Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2007–2008

31 200 VI Vaststelling van de begrotingsstaten van het Ministerie van Justitie (VI) voor het jaar 2008

F

VERSLAG VAN DE EXPERTBIJEENKOMST OVER GEGEVENSBESCHERMING VAN DE VASTE COMMISSIE VOOR JUSTITIE VAN DE EERSTE KAMER OP DONDERDAG 20 MAART 2008

Vastgesteld 29 mei 2008

De vaste commissie voor Justitie van de Eerste Kamer heeft op 20 maart 2008 een expertbijeenkomst over gegevensbescherming gehouden.

Van deze bijeenkomst brengt de commissie bijgaand stenografisch verslag uit.

De voorzitter van de vaste commissie voor Justitie,
Van de Beeten

De griffier van de vaste commissie voor Justitie,
Van Dooren

KST118933
ISSN 0921 - 7363
Sdu Uitgevers
's-Gravenhage 2008

Aanvang 14.00 uur

Aanwezig namens de Eerste Kamer: de leden Van de Beeten (CDA), Broekers-Knol (VVD), Van Bijsterveld (CDA), Franken (CDA), Haubrich-Gooskens (PvdA), Janse de Jonge (CDA), Lagerwerf-Vergunst (Christen-Unie), Peters (SP), Quik-Schuijt (SP), Strik (GroenLinks), Tan (PvdA), Ten Horn (SP) en Westerveld (PvdA), mevrouw Van Dooren (plaatsvervangend griffier) en de heer Breitbarth (stafmedewerker).

Overige aanwezigen: mevrouw Azough (Tweede Kamer, GroenLinks), de heer Bosma (Adviescommissie Informatiestromen Veiligheid), de heer Broeders (Universiteit Maastricht), de heer Brom (Rathenau Instituut), mevrouw V.H. Brouwer (College Bescherming Persoonsgegevens), mevrouw E.R. Brouwer (Universiteit Utecht), de heer Van Brummen (Openbaar Ministerie), de heer Buruma (Radboud Universiteit Nijmegen), de heer Çörüz (Tweede Kamer, CDA), mevrouw Dekkers (Regioplan), de heer Dijstelbloem (Rathenau Instituut), de heer Van Haersma Buma (Tweede Kamer, CDA), de heer Heerts (Tweede Kamer, PvdA), mevrouw Van den Heuvel (Rathenau Instituut), de heer Hijmans (Europees Toezichthouder Gegevensbescherming), de heer Van 't Hof (Rathenau Instituut), de heer Hustinx (Europees Toezichthouder Gegevensbescherming), mevrouw In 't Veld (Europees Parlement, D66), de heer Jacobs (Radboud Universiteit Nijmegen), mevrouw Jonker (Tweede Kamer, CDA), mevrouw Kets (Rathenau Instituut), de heer Kohnstamm (College Bescherming Persoonsgegevens), mevrouw Kröner (College Bescherming Persoonsgegevens), mevrouw Kuiken (Tweede Kamer, PvdA), de heer Muijen (Openbaar Ministerie), de heer Munnichs (Rathenau Instituut), mevrouw Van der Ploeg (Hogeschool Zuyd), mevrouw De Poot (WODC), mevrouw Prins (Universiteit van Tilburg en WRR), de heer Staman (Rathenau Instituut), de heer Teeuw (Telematica Instituut) en de heer De Vries (voormalig Europees Coördinator Terrorismebestrijding).

