaat in de andere fasen: wat wil je archiveren, waarom, hoe ga je dat doen en wanneer wil je de informatie vernietigen? De buitenste blaadjes vertegenwoordigen de waarde van de informatie. Daar gaat het uiteindelijk om. Die waarde moet tegelijkertijd gediend worden. Informatie dient om de bedrijfsvoering te kunnen uitvoeren, om recht- en bewijszoekenden te bedienen, om erfgoed te bewaren en eventueel om historisch onderzoek mogelijk te maken. Ik verwijs naar het voorbeeld van zojuist, de e-mails in het kader van het Srebrenica-onderzoek.
Het thema «kwaliteit van de ICT en databestanden» is een van de thema's in de vragen die vanuit de Eerste Kamer aan ons zijn gesteld. Wij zien dat ICT-projecten in problemen raken doordat de ICT-industrie, de minister en de politiek elkaar in een complexiteitspiraal gevangen houden. Dat hebben wij uitgelegd in ons rapport ICT-projecten. Ik zal dat hier niet herhalen, maar het gevolg daarvan is dat iedere partij een extra laag complexiteit op de projecten doet. De minister kan alleen scoren met een groot project, want dan laat hij grote daden zien. Een ICT-dienstverlener heeft graag grote projecten en de politiek heeft altijd haast. Ja, de politiek heeft altijd haast; dat geldt ook voor de Eerste Kamer.
De kwaliteit van de ICT schiet vaak tekort, omdat vooraf gemaakte bestuurlijke keuzes ontbreken. Het voorbeeld is P-direct, het HRM-systeem van de overheid. Van tevoren konden de ministeries het niet eens worden over wat het systeem allemaal wel of niet moest doen, maar vervolgens is wel een aanbesteding gestart. ICT-bouwers weten dan niet wat zij moeten

bouwen. Uiteindelijk heeft de aannemer die de opdracht gegund had gekregen, de stekker uit het project getrokken, omdat het te ingewikkeld werd.
Het laatste thema is dat de bescherming van burgers in het gedrang komt als projecten in problemen komen. Dat hebben wij gezien bij C2000, de IND en bij het project Toeslagen Belastingdienst.
Ik sta open voor vragen.

Mevrouw **Dupuis** (VVD): Ik dank u voor dit zeer heldere verhaal. Ik wil ook de eerste spreker bedanken. Bij zaken zoals het ekd, het elektronisch kinddossier, dat nu ook op de rol staat, is de vraag natuurlijk ook wanneer het wordt afgesloten, of dat kan en hoe dat gaat. Mij is gezegd dat je, als de informatie langs voldoende knooppunten komt, uiteindelijk niet meer weet waar alles zit en dat het dan werkelijk de vraag is of je een dossier ooit afgesloten kunt krijgen. Is dat nog een punt van aandacht of is het vanzelfsprekend dat dit in orde is en goed zal gaan? Het servicenummer blijft hetzelfde en als je als kind een beetje lastig bent geweest, is het natuurlijk erg bezwaarlijk dat je dat je hele leven met je meesleept. Mijn vraag is dus of er veel problemen zijn bij het afsluiten van dossiers. Of is het niet zo ingewikkeld, als je het maar goed regelt?

De heer **Wijsman**: Dat weet ik niet. Dit antwoord is natuurlijk erg onbevredigend, maar ik herken wel het probleem.

Mevrouw **Duthler** (VVD): Dank voor het zeer heldere overzicht. Ik werd getriggerd door twee dingen. Het eerste is dat er sprake is van drie tekortkomingen: onvoldoende autorisatiebeheer, onvoldoende informatiebeveiliging en onvoldoende functiescheiding. Dat zijn nu juist drie aspecten die betrekking hebben op de privacybescherming. Als de informatiehuishouding niet op orde is, is dus ook de privacybescherming niet op orde. Verder hoorde ik u zeggen dat u niets ziet in een ICT-autoriteit, want ICT is geen oplossing. Dat ben ik volledig met u eens, maar ICT is wel faciliterend voor het op orde krijgen van je informatiehuishouding. Ziet u wel iets in een informatieautoriteit? Dan wordt de toezichthoudende functie verbreed naar kwaliteit van informatie.

De heer **Wijsman**: Ik spreek nu namens mijzelf, want ik geloof niet dat de Rekenkamer hierover een standpunt heeft. Informatie is een onlosmakelijk onderdeel van het bedrijfsproces van elke organisatie en daar moet je de verantwoordelijkheid laten. Ik zie weinig heil in het in het leven roepen van een nieuwe autoriteit. We hebben inmiddels al een privacyautoriteit en daar zou ik eerder aan denken dan aan een nieuwe autoriteit.

Mevrouw **Duthler** (VVD): Natuurlijk blijft de verantwoordelijkheid voor de informatie bij de desbetreffende organisatie zelf, maar we krijgen de ICT-voorziening en de informatiehuishouding bij de overheid maar niet op orde. Ik zit met de grote vraag hoe wij dat wél op orde krijgen. We hebben genoeg toezichthouders – daarover zou ik nog wel even willen doorpraten – en dat ziet u dus niet als een oplossing. Wat ziet u wél als oplossing?

De heer **Wijsman**: Informatieproblemen probeert men op te lossen door zoveel mogelijk gegevens te verzamelen. Dat gebeurde bijvoorbeeld bij het elektronisch kinddossier. Het idee lijkt te zijn: als je maar voldoende gegevens vastlegt van een individu of cliënt, kom je min of meer vanzelfsprekend tot een goede behandeling.

Mevrouw **Slagter-Roukema** (SP): Voorzitter. Ik wil eerst iets zeggen over de ICT-autoriteit. Ik meen dat wij niet moeten vasthouden aan een bepaalde naam, maar dat het meer gaat om de functie. Het Rathenau

Instituut heeft benadrukt dat het belangrijk zou zijn om van te voren te bekijken wat het doel is en of de beoogde middelen wel correct zijn. Dan kun je nog kijken of dit ergens anders moet worden belegd, maar het gaat meer om het idee. Het lijkt mij niet goed om de term als zodanig te veroordelen; het zou beter zijn om te kijken wat de bedoeling erachter is. Dit ter aanvulling.
De vragen van mevrouw Duthler hadden ook betrekking op de informatievoorziening van de overheid. Ik meen dat wij ook nog wat breder kijken naar ICT-projecten die door de overheid worden opgezet. Informatievoorziening is voor mij meer hoe de overheid met de burger communiceert. Een voorbeeld is de Wabo waarover digitale informatie beschikbaar zou moeten zijn. Overigens wordt over dit project ook al gemeld dat het digitaliseren lang niet zo goed loopt als gewenst of verwacht werd.
Op sheet 7 staat dat ICT-projecten in problemen komen door een complexiteitsspiraal, een mooi woord trouwens. Het valt mij op dat er niet wordt gesproken over de gebruikers. Voor mijn gevoel is een van de oorzaken voor het fout gaan van projecten dat in de ICT-industrie minister en Kamers met elkaar een spiraal veroorzaken en dat de gebruiker vervolgens zegt: hier zat ik niet op te wachten. Daarop zou een ICT-autoriteit dan kunnen toezien. Is de heer Wijsman dat met mij eens? Volgens mij houdt de Rekenkamer toezicht op de financiën van dit soort projecten. Als de Rekenkamer projecten in ogenschouw neemt, kijkt zij dan alleen naar hetgeen door de beleidsmakers en het ministerie is geëntameerd, of bekijkt zij ook welke kosten zo'n project eventueel voor de gebruikers teweegbrengt? Wordt naast bureaucratie, extra handelingen en dat soort dingen ook naar investeringen in hardware en software, cursussen, enzovoorts gekeken?

De **voorzitter**: Er zijn twee vragen gesteld en ik vraag de heer Wijsman die in twee minuten te beantwoorden.

De heer **Wijsman**: Twee minuten per vraag? Mijn tijd gaat nu in? Ik begrijp het.
Mevrouw Slagter sprak over te weinig aandacht voor gebruikers. Wij hebben in ons rapport over grote ICT-projecten gesteld dat er veel lijsten zijn van oorzaken waardoor ICT-projecten in de problemen komen. Als je al die lijsten afwerkt, zou je min of meer automatisch tot een geslaagd project komen. Wij hebben gezegd: dat is een aanpak van Handboek Soldaat. Dat werkt niet, want onder de problemen aan de oppervlakte waarop al die aanwijzingen uit het handboek zijn gericht zoals «betrek de gebruikers erbij» liggen andere problemen. Die hebben wij benoemd in de complexiteitsspiraal. Wat ons betreft is dat de onderliggende oorzaak waardoor projecten met een belangrijke ICT-component, sommige mensen noemen dat ICT-projecten, problemen oplopen in die zin dat ze over tijd zijn, dat ze te veel geld kosten en uiteindelijk niet doen wat ze moeten doen.
Ik ben het met mevrouw Slagter eens dat aandacht voor gebruikers cruciaal is. Die schiet er nog al eens bij in, maar dat is naar onze mening niet het onderliggende probleem waardoor ICT-projecten in moeilijkheden komen.
Mevrouw Slagter vroeg verder of wij alleen naar financiën kijken. Wij kijken niet alleen naar financiën. Sterker nog: wij zijn niet structureel gericht op ICT-projecten of andere projecten van de overheid. Wij besteden hieraan alleen aandacht als daar redenen toe zijn, bijvoorbeeld omdat het voortvloeit uit onze strategie. Wij kijken verder niet alleen naar de financiën, maar ook, om niet te zeggen vaak, naar wat systemen precies doen en of die systemen slim in elkaar steken.
Voorzitter, ben ik daarmee binnen de tijd gebleven?

De **voorzitter**: Volgens mij hebt u het uitstekend gedaan. Dank u wel voor uw bijdrage, mijnheer Wijsman.
Voordat ik de heer Kohnstamm het woord geef, deel ik mijn collega's mee dat ik hen ga rantsoeneren. Vanaf nu sta ik nog maar één vraag toe en die moet bovendien kort worden ingeleid.

De heer **Kohnstamm**: Voorzitter. Dank voor de uitnodiging om hier mee te denken en te spreken over privacy.
Het is spannend dat de Eerste Kamer vandaag hierover spreekt, want deze dagen staan toch vooral de provinciale programma's centraal in de aandacht van de Eerste Kamerleden. Hoe het ook zij, het is hartstikke goed om meer in het algemeen over privacy na te denken.
Ik wil het over de wetgeving hebben. Schuivende panelen in de wetgeving rond privacy zijn aan de orde van de dag. Ik noem de evaluatie van de Wet bescherming persoonsgegevens en het Brouwer-Korf-wetsvoorstel van het kabinet, een wetsvoorstel dat rond de zomer wordt verwacht. Hetzelfde gebeurt in Europa, zie de herziening van de privacyrichtlijn die voor deze zomer is voorzien. Verder worden de guidelines van de OECD herzien en wordt conventie 108 van het Verdrag van de Raad van Europa tegen het licht gehouden. Aan de andere zijde van de oceaan wordt overigens ook behoorlijk intensief nagedacht over privacy. Zo is de Federal Trade Commission met een stuk gekomen met de naam «Rethinking privacy and cloud computing» en het department of Commerce met zijn – ik hoop dat ik het goed zeg – «yellow papers». Dat zijn allemaal buitengewoon interessante stukken, waardoor het denken over privacy weer hoog op de agenda is komen te staan. Overigens is het voor mij persoonlijk erg spannend om in deze periode de positie van voorzitter van de European Data Protection Supervisor te mogen bekleden, omdat er heel veel aan het bewegen is.
Met die dubbele pet op wil ik een paar hartenkreten slaken over het onderwerp dat mij is toebedeeld: nationale ontwikkelingen wat betreft het gebruik van persoonsgegevens en de privacy van burgers. Ik doe dat tegen de achtergrond, een punt dat tot nu toe niet naar voren is gebracht, van de zegenrijke ontwikkelingen in de informatietechnologie. Informatietechnologie is vaak buitengewoon nuttig en functioneel! Er zitten natuurlijk problematische kanten aan, maar wij moeten zeker niet alleen daarnaar kijken. Verder wil ik ingaan op de hieruit voortvloeiende globalisering van gegevensstromen in publieke én private sectoren. Mijn verhaaltje slaat dus nadrukkelijk niet alleen op de publieke sector.
Naast wet- en regelgeving zijn er voor de privacypraktijk drie spelers van groot belang. Dat zijn ten eerste de burgers. Ik vind het overigens nog steeds gek dat wij geen Nederlands woord hebben voor wat in het Engels «data subjects» wordt genoemd. Ten tweede zijn dat de verantwoordelijken, zowel publiek als privaat georganiseerd, en ten derde de toezichthouders. Ik begin met de burgers.
In onze westerse opvattingen over recht en rechtvaardigheid is de rol van het individu, van de burger van groot belang, zo niet bepalend. Het is dus politiek correct om in te zetten op elementen in onze wetgeving die de positie van de burger versterken. In het jargon: transparantie, toestemming, informed consent, recht op inzage, correctie en verzet, inclusief gezamenlijk optreden in rechte van consumer collective redress.
Er doen zich bij de rechten van burgers bijna altijd twee problemen voor. Ten eerste is de schade veelal niet materieel. Als je thuis een advertentie toegestuurd krijgt omdat je op de een of andere manier gestempeld bent als iemand die dat soort advertenties wil hebben, voel je je ongemakkelijk. Misschien voel je je wel bespied, maar je kunt niet zeggen: het kost een ton. Die schade is immaterieel.
Ten tweede is er de omvang. Ik neem aan dat in deze zaal vooral maatschappelijke actieve mensen zitten. Ik kan hen dan zeggen dat zij in ten minste 1500 databases zijn opgenomen. Dat is niet te overzien. Ik heb

nu ground computing erbij betrokken als technologische uitwerking van het geheel. Ik wist niet dat er hier zo'n mooie beamer stond want anders had ik een sheet gemaakt; ik geef de informatie nu op papier. Dit is wat bij behavioral advertising allemaal aan de orde is. Als je dan moet proberen te overzien wat er gebeurt als je je toestemming verleent, dan is het echt volstrekt ondenkbaar dat je daar echt volledig inzicht in hebt. Zelfs als de positie van de burger beter wettelijk wordt verankerd, waarvan ik overigens een groot voorstander ben, is het effect daarvan op de bescherming van persoonsgegevens in de praktijk klein; ik zal niet zeggen «verwaarloosbaar», maar hiermee zou niet meer dan 10% van de cake worden geraakt. Er moet veel verder worden gekeken. Voor de verbetering van de bescherming van persoonsgegevens van en voor burgers is het nodig dat de aandacht bijna volledig uitgaat naar de twee andere spelers in het veld: de verantwoordelijke en de toezichthouder.
De toezichthouder is verantwoordelijk in publieke en private sfeer. Bovenaan mijn verlanglijstje staan dan, voor nieuwe elementen in komende wet- en regelgeving: privacy by design en privacy impact assessment. Aan de basisnormen, neergelegd in de huidige privacywetgeving, zou mijns inziens, om dat in het correcte politieke jargon te zeggen, niet moeten worden getornd. Stel eerst de noodzaak vast – proportionaliteit, subsidiariteit – waarbij dataminimalisatie, doelbinding, beveiliging en transparantie de elementen zijn die daarvoor gelden. De abstracte, maar soms ook heel concreet te maken heipalen onder de bescherming van persoonsgegevens zullen echter steeds door organisaties die nieuwe producten, diensten en wetgeving ontwikkelen aantoonbaar tegen het licht moeten worden gehouden. Privacy impact assessment: al dan niet wettelijk verplicht, opdat bij de ontwikkeling van nieuwe producten, diensten of wetgeving de risico's rond de bescherming persoonsgegevens misschien kort maar wel indringend, en zo openbaar mogelijk, op het netvlies komen te staan. Privacy by design: op de tekentafel van de nieuwe producten, diensten en wetgeving, in de architectuur ervan, al elementen inbouwen waardoor privacy effectiever beschermd kan worden.
Een beetje een losse gedachte, die eerder al een beetje aan de orde kwam in de discussie, is: laat de verantwoordelijke echt verantwoordelijke zijn. Ik kom na de pauze in de vraagstelling nog terug op de reden dat ik echt heel erg twijfel aan de IT-autoriteit. Laat de verantwoordelijke in vredesnaam verantwoordelijk zijn, in zijn geheel, en aanspreekbaar. Het is toch typisch dat de autofabrikant aansprakelijk is voor fouten in verkochte auto's en die allemaal moet terughalen, maar in de privacysfeer nauwelijks een vergelijkbare «productaansprakelijkheid» in de praktijk tot stand komt? Bij organisaties in publieke of private sfeer voor de effectieve bescherming van persoonsgegevens in de op de markt gezette producten en diensten waarbij persoonsgegevens worden verzameld en verwerkt, zou in die richting, net als bij autofabrikanten, kunnen en moeten worden nagedacht. Uit die discussie in de Verenigde Staten en de APAC-landen is het begrip «accountability» overgewaaid; als verantwoordelijke desgevraagd kunnen aantonen dat je ten minste stil hebt gestaan bij de noodzaak om persoonsgegevens te beschermen en dat je je bij de ontwikkeling van je product, dienst of wetgeving daarvan ook iets hebt aangetrokken. Dat is de essentie van mijn pleidooi wat het de verantwoordelijken betreft.
Ik kom nu te spreken over de toezichthouder. Ik kom daarop na de pauze nog een keertje terug omdat daarover een paar vragen bestaan. Voor dit moment zeg ik het volgende. Als de pakkans niet groter wordt, als de sanctie niet afschrikwekkend wordt, als er geen sterke positie komt van toezichthouders in het geval van grensoverschrijdend gegevensverkeer en als er geen verplichting komt om openbaar te rapporteren over alle bevindingen, dan kan de toezichthouder naar mijn privéoordeel beter worden opgeheven. Doe mij een leeuw en noem hem dan toezichthouder.