De heer **Van de Beeten** (CDA): Dames en heren, namens de vaste commissie voor Justitie heet ik u van harte welkom, mede namens het Rathenau Instituut, dat een belangrijke inhoudelijke bijdrage heeft geleverd aan de voorbereiding van deze bijeenkomst. Ik heet in het bijzonder de deskundigen welkom. Zij zullen straks ongetwijfeld door professor Buruma nog eens in het bijzonder welkom worden geheten. Hem heet ik zeer bijzonder welkom, omdat hij bereid is gebleken om vandaag als dagvoorzitter op te treden. Hij staat garant voor een flitsend debat over de aangedragen thema's.
Ik ben 27 jaar geleden begonnen als plattelandsadvocaat in Zevenaar. In die tijd was het nog zo dat informatie die werd verkregen van verzekeraars, bankiers en de overheid, door rechters altijd voor waar werd aangenomen. Wat je uit die hoek kon verwachten, was buitengewoon betrouwbaar. Dat gold in het bijzonder voor een ambtseed of voor processen-verbaal, hoewel de meer ervaren rechters het altijd wel roken als er iets niet helemaal pluis was met processen-verbaal. Ik heb ervaren dat rechters inmiddels aanzienlijk kritischer zijn geworden over informatie die wij van de zojuist genoemde bronnen verkrijgen. Dat is een heel leerproces geweest waarin de advocatuur natuurlijk ook een rol heeft gespeeld. Zoals professor Buruma als geen ander weet, is dat leerproces nog volop gaande, bijvoorbeeld op het punt van deskundigenberichten waarover rechters zich een oordeel moeten vormen.
Als ik als advocaat een zaak heb tegen een Amsterdamse advocaat, kan ik er bijna zeker van zijn dat de eiser altijd een heel summiere dagvaarding krijgt – hoewel de rechtsvordering daar tegenwoordig andere eisen aan stelt – en dat de verweerder altijd een overmaat aan informatie krijgt om hem in de positie te manoeuvreren dat hij zoveel mogelijk moeilijkheden ondervindt in de procedure. Als ik te maken krijg met een eis in recon-

ventie, word ik altijd – zoals dat tegenwoordig gebruikelijk is twee weken voor de mondelinge behandeling – weer met een enorme hoeveelheid informatie overladen. Ook de rechter moet trouwens maar wijs zien te worden uit die informatie.
Informatie wordt ook vaak gevraagd. De bankier van mijn bijna 85-jarige moeder heeft mijn moeder voorzien van een reeks brieven waarin gevraagd werd om een kopie van haar identificatiebewijs. Zij had al jaren geen paspoort meer. Het identificatiebewijs dat zij ooit voor haar laatste buitenlandse vakantie had aangevraagd, was allang verlopen. Ik heb de bank vervolgens meerdere brieven gestuurd om aan te geven dat mijn moeder echt niet van plan was om een identificatiebewijs aan te schaffen ten behoeve van de paar rekeningetjes die zij had, onder andere spaarrekeningen voor mijn kinderen. Toch werd ik regelmatig gemaand dat dat moest gebeuren, totdat uiteindelijk een heel vriendelijke mevrouw van de bank opbelde om te zeggen dat het niet meer hoefde en dat men had aangetekend dat het wel goed was. Toen het goed was, kreeg zij vervolgens brieven dat er vanwege de spaarrekeningen voor de kinderen een door de ouders ondertekend formulier moest zijn, met een opgave van het fiscale nummer van de ouders, want dat had men nodig voor de financiële administratie. Dat alles – zowel de brieven over het identificatiebewijs als de brieven met betrekking tot mijn fiscale nummer – werd gemotiveerd met het argument dat het op grond van de wetgeving ter bestrijding van terrorisme noodzakelijk was om zicht te hebben op wat mijn moeder daar allemaal spaarde.
Informatie is een buitengewoon belangwekkend onderwerp waar wij ook als wetgever – zowel leden van de Tweede Kamer als van de Eerste Kamer – regelmatig mee te maken krijgen. De ambitie van deze bijeenkomst is vrij hoog. Er wordt gesproken over het formuleren van criteria aan de hand waarvan wij de problematiek als medewetgever zouden moeten proberen te hanteren. Ik zou al heel blij zijn als wij uit deze bijeenkomst een aantal gezichtspunten zouden kunnen overhouden die wij hierbij in het bijzonder zouden kunnen hanteren. Niettemin hebben wij goede hoop dat de vele deskundigheid die hier vandaag verzameld is, ons daarbij zeer behulpzaam zal zijn. Zoals gezegd, gebeurt dat onder de inspirerende leiding van de heer Buruma. Wij wensen u een heel plezierige en – ook voor ons als Kamerleden – heel nuttige bijeenkomst toe.
Ik sluit af met een enkel dankwoord. Ik bedank allereerst de medewerkers van het Rathenau Instituut voor hun buitengewoon belangrijke bijdrage aan de voorbereiding. Ik bedank verder de medewerkers van de Griffie van de Eerste Kamer en de overige ondersteuning. Verder ben ik dank verschuldigd aan de leden van de werkgroep. Van hen moeten wij vandaag één lid missen en wel Anne-Wil Duthler, omdat zij vorige week dinsdag moeder is geworden. Daarmee heeft zij een voor deze Kamer unieke situatie geschapen, want zij is het eerste zittende lid van de Eerste Kamer dat een kind ter wereld heeft gebracht. Uiteraard verheugen wij ons allemaal zeer over deze gebeurtenis.
Helemaal tot slot een huishoudelijke mededeling: ik zal niet het slotwoord uitspreken. Ik moet namelijk iets eerder weg. Ik vind dat jammer, omdat ik iedereen ook graag persoonlijk had bedankt. Aan de andere kant vind ik het verheugend, omdat mij daardoor de plicht ontvalt om hetzij met ironie hetzij met humor als dank een aantal fantasieloze cadeaus aan de sprekers aan te bieden. Deze taak zal worden overgenomen door Mies Westerveld en Hans Franken. Ik wens hen daarbij heel veel succes.
Ik geef het woord aan professor Buruma.

De heer **Buruma**: Dames en Heren. Ik vind het heel bijzonder om in dit gewijde gebouw te mogen staan, een gebouw waarin al heel veel eeuwen politiek wordt bedreven. Het is echt fantastisch om de microfoon vast te mogen houden in het centrum van de activiteiten van de Eerste Kamer. Medewerkers van de Eerste Kamer en het Rathenau Instituut hebben een

schema opgesteld voor deze middag. Wij zullen dat schema zo goed mogelijk volgen. Het is de bedoeling dat een aantal deskundigen u iets zal vertellen over de databanken. Mij is nadrukkelijk gevraagd om ervoor te zorgen dat hetgeen zij vertellen, zo concreet mogelijk is. Het is namelijk aan ons om te proberen de leden van de Eerste en de Tweede Kamer te wijzen waar voor hen een taak zou kunnen liggen in de wereld van de informatica en de databanken. Het is met andere woorden de bedoeling om hen handvatten te geven voor hun optreden bij al die onderwerpen die hiermee te maken hebben.
In deze zaal hebben zich zo veel superspecialisten verzameld dat ik hen bij voorbaat mijn excuses aanbied. Ik doe dat, omdat ik nu al weet dat ik velen van hen tekort ga doen, doordat ik zo meteen ongetwijfeld heel vaak moet zeggen: Sorry, het was interessant wat u zei, maar wij moeten weer door! Het moet een snelle en doortastende discussie worden en dat betekent dat ik zelf ook niet te lang moet spreken.
Zo dadelijk zullen vijf deskundigen plaatsnemen achter de tafel die eigenlijk is bedoeld voor leden van de regering. Voordat het zo ver is zal er een korte inleiding worden gehouden over het eerste thema van vanmiddag. Dat is overigens ook het hoofdthema of, zo u wilt, het overkoepelende thema van de databanken. Deze inleiding zal worden gehouden door de heer Munnichs, een medewerker van het Rathenau Instituut.
Na de inleiding van de heer Munnichs zal ik het woord geven aan de deskundigen. Ik waarschuw hen echter dat wij vandaag te maken hebben met parlementariërs, van wie de hoofdreden van bestaan praten is. Ik herinner mij nog heel goed dat Maarten van Traa een keer op mij toe stapte toen ik voor zijn enquêtecommissie werkte. Ik had juist een hele nacht doorgewerkt, maar hij zei: kom, wij gaan nu echt werken. En wat bedoelde hij daarmee? Praten!
Parlementariërs horen te praten en dat betekent dat wij hen vanmiddag de gelegenheid moeten geven in te breken in andermans bijdrage. Ik zal proberen om het zo te organiseren dat ze de deskundigen hun punt laten maken, maar op een zeker moment, waarschijnlijk halverwege hun bijdrage, zal ik hen toestaan om vragen te stellen. Zij zullen dit doen ter verduidelijking, maar ook om te zien op welke punten de deskundigen van mening verschillen. U weet nu hoe wij de middag voor ons zien en ik geef dan ook met plezier het woord aan de heer Munnichs voor zijn inleiding over het eerste thema, de databanken.