Doe mij niet een lam als je hem toezichthouder wilt noemen. Als ik op de autosnelweg van de bescherming persoonsgegevens, zeg de A4, iemand aantref die daar starnakelbezopen met 180 km/u rijdt, kan ik de bestuurder van die auto een last onder dwangsom opleggen. Dat wil zeggen hem dreigend aankijken en zeggen: mijnheertje, wilt u zo vriendelijk zijn om daarmee op te houden, want de volgende keer bent u er gloeiend bij. Voor een goede en welwillende verantwoordelijke die even de weg kwijt is, is dat de beste methode. Maar voor degene die denkt: het zal mij een rotzorg zijn, de pakkans is gering en als ik er gloeiend op kom te staan, is het enige wat de toezichthouder als het ware kan doen, vragen: heer Bommel, wat is uw naam? Als rupsje-nooit-genoeg: geef de toezichthouder meer budget en betere bevoegdheden, verplicht hem onder omstandigheden tot materiële en formele samenwerking met collega-toezichthouders over de grens en verplicht hem tot het openbaar maken van zijn bevindingen. Het is toch te gek voor woorden dat wij over de openbaarmaking van onze bevindingen met betrekking tot de beveiliging van IT-systemen in ziekenhuizen hebben moeten procederen. Dat is net zo gek als ik het vind dat wij een arbobedrijf dat een bij hen aangesloten werkgever de inlogcode gaf van het medische dossier van de zieke werknemer, niet direct een Neelie Kroes-achtige boete hebben mogen geven.
Voorzitter. Ik laat het hier even bij. Dank voor uw aandacht.

Mevrouw **Strik** (GroenLinks): Het is lastig, want je weet niet wat er nog allemaal komt. Maar goed, ik zet mijn kaart nu in. De heer Kohnstamm had het over al dan niet verplichte privacy impact assessments. Dat triggerde mij natuurlijk meteen om de volgende vraag te stellen. Vindt de heer Kohnstamm dat ze verplicht moeten zijn? Hij hield ook een slag om de arm wat de openbaarmaking betreft. Hij zei: voor zover mogelijk moet dat openbaar zijn. Moeten ze niet sowieso openbaar zijn zodat mensen ook kunnen weten wat het assessment heeft opgeleverd? Als het «zover mogelijk» is, waar liggen dan voor de heer Kohnstamm de grenzen of mogelijke criteria?

De heer **Kohnstamm**: Ik vind in ieder geval dat een PIA voor alle overheidsactiviteiten verplicht moet worden gesteld en openbaar moet zijn. Ik houd een slag om de arm omdat je soms bij het ontwikkelen van een product ... Google en Microsoft zijn concurrenten. Dan kun je de PIA niet zo maar openbaar maken. Het moet dan wel zo zijn dat te eniger tijd, op het moment dat er problemen zijn, de desbetreffende industrie kan aantonen dat zij een PIA heeft gedaan. Ik vind overigens dat dit in de laatste fase, waar de toezichthouder in beeld komt, een rol zou kunnen spelen. Stel dat iemand die een product heeft ontwikkeld in de private sector, met een probleem komt te zitten en vervolgens aantoont dat hij echt alles heeft gedaan maar dat er ergens iets onhandigs is gebeurd. De boete is dan een heel andere dan als hij dat niet heeft gedaan. Mijn slag om de arm zat hem in het verschil tussen privaat en publiek. Ik vind dat de wetgever bij alle grote overheidsactiviteiten waaraan wetgeving ten grondslag ligt, maar ook waar dat niet het geval is, met een privacy impact assessment zou moeten werken. Als het overheid is, hebben de provinciale staten, de gemeenteraad, het waterschap, de Eerste Kamer of de Tweede Kamer de mogelijkheid om dat buitengewoon serieus te bekijken. Heb je checks and balances, dan rest de politieke besluit-vorming.

De heer **Franken** (CDA): De heer Kohnstamm wil graag een sanctie opleggen die ertoe doet. Hij denkt zelfs aan Neelie Kroes-achtige boetes. Denkt hij dat het dan niet veel beter is dat een rechter zoiets doet, zodat het de bevoegdheid van het CPB zal worden om zaken bij de rechter te kunnen aanbrengen? Dan is hij, denk ik, getrapt maar effectief bezig.

De heer **Kohnstamm**: Ik begrijp de vraag heel goed. Het is echter niet per se nodig om het bij de rechter neer te leggen. In een aantal van de ons omringende landen hebben mijn collega's wel degelijk die bevoegdheid gekregen. Ik ben met name vreselijk jaloers op mijn Engelse collega omdat daar heel veel datalekken hebben plaatsgevonden. Ik zou wensen dat dit in Nederland wat meer gebeurde, want dan krijg je dat soort bevoegdheden snel toegespeeld. Hij heeft nu de behoorlijke bevoegdheid om een boete op te leggen. Hij heeft zelfs de mogelijkheid, er indirect voor te zorgen dat iemand gevangenisstraf krijgt. Daar ben ik zelf niet erg voor, maar een boetebevoegdheid wel. Je hebt immers een toezichthouder of je hebt hem niet. Een toezichthouder moet tanden hebben om te kunnen laten zien. Als hij die niet heeft, kan hij nog zo hard en goed zijn best doen, communicatief bezig zijn en weet ik veel wat, maar uiteindelijk is de naleving van wettelijke verplichtingen zeer afhankelijk van de mate waarin iemand op een gegeven moment zegt: zo kan het niet, betalen maar! Ik sprak Neelie Kroes vorige week juist nog over datalekken en dergelijke aangelegenheden. Toen dacht ik: zo iemand is ver gekomen. Toen ik haar mijn verhaal deed, begreep ze heel goed wat ik bedoelde. Ze vond het verstandig wat ik zei.

Mevrouw **Slagter-Roukema** (SP): Ik moet een heel kleine inleiding houden, ondanks het verzoek van de voorzitter, dat niet te doen. Het valt mij op dat de heer Kohnstamm zei dat het voor de gewone burger niet te overzien was, omdat hij – ikzelf kennelijk ook – in 1500 databases zit. Ik vind dat een doodeng idee. Het moet dus naar een ander plan. Ik vraag mij alleen af of er iemand is die het wel kan overzien en of degene die het moet overzien, dat ook kan.
De heer Kohnstamm zei verder: laat de verantwoordelijke verantwoordelijk zijn. Dat klonk erg mooi, maar ik denk dat het vaak niet eens duidelijk is wie er verantwoordelijk is en dat er vaak meerdere verantwoordelijken zijn, waardoor hete aardappels toch weer worden doorgeschoven. Of dat het nu allemaal oplost of dat het gewoon een loze kreet is, daar twijfel ik over.

De heer **Kohnstamm**: Dan ga ik die twijfel gauw wegnemen, althans dat pogen. De vraag is zeker wanneer wie verantwoordelijk is, al is deze abstracte vraag in bijna 999 van de 1 000 gevallen volstrekt helder te beantwoorden. Dan blijft er nog altijd de bewerker en de verantwoordelijke, maar die discussie hoeven we hier nu denk ik niet te voeren. In het merendeel van de gevallen, zeker de gevallen waarin het de overheid betreft, is het volstrekt helder wie de verantwoordelijke is, alhoewel ik u moet zeggen dat we nu in een zaak over de koppeling van SIOD-gegevens verwikkeld zijn, waarin de stelling werd betrokken dat de minister of staatssecretaris uiteindelijk niet verantwoordelijk was. Daarover was ik verbaasd, want ik ben tot drie of vier keer toe bij de opeenvolgende staatssecretarissen en ministers geweest die mij hebben aangesproken over dat punt. Er zit dus ook daar een lijn dat je soms politiek verantwoordelijk bent, maar hoopt dat je dat Wbp-technisch niet bent. Daar stink ik niet in.
Over de burger en het overzicht merk ik het volgende op. We hebben onderzoek laten doen naar de vraag in hoeveel databases mensen zitten. De uitkomst daarvan was wel komisch in de zin dat iemand die zich echt geheel terugtrekt in een holletje, zo dat ergens mogelijk is in Nederland, toch nog altijd in 250 databases in Nederland zit. Maatschappelijk actieven komen in 1 000, 1 500 of zelfs meer databases voor. Ja, dat houd je natuurlijk niet meer in de gaten. Dat kan ook niet. Daarom vind ik dat er openbaarheid moet zijn. Diegenen die informatie willen, inzicht willen omwille van een al dan niet toegestane rectificatie of zelfs verwijdering willen, moeten daartoe de mogelijkheid hebben. Ik ben erg voor collectieve acties op dat terrein, omdat je het anders niet redden gaat en omdat

het handzamer is voor een individu om hierover via de Consumentenbond of anderszins procedures te starten, alhoewel er in de Wbp een makkelijkere procedure is voorzien. De reden is dat een individu, zoals gezegd, over het algemeen niet in een materieel, maar in een immaterieel probleem terechtkomt. Dan nog ben je er niet. Mijn stelling is dus niet dat je het niet moet doen, want je moet het absoluut wel doen – je kunt het rechtstheoretisch ook niet anders willen – maar dat je moet weten dat je, als je het heel goed doet, 10% van de taart hebt gedekt. De overige 90% komt echt door die andere twee rollen: de verantwoordelijke en de toezichthouder, uiteraard ook voor een deel van de wetgever.

De **voorzitter**: Mag ik persoonlijk een vraag stellen over de verantwoordelijkheid? U stelt voor, de verantwoordelijkheid bij de verantwoordelijken te laten en het niet te zoeken in een nieuwe autoriteit, maar wel te zoeken naar een zekere mate van bescherming in de privacy impact assessment. Wie gaat dat dan doen? Die verantwoordelijke? Moet die dat uitbesteden? Als ik naar de overheid en naar een wetsvoorstel over de jeugdzorg, dat hier voorlag, kijk, verwacht u dan dat de minister zijn ambtelijke apparaat georganiseerde impact assessments laat doen of moeten die van buiten komen? Hoe moeten we ons dat voorstellen?

De heer **Kohnstamm**: Ik zou altijd adviseren om dat van buiten te laten komen, checks and balances inbouwen in de totstandkoming van product, dienst of wetgeving. Dat is geen wet van Meden en Perzen. Van het privacy impact assessment is het wel geestig dat dit in Europa – de heer Hustinx weet daar ongetwijfeld meer van – gebruikelijker is dan in het Nederlandse systeem. In een aantal APAC-landen is het een verplichting om zo'n privacy impact assessment te maken. Daarmee is veel meer ervaring opgedaan. Het is interessant om te zien hoe dat dan vervolgens uitpakt. Van grote technologische projecten is het vervelend dat zij altijd heel veel meer kosten, dat het veel langer duurt voordat zij er zijn en dat zij nog niet de helft kunnen van wat zij oorspronkelijk gepland waren te doen. Count your losses, zou ik zeggen, maar probeer er in ieder geval voor te zorgen dat ten aanzien van de bescherming van persoonsgegevens een aantal risico's vooraf heel zichtbaar is gemaakt en op het netvlies staat voordat je doorakkert in de richting van grote operaties zoals wij die gezien hebben.
Ik ben het zeer eens met de heer Munnichs, los van de vraag of je voor rekeningrijden – ik moet dan politiek correct zeggen: anders betalen voor mobiliteit – bent of niet. De twee mogelijkheden daarbij waren zeer zichtbaar aanwezig: het dikke kastje en het dunne kastje. Zij zijn van meet af aan ook meegenomen, overigens in politieke zin. Zo heeft ook de minister mij destijds gezegd, omdat hij zag dat dat project alleen maar succesvol zou zijn als het privacyvriendelijk zou zijn, omdat het publiek het anders niet zou pikken, de ANWB in het bijzonder. Dan zie je dat daar een soort checks and balances ontstaan, waarbij de minister, of het ministerie, ervoor heeft gekozen om dit heel goed, ook extern, mee in ontwikkeling te geven. Ik vind het feit dat het gebeurt belangrijker. Ik zou denken: laat het altijd onafhankelijk gebeuren, dat is net iets beter dan het in eigen beheer te doen.

De **voorzitter**: Dank u zeer. Dan komen wij toe aan Europa. De heer Hustinx heeft het woord.

De heer **Hustinx**: Voorzitter. Laat ik beginnen met te zeggen dat mijn functie in Brussel ook een Nederlandse vertaling heeft. Het gaat dan om de Europese toezichthouder bescherming persoonsgegevens, die een toezichthoudende taak heeft als het gaat om de Europese instellingen en organen, toezicht op en handhaving van de Commissiebevoegdheden, die ver reiken; een adviserende taak met betrekking tot Commissie, Raad en

Parlement als het gaat om nieuwe wetgeving en beleid; een lijntje met het Europese hof, met soms een adviserende taak, en een samenwerkende rol met collega's, onder meer in de 29-groep waarnaar Jacob Kohnstamm zo-even verwees. Dit noem ik even als achtergrond.
Als het gaat om Europese politieke ontwikkelingen is het misschien juist om te zeggen dat de relevantie van privacy en de bescherming van persoonsgegevens nooit groter is geweest dan juist nu. Daar zijn twee heel duidelijke achtergrondverklaringen voor. De eerste is kort aan te duiden met de impact van het Verdrag van Lissabon. Dat valt in een paar stukjes uiteen, maar een onderdeel van het Verdrag van Lissabon, dat in werking trad in december 2009, is dat het handvest van de grondrechten bindend is geworden. Een van de nieuwe elementen is de uitdrukkelijke erkenning van het recht op de bescherming van persoonsgegevens naast het recht op privacy. Ik kom daar nog op terug.
Dat is vervolgens ook in de verdragen zelf, waaronder het verdrag over de werking van de Europese Unie, nogal stevig neergezet. In artikel 16 bij de algemene beginselen van de Europese Unie is de bescherming van persoonsgegevens nogmaals neergezet, met een algemene, horizontale juridische basis, waar regels kunnen worden gesteld over de werking van persoonsgegevens. Er staat niet «richtlijnen» of «verordening», maar «regels». Er is dus een multifunctionele basis, die Uniebreed alle terreinen bestrijkt. Daarbij zijn de taken in het Lissabonverdrag opnieuw verdeeld. Op een aantal punten is het Parlement daarbij de winnaar, ook op terreinen waar het Parlement tot dusver niet aan kon tippen, anders dan misschien als adviseur. Met name op het terrein van politie en justitie is het Parlement meer betrokken. Daar komt nog bij – ik heb het nog steeds over de impact van Lissabon – dat er een nieuwe Commissie is aangetreden, waarin een commissaris op aandringen van het Parlement werd belast met een grondrechtenportefeuille. Deze portefeuille werd gecombineerd met de justitieportefeuille. De zeer ervaren Viviane Reding is nu de commissaris die zich met Justitie, Grondrechten en Burgerrechten bezighoudt. In het Engels heet haar portefeuille Fundamental rights and citizenship. Tijdens haar selectiehoorzittingen heeft EU-commissaris Reding gezegd dat het tijd wordt dat we de veiligheid niet voortdurend laten voorgaan op de gerechtigheid. Zij heeft gezegd dat zij meer gerechtigheid gaat leveren voor een betere balans. Zij heeft ook gezegd dat haar hoofdprioriteit de dataprotectie wordt. Dit is een heel duidelijke lijn, waardoor er rond dit onderwerp een dynamisering gaande is.
Dit onderwerp is verre van marginaal, maar juist heel zichtbaar aanwezig in heel wat dossiers. De naam van Neelie Kroes viel zojuist al een paar keer. Zij is verantwoordelijk voor de digitale agenda. Dit betekent dat alles met een «e» ervoor – e-health, e-government, e-security, e-finance en e-commerce – allemaal niet denkbaar is zonder dat je heel stevig investeert in veiligheid, vertrouwen, privacy en transparantie. Dit staat centraal in de agenda van Neelie Kroes. De herziening van het dataprotectierecht heeft repercussies op allerlei beleidsterreinen. Als het gaat om economic recovery, begrijpt iedereen dat je moet investeren in een digitale agenda. Dit heeft weer te maken met privacy.
Ik zal het op een andere manier illustreren. Toen het Verdrag van Lissabon in werking trad, hebben de staatshoofden en regeringsleiders die van de Europese Raad het Stockholmprogramma aangenomen. Dat is ongetwijfeld ter sprake geweest in de commissies en in de plenaire vergadering van de Eerste Kamer. In het Stockholmprogramma kun je op allerlei niveaus de neerslag van de impact van de grondrechten tegenkomen. Met name dataprotectie is daarin opgenomen. Dit is het geval bij de sturende beginselen, maar ook bij de uitwerking. Huiselijk staat er: wij gaan geen nieuwe systemen bouwen zonder dat deze onderworpen zijn aan een heel kritische analyse van de businesscase en het doel. We zorgen ervoor dat dataprotectie daarbij is ingebouwd. Ik moet zeggen dat de praktijk altijd lastiger is dan de leer. Op dit moment zijn we bezig om