Casuspositie I: Gebruik van databanken

De heer **Munnichs**: Dank u wel. Mijn naam is Geert Munnichs en ik werk bij het Rathenau Instituut. De medewerkers van het Rathenau Instituut zullen bij iedere sessie een korte inleiding verzorgen. Ik begin met het gebruik van databanken.
In de strijd tegen misdaad en terreur zijn de bevoegdheden van politie en justitie de afgelopen jaren drastisch uitgebreid. De belangrijkste ontwikkeling is dat opsporings- en veiligheidsdiensten in toenemende mate gebruikmaken van allerlei gedigitaliseerde databestanden. Daarbij gaat het niet alleen om eigen bestanden, zoals politieregisters, maar ook om externe databanken, zoals die van de Belastingdienst, de Kamer van Koophandel, de bibliotheek of de internetprovider. Deze bestanden kunnen aan elkaar worden gekoppeld en met computerprogramma's worden geanalyseerd. Dit heet datamining.
Een belangrijke trend hierbij is een preventieve inzet hiervan. Aan de hand van risicoprofielen worden bestanden doorgeploegd op zoek naar patroonafwijkingen en potentieel verdacht gedrag. De bedoeling hiervan is, in een zo vroeg mogelijk stadium crimineel gedrag of voorbereidende terroristische handelingen op te sporen. Omdat misdaad- en terreurorganisaties in toenemende mate gebruikmaken van de mogelijkheden van ICT, kunnen politie en justitie op dit gebied moeilijk achterblijven. Dit