dit in onze discussie stapje voor stapje te realiseren. Dit verklaart waarom het samen zo relevant is.
In de geschiedenis is een duidelijke grondslag zichtbaar in de ontwikkelingen. In artikel 8 van het EVRM is het recht op privacy beschreven. Dit recht is er al vijftig tot zestig jaar. In de vorige eeuw is in de loop van de jaren – dit gebeurde vooral in de jaren zeventig en tachtig – het dataprotectierecht daaromheen gegroeid, als een structurele benadering van een aantal problemen van een informatiemaatschappij, die met privacy en met allerlei andere zaken samenhangen. Er is een relatie gezien met antidiscriminatie, met fair play en met transparantie. Daarom zijn in het handvest van de Europese grondrechten dataprotectie en privacy naast elkaar gezet. Ik vind dit een heel gunstig onderscheid. Het is een erkenning van de structurele betekenis van de beginselen van gegevensbescherming, die nu in allerlei fasen terugkomen. Naarmate dit relevanter werd voor de interne markt, is de Unie, toen de EG, zich ermee gaan bemoeien, om dit te harmoniseren. De nationale wetgeving is geharmoniseerd in richtlijn 95/46. Maar sindsdien is daar een en ander omheen gebouwd. Een aantal richtlijnen spitst zich toe op bijzondere terreinen, telecommunicatie is er een van, maar niet het enige. Er is veel recenter, in 2008, een kaderbesluit inzake justitiële en politiële samenwerking bijgekomen. Er zijn ook componenten die alleen op Unie-niveau spelen. Dat hele pakket is op dat moment onderdeel van de review. Deze zomer verwacht ik de eerste voorstellen.
Een van de drivers voor dat herzieningsproject is dus in de eerste plaats dat het centrale stuk van het hele pakket inmiddels al wat gedateerd is. In 1995 was internet nauwelijks zichtbaar. Er is dus evident behoefte aan onderhoud. Vervolgens noem ik de dynamisering die uitgaat van de impact van Lissabon, waarmee wij ongetwijfeld een verbreding zullen zien, niet van de interne markt maar over de volledige breedte van het Unie-beleid. Het zal een geweldige strijd zijn of politie en justitie in hetzelfde document terechtkomen of toch niet. Dat is een belangrijke testcase, maar ik verwacht toch dat het pakket in codetaal «comprehensive» zal zijn. De derde driver is de interface met al die belangrijke onderwerpen, kort gezegd de digitale agenda. Er is een vierde driver, minder zichtbaar, maar toch heel voelbaar, namelijk de onderhandelingen met de Verenigde Staten over het transatlantisch kader. Er zijn de afgelopen jaren wat ongelukken gebeurd, PNR and SWIFT, maar er wordt geprobeerd om een grotere consistentie te bereiken. Dat is belangrijk omdat de grote providers op dit terrein in de Verenigde Staten zijn gevestigd.
Als ik een heel korte blik mag slaan op de jurisprudentie, dan zijn er twee plaatsen om in de gaten te houden, te weten Straatsburg en Luxemburg, in Europees-rechtelijke zin evident. Wat Straatsburg betreft, is er rond artikel 8 gaandeweg steeds meer jurisprudentie gegroeid. Dat heeft ertoe geleid dat de interpretatie van de reikwijdte van wat privésfeer is, persoonlijke levenssfeer, gaandeweg breder is geworden. Het Hof heeft een paar keer gezegd dat er geen principiële reden is waarom het beroepsleven niet ook privacyvragen zou opleveren, dus privacy op de werkplek en zelfs privacy in het openbaar: camera's, demonstraties, waarbij je die interface ziet. Dat is allang geen typisch klassieke privacy meer. Verder heeft dat ertoe geleid dat in een aantal arresten ook een horizontale werking is erkend. Een interessant arrest, ook wat het patiëntendossier betreft, is de Finse zaak in 2007/2008 waarin de aansprakelijkheid van een ziekenhuis over de beveiliging van zijn informatiesystemen is vertaald in de aansprakelijkheid van een land om ervoor te zorgen dat de beveiliging van zijn medische informatiesystemen voldoende in orde is. Natuurlijk is er op het punt van proportionaliteit en wettelijke grondslag het nodige. De Marper-zaak over DNA databases is het meest recent, maar zo zijn er meer. In toenemende mate is het Hof in Straatsburg ook geneigd om naar Verdrag 108 te kijken, als het ware als

inspiratiebron voor de betekenis van artikel 8 EVRM. Ik zal niet zeggen dat ze elkaar volledig overlappen, dat nog niet.
Wat Luxemburg betreft, was het eerste arrest over de dataprotectierichtlijn in 2003 een heel interessante zaak: Rechnungshof/Österreichischen Rundfunk, waarin het Hof ook meteen heeft uitgelegd hoe de twee grondrechten op elkaar inwerken. Men ging er, kort gezegd, van uit dat de richtlijn ook van toepassing was op vragen die zich in de publieke sector van één land voordeden, in dit geval Oostenrijk. Vervolgens is men gaan kijken naar artikel 8 EVRM om te zien of die nationale maatregel wel aan de klassieke eisen van rechtmatigheid voldeed. Zo ja, dan kwam je weer aan de volgende vragen van het dataprotectierecht toe.
Na het arrest van 2003 is er een langzaam toenemende stroom van zaken, niet alleen bij het Hof van Justitie, maar ook bij de gerechten van eerste aanleg en het ambtenarengerecht, die inmiddels andere namen hebben gekregen.
Ik wil afsluiten door in aanvulling op wat Jacob Kohnstamm al gezegd heeft, iets te zeggen over wat er op ons afkomt. Dit is niet de tijd om te denken dat dataprotectierecht opnieuw wordt uitgevonden. In deze hele geschiedenis is dat volstrekt niet aan de orde, ook al omdat het handvest van de grondrechten in een aantal details treedt waarin de kenmerkende onderdelen van de richtlijn nu als het ware grondrechtelijk zijn vastgeklonken. Toestemming of een andere wettelijke basis, gebruik voor een gericht doel, recht op inzage, correctie, verzet en onafhankelijk toezicht zijn allemaal grondrechtelijk vastgeklonken.
Wat wij wel gaan krijgen, is een veel grotere nadruk op de effectiviteit van de waarborgen in de praktijk. Hoe gaat dit doorwerken? Dat klinkt door de opmerkingen van de voorganger heel helder heen. Het is tijd om over te schakelen naar de echte wereld. De parallel met de autofabrikant was heel erg veelzeggend. Vroeger werden auto's een voor een gekeurd voordat er een kenteken voor werd gegeven. Dat is al lang niet meer zo. Productieprocessen worden getest en de verantwoordelijkheid van de autoproducent is glashelder. Ik denk dat wij die verantwoordelijkheid, wat de consequenties zijn van verantwoordelijk zijn voor informatie-infrastructuur, verhelderd gaan krijgen.
Dit leidt zonder twijfel tot de verplichting om maatregelen te nemen die ertoe leiden dat de privacy vanaf het eerste begin van een ontwikkelingsproject moet worden meegenomen. Daar spreken wij nu over als privacy by design. Privacy impact assessments zijn legendarisch om verantwoording af te leggen over de regelmatige voorbereiding. Ik zou er ook erg voor zijn – daarin ben ik het eens met Jacob Kohnstamm – om dat publiekelijk te doen. In de Verenigde Staten is dat vast gebruik. Daarop wordt door het publiek, net als bij bestemmingsplannen, ingestoken. Natuurlijk is men het niet allemaal eens, maar dat leidt in ieder geval tot een controleerbaar proces.
Consequenties zijn ook dat toezichthouders stevige bevoegdheden moeten krijgen. Ik verwacht dat dit in de herziening tot grotere harmonisatie gaat leiden, niet alleen wat betreft de positie maar ook zeker wat betreft de bevoegdheden, handhavingsbevoegdheden en duidelijke enforcementtaken.
Ik verwacht ook wel dat de positie van de betrokkenen, de geregistreerden, de datasubjects, de burgers, wordt aangescherpt met een aantal mogelijkheden waarover een discussie is. Op dit moment is dat de zogenaamde dataportability en the right to be forgotten, het recht om vergeten te worden. Sorry, maar het is nu alleen maar in het Engels beschikbaar. Dat instrument zal, denk ik, vooral online toegepast gaan worden. Het zou bij uitstek gericht zijn op sociale netwerken. Het is dan zoals bij de telefoon, als je besluit een andere provider te nemen en het nummer mee te nemen. Vivian Reding stelt zich voor – ik verwacht dat zij met dat voorstel komt – dat je tegen een netwerkbeheerder kunt zeggen dat je naar een ander gaat en dat je al je gegevens meeneemt, dat je kunt

zeggen dat je al je gegevens, of er nu een businesscase aan vast zit of niet, gedeletet wil hebben en ergens anders heen wilt brengen.
Dat kun je in de overheidssfeer natuurlijk niet zo goed denken. Er komen evidente bezwaren als je bij de Belastingdienst of de politie met dat verzoek komt. Het leidt echter wel tot een veel dynamischer maken van de discussie en tot een creatieve aanpak, waarbij ik meer effectieve bescherming verwacht.

Mevrouw **Duthler** (VVD): Veel dank voor dit heldere overzicht. Het recht om vergeten te worden; is dat nog mogelijk in deze tijd met social media en internet? Je gegevens zijn toch bijna niet meer te wissen? Ik zou niet weten hoe ik als burger dat zou moeten doen. Gegevens blijven volgens mij altijd zichtbaar en altijd terug te vinden. Hoe zouden wij dat moeten effectueren?

De heer **Hustinx**: In de discussie is dit een enorme aanjager geweest. Reding weet heel goed van communiceren en dit onderwerp trekt heel veel aandacht. Er is evident tegenin te werpen dat het principieel niet toelaatbaar zou zijn om je geschiedenis ongedaan te maken. Bovendien is het de vraag of het technisch gesproken haalbaar is. Als wij ertoe komen, is er natuurlijk een geweldig overgangsprobleem van legacy naar nieuw. Het valt toe te spitsen op de onlinesector, waarin structureel niet wordt vergeten. Sterker nog, daar wordt ontzettend veel geld verdiend en er worden plannen gebouwd om nog veel meer geld te verdienen op basis van het structureel exploiteren van niet-vergeten. De kernvraag is: kun je het technisch organiseren? Er zijn creatieve oplossingen die duidelijk maken dat het heel goed kan, mits je bereid bent een aantal beperkingen te accepteren. Je zou een datum aan gegevens kunnen hechten. Dan zijn ze op een goed moment weg. Als je het gepubliceerd hebt, wordt het een stuk lastiger, maar op zichzelf kun je de timeline inbouwen in gegevensbeheer. Het organiseren van vergeten zit in strafregisters en disciplinaire files. Op heel wat plaatsen organiseren wij vergeten. Het is dan niet in absolute zin, maar wel in praktische zin weg. Het is voorstelbaar dat het bij sollicitaties niet aanvaardbaar is om bepaalde dingen te vragen. Zo gaan wij ook om met genetische gegevens bij verzekeraars. Er zijn heel wat smaken beschikbaar die als je er goed over nadenkt bruikbaar zijn om het onderwerp te organiseren. Het is geen digitaal ja/nee, het ligt wat genuanceerder. In een advies van half juni heb ik na aanvankelijke scepsis de stelling betrokken dat dit een heel nuttige aanvulling is op het bestaande instrumentarium in bepaalde sectoren. Nogmaals, ik denk niet dat je er bij de Belastingdienst en de politie veel steun voor krijgt.

De heer **Hamel** (PvdA): Ik zeg erbij dat ik een amateur ben, maar het spreekt mij zeer aan dat je uiteindelijk de autofabrikant aansprakelijk stelt. Hoe ga ik dat met de overheid jegens de burger doen?

De heer **Hustinx**: Dat lijkt mij niet zo'n enorme klus, hoewel het niet in een handomdraai kan. Dichter bij de actualiteit dan dit kom ik niet, zo zeg ik bij voorbaat, want ik heb mij heilig voorgenomen om geen commentaar te geven op actuele Nederlandse zaken. Er is een aantal voorbeelden van grote ICT-projecten genoemd. Als die projecten niet denkbaar zijn zonder dat in een gefaseerde aanpak in elk van de fasen daarover verantwoording zou zijn afgelegd op de manier waarop ernaar verwezen is, dan creëer je de handvatten voor het publiek. Dan creëer je de handvatten voor Kamerleden die vragen stellen. Ik denk aan de jaarlijkse discussies over voortgang. Men kan dan veel geïnformeerder en veel insnijdender een debat voeren. De toezichthouder kun je de bevoegdheid geven om ermee te stoppen als je die verantwoording niet aflegt en dus onrechtmatig bezig bent. Dat is de consequentie van het aanscherpen van de verantwoordelijkheden. Wij moeten niet bang zijn om de overheid aan

dezelfde maten te houden waaraan het bedrijfsleven en bijvoorbeeld ziekenhuizen zich moeten houden. Ik zal het wat provocerend zeggen. Strong incentives zijn belangrijk om mensen bij de les te houden. Als wij zachte heelmeesters aan het werk zetten, komen wij niet veel verder. Data breach notification, melding van ongelukken, is belangrijk. Dat komt er ook aan. Er is echt behoefte aan een veel grotere professionalisering, een steviger aanpak van het publieke domein, inbegrepen het informatiebeheer. Niet alle ongelukken zullen dan voorkomen worden, maar de overheid wordt op alle niveaus gedwongen om dat veel steviger aan te pakken.

De **voorzitter**: Ziet u het dan ook gebeuren dat uw ambt de mogelijkheid krijgt om Kroes-achtige boetes op te leggen aan lidstaten of aan private partijen die grensoverschrijdend overtredingen begaan?

De heer **Hustinx**: Het gaat niet om mijn ambt en ook niet om nieuwe bevoegdheden. Ik heb op dit moment al de mogelijkheid om tegen de Europese Commissie te zeggen: stoppen ermee, stekker eruit. Ik heb niet de mogelijkheid om boetes op te leggen maar ik kan verder alle onderzoeken doen die ik nodig vind, zonder toestemming. De conclusie kan zijn: ermee stoppen, termijnen stellen et cetera. Houdt men zich er niet aan, dan kan ik de zaak verwijzen naar het Europese Hof.
U sprak ook over lidstaten. Welnu, dat is weer een andere dimensie. Op dit moment is de Europese Commissie bezig met een programma om lidstaten in gebreke te stellen die de bestaande richtlijnen niet goed hebben uitgevoerd. Men is begonnen met Duitsland. Dat was heel veelzeggend. Het land met de grootste ervaring op het terrein van dataprotectie is veroordeeld omdat zijn regionale toezichthouders niet voldoende onafhankelijk zijn. Nu is men met Oostenrijk bezig. Engeland zit in de pijplijn en dat weet men in Brussel. Ik ken niet alle en het is ook niet openbaar, maar er is een aanpak. Dus de lidstaten die het niet goed hebben gedaan, kunnen dat verwachten.
Verder zijn er een aantal tekorten die via de herziening worden aangepakt. Zo wordt er op dit moment uitbundig gebruikgemaakt van de bestaande mogelijkheid om binnen de richtlijn te manoeuvreren. Zelfs de legitieme flexibiliteit leidt in 27-voud tot een onhanteerbare complexiteit. Dus er zijn wegen om dat te doen. Ik denk dat de verantwoordelijkheid voor de naleving, het toezicht en de handhaving op lidstaatniveau hoort te liggen, maar in dat kader kan er sprake zijn van klachten bij de Commissie en uiteindelijk van vragen aan het Hof. Op alle mogelijke manieren kan de handhaving, de leercyclus benut worden. Dat betekent natuurlijk niet dat je elke twee jaar iets nieuws moet invoeren. Dat gebeurt ook niet. Nu komen de vragen langzamerhand voor het Hof en die komen uit alle lidstaten. De antwoorden van de gerechten spelen ook een rol bij de herziening. Laten wij hopen dat het dan meegenomen wordt en ook beter wordt.

De **voorzitter**: Dank u zeer voor de toelichting.
Dan zijn wij nu toe aan de laatste spreekster. Ik hoop dat iedereen nog voldoende helder en scherp is. Het woord is aan mevrouw Prins.

Mevrouw **Prins**: Voorzitter. Ik hoop u allen helder van geest te houden tot aan de soep en de broodjes.
Allereerst dank voor de uitnodiging. Ik had hier graag iets verteld over het WRR-rapport, maar dat gaat nu niet lukken. Ik ga er wel wat zaken uit vertellen maar ik ga u geen conclusies en aanbevelingen noemen, omdat die per slot van rekening op 15 maart nog aan het kabinet gepresenteerd worden en we ze als raad dus nog even voor ons moeten houden. Ik wil u wel het een en ander vertellen over een aantal studies die rondom het rapport gepresenteerd zijn en worden. Straks is er wellicht aandacht voor

het rapport maar er is zoveel meer dan het rapport alleen. Daar begin ik mee om vervolgens ook iets te zeggen over wat wij zoal hebben gedaan in het onderzoek en over een aantal zaken die ons daarbij zijn opgevallen. Maar allereerst even het rijke materiaal waarvan we een deel al gepubliceerd hebben op onze webpagina. Ik noem de studie van Vincent Böhre over biometrie, de studie van Max Snijder over biometrie, de studie over het epd van Bettine Pluut en een studie over het Veiligheidshuis. Op 15 maart als wij het rapport presenteren, presenteren wij ook een verkenning met daarin een aantal studies. Een daarvan is de studie van Ybo Buruma die specifiek gaat over het recht op vergetelheid. In die studie – daar mag ik wel iets over verklappen – laat hij zien dat het belang van het recht op vergeten zich breder uitstrekt dan alleen online. Ybo Buruma laat zien dat er in politiesystemen een groot belang is om aandacht te hebben voor vergeten; misschien wellicht niet het recht op vergeten maar wel het belang van vergeten. Daar is een onderscheid in te maken.
Verder noem ik een studie van Paul de Hert over de verantwoordelijkheid van de overheid, waarin hij terugkomt op de Finse zaak waaraan zojuist werd gerefereerd. Ik noem ook de studie van Michel van Eeten over verantwoordelijkheid en beveiliging. Dit laatste is belangrijk in de discussie rondom het epd. Daarin gaat het om percepties over veiligheid en beveiliging van systemen die wellicht in het publieke debat wat ondergesneeuwd raken maar die zeer belangrijk zijn. Ook noem ik de studie van Mark Bovens en Albert Meijer, eveneens over verantwoordelijkheid van de overheid. Ik noem een studie over de CIO. Die gaat over de rijks-CIO, Maarten Hillenaar, maar zeker ook over de verschillende CIO's van de departementen. Ook is er een studie over goed opdrachtgeverschap. Wij hebben zelf, als projectgroep bij de WRR, een aantal domeinverkenningen uitgevoerd. Ik noem in dit verband de Verwijsindex Risicojongeren, die door de Kamer is bediscussieerd. Daaruit blijkt dat op het niveau van het Rijk een goed, kaal en «integer» systeem is neergezet, maar dat zich op het lokale niveau inmiddels een enorme dynamiek ontwikkelt rondom de Verwijsindex Risicojongeren. Er zijn allerlei zaken aan de gang die we op voorhand op dit niveau niet zo bedacht hadden. Eveneens staat in de verkenning een bredere studie over het epd en een studie over migratiebanken. Daarin komt met name de Europese thematiek tot zijn recht. Uiteindelijk komt er op de dag zelf ook nog een webpublicatie over mobiliteit, de ov-chipkaart, maar ook over ANPR. Over dit laatste is een wetsvoorstel in voorbereiding. Dit is zeer actueel.
Hierin heb ik kort neergezet wat het achtergrondmateriaal is bij het rapport. Wat is de ambitie van het WRR-rapport? Het rapport gaat uitsluitend in op de inzet van ICT in de relatie burger/overheid, dus niet in de relatie overheid/bedrijfsleven. Daarmee is het rapport dan ook breder dan privacy alleen. Het gaat over meer dan alleen maar het gebruik van ICT en de privacy-implicaties bij het gebruik van persoonsgegevens. Het gaat bijvoorbeeld ook over goed opdrachtgeverschap, waar de Rekenkamer al meerdere rapporten aan gewijd heeft. Maar uiteindelijk zie je dat het neerkomt op informatiegegevens en de kwaliteit daarvan. Ik kom daar zo op terug.
Onze ambitie is om iets te zeggen over de verantwoordelijkheid die de overheid te nemen heeft naar aanleiding van het effect van ICT op de relatie tussen burger en overheid. Wij ambiëren daarbij iets meer dan alleen het voeren van een discussie over losse applicaties. Wij zullen wel degelijk vanuit het empirisch materiaal, dat wij in deel 2 van het rapport presenteren, iets zeggen over het biometrisch paspoort, over het epd, over de internationale dynamiek, over de lokale dynamiek, over de rollen van de verschillende toezichthouders en over de invloed van burgers, die zelf met ICT aan de gang gaan en de overheid aan de zijkant inhalen. Ook burgerrechtenbewegingen sturen en beïnvloeden, terecht, het debat. Uiteindelijk pogen we met het rapport iets meer te doen dan alleen een

discussie voeren over losse applicaties. Dat is de eerste ambitie die wij hebben.
De tweede ambitie is om iets meer te doen dan privacy zwart-wit tegenover veiligheid of tegenover efficiency en effectiviteit te zetten. Kortom, we proberen een redenering neer te zetten die beoogt de discussie langs een andere band te voeren en daarbij de belangenafweging op een andere manier vorm en inhoud te geven. Natuurlijk komt de burger in de knel, maar, zoals in een aantal presentaties al is aangekaart, wordt de overheid zelf ook steeds kwetsbaarder. De kwetsbaarheid van de burger, maar zeker ook de potentiële kwetsbaarheid van de overheid is een thema in het WRR-rapport.
Ik noem redelijk willekeurig, maar niet helemaal willekeurig, een aantal zaken die direct door mij aan het papier zijn toevertrouwd.

1. Wat zien wij? Dit refereert al een beetje aan wat ik zei: het gaat over meer dan losse applicaties. Wij zien een gekoppelde wereld ontstaan. Ik ben het dan ook niet helemaal eens met de stelling: laat de verantwoordelijke zijn verantwoordelijkheid maar nemen. Natuurlijk is dat zo, maar als je dat bekijkt vanuit het perspectief van de burger en als je kijkt naar de gekoppelde, verketende en vernetwerkte overheid die ontstaat, dan zie je dat inmiddels 100 organisaties binnen een dossier verantwoordelijkheid hebben te nemen. De burger moet dus 100 keer ergens aankloppen. De discussie zal dus vooral moeten gaan over de vraag hoe wij het voor de burger nog werkbaar kunnen maken in de gekoppelde, vernetwerkte en verketende wereld. Laat de verantwoordelijke absoluut zijn verantwoordelijkheid nemen, maar de vraag is of dat voldoende is. Gekoppelde werelden zeggen iets over verantwoordelijkheid en hebben betekenis voor de discussie over verantwoordelijkheid.
2. Gekoppelde werelden betekenen iets in de discussie over de kwaliteit van de informatie. Vanmiddag hebben wij nog niet gesproken over de vraag waar wij het eigenlijk over hebben. Wij praten over informatie, gegevens, persoonsgegevens en van alles en nog wat, maar wat is nu eigenlijk onderwerp van debat? Is dat puur informatie? Zijn dat losse gegevens? Zijn dat persoonsgegevens? Zijn dat profielen, waar Geert Munnichs al op inging? Neem het recht op vergeten. Natuurlijk kun je in de justitieketen zeggen dat niet alles zomaar vergeten moet worden. Je zou toch willen dat het kind – ik denk nu aan het elektronisch kinddossier – op enig moment mag vergeten dat het een probleemkind was? Als profiel, als beeld dat de overheid van een burger heeft. Vergeten is dus meer dan een discussie over losse informatie. In de vernetwerkte en gekoppelde wereld hebben wij dus ook een discussie te voeren over de vraag wat nu eigenlijk het object van aandacht is. Gaat het om informatie, gegevens, profielen, beelden et cetera? Uiteindelijk moet de discussie gaan over «maatvoering», zo noem ik het nu maar even. Waar houdt het op? Welke overwegingen, welke belangen? Hoe weeg je die ten opzichte van elkaar? De antwoorden op die vragen bepalen de maatvoering.

Het dient te gaan om de positie van burgers en om instrumenten voor burgers. Ik heb al gesproken over vergeten, maar er is nog meer. Wij dienen het naar mijn mening ook te hebben over de positie van de overheid zelf, de kwetsbaarheid. De toekomst van digitalisering binnen de overheid staat in feite met deze discussie ook op het spel. De WRR vindt het heel belangrijk dat die discussie wel wordt gevoerd. Het gaat uiteindelijk ook om de vraag wat voor een informatiesamenleving en wat voor een digitaliserende overheid wij willen inrichten en welke piketpalen wij daarbij slaan.
De WRR zal op 15 maart een aantal aanbevelingen doen. Deze zijn zowel inhoudelijk als institutioneel van aard. Dat kan ik alvast verklappen. Misschien moet ik daar alvast het volgende bij vertellen. Wij hebben zojuist een discussie gevoerd over verschillende vormen van autoriteiten

et cetera. Het gaat niet om het uithangbordje. Het gaat om de boodschap die daarachter zit, om datgene wat er gedaan moet worden.
Daar wil ik het bij laten.

De **voorzitter**: Wie van de collega's wil nog een vraag stellen?

Mevrouw **Ten Horn** (SP): Hoeveel aandacht gaat de WRR besteden aan de haalbaarheid van het bepalen van doelbinding van een systeem in die gekoppelde wereld?

Mevrouw **Prins**: Ik kan alvast zeggen dat wij daar weinig over zeggen. Ik wil de boodschap meegeven dat wij als WRR menen dat de discussie niet daar uitsluitend op toegespitst zou moeten worden. Wij menen dat de discussie op een ander punt zit. De alsmaar focus op doelbinding verhult kwesties die erachter zitten die eveneens belangrijk zijn. Ik wil niet zeggen dat ze belangrijker zijn. Dat zijn kwesties die we wel in het WRR-rapport uitdrukkelijk adresseren. Ik denk dat we indirect dus wel weer bij de. doelbinding uit komen en wel het een en ander over doelbinding zeggen. Mijn antwoord is een beetje omslachtig, want ik kan niet zo heel veel zeggen.

Mevrouw **Ten Horn** (SP): Ik wil nog een aanvullende vraag stellen. In de wetgeving bestaat onder andere de mogelijkheid voor het CBS om meerdere databases aan elkaar te koppeling, daar waar de overheid eigenaar of financier van de database is. Mevrouw Prins heeft gesproken over de kwetsbaarheid van de overheid. Denkt zij dan aan de situatie waarin mensen toestemming geven om hun gegevens aan een bepaalde database te leveren, niet wetende dat dit gecombineerd gaat worden met andere databases die zich in hetzelfde instituut bevinden?

Mevrouw **Prins**: Het punt van transparantie is een belangrijk punt in ons rapport. Daarover moet meer duidelijkheid komen. Technologie zou daar ook de helpende hand bij kunnen bieden.
Voorzitter. Hier wil ik het bij laten.

De **voorzitter**: Daar moet u het mee doen, zegt een bekende kantonrechter in dit land af en toe. Mevrouw Prins, zeer bedankt. Het is net zes uur geweest. We zijn dus redelijk op schema. Ik wil een half uur schorsen. Om half zeven stipt beginnen wij weer, nadat wij de soep en de broodjes hebben verorberd, althans degenen die daarvoor uitgenodigd waren. Ik hoop iedereen straks weer terug te zien.

De vergadering wordt van 18.01 tot 18.30 uur geschorst.

De **voorzitter**: Dames en heren, de aanleiding voor deze bijeenkomst was het rapport van de commissie-Brouwer-Korf, Gewoon doen; beschermen van veiligheid en persoonlijke levenssfeer. De discussie tot nu toe gehoord hebbend, is «gewoon doen» misschien niet zo makkelijk als de titel van het rapport suggereert. Mede op verzoek van de collega's heb ik enkele thema's op een rijtje gezet die uit de inleidingen naar voren zijn gekomen en waarvoor bijzondere belangstelling bestaat. Ik loop die thema's nu even langs, zodat wij aan de hand daarvan straks de discussie kunnen voeren.
Het eerste thema waarvoor ik uw aandacht vraagt, is de doelbinding. Mevrouw Prins merkte al op dat daar vaak meer achter zit dan alleen de doelbinding zelf. Ik denk dat het goed is om daar nog even bij stil te staan en om daarbij ook onder ogen te zien wat mevrouw Prins daar precies mee bedoelt. Hierbij hoort ook het door meerdere sprekers genoemde aspect dat er begonnen wordt met een systeem voor A maar dat B, C en D daar vervolgens aan vastgeplakt worden. Daarmee kom je natuurlijk op

gespannen voet met de doelbinding. Hoe beheers je dat proces, zowel binnen de overheid als daarbuiten?
De tweede thematiek die ik heb geïdentificeerd, is de privacy. Misschien moet ik daar, de heer Hustinx gehoord hebbend, data protection by design aan toevoegen. Moet een dergelijke methode wettelijk worden vastgelegd? Kan dat ten aanzien van het bedrijfsleven of moet je dit door middel van audits organiseren? Is dat dan wettelijk vast te leggen? Alles wordt, wat ons betreft, immers steeds door de bril gezien van medewetgever. Kan daarbij ook «het recht om vergeten te worden» worden meegenomen? Is dat haalbaar en wenselijk? Is dat een aspect dat daarbij aan de orde kan worden gesteld?
De derde thematiek duid ik aan als «centraal/decentraal». Die thematiek speelt natuurlijk bij nogal wat onderwerpen. Ik zie de heer Franken wijzen naar een notitie, maar ik wijs erop dat ik van die notitie gebruikmaak bij wat ik nu oplees.

De heer **Franken** (CDA): O, dan doet u dat zo creatief dat ik dat nog niet herkende, maar ik hoop dat u die algemene lijn wilt aanhouden. Die vragen hebben wij immers van tevoren opgesteld om de leden van het panel daarmee te bombarderen.

De **voorzitter**: Zeker, maar ik weet ook dat de heer Franken buitengewoon handig is in het, waar nodig, mij aanvullen of corrigeren als dat straks in de discussie te pas zou komen.
Zoals gezegd: «centraal/decentraal» is een belangrijk onderwerp, gelet op diverse onderwerpen die hier in termen van wetgeving de revue hebben gepasseerd.
De vierde thematiek is de rechtsbescherming, ook ten aanzien van het onderwerp «lekken», en de kwetsbaarheid van systemen, ook wat de overheid zelf betreft. Die thematiek is ook in de inleidingen aan de orde geweest. Misschien moet nader verdiept worden hoe het met die kwetsbaarheid zit. Daar zit volgens mij ook het punt van de klokkenluidersproblematiek aan vast, dat een beetje buiten het kader blijft.
Een niet onbelangrijk punt in de discussie is ook: autoriteit, ja of nee. En wat zouden dan de bevoegdheden moeten zijn? Boetes, toezicht en eventueel ook toezicht vooraf, zeker ten aanzien van de overheid? Daarbij is ook de vraag aan de orde – daarbij kijk ik naar de heer Kohnstamm – of de burger inderdaad zo machteloos is dat hij eigenlijk volledig afhankelijk is van de toezichthouder en van enige autoriteit. Ik ben er zeker van dat daarbij ook enkele kleinere punten uit de notitie aan de orde zullen komen. We beginnen bij het onderwerp «doelbinding».

De heer **Hustinx**: Mijn vertrekpunt is dat doelbinding een heel fundamenteel beginsel van het gegevensbeschermingsrecht is. Dat is neergelegd in verdragen en richtlijnen en nu ook in het Handvest van de Grondrechten. Gesteld wordt dat gegevens worden vastgelegd voor een specifiek doel. Dat heeft alles te maken met «select before you collect». Ik denk dat dit een goede focus is in het voortraject. Daar zitten twee problemen bij. Het eerste is: op welk niveau van abstractie definieer je het doel en wie doet het precies? Het andere probleem is: zijn er mogelijkheden om verzamelde gegevens voor een ander doel te gebruiken?
In het huidige stelsel is het mogelijk om onder bepaalde voorwaarden gegevens ook voor een ander doel te gebruiken. Ook al is een doel precies omschreven, het werkt nooit mathematisch. Het gaat over «en ander daarmee direct verenigbaar vervolggebruik». Er is dus sprake van een zekere flexibiliteit. Als het onverenigbaar is, is het alleen toegestaan na speciale legitimatie. Dat is niet zo uitzonderlijk, want ook bij de belastingheffing is voortdurend sprake van onverenigbaar gebruik. Gegevens van de werkgever worden vervolgens gebruikt voor de belasting. Dat soort garingsbevoegdheden zijn dus momenten om na te gaan of zo'n inbreuk

wel of niet aanvaardbaar is. Dat geldt ook voor opsporingsactiviteiten van de politie. Bij het vraagstuk van horizontaal verkeer binnen de overheid heb je met dit punt te maken.
De vraag op welk niveau doelbinding wordt gedefinieerd, is lastig te beantwoorden. Het gaat om de vraag wat het concrete doel is waarvoor gegevens in eerste instantie zijn verzameld in het kader van de taak van het desbetreffende bestuursorgaan. Als we het persoonsnummer invoeren, gaat het om een infrastructurele beslissing van een zo grote impact, dat het doel heel erg vluchtig wordt. Dat vergt zorgvuldige toetsing van de consequenties van het zo breed maken van een doelstelling.
Het opgeven van de doelbinding zou ik dus onder geen voorwaarde willen overwegen. Ik denk wel dat er rond die doelbinding beslissingsmomenten zijn die wij goed moeten bewaken. En daarbij komen dan allerlei vragen aan de orde. Wie bepaalt het? Hoe meet je dat? Waar wordt het vastgelegd? Hoe wordt daarover verantwoording afgelegd? Maar in het bestaande kader zit meer flexibiliteit dan men soms bereid is toe te geven. Er zijn echter ook grenzen en die moeten wij goed bewaken. Het is meer dan de moeite waard om dat te doen.