niet kunnen achterblijven is een belangrijke beweegreden voor veel bevoegdheidsuitbreidingen van de afgelopen jaren. Ook op EU-niveau valt een groeiend gebruik van databanken waar te nemen. Ik noem het Schengeninformatiesysteem, dat gegevens bevat van ongewenst verklaarde vreemdelingen, en Eurodac, dat vingerafdrukken bevat voor de identificatie van asielzoekers. Er is ook sprake van een toenemende uitwisseling tussen EU-lidstaten van nationale politieregisters of DNA-databanken. Verder vindt gegevensuitwisseling plaats met derde landen, zoals vluchtgegevens die aan de Verenigde Staten worden verstrekt. Kortom, onze veiligheid wordt in toenemende mate een digitaal bewaakte veiligheid.
Bij deze ontwikkeling passen een aantal kanttekeningen. Ik baseer mij hierbij onder meer op het rapport *Data voor daadkracht* van de commissie-Bosma. De eerste kanttekening betreft de bestandsvervuiling die een reëel probleem vormt. Spelfouten en naamsverwisselingen kunnen ertoe leiden dat een onschuldige burger een verdachte wordt: een vals positief resultaat. Daarnaast laat de beveiliging van databestanden nogal eens te wensen over. Ik wijs op de recente incidenten in Engeland, waar gegevens van miljoenen Britten op straat lagen, op de problemen rond de invoering van de OV-chipkaart en op de Mifare-affaire die deze week speelde. Hiermee samenhangend vormt de identiteitsdiefstal een groeiend probleem. De vraag is wat dat betekent voor de invoering van een maatregel als het burgerservicenummer. Een derde aandachtspunt betreft de effectiviteit van datamining. Het koppelen van bestanden leidt in de praktijk meer dan eens tot een overvloed aan data. Zo heeft het Amerikaanse State Department een lijst met 100 000 mogelijke terreurverdachten. Zijn dat nog werkbare aantallen? Hierbij moet worden bedacht dat computeranalyses platte data opleveren die losgekoppeld zijn van hun oorspronkelijke context en die derhalve altijd nog nadere interpretatie behoeven met behulp van human intelligence. Daarnaast is het de vraag of er voldoende waarborgen bestaan voor de rechtsbescherming van burgers. Welke mogelijkheden heeft een burger om in beroep te gaan tegen een verdenking van crimineel of terrorist? Als iemand eenmaal op een lijst met terreurverdachten staat, kan hij dat dan nog aanvechten? Specifiek voor de databanken op EU-niveau komt daar nog bij dat verschillende lidstaten verschillende registratiecriteria hanteren en dat een uniform stelsel van gegevensbescherming ontbreekt.
Eigenlijk komen twee centrale aandachtspunten naar voren. Het eerste punt betreft de rechtsbescherming van burgers. Daarbij is te denken aan risico's van bestandsvervuiling en identiteitsdiefstal waardoor burgers ten onrechte verdacht kunnen worden. Een en ander hangt echter ook samen met de mogelijkheden om een verdenking aan te vechten en om in beroep te gaan tegen de plaatsing op een lijst.
Het tweede centrale aandachtspunt is de effectiviteit van het gebruik van databanken. Dit hangt eveneens samen met het risico van bestandsvervuiling en ID-diefstal, maar ook met de vraag hoe gericht of ongericht dit soort bestanden wordt doorzocht. Daaraan gekoppeld speelt de vraag of dit daadwerkelijk bijdraagt aan de strijd tegen misdaad en terreur; zie de lijst met honderdduizend mogelijke verdachten. Is dat werkbaar? De drie discussiestellingen hangen direct samen met deze aandachtspunten.
Ten slotte wil ik kort stilstaan bij de effectiviteitsvraag. Deze vraag wordt vaak gesteld vanuit de privacyhoek; wegens de mogelijke inbreuk op de privacy waarmee maatregelen als datamining gepaard gaan. De effectiviteitsvraag is echter net zo relevant vanuit opsporingsperspectief. Het gaat om de vraag of ze doen wat ze moeten doen. Dat is zeker van belang als je let op de hoeveelheid geld en menskracht die met dergelijke maatregelen is gemoeid.

De heer **Buruma**: Dank u wel, mijnheer Munnichs.
Ik nodig nu de deskundigen van de eerste ronde uit om achter de tafel

plaats te nemen: mevrouw Evelien Brouwer, universitair docent aan de Universiteit Utrecht en onder meer deskundige op het gebied van alles wat met het Schengeninformatiesysteem te maken heeft; de heer Peter Hustinx, Europees Toezichthouder Gegevensbescherming; de heer Bart Jacobs, hoogleraar computerbeveiliging aan de Radboud Universiteit Nijmegen; de heer Peter Muijen, Officier van Justitie en mevrouw Christianne de Poot, onderzoeker bij het WODC.
Het onderwerp is databanken. Er zijn drie stellingen opgevoerd. Ik zal steeds twee deskundigen vragen op een stelling te reageren. Vervolgens kunnen de andere deskundigen er iets over zeggen, maar de eerste twee hebben dan iets meer de tijd om het een en ander te vertellen. De anderen worden geacht het iets korter te houden. Vervolgens krijgen ook de mensen in de zaal de gelegenheid te reageren.
De stellingen zijn bedoeld als handvat. Het gaat er uiteindelijk om dat wij criteria vinden voor de Kamerleden. De stellingen zijn soms wat grofkorrelig, maar vormen een goed startpunt voor de discussie. Over de eerste stelling wil ik graag vooral de heren Jacobs en Hustinx aan het woord laten. Die eerste stelling luidt als volgt:
«De risico's van incorrecte data en identiteitsfraude zijn te groot voor een verantwoord gebruik van databanken en gegevensuitwisseling».
Zoals het er staat, kunnen wij er niets mee: de risico's zijn te groot voor verantwoord gebruik. Die stelling gaat dus heel ver, maar laten wij beginnen met te bezien wat de risico's zijn met de databestanden. Professor Jacobs, u hebt veel verstand van wat je mis kunt doen en zelfs bewust mis kunt doen met computers, stemlokalen, ov-chips en dergelijke. U hebt met uw team met enige regelmaat in de krant gestaan. Welke risico's ziet u met uw «computerologische blik»? Wat kunt u daarover vertellen waar de Kamerleden iets aan hebben?