Mevrouw **Prins**: Laat ik zeggen dat ik mij daarbij aansluit om vervolgens een stapje verder te zetten, want alsmaar herhalen heeft niet zo veel zin. De grote uitdaging is vervolgens het zetten van stappen en het plaatsen van piketpalen rond de flexibiliteit. Die flexibiliteit is er. De vraag is welke belangen een rol spelen als het gaat om de keuze hier of de keuze daar maken. Dan kom ik op een overkoepelend beoordelingskader zoals dit achter het eerste gedachtestreepje staat. Je zou wellicht ook kunnen spreken van een overkoepelend afwegingskader, want uiteindelijk gaat het om het afwegen van belangen. Als je de flexibiliteit iets meer zou willen oprekken, doe je dat omdat je bepaalde andere belangen dan gegevensbescherming op dat moment voorrang wilt geven.
Voor mij zou een belangrijk discussiepunt voor de toekomst zijn dat wij eens nadenken over de vraag hoe wij dit afwegingskader zodanig handen en voeten kunnen geven dat wij vervolgens in concrete discussies over waar wij de ruimte zoeken in die flexibiliteit en welke keuzes wij maken, handelen op basis van een consistent kader dat duurzamer is en in meerdere situaties kan worden toegepast.

Mevrouw **Ten Horn** (SP): Ik zou het beoordelingskader nog iets meer willen toespitsen. Ik noem als concreet voorbeeld het elektronisch patiëntendossier. Stel dat het er komt, dan is het doel het verbeteren van de gezondheid in den brede. Als de farmaceutische industrie zich dan meldt met de vraag of alle gebruikers van middel X in Nederland verzameld in het elektronisch patiëntendossier, kunnen worden getoetst op een ander kenmerk, zou dit dan onder een beoordelingskader vallen om te toetsen of het gebruik van deze database daarvoor mogelijk is?

Mevrouw **Prins**: Ja, wat mij betreft wel. Als ik het elektronisch patiëntendossier als voorbeeld neem, kan ik verwijzen naar een mooi voorbeeld binnen de overheid; wij hoeven de commerciële sector dus niet eens in deze discussie binnen te halen. Op dit moment wordt gediscussieerd over een aanpassing van Boek 1 BW, voor de elektronische geboorteaangifte. Namens de Nederlandse Vereniging voor Burgerzaken is bij de regering de wens neergelegd om het elektronisch patiëntendossier te koppelen aan het elektronisch geboorteregister. Dit zijn twee volstrekt verschillende doelen. De regering heeft terecht gesteld dat het elektronisch patiëntendossier daarvoor niet kan worden gebruikt. Bovendien wordt het elektronisch patiëntendossier vooral gebruikt door heel andere typen actoren dan de gemeenten. Daar zie je dat zelfs binnen de overheid een discussie plaatsvindt omdat het elektronisch patiëntendossier wel zo

handig is, omdat wij dan 100% zeker zijn in het kader van in dit geval de bestrijding van identiteitsfraude, toch ook een te dienen belang. Zo ver wil de overheid echter niet gaan en dus wordt het elektronisch patiëntendossier daarvoor niet gebruikt.

De heer **Kohnstamm**: Voorzitter. Als u mij toestaat wil ik twee casusposities naar voren brengen, een in de private sector en een andere in de publieke sector, waaruit blijkt dat je als je niet strikt probeert de doelbinding serieus te nemen, hoe dat beoordelingskader ook is, op de een of andere manier op een glijdende schaal kunt terechtkomen. In de private sector zijn er nogal wat algemene voorwaarden waarin staat dat degene die gebruikmaakt van een bepaalde site of van een bepaald product, toestemming geeft voor het gebruik van de gegevens die aldus worden gegenereerd voor «zorgvuldig geselecteerde derden». Dit gebeurt veel meer dan wij wel denken. Bovendien ben je veelal afhankelijk van het product. Je kunt wel nee zeggen, iedereen kan kluizenaar worden als hij dat wil, maar dat is geen echte vrije keuze. Dit is een voorbeeld van hoe serieus de discussie uiteindelijk is.
Het tweede is dat ook in de sfeer van function creep in dit gebouw uitvoerig is gesproken over de beperkingen aan het gebruik van het burgerservicenummer. Of wij nu gelijk hebben of niet: in de discussie werd bij voortduring gesteld dat het bsn gebruikt zou worden voor de publieke taak van de overheid. Het bsn wordt op dit moment echter ook gebruikt voor de passen die nodig zijn om het departement binnen te kunnen komen. Het is een activiteit van de overheid, maar zeker geen publieke taak. Doordat het doel onvoldoende helder was geformuleerd of doordat er sprake was van function creep, zijn wij al heel snel op een hellend vlak terechtgekomen. Wat het oorspronkelijke doel was, was daardoor op een gegeven moment niet meer te achterhalen. Ik sluit mij dan ook van harte aan bij de twee andere sprekers in deze ronde.
De relevantie van het vasthouden aan de doelbinding voor de bescherming van persoonsgegevens is en blijft in ieder geval heel erg groot.

Mevrouw **Strik** (GroenLinks): De heer Hustinx zei dat het voor andere doelen mag worden gebruikt, mits die verenigbaar zijn met het oorspronkelijke doel. Dat vergt echter wel dat het doel heel precies wordt afgebakend en heel nauwkeurig wordt omschreven. Gebeurt dat niet, dan vallen er uiteindelijk alleen maar meer zaken onder dat oorspronkelijke doel. Voor de wetgever is dat in ieder geval niet meer te controleren.
Als gegevens worden verwerkt voor een ander doel, ook al is dat verenigbaar met het oorspronkelijke doel, moeten burgers daarvan dan niet altijd op de hoogte worden gesteld? Zo ja, welke waarborgen moeten wij daarvoor dan in de wet- en regelgeving opnemen? Ik vraag dit, omdat burgers natuurlijk wel bezwaar moeten kunnen maken als dit gebeurt.

De heer **Hustinx**: Ik probeerde zojuist duidelijk te maken dat er twee mogelijkheden zijn als het doel eenmaal is omschreven. Ten eerste kan de vraag rijzen welke doelen met het oorspronkelijke doel verenigbaar zijn en ten tweede de vraag hoe omgegaan moet worden met het gebruik voor onverenigbare doelen. Die twee mogelijkheden moet je goed van elkaar onderscheiden, want het laatste is onder bijzondere voorwaarden mogelijk.
In een van de vragen staat: als het noodzakelijk is voor de veiligheid. In dat geval hebben wij het in veel gevallen over onverenigbaar gebruik, gebruik dat is toegestaan, mits er aan bepaalde voorwaarden is voldaan. Voorbeelden daarvan zijn: dringend, voldoende beargumenteerd, proportioneel et cetera. Dat moet je echter wel kunnen toetsen om te voorkomen dat je een enorme hooiwagen door een muizengaatje laat gaan.

De kwestie van verenigbaarheid ligt veel subtieler. Wat is wel of niet verenigbaar? Het is nu eenmaal de werkelijkheid dat een kleine formulering al snel een ander doel mogelijk maakt. Het zou overigens ook onwerkbaar worden als je niet een zekere flexibiliteit accepteert. Mijn ervaringen langer geleden in Den Haag en nu in Brussel hebben mij geleerd dat het mogelijk is om een werkbare systematiek te ontwikkelen en die scheidslijn duidelijk aan te geven.
Het is verder heel heilzaam om eventueel te zeggen: nee, dit kan niet, tenzij er iets bijzonders aan de hand is, maar daar heb ik nog niets van gehoord. Je moet dat wel durven! Het trekken van die grenzen is heel heilzaam. Het leidt namelijk tot jurisprudentie.
De wetgever kan zich op een handige manier door al die bochten wringen door het heel moeilijk te maken. Daardoor wordt het gaandeweg wel een warboel. Ik zou dan ook willen zeggen dat het de taak van de wetgever is om te bewaken dat function creep niet alsnog mogelijk wordt doordat er abstracte formuleringen zijn gebruikt, men een wirwar aan uitzonderingen heeft opgenomen, de procedures niet op orde zijn of achteraf niet is nagegaan hoe het is gebruikt.
De toezichthouders dienen hierbij een rol te spelen, maar ik zou zelf toch vooral inzetten op de wetgevingsprocedure. Als het om grote beslissingen gaat, moet het in de wet worden geregeld en als het om zaken op een lager niveau gaat, moet men achteraf onderzoeken hoe ervan gebruik is gemaakt. Maar die methodiek kent u natuurlijk ook. Helaas zien wij nog wel eens wetgeving in eigen zaak waarbij de wetgever op een lager niveau maar al te goed weet welk nut en gebruik van de uitzondering kan worden gemaakt. Die ziet dan een legitimiteit die er misschien niet is. De Eerste of Tweede Kamer moet daarvoor een stokje steken. Zo ontstaat een geïnformeerd debat.

De **voorzitter**: Een duidelijk oproep aan ook deze Kamer om haar werk goed te blijven doen en zelfs beter te doen. Misschien kunnen wij nu overgaan naar het tweede thema, dat ik heb aangeduid als: privacy data protection by design, wel of niet wettelijk vastleggen, kan dat en hoe doe je dat ten aanzien van het bedrijfsleven? Is het recht om vergeten te worden een punt dat daarbij aan de orde kan komen? Ik weet dat door de heer Franken andere aspecten zijn genoemd, maar de sprekers kunnen die door hun eigen verhaal vlechten. Ik kijk nu met name naar de heren Munnichs en Wijsman en vraag hen of zij hierover iets kunnen en willen zeggen.

De heer **Munnichs**: Ik wil nog wel iets zeggen over die toezichthouder, hoewel ik niet al te veel verstand heb van de wijze waarop dat wettelijk precies verankerd moet worden. Ons pleidooi is niet zozeer gericht voor of tegen een ICT-toezichthouder, maar op meer structureel toezicht in de beginfase. Dat wordt heel vaak aangeduid met privacy by design. Die privacy impact assessments zijn daar misschien gelijk aan. Welke vragen leg je daarbij precies op tafel? Kijk je alleen naar de privacyaantastingen of verbreed je de scope naar onderwerpen als de doelmatigheid van zo'n systeem? Dat ligt misschien in het verlengde van die doelbinding. Moet je soms niet extra goed nadenken over het doel dat je wilt bereiken met een bepaald systeem? Dat moet vervolgens weer worden bezien in het licht van de technische mogelijkheden en onmogelijkheden. Als dat een externe privacy impact assessment wordt, die uitgevoerd wordt door een onafhankelijke organisatie, en daarover vervolgens een kritisch debat wordt gevoerd, dan zie ik geen principieel verschil met een pleidooi voor een ICT-toezichthouder. Voor de pauze werd al gezegd dat het niet gaat om het naampje dat eraan wordt gegeven. Het gaat er vooral om dat er in een vroeg stadium aandacht aan wordt besteed en dat dat niet wordt overgelaten aan de willekeur van de verantwoordelijke die een datasysteem inricht.

Mevrouw **Prins**: Voorzitter. Ik maak een paar verschillende opmerkingen, allereerst over privacy enhancing technologies. Als ik het goed heb, dan is er in 1998 in de Tweede Kamer al een motie aangenomen waarin opgeroepen werd tot het gebruik van privacy enhancing technologies. Het is dus niet iets van vandaag. In feite ligt de oproep er al veel langer en is het uiteindelijk aan allerlei instanties en organen om er daadwerkelijk werk van te maken. Verder komt privacy enhancing technologies uiteindelijk ook neer op het maken van een afweging die vervolgens technisch wordt verdisconteerd. Privacy enhancing technologies is niet de prachtige technische oplossing waarmee alles wordt opgelost. Uiteindelijk moeten met PETS net zo goed keuzes worden gemaakt. Die krijgen vervolgens een technische vertaling. Die keuzes zullen wij echter moeten blijven maken. Dat wilde ik nog even scherp zeggen.
Ik neem daarnaast graag nog even een andere rol aan. Ik was lid van de commissie-Brouwer-Korf. Bij de evaluatie van de Wbp is gesproken over een handhavingstekort. Ik weet niet zeker of ik in de woorden van de commissie spreek, maar wij hebben wel vastgesteld dat er een soort «helpendehandtekort» is; in de praktijk, zowel bij de overheid als in het bedrijfsleven, is er wel degelijk motivatie aanwezig om conform de Wbp dan wel de overige regels die de bescherming van persoonsgegevens hoog hebben, te leven, te werken en te handelen. Het is alleen ontzettend ingewikkeld. Bijvoorbeeld op het punt van de interpretatie van doelbinding – waar zetten wij de piketpalen – en de afwegingen die je technisch moet vertalen in privacy enhancing technologies, is het een kwestie van: hoe moet ik dat doen, hoe moet ik die wet interpreteren, et cetera. Dus wij hebben als commissie ook gezegd dat naast handhaving advisering cruciaal is, wil je doelbinding of eigenlijk alle dingen die uit die wet voortvloeien, heel concreet praktisch realiseerbaar maken. Naast handhaving dus voorlichting.

De **voorzitter**: Moet die voorlichting door dezelfde instantie worden gegeven als die ook met handhaving belast is en dus eventueel de eigen advisering moet toetsen?

Mevrouw **Prins**: De commissie heeft gezegd dat het in twee handen moet liggen.

De **voorzitter**: Ik begrijp dat de heer Kohnstamm zich aangesproken voelt.

De heer **Kohnstamm**: Ik ben het daar heel erg mee eens. Het College bescherming persoonsgegevens kan zijn rol niet overtuigend en Awb-technisch fatsoenlijk spelen als we eerst allerlei mensen adviseren om een beetje meer naar links of een beetje meer naar rechts te gaan en vervolgens de knuppel halen en zeggen: zo kan het niet; betalen maar. Die twee dingen moet je echt uit elkaar halen. Tegelijkertijd moeten de contacten tussen de organisatie, hoe ook geformuleerd, die in voorlichtende zin bezig is en het CBP, dat toezicht houdt, zo zijn dat de kennis uit het veld die uit de toezichthoudende activiteiten wordt geput, als het ware worden overgebriefd aan de organisatie die de helpende hand biedt.
Mag ik hierover ook nog een beetje een politiek getinte opmerking maken? Ik zag deze week of vorige week een brief waarin stond dat de commissie-Brouwer-Korf op 1 maart van start ging. Dat is dan de advisering aan de zogenaamde professionals. Ik heb nog nooit precies kunnen achterhalen wie dat wel zijn en wie niet, maar goed, daarvoor worden drie fte's vrijgemaakt. Ik voorspel dat als dat inderdaad het effect is van het advies van de commissie-Brouwer-Korf, het een ongelooflijke teleurstelling wordt. Het is namelijk onmiskenbaar zo dat professionals, maar ook individuele mensen en organisaties bij tijd en wijle geholpen willen en moeten worden met een beetje de weg vinden in doelbinding,

afscheiding et cetera. Daar is veel meer werk te doen dan dat. Je moet er dus hetzij voor zorgen dat er in de private sfeer hulpverleners ontstaan die op dit punt meer helpen, hetzij dat je meer dan drie fte's vrijmaakt als je vindt dat je er als overheid voor de overheidsprofessionals iets aan moet doen, met alle respect, anders zul je er nooit uitkomen.

De **voorzitter**: Zo te zien is deze politieke opmerking alvast genoteerd.

De heer **Meijer**: Misschien moet ik toch nog iets over de toezichthouder zeggen. Mij houdt nog heel erg de vraag bezig wat zo'n toezichthouder nu zou moeten doen. Ik ben ook geneigd, daar niet een heel grote voorstander te zijn. Ik denk dat er nog veel te winnen is op het vlak van de professionalisering van de ICT-functie binnen de overheid zelf. Dat komen wij keer op keer in onze onderzoeken tegen. We hebben op dat gebied dan ook aanbevolen om de CIO-functie binnen ieder departement op touw te zetten. Maarten Hillenaar als CIO van het Rijk is al genoemd. Ik denk dat je ook zou moeten uitkijken voor het ontslaan van de echte verantwoordelijke voor het ICT-beleid en de privacywaarborgen daaromheen. Laat die maar verantwoordelijk zijn, zou ik zeggen. Je kunt ook het effect krijgen – daarvoor wil ik waken – dat de toezichthouder aan wie een bepaald concept wordt voorgelegd, het prachtige advies geeft om daarvoor te gaan, maar dat het in de uitvoering misloopt. Dat zien we op dit moment veel in de praktijk terugkeren. Dan heb ik het over meer dan alleen privacy. Ik zie nog niet in wat de toezichthouder precies voor een rol zou moeten spelen. Dat hoor ik graag van de mensen achter deze tafel, want voor mij blijft dit nog een beetje boven de markt hangen. Bovendien schuilt er in mijn ogen een risico in.

De heer **Wijsman**: Voorzitter. Juist om de verbinding te kunnen leggen tussen de business, dus het bedrijfsproces, en de technologie die dat bedrijfsproces ondersteunt, hebben wij aangeraden om te denken aan het aanstellen van chief information officers. Wanneer je een situatie hebt waarbij je een College bescherming persoonsgegevens hebt dat zich bezighoudt met de procedurele zaken, met design en met privacy enhancing technologies en wanneer je een ICT-autoriteit hebt die zich bezighoudt met de vraag of dat allemaal goed in systemen is terechtgekomen, dan heb je nu juist die twee dingen uit elkaar gehaald die wat ons betreft essentieel zijn om ervoor te zorgen dat ICT doet waarvoor het bedoeld is. Dus ik ga iets verder dan mijn naamgenoot Thomas Meijer. Het staat in feite haaks op wat wij hebben aanbevolen, maar wel met de toelichting die ik er nu bij heb gegeven.