De heer **Jacobs**: Er zijn wel degelijk risico's. In de stelling staat dat de risico's te groot zijn, maar ik denk dat «te» niet terecht is. Als veel gegevens centraal worden verzameld, kunnen zij worden misbruikt door degenen die ze beheren. Zij kunnen bijvoorbeeld onder druk worden gezet om de gegevens prijs te geven. Neem bijvoorbeeld de kilometerheffing in Nederland. Als van alle auto's de vervoersbewegingen centraal worden geregistreerd, maak je mensen kwetsbaar. Voor kwaadwillenden zal het bijvoorbeeld interessant zijn om te weten waar politici zich op welk moment bevinden, om iets gerichter een aanslag te kunnen laten plaatsvinden.
Dus een algemeen punt dat hierbij op de achtergrond speelt is dat privacybescherming belangrijk is voor de persoonlijke veiligheid van mensen. Daarom moet er zorgvuldig met gegevens in databanken worden omgegaan. Eigenlijk kun je in Nederland tot op dit moment niet spreken van grootschalige identiteitsfraude, maar de risico's nemen de komende jaren wel snel toe vanwege een aantal mechanismen die wij aan het invoeren zijn, waardoor gegevens gemakkelijker kunnen worden gekoppeld. Ik denk aan het burgerservicenummer. Als zo'n nummer gecompromitteerd raakt en in veel sectoren gebruikt wordt, kan iemand daar ook in al die sectoren misbruik van maken.

De heer **Buruma**: Dit is belangrijk. U zegt dat door de koppeling identiteitsfraude gemakkelijker wordt.

De heer **Jacobs**: Laat ik een voorbeeld geven. In Nederland loopt natuurlijk een flink aantal mensen om wat voor een reden dan ook onverzekerd rond. Zij willen mogelijk op uw verzekering gebruikmaken van medische zorg. Dat kan als die zorg aan het burgerservicenummer is gekoppeld. Dan moeten zij zich identificeren als zij in een ziekenhuis komen. Hoe zou een kwaadwillende dat aanpakken? Zelf zou ik een kopie van mijn paspoort maken, daarin een ander burgerservicenummer «photoshoppen» en

daarmee naar het ziekenhuis gaan. Daar zal wellicht gezegd worden: «u hebt uw origineel niet bij zich». Dan zeg ik: «ja, ik ben het al drie keer kwijtgeraakt, dus sindsdien draag ik een kopie bij me». Dit werkt overal. Waarom doet u nu zo moeilijk? Denkt u dat ik binnenkom?

De heer **Buruma**: Ja.

De heer **Jacobs**: Ik denk ook dat ik daar geholpen word. Misschien heb ik wel een andere bloedgroep dan degene op wiens naam ik daar zorg krijg. Die komt misschien in het dossier van die persoon terecht. De volgende keer dat die persoon in de medische sector terechtkomt, krijgt die misschien op een verkeerde manier bloed toegediend. Waar ligt dat aan? Mijns inziens speelt de koppeling daarin een belangrijke rol in, want als het allemaal gecompartimentaliseerd is, heb je dit soort problemen minder.

De heer **Buruma**: Maar u waarschuwt dus vooral tegen de koppeling van de verschillende bestanden.

De heer **Jacobs**: Ja, al heeft de koppeling voordelen omdat je dingen kunt opsporen. Zij heeft alleen ook nadelen. Nadelige effecten propageren zich ook door al die systemen heen. Daar moet je een balans in zien te vinden. Dat is moeilijk.

De heer **Buruma**: De voorbeelden van de veiligheid van de chauffeur van de politicus en van de politicus zelf die op de weg in gevaar kan komen als iedereen weet waar die rondrijdt en van het geheel dat door de koppelingen kwetsbaarder wordt, zijn feitelijk heldere voorbeelden. Nu ga ik naar de juridische blik waarmee er naar deze problematiek kan worden gekeken. Mijnheer Hustinx, u bent Europees toezichthouder gegevensbescherming en u hebt wat dat betreft ongetwijfeld een blik vanuit heel Europa. Op allerlei verschillende manieren wordt daar over de gevaren van databanken en dergelijke nagedacht. Wat zijn volgens u de meest in het oog springende punten om rekening mee te houden, mocht er ooit iets wat verband houdt met databanken aan de orde zijn in de Kamer?

De heer **Hustinx**: Als concreet feit is aan de orde dat in de afgelopen 25 à 30 jaar in alle landen van Europa een gemeenschappelijk stelsel van regels en principes is ontwikkeld. In Nederland praten wij daarover als ware het privacyrecht, maar eigenlijk zijn het verkeersregels voor het gebruik van databanken. Als wij praten over verantwoord gebruik van databanken, doen wij dat mede op basis van die regels. Die zijn er niet voor niets; die zijn er in belangrijke mate ook voor om dit goed te laten aflopen.
Ik geef enkele concrete voorbeelden. Gegevensuitwisseling kan nooit beter zijn dan de gegevens die je in databank 1 invoert en die naar databank 2 moeten gaan. Het is een bekend probleem dat er grote kwaliteitstekorten zijn. Hoe weten wij of een gegeven juist is? «Dat zei hij». Hebben wij vastgelegd? «Ja, hij zei dat». Toen wij in het verleden onderzoek bij politie- en inlichtingendiensten deden, was er een groot tekort aan verantwoording van de waarde van de gegevens die erin zaten.
Als je gaat uitwisselen, neemt de hardheid toe. Dat lijkt juist, maar dat is het niet. Je moet er dus context bij geven. Naarmate de schaal van de uitwisseling toeneemt, neemt die context vaak af en verandert de informatie van waarde. Men gaat erop vertrouwen en men krijgt allerlei vervormingen. Dat is een heel groot probleem.
Daaraan vast zit dat de informatie ook alleen maar was verzameld met het oog op een bepaald doel. De doelbinding is een van de principes daarbij. Wanneer die informatie er is, gaat men die echter ook voor andere zaken gebruiken omdat men zegt «het is er toch, daar moet je wat mee».

Daardoor ontstaat een nieuwe tendens, waardoor aan de grondbeginselen van de databescherming, die er ook voor de effectiviteit zijn, schade wordt gedaan.
Mijn voorbeeld komt uit het Schengeninformatiesysteem. Dat is een heel groot systeem waarop wij allen in Europa vertrouwen. Alle lidstaten voeren gegevens in, maar doen dat naar hun eigen praktijk. Zo blijkt bij beschouwing van de rubriek «ongewenste vreemdelingen» dat men daar wel iets in stopt, maar het er niet altijd weer uit haalt. Men verzuimt om dat bij te houden. Er zit dus een heel groot tijdsverloop in.
Zo ontstaan er vervormingen, die eigenlijk het gevolg zijn van een gebrek aan implementatie en toepassing van de regels die er zijn, gevolgd door een gebrek aan gedisciplineerd volhouden om daaraan te blijven werken. Dat geldt zelfs voor de verkeersregels. De veiligheid is nooit groter dan de som van iedereen die zich aan de regels houdt. Dat zie je hier ook. Er is een ontzettend groot vertrouwen in gegevensuitwisseling. Die spanning leidt tot brokken. Dat zien wij gebeuren als de besluitvorming hierover te snel gaat.