Mevrouw **Tan** (PvdA): Ik wil reageren op wat er net werd betoogd vanuit de Algemene Rekenkamer over de CIO, om de countervailing powers wat meer binnen dan buiten het apparaat te leggen, als ik het zo mag noemen. Hoe verhoudt zich dat tot de knelpunten zoals die ook door de Rekenkamer zijn gesignaleerd op een van de laatste sheets, dat ICT-projecten in de problemen raken doordat de ICT-industrie, de minister en de politiek elkaar in een complexiteitsspiraal brengen? Want op het moment dat de CIO onderdeel uitmaakt van de ambtelijke hiërarchie staat hij dus ook onder de politieke sturing van dat proces. Dan loop je daar dus ook heel grote risico's mee, lijkt mij. Zou je dan niet als samenleving en als burger meer gebaat zijn bij een onafhankelijke toezichtsinstantie, die minder rechtstreeks onder het gezag staat van het politiek bestuur?

De heer **Wijsman**: Ik heb niet alle conclusies en aanbevelingen op de site gezet. Een van de aanbevelingen was ook – ik zeg het nu een beetje onparlementair – dat de minister een rechte rug moet houden ten opzichte van de Tweede Kamer, die altijd maar meer en sneller wil. Wat wij wel hebben geconstateerd, juist in het onderzoek waaruit deze aanbevelingen

afkomstig zijn, is dat het ministerie te weinig weerwoord heeft om die rechte rug te houden. Wij hebben naar vijf projecten gekeken en bij geen van die projecten vonden wij in de documentatie heel duidelijk wat nu precies de omvang was van het systeem dat gebouwd gaat worden. Op het moment dat je niet weet wat de omvang van het systeem is, kun je ook alleen maar een vinger in de lucht houden om te bepalen hoeveel het gaat kosten en wanneer het klaar kan zijn. Dus de kenmerken en karakteristieken van het te bouwen systeem waren niet bekend. Dat zijn zaken waarin een chief information officer (CIO) een heel goede functie kan hebben, want hij kan juist werken aan het introduceren van matrices, meetbare grootheden om datgene wat in de parlementaire discussies vaak vanuit de onderbuik wordt genoemd te kwantificeren en op die manier ook objectiveerbaar te maken.

De heer **Kohnstamm**: Ik vind het prettig om in deze discussie nog even helder te maken wat in ieder geval keuze is geweest van het College bescherming persoonsgegevens, een beetje in lijn met de advisering van de commissie-Brouwer-Korf. «Robuust», was geloof ik het woord, «een robuuste toezichthouder», in het rapport. Dat is waarmee wij het meest effectief een bijdrage kunnen leveren aan de naleving van de Wbp-cum annexis, want het is niet alleen de Wet bescherming persoonsgegevens. Ik reageer op de zin die de heer Munnichs net uitsprak: waar het uiteindelijk om draait, is dat in een vroeg stadium veel aandacht aan het een en ander wordt besteed. Dat kun je linksom of rechtsom doen, maar mijn grootste pleidooi – los van de vraag of ik dit nu precies goed gehoord heb – is om ervoor te zorgen dat uiteindelijk de verantwoordelijke voor het in de markt zetten van een product, dienst of wetgeving daarvoor aansprakelijk is. Dat betekent dus dat de organisatie zo moet zijn dat de weging daadwerkelijk gemaakt is en dat het ook zichtbaar moet worden voor de publieke sfeer hoe die weging is uitgevallen. Er blijft altijd een politieke keuze over, maar heel veel verder dan dat kom je niet. Een aparte autoriteit daarvoor is iets wat wij absoluut niet zouden ambiëren en wat wij ook niet willen zijn. Montesquieu heeft over de scheiding der machten slimme dingen gezegd; dat moet je bij ons niet neerleggen. Dan zou je er namelijk weer een autoriteit bij krijgen. Daarmee neem je als het ware de verantwoordelijkheid weg voor wat iemand ontwikkelt en op de markt zet. Daarmee raakt de verantwoordelijkheid zoek raakt. Dat is het allerlaatste dat je zou moeten laten gebeuren in dit veld. Ik ben er vanuit mijn kennis en met mijn petje op erg van overtuigd dat je het in de sfeer van aansprakelijkheden van de verantwoordelijken moet zoeken, met checks-and-balances die zichtbaar en controleerbaar zijn en in het maatschappelijke debat een rol kunnen spelen. Ik voel er niet zo gek veel voor om daar een aparte ICT-autoriteit op te zetten.

De heer **Munnichs**: Het gaat nu heel veel over de ICT-autoriteit, terwijl het moet gaan om structureel toezicht. De ICT-autoriteit is een mogelijke vorm. Ik wil mij helemaal niet ophangen aan deze vorm. Ik wil iets aan het verhaal van de heer Kohnstamm toevoegen. Als je een verplichte privacy impact assessment door een externe onafhankelijke instantie invoert, moet er vervolgens een uitspraak worden gedaan over de adequaatheid van het ontwerp, in het licht van die assessment. Je hebt specifieke ICT-kennis nodig om dat soort ontwerpen goed te kunnen beoordelen. Het is prima als dit publiekelijk gebeurt, zodat onafhankelijke experts en anderen, ngo's en weet-ik-wie, zich daartegenaan kunnen bemoeien. Je moet er in ieder geval voor zorgen dat er een zekere mate van ICT-deskundigheid in die toetsing zit. Ik zou dit niet aan de politiek durven overlaten.

De heer **Franken** (CDA): Zou je dit niet gewoon door EDP-auditors kunnen laten doen? Dit zijn onafhankelijke deskundigen die snel en flexibel

kunnen optreden. In Boek 2 BW, artikel 393, lid 3, staat bijvoorbeeld dat de accountant verplicht is om bij de jaarrekening ook de informatiehuishouding te toetsen van een onderneming. Zo kun je ook ten aanzien van de overheid te werk gaan. Dit hoeft niet door een instituut te worden gedaan, maar dit kan worden gedaan door mensen die zomaar vrij lopen op de markt.

De heer **Munnichs**: Ik heb mij niet zo detaillistisch in onze eigen aanbeveling verdiept. Heel belangrijk is het dat het om echt onafhankelijke mensen gaat. Ook bij accountants zie je het wel eens misgaan. Het zou best kunnen dat het zo'n vorm krijgt. Ik heb daar niet bij voorbaat bezwaren tegen.

De heer **Wijsman**: Hier zit zo'n EDP-auditor of IT-auditor. Ik ben namelijk niet alleen projectleider, maar ook IT-auditor. Ik wil even teruggaan naar het onderwerp privacy by design. Ik heb het gevoel dat deze term erg losjes wordt gebruikt. Men zegt dat je hierover moet nadenken bij het ontwerp van het systeem. Mevrouw Prins heeft dit wat nader gepreciseerd door te spreken van privacy enhancing technologies, de PETS. Een voorbeeld daarvan is een online transactie. Als ik mijn creditcardnummer opgeef, kan de webwinkelier naar de creditcardmaatschappij bellen, mailen of whatever doen om te vragen wat mijn tegoed is, € 1 000, € 100 000 of € 0. In een ander systeem kan hij alleen vragen of ik voldoende krediet heb om de transactie van € 1 500 te voldoen. Als het laatste het geval is, heb je een veel betere waarborging van de privacy. Ik vind het dus van belang dat wij precies zijn met de terminologie.
Design is ook niet meer dan design. We hebben vele systemen bekeken. Ik heb maar weinig systemen gezien die als zij worden opgeleverd, voldoen aan de ontwerpdocumentatie. Je zou geneigd zijn om te denken dat als het systeem wordt opgeleverd, de ontwerpdocumentatie dus wordt aangepast. Dat is echter niet de praktijk.
Ik geef een klein voorbeeld. Een flink aantal jaren hebben wij de socialezekerheidssector onderzocht. Toen constateerden we dat de uitvoeringsinstellingen persoonsgegevens zoals naam, woonplaats en geboortejaar moesten verifiëren bij de GBA. Die werd echter zo onbetrouwbaar geacht dat de uitvoeringsinstellingen dit bij de Belastingdienst deden. Het ging zelfs zo ver dat één van de uitvoeringsinstellingen de gehele tape met de gegevens van alle aangifteplichtigen in huis haalde om daarmee de check te doen. Het design is dan wel goed, dus het systeem is goed ontworpen, maar slecht geïmplementeerd, om het technisch te zeggen. Als je zegt dat anders betaald gaat worden voor mobiliteit, waarbij de gegevens alleen in het kastje worden opgeslagen waar slechts de eigenaar bij kan, dan is het de vraag of dat ook zo gebeurt. Ik praat nu even in mijn rol als IT-auditor. Wij kijken graag niet alleen naar de opzet van de maatregelen die gecreëerd zijn om privacy te waarborgen, maar ook of zij daadwerkelijk aanwezig zijn en hebben gewerkt gedurende de periode waarover wordt gesproken.

De heer **Hustinx**: De heer Munnichs maakt een nuttig onderscheid tussen het concept van de toezichthouder en de behoefte aan meer structureel toezicht. Die lijn volgend, denk ik dat intern en extern toezicht in de procedures ingebouwd kunnen worden. We hebben het dan eigenlijk over de vraag wat vooraf gaat aan de start van een belangrijk systeem bij zowel de overheid als het bedrijfsleven. Privacy by design, accountability en een aangescherpte verantwoordelijkheid zullen in het kader van wat ik verwacht, horizontaal werken. We hebben het dan over incentives voor een verantwoordelijke. Een overheidsorgaan, bedrijf, ziekenhuis of you name it, een bank, moet als onderdeel van zijn verantwoordelijkheid nagaan of er inderdaad dataminimalisatie is geweest of er adequate middelen zijn bereikt om het doel te bereiken enzovoorts, zal behoefte

hebben aan evidence. Hij zal die voor een deel intern via een insurance – we kennen al deze termen van andere terreinen van beleid zoals milieu en financiën – halen en voor een deel bij consultance. Uiteindelijk zal hij op die manier moeten aantonen dat hij de juiste middelen heeft gebruikt. Dat raakt ook de kwestie van het ontwerp, het bestaan en de werking, want gaandeweg zal hij moeten kunnen bewijzen dat de werking van het systeem conform de uitgangspunten is. Op dat punt worden de eisen de komende jaren sterk aangescherpt. Dat kan een groot deel van de oplossing bieden waar wij naar zoeken. Ik kan mij wat dat betreft aansluiten bij de grote terughoudendheid op het punt van een nieuwe toezichthouder. Ik zie liever een structurele oplossing horizontaal aangepakt.

Mevrouw **Strik** (GroenLinks): Ik heb nog een vraag over privacy impact assessment. De heer Munnichs gaf duidelijk aan dat je daarin eigenlijk ook doelmatigheid, neveneffecten enzovoorts moet hebben, zeker als je het over wet- en regelgeving hebt. Ziet de heer Kohnstamm dat ook zo? Hij is namelijk een pleitbezorger voor zo'n privacy impact assessment. Zou je het dan ook niet meer dataprotection impact assessment moeten noemen om te waarborgen dat het breder is dan puur alleen de privacy? Wie zou dat dan moeten uitvoeren?
Aan de heer Hustinx vraag ik nog het volgende. De Europese Commissie maakt impact assessments zelf. Ik heb voor mij het nieuwste ten aanzien van P&R. Heeft hij daar goede ervaringen mee? Heeft hij het idee dat dit goed werkbaar is als het valt onder de verantwoordelijkheid van dezelfde initiatiefnemer of de verantwoordelijke voor de ontwerpwetgeving?

De heer **Kohnstamm**: Het maakt niet zo gek veel uit hoe je het noemt. Het gaat er uiteindelijk om dat de leidinggevende bij de aanvang van het proces waar een product, dienst of wetgeving uit voort moet komen, aangeeft wat hij ermee voorheeft en dat wordt bekeken welke problemen er kunnen ontstaan. Om het even flauw weer met auto's te zeggen, als je een opdracht geeft voor een auto die van Den Haag naar Amsterdam kan rijden en dit aan IT-mensen overlaat, komt er geheid een Rolls Royce uit. Dan wil ik volhouden dat een Volkswagen Golf dit ook zou kunnen. Dit zie je bij IT-projecten ontzettend vaak. Als je de doelstelling weet te formuleren en als er bij degene die verantwoordelijk is voor het proces waaruit het product, de dienst of de wetgeving voorkomt, een test is waar de risico's zitten, dan ben je al een heel eind. En dan gaat het inderdaad meer om dataprotectie dan om de privacy in zijn geheel. Dan nog blijven de keuzen gemaakt kunnen worden die gemaakt worden. Dat kunnen overigens ook de foute keuzes zijn, maar je bent dan wel een heel eind verder.
Ik meld ten slotte, enigszins gefrustreerd overigens, nog iets over een privacy impact assessment dat door mijn Engelse collega is ontwikkeld, dat zowel publiek als privaat gebruikt zou kunnen worden. Ik mocht van hem proberen om die te vertalen in een Nederlands model. Wij hebben dat met een groot aantal organisaties opgepakt en bij een consultant uitbesteed om verder te ontwikkelen, met de VNG, de relevantste ministeries, VNO-NCW en MKB-Nederland, omdat echt het idee was om het te doen. Ik betreur sterker dan ik kan verwoorden dat VNO-NCW en MKB-Nederland uiteindelijk eruit zijn gestapt, omdat zij alleen maar wilde weten wat ten opzichte van de toezichthouder voor hen uiteindelijk de toegevoegde waarde zou zijn van zo'n privacy impact assessment. Ik zou als baas van zo'n organisatie willen weten welke risico's ik loop en hoe ik dichter bij compliance kom en niet de hele tijd Waterloopleintje willen spelen in de zin van wat zit er voor mij in en wat krijg ik van de toezichthouder terug. Dit project is dus aan de wilgen gehangen en heeft niet geleid tot een eindproduct.

Dat is overigens anders voor een PIA op het punt van RFID. Als je het over privacy by design hebt, dan is RFID natuurlijk een prachtig voorbeeld. Eigenlijk, privacy by default ...

De **voorzitter**: Kunt u die afkorting uit de doeken doen voor de analfabeten?

De heer **Kohnstamm**: Radio Frequency Identification chips. Heel huiselijk geformuleerd, waarschijnlijk binnen vijf jaar zit er in al onze kleren een heel klein chipje. Als je dan de rode en witte sokken in de wasmachine doet, vraagt de wasmachine of je wel zeker weet dat je dat wilt. Dat kan allemaal op afstand afgelezen worden. De afstand verschilt een beetje. Daarbij speelt de privacy of things, het internet of things. Die ontwikkeling kan heel nuttig zijn, die kan ook heel dramatisch zijn in de sfeer van bescherming van persoonsgegevens. Dus is de industrie, de RIFD-industrie, zeer succesvol bezig geweest met een PID, dat we onlangs in de artikel 29-werkgroep goedgekeurd hebben omdat wij het recht hebben, als er zo'n soort voorstel is, te zeggen dat het procedureel-inhoudelijk een goede weg is om te gaan. Het kan dus wel. Ik merk dat iedereen er nog vreselijk schrikachtig over is. Het heeft misschien met het milieu impact assessment te maken, waarvan mensen vonden dat het wel heel veel werk en ellende teweegbracht en niet meteen direct resultaat had. Maar onafhankelijk, zorgen dat de risico's in kaart zijn gebracht en op basis daarvan de keuze maken. Dan ben je al een hele stap vooruit.

De heer **Hustinx**: Mevrouw Strik had mij nog een vraag gesteld. Privacy impact assessments worden in Canada standaard toegepast. Daar zijn de ervaringen heel gunstig. Het kan natuurlijk altijd beter, maar het werkt prima.
De Commissie heeft al enige tijd de praktijk van een impact assessment, maar dat gaat dan over subsidiariteit, proportionaliteit en financierbaarheid. Dat is dus een veel ruimer begrip. Daar heeft men de laatste jaren een aangescherpte grondrechtentoetsing aan gekoppeld. Mevrouw Reding heeft het al over een zero tolerance policy. In dat kader speelt ook dataprotectie een rol.
Dat proces is heel redelijk, hoewel niet perfect. Er is wel een poging om een impact assessment zo te doen dat het altijd goed uitkomt. Dat wordt wel ontmaskerd. Er is een interne stuurgroep die daar heel kritisch op zit. Niettemin zien wij wel eens uitkomsten waar wij niet helemaal tevreden mee zijn. Het is standaard bij alle voorstellen een bijlage die wordt overgelegd en die heel nuttig is als aanknopingspunt.
Voor de risicoprojecten dringen wij sterk aan op een gerichte toetsing vooraf die veel dieper gaat. Voor risicoprojecten – de voorbeelden zijn genoemd – is dat zeer aan te bevelen, omdat het altijd een begin van discussie is. Dat is in mijn ervaring heel veel beter dan het overlaten aan beleidstaal.

Mevrouw **Prins**: Voorzitter. Ik besef dat ik hier zit voor antwoorden in plaats van voor vragen, maar ik wil de Kamer toch iets voorleggen. In de nieuwe samenstelling van de Kamer komt het wetsvoorstel ANPR (automatic number plate recognition) te zijner tijd voor te liggen. Ik worstel in dit kader met doelbinding, impact assessments en accountability. Bij de behandeling van het wetsvoorstel kunnen de leden terugdenken aan deze sessie. ANPR is voor mij een prachtig voorbeeld van de complexiteit van meerdere actoren. De korpsen worden individueel verantwoordelijk voor de camera's boven de weg. In de memorie van toelichting bij het wetsvoorstel wordt de maatvoering niet genoemd. Nergens in het hele stuk staat iets over het aantal dingen dat in Nederland komt te hangen. Nergens staat wie dat bepaalt. Wie doet er over het totaal een impact assessment? Wie gaat er nadenken over de doelbinding? Dat

zal op wetgevingsniveau wellicht nog lukken, maar ik zit met name met die accountability en de impact assessment. Voor mij is de grote uitdaging de netwerksamenleving, een samenleving waar wij met meer dingen werken dan alleen maar individuele systemen en applicaties. Nee, dan gaat het om een applicatie waarmee heel veel verschillende actoren met allemaal verschillende verantwoordelijkheden aan de slag gaan. Hoe zal in dit huis worden gediscussieerd over de maatvoering bij ANPR? Langs welke band zal die discussie worden gevoerd? Bij de impact assessment heeft de Kamer bij ANPR nog een slag te slaan.

De **voorzitter**: Wij hebben deze discussie vandaag teneinde onze collega's van straks behulpzaam te zijn.

De heer **Kohnstamm**: Deze sessie is een soort privacy impact assessment.

De **voorzitter**: Bijvoorbeeld. Maar ik zie dat de heer Wijsman zich meldt voor een antwoord.

De heer **Wijsman**: Niet voor een antwoord, maar mij bekruipt een gevoel op het moment dat er gediscussieerd wordt over een nieuw in te stellen autoriteit. Ik noem dat intern altijd de sterkemanoplossing. Hebben wij een probleem? Dan stellen wij iemand aan die wij een autoriteit noemen. Hij krijgt robuuste bevoegdheden. Wat dat precies betekent, weet ik nooit. En daarmee is het probleem opgelost. De heer Meijer wees al op de aanbeveling om CIO's in te stellen: chief information officers.

De **voorzitter**: Is dat niet ook een sterke man, maar dan op een departement?

De heer **Wijsman**: Dat zou je heel gemakkelijk kunnen invullen als een sterke man. Op die manier is de aanbeveling niet bedoeld, maar je weet natuurlijk nooit op welke manier anderen met je aanbevelingen aan de gang gaan. Ik wilde bijna «aan de haal gaan» zeggen.
Wij hebben ook de aanbeveling gedaan om te bekijken of je niet een stelsel van peer reviews kunt invoeren. Dan maak je gebruik van de deskundigheid die bij degenen aanwezig is die in het verleden met hetzelfde bijltje hebben gehakt. Zij kennen de problematiek, zij hebben de ICT-deskundigheid in huis en zij kunnen je adviseren of je op de goede weg bent. Het aardige van deze systematiek is dat zij in Engeland al helemaal uitgedokterd is. Het heeft daar de naam «gateway review». In Nederland is het bij het Rijk ingevoerd. Er is een organisatie opgetuigd die reviewers opleidt en die teams instelt. Een van de aardige dingen daarvan is dat het niet op één moment, namelijk aan het begin van een project gebeurt, maar op een aantal momenten gedurende het project. Er zijn vijf van die gateway reviews. Elke keer als een project overgaat naar een volgende cruciale fase, bijvoorbeeld als het overgaat van de ontwerpfase naar de bouwfase, de aanbestedingsfase, dan wordt er zo'n gateway review gedaan. Dat zou in het kader van het onderwerp dat wij vandaag behandelen goede mogelijkheden bieden om de voortgang in de gaten te houden en die te waarborgen van ontwerp naar gebouwd product. Dat zou dus een methode kunnen zijn om niet alleen ontwerpbeslissingen te toetsen en impact assessments te doen maar om ook gaande de rit te blijven kijken of het project gaat in de richting die bedoeld was.

De **voorzitter**: Ik wil proberen de discussie een stapje verder te brengen, ook weer kijkend naar het thema decentraal-centraal, waarbij ik dan tevens de rol van professionals wil betrekken. Bij de wetsvoorstellen zoals die voorliggen en met name bij het epd is aan de orde dat de professionals die met de gegevens die opgeslagen worden gaan werken een

belangrijke rol spelen. Mij bekruipt wel eens het gevoel dat het feit dat men beschikt over gedigitaliseerde dossiers die soms al heel oud zijn en gegevens van een heel lange tijd bevatten en een bepaald beeld oproepen van een kind of een patiënt – ik kom dan een beetje in de richting van mevrouw Prins en haar netwerksamenleving, ook in de zin van allerlei gegevens die een eigen leven gaan leiden – ook het professionele handelen gaat beïnvloeden. Anders gezegd: daardoor worden de professionals weer afhankelijk gemaakt van die informatie wat hen ertoe brengt om minder op hun eigen oordeel of hun eigen intuïtie, ervaring of deskundigheid af te gaan. Ziet u dat als een probleem? Is dat een probleem dat je hierbij aan de orde moet stellen? We praten nu heel sterk vanuit de techniek, de institutionalisering et cetera, maar als het gaat om bijvoorbeeld de manier waarop de artsen met die informatie omgaan en de gevolgen daarvan voor hun eigen handelwijze, is het natuurlijk vaak voor de samenleving en het effect ervan op individuele gevallen enorm belangrijk. Hoe gaan de professionals ermee om? Dit nog even afgezien van het feit dat zij ook geacht worden heel veel van die dossiers te voeden met informatie, wat op zichzelf ook weer tot allerlei problemen aanleiding kan geven als men verschillende uitleggen geeft aan datgene wat men daarin tegenkomt.

De heer **Meijer**: Ik werk nu voor de Rekenkamer. In het verleden was ik directeur Onderwijs en onderzoek van de Erasmus Universiteit. Van dat epd kan ik mij ook nog wel iets voorstellen, maar laat ik het toch even in een andere sfeer treken dan alleen het epd. Als het gaat over de vraag welke informatie beschikbaar is, is voor mij een groot probleem dat die informatie er niet is. Een aantal voorbeelden kan dat wellicht illustreren. Bij de Belastingdienst hanteert men de interne norm dat 75% van de dossiers op orde moet zijn. Blijkbaar 25% niet, zeg ik er gemakshalve dan maar even bij. Die norm wordt gemiddeld genomen over alle belastingregio's niet gehaald. Je ziet ook dat het door de jaren heen behoorlijk fluctueert. Dat leidt in de uitvoering van overigens met name de Toeslagenwet – de Belastingdienst keert veel uit, naast het heffen en innen wat ooit de kerntaak was – wel tot een heel groot probleem. Dus die informatie is er vaak niet, zeg ik op wellicht een andere manier dan u bedoeld heeft maar ik wil dat tegengas toch wel even geven. Op dit moment zijn wij bezig met een onderzoek naar de ICT bij de politie. Daar zie je hetzelfde probleem. Als je ergens naar binnen moet, is het wel verdraaid handig als je weet wat er de afgelopen jaren aan politiemensen en ambulanceverpleegkundigen naar binnen is gegaan. Dus daar zit ook een andere kant aan. Dat lijkt niet de achterkant van uw vraagstelling te zijn, maar ik denk dat daar wel een groot probleem ligt dat we ook onder ogen zouden moeten zien. De compleetheid van informatie is lang niet altijd gegarandeerd, veel minder dan de meesten van ons voor ogen hebben.

Mevrouw **Prins**: Ik ben medeverantwoordelijk voor de evaluatie van de Wet persoonsregistraties, de voorganger van de Wbp. Wij hebben daarvoor empirisch onderzoek uitgevoerd, waaruit blijkt dat professionals cruciaal zijn als het gaat om de naleving van de privacybepalingen. Een professional in de medische wereld had destijds andere redenen dan de Wpr om zorgvuldig met zijn gegevens om te gaan. Je zag in ieder geval toen en ik denk ook nu bij de evaluatie van de Wbp dat de ethiek en beroepscodes die een rol spelen voor professionals, ook in de jeugdhulpverlening, van groot belang zijn voor het zorgvuldig omgaan met persoonsgegevens. De rol van professionals is heel belangrijk als het gaat om privacybescherming, de bescherming van persoonsgegevens.
Ik heb voor de WRR samen met Esther Keymolen een studie uitgevoerd naar de Verwijsindex Risicojongeren. Je ziet dat gemeenten sturen op risicosignalen die afgegeven moeten worden door zorgprofessionals. Dat wordt gestuurd op aantallen. Er moeten genoeg signalen afgegeven

worden. Daar wordt het succes van het systeem aan afgemeten. Bizar, maar dat terzijde. Dit zegt overigens iets over hoe we evalueren. Ik vind dat een zorgwekkende ontwikkeling. De professional kent de context waarin de gegevens hun kleur krijgen. Als je persoonsgegevens loshaalt uit de context, worden ze steeds harder. Hoe meer mensen of actoren met gegevens werken, hoe anoniemer het wordt. Als wij hier met zijn vijftigen gegevens delen, dan heb ik het gevoel: nou, dat doen we met z'n vijftigen; het zal wel goed zijn. Maar als ik met mijn promotor Hans Franken een gegeven deel, denken wij er met zijn tweeën even scherp over na of dat gegeven nog steeds klopt. Dan blijven we bij de les. Dat zegt ook iets over zorg voor kwaliteit van gegevens. We moeten goed oppassen met wat we doen met de professional, die op een bepaalde manier de hoeder van kwaliteit van gegevens is en daarmee een bijdrage levert aan de bescherming van persoonsgegevens.

De **voorzitter**: Is dit aspect niet veel belangrijker dan de wat abstracte juridische discussie over doelbinding?

De heer **Hustinx**: Het heeft alles met elkaar te maken. Daar kom je achter wanneer je de basisbeginselen van gegevensbescherming toepast. Dan blijken de kwesties met elkaar nauw verband te houden. Dan hebben context en doelbinding alles met elkaar te maken. De kwaliteit van gegevens hangt daarmee samen.
Luisterend naar de discussie heb ik twee kleine aanvullingen. In de eerste plaats de kwestie centraal/decentraal, de binnenkomer. Dat is een heel veelzijdige en wat misleidende tegenstelling. Tijdens deze bijeenkomst is verwezen naar «decentraal» in de zin van «de burger heeft het op zak». Er is ook nog gesproken over «decentraal» in de zin van «de professional heeft het onder direct beheer». Dan heb je een schaal hoger: het is een regio, een provincie, nationaal. Ik heb ook te maken met de discussie over de vraag of het centraal-Europees moet of nationaal. Dus eigenlijk is het een kwestie van gelaagdheid en scoop. Wie zit het dichtst bij het verschijnsel en waar kan het het beste? Ik geloof niet dat je kunt zeggen dat het antwoord is «decentraal, tenzij» of «centraal». Het is een onderdeel van die impact. Dat is één. Als je tussen de niveaus, maar het kan ook op hetzelfde niveau, van regio naar regio gegevensverkeer mogelijk maakt, dan kan het niet anders dan dat de bron gegevens doorgeeft aan een ontvanger. Die gaat die gegevens voor meer zaken gebruiken dan de oorspronkelijke bron bedoelde. Dus de kwestie van wat de gegevens in zo'n systeem betekenen, is essentieel. Als er in de vraagstelling staat «overige informatie» en vervolgens «simulant?», denk ik dat alle volgende gebruikers een «byass» hebben en dus is dat een voorbeeld van wat je niet in een systeem moet hebben. Maar om dat goed hard te krijgen, is uiterst lastig.

Mevrouw **Prins**: Een andere uitdaging voor de toekomst ligt bij het profileren: het typeren van risicojongeren, het typeren van belastingbetalers et cetera. Wat je daarbij nodig hebt is zo veel mogelijk gegevens. Met te weinig gegevens heb je immers een onvolledig profiel en loop je het risico dat je een burger in een bepaalde categorie neerzet terwijl je niet alle gegeven op orde hebt. Juist bij profileren, bij datamining, hebben wij na te denken over de vraag wat de juiste hoeveelheid gegevens is die wij nodig hebben om recht te doen aan een burger in een bepaalde context.

De heer **Meijer**: Als mevrouw Prins zegt dat erom gaat zo veel mogelijk gegevens te hebben, dan ben ik niet met haar eens. Ik vind wel dat je die in een context moet plaatsen. Het hangt af van het doel dat je nastreeft. Heb je het over belastingplicht en belastingmoraal, dan moet je dat risicogedreven doen. Dan moet je een systeem van horizontaal toezicht

ontwerpen dat risicogedreven is. Bij Albert Heijn hoef je niet veel ingewikkelde dingen te doen om ervoor te zorgen dat je een goede aangifte krijgt. Dat zit wel goed in elkaar. Bij het midden- en kleinbedrijf zul je daar echter veel meer inspanning voor moeten plegen omdat daar de gemiddelde moraal net iets anders is. Het gaat om het op de juiste manier veredelen van informatie. Daar zou je een goede, contextgedreven en soms risicogerichte aanpak bij moeten kiezen. Hoe meer hoe beter – ik dacht even dat ik mevrouw Prins dat hoorde zeggen – moet het vooral niet zijn.

Mevrouw **Prins**: Ik zei: de juiste hoeveelheid gegevens.

De heer **Meijer**: Dan zijn wij het helemaal eens.

De **voorzitter**: Als 75% van de dossiers van de Belastingdienst in orde is, kan de minister van Financiën zeggen dat hij dat accepteert. Dat betekent dat hij een hoeveelheid toeslagen te veel betaalt, maar dat wordt via de wet van de grote getallen verdisconteerd in de begroting en dan ziet hij dat via de belastingheffing wel terug. Probleem opgelost. Als je er bij de elektronische patiëntendossiers van uit moet gaan dat maar 75% betrouwbaar is, dan heb je een ander probleem. De professionals die daarmee werken, zouden van dat getal moeten weten, zodat zij aan de hand daarvan al dan niet een eigen beleid kunnen vormgeven. Moet je de vormen van toezicht niet ook daarop afstemmen, zodat de gegevens betrouwbaarder worden en de contextproblemen die nu zijn gesignaleerd, zichtbaar worden gemaakt? Anders heb je in formeel-juridische zin misschien wel dataprotectie en privacybescherming gerealiseerd, maar dan ben je tekortgeschoten voor het oorspronkelijke materiële doel waarvoor de gegevens werden verzameld.

De heer **Munnichs**: Ik vind het heel lastig om hier in algemene zin over te spreken. Op welke manier je daaraan invulling kunt geven, hangt af van het dossier. Bij het elektronisch patiëntendossier gaat het bijvoorbeeld heel erg om de eenheid van taal, die nodig is om standaard te maken hoe je over medische gegevens communiceert. Sommige gegevens zijn vrij objectief, zoals de bloeddrukwaarde, maar andere gegevens zijn minder objectief, zoals de diagnose van een arts of de klachten van een patiënt. Daar treedt al een spanning op: hoe precies zijn de data? Je moet dus eigenlijk bijna van dossier tot dossier bekijken hoe je daaraan handen en voeten kunt geven en in welke mate die gegevens als nauwkeurig kunnen worden bestempeld. Bij het epd bestaat de plicht dat artsen die het niet helemaal vertrouwen, zelfstandig onderzoek uitvoeren. Het blijft in die zin dus toch vaak een beetje schipperen. Misschien is dat wel het goede antwoord.

De heer **Hamel** (PvdA): Ik wil dit even praktisch maken. Stel dat een huisarts verwijst naar een specialist in een ziekenhuis in Groningen. Zij kennen elkaar van een aantal verwijzingen. Waarschijnlijk weten zij over en weer wat zij bedoelen. Nu verwijst een huisarts uit Maastricht iemand naar Groningen. Dat is een andere context. De culturele verschillen zijn in de zorg niet gering, ook in Nederland niet. Dat betekent dat dus de gegevens in beide situaties een andere interpretatie zouden kunnen krijgen. Dan hebben we het over de context, dezelfde gegevens. Ik probeer even de vraag van de voorzitter wat concreet in te vullen. Daar hebben we het over.

De heer **Munnichs**: Dan gaat het niet om bloeddrukwaarden maar wel om meer zogenaamde subjectieve gegevens.

De heer **Hamel** (PvdA): Ik kan u zeggen dat zelfs daar zich wel eens verschillen willen voordoen, maar dat terzijde!

De **voorzitter**: Het komt neer op de vraag of je wel of niet in het epd moet kunnen vermelden «een simulant?», zoals de heer Hustinx het net formuleerde. Ik kijk ook even naar de huisarts in ons midden.

Mevrouw **Slagter-Roukema** (SP): Het zijn natuurlijk allemaal dingen die horen bij de discussie, hoe dan het adequaat registreren of het goed beheerde zorgsysteem eruit zien. Daar horen geen opmerkingen als «simulant» in. Als je gegevens beschikbaar stelt voor de koppeling via het LSP, moet je in feite met de patiënt in overleg treden of die akkoord gaat met het doorgeven aan het Landelijk Schakelpunt van deze diagnose. Dan zou je nog iets kunnen bedenken als hypochondrie en dan zou je dat nog een beetje adequater kunnen formuleren. Maar dit maakt natuurlijk dat je schaduwdossiers krijgt. Aan de andere kant is dit gegeven in de huidige opzet ook niet bedoeld om door te schakelen, hoewel de Tweede Kamer denkt dat op den duur alle patiënten die dat zouden willen, rechtstreeks in de brongegevens inzage zouden kunnen hebben. Dan zal het inderdaad betekenen dat je een heel andere manier van registreren krijgt. Dat zal dus een enorme impact hebben op de praktijkvoering. Dat is ook een impact waardoor de gewone praktijkvoering van een huisarts bijna niet meer mogelijk is.

Mevrouw **Tan** (PvdA): Ik wil van de gelegenheid gebruikmaken om aan de deskundigen achter de tafel te vragen of zij een advies hebben voor een eenvoudig Eerste Kamerlid. Meerdere instanties hebben geconstateerd dat het epd oorspronkelijk is opgezet, met name gericht op de professionals en de informatie-uitwisseling tussen professionals, en dat de belangen en de rechtsbescherming van de burger eigenlijk pas in tweede instantie wat meer aan de orde kwamen, onder andere ook bij de behandeling in de Tweede Kamer via verschillende moties. De hele architectuur, het hele ontwerp, is dus opgezet volgens die oorspronkelijke focus op de professional. De vraag is nu of je dat via moties of andere middelen nog kunt herstellen en kunt bewerkstelligen dat die rechten van de burger op een adequate manier in dat systeem worden verwerkt. Hoe kom je erachter of dat überhaupt technisch mogelijk is? Of zou je eigenlijk, als je dat goed wilt regelen, moeten overstappen op zo'n Gesundheitskarte? Zou je dus een heel ander systeem moeten opzetten? Immers, beter ten halve gekeerd dan ten hele gedwaald! Hoe kom je daar nu achter?

De **voorzitter**: Wie achter de tafel voelt zich geroepen om deze hoogst politieke vraag te beantwoorden?
Ik zie dat de heer Wijsman dat wel wil. Hij steekt zijn hand daarvoor niet in het vuur, maar hij steekt zijn hand op.

De heer **Wijsman**: Mijn antwoord is eigenlijk heel eenvoudig. Op het moment dat je een organisatie een systeem laat bouwen waar een probleem mee opgelost moet worden – of dat nu te maken heeft met kindermishandeling, met andere ongelukken in de jeugdzorg, met medische gegevens of met het betalen van reizen – komt er een systeem dat dit probleem ook oplost. Dat gaat ook voorbij aan de belangen van alle andere belanghebbenden. Je ziet dat bijvoorbeeld aan de ov-chipkaart die helemaal in het voordeel is van de vervoerders en waar de belangen van de reizigers achteraan komen. Bij elektronische patiëntendossiers, en ook in het algemeen bij elektronische dossiers, zie je dat het doel waar die dossiers voor gemaakt zijn, voorop staat en dat al het andere bijzaak is. Dan de vraag of je dit per motie tussentijds kunt repareren. Meestal niet. Als dat al mogelijk is, is dat vaak zeer kostbaar. Denk er van tevoren dus goed over na. Wij hebben het beeld van de bloem gebruikt voor de

informatiehuishouding. De bedoeling van dat beeld is juist dat je bij het inrichten van de informatiehuishouding rekening houdt met alle mogelijke belangen en alle mogelijke waarden die de informatie vertegenwoordigt, niet alleen voor degene die het systeem bouwt of wil uitbouwen maar ook voor anderen, zoals klanten en bewijszoekenden. Denk daar goed over na. Bij het impact assessment moeten deze zaken zeker meegenomen worden, niet alleen aan het begin van de rit maar ook tijdens de rit, bijvoorbeeld bij de gateway reviews.

De **voorzitter**: Professor Franken en de heer Munnichs hebben zich gemeld.

De heer **Franken** (CDA): Op de politieke vraag zou ik nog geen antwoord willen geven, maar ik wil de vraag iets algemener stellen. Daarvoor zijn hier deskundigen aanwezig. Is de technische normalisatie – dan denk ik dus aan NEN-normen en ISO-standaarden – in zekere zin al ontwikkeld, zodat die ook bij de bouw van dit soort systemen gehanteerd kan worden? Zo ja, in hoeverre?

De **voorzitter**: Kan en wil de heer Munnichs die vraag meteen beantwoorden?

De heer **Munnichs**: Van dat laatste heb ik geen verstand, maar ik wil wel iets zeggen over de inrichting van het epd. Die inrichting illustreert heel mooi dat er voor- en nadelen zitten aan ontwerpkeuzes. Als je een systeem inricht dat de communicatie tussen zorgverleners optimaal moet ondersteunen en faciliteren, is dat een ander doel dan het op een inzichtelijke manier inzage geven aan de patiënten in de medische dossiers. De neiging bestaat wel eens om ICT-systemen als een soort black box op te vatten waaraan je willekeurige politieke doelen kunt ophangen. Dat kan niet altijd: de doelen kunnen strijdig worden, waardoor je op een andere manier over zo'n systeem moet nadenken. Het antwoord op de vraag over de NEN-normen moet ik schuldig blijven.

De **voorzitter**: Misschien mevrouw Prins?

Mevrouw **Prins**: Het concrete antwoord kan ik niet geven, maar ik kan wel een tip geven voor het vinden van het antwoord. Het antwoord is namelijk te vinden bij het Forum Standaardisatie. Ik zag de heer Bronkhorst, lid van dat forum, op de tribune. Ik weet ook 100% zeker dat het hoofd van het Bureau Forum Standaardisatie, Peter Waters, daar telefonisch antwoord op kan geven.

De **voorzitter**: Er zijn twee aanmeldingen: eerst de heer Kohnstamm en dan de heer Wijsman.

De heer **Kohnstamm**: Ik weet het antwoord over de NEN- en ISO-normen niet precies, maar ik weet wel dat wij in sommige van onze handhavingszaken NEN- en ISO-normen expliciet gebruiken als normstelling en lat waarlangs wij de door ons gevonden feitelijkheden leggen en dus ook met lasten onder dwangsom komen. Daarbij wordt de NEN-norm als richtinggevend gebruikt. Ik weet eerlijk gezegd niet uit mijn hoofd of dat ook geldig is voor het epd. Een verbouwing van een systeem op twee heel verschillende invalshoeken en doelstellingen vergt overigens dat je het systeem buitengewoon zorgvuldig tegen het licht moet houden om te zien of het aan die beide elementen kan voldoen. Bij de vraagstelling dacht ik aan een uitdrukking, volgens mij van oud-collega Hannie van Leeuwen, die ooit iets heeft gezegd over straaljagers. Volgens mij koop je bij motie ook niet direct een nieuwe informatiearchitectuur.

De **voorzitter**: Mevrouw Van Leeuwen werd «straaljager-Hannie» genoemd, maar die uitspraak over het kopen van straaljagers was van de heer Vredeling: «Congressen kopen geen straaljagers». Dat is een stukje parlementaire geschiedenis.

De heer **Wijsman**: Er zijn enkele normensets beschikbaar om systemen aan te toetsen, maar die zijn vaak redelijk domeinspecifiek. Voor informatiebeveiliging zijn er enkele normensets en criteria. Het Amerikaanse ministerie van defensie heeft zijn eigen normensets en iedereen die wil leveren aan het ministerie moet aan die normen voldoen. Ik denk overigens niet dat je het met die normensets oplost. Ze zijn namelijk heel erg specifiek. Fouten aan elektronische patiëntendossiers, verwijsindexen en ov-chipkaarten kunnen burgers en Kamerleden door logisch nadenken heel gemakkelijk zelf ontwaren. Met die normensets schiet je wat dat betreft weinig op. Bovendien bestaat het risico dat je een vals gevoel van veiligheid creëert. Het elektronisch patiëntendossier is misschien niet van buitenaf in te zien, maar dan heb je nog niets gedaan aan het feit dat binnen de organisatie veel te veel mensen geautoriseerd zijn. Normensets? Prima. Maar wees je er wel van bewust wat ze precies toetsen. Je moet niet met een kanon op een mug schieten.

De **voorzitter**: Tussen neus en lippen door heb ik begrepen dat wij als Eerste Kamerleden onvoldoende logisch nagedacht hebben.

De heer **Hamel** (PvdA): Bij de Belastingdienst was 25% van de dossiers niet op orde. Klopt dat?

De heer **Meijer**: Bij de Belastingdienst geldt de interne norm dat 75% van de dossiers op orde moet zijn. Die wordt gemiddeld genomen in de belastingregio's en qua belastingmiddelen niet gehaald.

De heer **Hamel** (PvdA): Als een dossier op orde is, klopt het dan? Iedereen praat over gegevensverzameling, maar je moet het ook hebben over het gegeven dat een aantal gegevens statistisch per definitie onjuist is. Dat speelt ook bij het elektronisch patiëntendossier. Iedereen heeft het over veiligheid, maar wat is ongeveer de foutenscore?

De heer **Meijer**: Een foutenscore kan je niet in een percentage vangen. Het dossier moet in voldoende mate op orde zijn en dat wordt getoetst volgens een bepaald protocol. Er valt natuurlijk wel iets te zeggen over de vraag wanneer een dossier 100% op orde is, maar dat 75% van de dossiers op orde is en 25% blijkbaar niet, zegt niets over de mate waarin die laatste categorie niet op orde is. Daar kun je niet getalsmatige gegevens over verstrekken.

De heer **Wijsman**: Ik geloof dat de vraag iets anders luidde. Een dossier is pas op orde als het compleet en juist is.

De heer **Hamel** (PvdA): Ik vraag mij af of dat klopt. Is dat nagegaan toen de doelstelling van 75% werd vastgesteld? Los daarvan, het ging mij er veel meer om dat onjuiste gegevens de privacyrisico's alleen maar vergroten. Er kunnen gegevens rondgaan die niet kloppen: men heeft iets niet gedaan of men heeft nooit een bepaalde bloedwaarde gehad. Het valt mij op dat dit onderdeel in de discussie weinig naar voren komt.

De heer **Kohnstamm**: Dat hangt af van de soort discussie af. Bij biometrie in paspoorten zijn veel cijfers bekend over vals-positief en vals-negatief. Daarnaar kun je per dossier wel degelijk onderzoek doen. Soms wordt dit gegeven in de discussie intensief gebruikt om iets tegen

te gaan of om zaken te veranderen. Hoe dat zit bij het elektronisch patiëntendossier weet ik niet.

De heer **Hamel** (PvdA): Het gaat mij nu niet om het elektronisch patiëntendossier, maar is duidelijk wat er aan fouten in zit? Vroeger kon je er per omvang van het gegevensbestand met behulp van de statistiek wel een redelijke slag naar slaan.

De heer **Hustinx**: Ik weet dat in de loop van de tijd onderzoeken zijn gedaan naar de kwaliteit van gegevensbestanden. Dat was bijvoorbeeld bij de bevolkingsboekhouding het geval. Men wist op een goed moment hoe laag het percentage fouten was. Dit had natuurlijk alles te maken met de feedback op voorkomende fouten. Voor het bsn werd ingevoerd, was ook sprake van de hoeveelheid mogelijk valse sofinummers die in omloop waren. Dat soort gegevens is er wel, maar systematisch onderzoek naar de juistheid van gegevensbestanden is schaars. Ik weet dat er onderzoek is gedaan naar de gegevens van het Schengeninformatiesysteem in het kader van de grenscontroles. De uitkomsten waren nogal schrikbarend en als je die extrapoleert, weet je zeker dat er heel veel ruis zit in die systemen. Dat verklaart weer dat je het kleinschalig moet houden, dat je feedback moet inbouwen. Hoe meer koppeling, hoe meer je die dingen vermenigvuldigt. Dat is de les, maar het is buitengewoon lastig om dat te kwantificeren.

De **voorzitter**: Dank u zeer. Het is acht uur geweest. Ik constateer dat wij een buitengewoon informatierijke en vruchtbare bijeenkomst hebben gehad. Zoals u hebt gezien, hebben onze stenografen daarvan nauwkeurig aantekening gehouden. Het stenografisch verslag wordt gepubliceerd en is straks voor een ieder terug te vinden bij de parlementaire stukken van de Eerste Kamer, ook voor hen die hopelijk niet te veel aantekeningen hebben gemaakt op de tribunes, want dat zou dan voor een deel overbodig werk zijn geweest.
Hartelijk dank voor uw bijdrage, in de eerste plaats uiteraard de mensen achter de regeringstafel. Ik zal, nadat ik de vergadering heb gesloten, hen de bekende fantasieloze attenties van de Eerste Kamer – even saai als het werk dat wij hier doen – overhandigen. Ik nodig u en de andere aanwezigen, ook de ambtenaren, uit om nog even een kop koffie of eventueel iets anders in de hal te drinken.
Ik dank u nogmaals hartelijk voor uw bijdrage. Wij zullen als leden van deze Kamer daarmee ons voordeel doen en dit geldt zeker ook voor onze opvolgers.
Zeer bedankt. De vergadering is gesloten.

Sluiting 20.05 uur.

Lijst met afkortingen

ANPR Automatic Number Plate Recognition
APAC-landen Asia Pacific landen
Awb Algemene wet bestuursrecht
BSN Burger Service Nummer
CBP College Bescherming Persoonsgegevens
CBS Centraal Bureau voor de Statistiek
CIO Chief Information Officer
CPB Centraal Planbureau
EDP Electronic Data Processing
ekd Elektronisch kinddossier
epd Elektronisch patiëntendossier
EVRM Europees Verdrag voor de Rechten van de Mens
GBA Gemeentelijke Basis Administratie
ICT Informatie- en communicatietechnologie
ISO Internationale Organisatie voor Standaardisatie
IT Informatietechnologie
LSP Landelijk schakelpunt
NEN NEderlandse Norm
OECD/OESO Organisatie voor Economische Samenwerking en Ontwikkeling
PNR Passenger Name Records
PETS Privacy enhancing technologies
PIA Privacy impact assessments
PID Public Interest Determinations
PNR Passenger Name Record
RFID Radio Frequency IDentification chips
SIOD Sociale Inlichtingen- en Opsporingsdienst
SIS Schengen Informatie Systeem
SWIFT Society for Worldwide Interbank Financial Telecommunication
UZI Unieke Zorgverlener Identificatie
Wabo Wet algemene bepalingen omgevingsrecht
Wbp Wet bescherming persoonsgegevens

[1] Samenstelling: Holdijk (SGP), Dölle (CDA), Van de Beeten (CDA), Broekers-Knol (VVD), Eigeman (PvdA), Kox (SP), voorzitter, Staal (D66), Franken (CDA), vice-voorzitter, Van Bijsterveld (CDA), Duthler (VVD), Van Kappen (VVD), Haubrich-Gooskens (PvdA), Meurs (PvdA), K.G. de Vries (PvdA), Peters (SP), (PvdA), Reuten (SP), Vliegenthart (SP), Kuiper (CU), Lagerwerf-Vergunst (CU), Böhler (GL), Strik (GL), Koffeman (PvdD), Yildirim (Fractie-Yildirim), Tiesinga (CDA) en Knip (VVD).

[2] Samenstelling: Holdijk (SGP), Bemelmans-Videc (CDA), Dölle (CDA), Meindertsma (PvdA), Eigeman (PvdA), Putters (PvdA), vice-voorzitter,Kox (SP),Ten Hoeve (OSF), Westerveld (PvdA), Engels (D66), Van Bijsterveld (CDA), Hendrikx (CDA), De Vries-Leggedoor (CDA), Duthler (VVD), Hermans (VVD), voorzitter, Van Kappen (VVD), Schaap (VVD), K.G. de Vries (PvdA), Ten Horn (SP), Quik-Schuijt (SP), Vliegenthart (SP),De Boer (CU), Lagerwerf-Vergunst (CU), Böhler (GroenLinks),Laurier (GL), Koffeman (PvdD) en Yildirim (Fractie-Yildirim).

[3] Samenstelling: Holdijk (SGP), Dölle (CDA), Tan (PvdA), Van de Beeten (CDA), voorzitter, Broekers-Knol (VVD), Doek (CDA), De Graaf (VVD), Kneppers-Heynert (VVD), Kox (SP), Westerveld (PvdA), vice-voorzitter, Staal (D66), Franken (CDA), Van Bijsterveld (CDA), Janse de Jonge (CDA), Duthler (VVD), Haubrich-Gooskens (PvdA), De Vries (PvdA), Ten Horn (SP), Peters (SP), Quik-Schuijt (SP), Lagerwerf-Vergunst (CU), Böhler (GL), (CDA), Strik (GL), Koffeman (PvdD) en Yildirim (Fractie-Yildirim).

[4] Samenstelling: Schuurman (CU), Holdijk (SGP), Dölle (CDA), voorzitter, Dupuis (VVD), Linthorst (PvdA), Tan (PvdA), vice-voorzitter, Essers (CDA), Meulenbelt (SP), Ten Hoeve (OSF), Leijnse (PvdA), Staal (D66), Thissen (GL), Hamel (PvdA), Goyert (CDA), Leunissen (CDA), Asscher (VVD), Hermans (VVD), Ten Horn (SP), Slager (SP), Vliegenthart (SP), De Boer (CU), Duthler (VVD), Kuiper (CU), Lagerwerf-Vergunst (CU), Laurier (GL), Koffeman (PvdD), Yildirim (Fractie-Yildirim) en Flierman (CDA).

[5] Samenstelling: Werner (CDA), Van den Berg (SGP), Dupuis (VVD), vice-voorzitter, Swenker (VVD), Linthorst (PvdA), Tan (PvdA), Van de Beeten (CDA), Biermans (VVD), Putters (PvdA), Slagter-Roukema (SP), voorzitter, Engels (D66), Thissen (GL), Hamel (PvdA), Goyert (CDA), Leunissen (CDA), De Vries-Leggedoor (CDA), Huijbregts-Schiedon (VVD), Meurs (PvdA), Ten Horn (SP), Peters (SP), Quik-Schuijt (SP), Kuiper (CU), Lagerwerf-Vergunst (CU), Laurier (GL), Koffeman (PvdD), Yildirim (Fractie-Yildirim), Benedictus (CDA). Flierman (CDA) en Knip (VVD).