De heer **Buruma**: U noemde drie punten. De invoer kan slecht zijn, de informatie is contextloos– waardoor je soms de verkeerde conclusies trekt – en de informatie veroudert. Als wij spreken over het burgerservicenummer of het elektronisch patiëntendossier of het kinddossier, hoe kunnen wij dan iets met deze drie, door iedereen erkende, punten doen?

De heer **Hustinx**: Dat wordt van groot belang wanneer wij spreken over het burgerservicenummer als het vehikel waarmee gegevens worden uitgewisseld. Daarmee wordt uitwisseling gestimuleerd, maar men gaat er ook van uit dat dat gegeven onverbiddelijk op dezelfde persoon betrekking heeft. Voordat de operatie burgerservicenummer werd gelanceerd, was er het sofinummer. Daarvan werd op een goed moment vastgesteld dat er 800 000 dubieuze sofinummers in omloop waren. Dat is niet gering op een bevolking van 15 tot 17 miljoen mensen, met buitenlanders erbij. Dat is een fors percentage van de bevolking.
De oplossingen die toen zijn bedacht om dat beter te doen gingen uit van een sectorgewijze aanpak en kleinschaligheid, door te zorgen dat men die sectoren hielp. Dat sectorgedeelte uit de voorstellen is niet overgenomen door de regering. Men heeft gekozen voor – ik zeg het wat gechargeerd – «eenvoudig en rechtdoor rijden». Daardoor is die grootschaligheid in het burgerservicenummer alleen maar benadrukt. Alle sectoren hebben te maken met datzelfde nummer. In het rapport van de commissie-Van Thijn – oud-lid van deze Kamer – kan men uitgelegd zien waarom dat geen verstandige aanpak was. Daarover heeft het CBP ook grote moeite gehad, zo heb ik begrepen.

De heer **Buruma**: Het logische antwoord na deze twee waarschuwende geluiden brengt met zich mee dat wij even de andere kant op moeten kijken. Je zou denken dat wij al zo veel kunnen. Helaas hebben wij op het laatste moment gehoord dat de heer Van Zunderd ziek is, waardoor hij er vandaag niet bij kan zijn. De heer Van Zunderd is politiechef. Wij gaan er altijd van uit dat het Openbaar Ministerie, zeker waar het de opsporing betreft, leiding geeft aan en gezag heeft over de opsporing. Daarom ga ik ervan uit dat de heer Muijen alles weet van wat de politie in de praktijk niet kan en wat hij ook als officier van justitie ziet.
Dit zijn allemaal waarschuwingen. Het is net alsof wij niet zouden moeten beginnen aan gegevensuitwisseling, omdat de gegevens verouderd kunnen zijn, of omdat die verkeerd kunnen zijn ingevoerd. Als er ook nog een koppeling met andere bestanden plaatsvindt, kan dit leiden tot gigantische problemen. Mijnheer Muijen, waarom zijn deze twee heren te voorzichtig?

De heer **Muijen**: Ik zou dat niet willen beweren, want ik ken beide heren vanuit een andere optiek. Hun gewaardeerde opmerkingen worden ingegeven door zorg. U maakt terecht onderscheid tussen justitie en politie, maar de beginselen, zoals die zijn geformuleerd, zijn inderdaad van toepassing op het werk van justitie en politie. De waarschuwingen die hier naar voren komen, zie je ook terugkomen in de politiepraktijk, maar ik zet het volgende er tegenover. Ik volg deze kwestie vanaf de start van het Korps Rijkspolitie in 1945. Wij werken al sinds jaar en dag met informatie. Ook destijds, als gegevens niet in de juiste context werden geplaatst, kon dat vervelende gevolgen hebben. Met de huidige technologische ontwikkelingen wordt er een extra dimensie aan toegevoegd. Dat ontken ik niet.

De heer **Buruma**: Wat houdt die extra dimensie in? Wij hebben allemaal gehoord van datamining, data matching en data profiling. De definities buitelen over elkaar heen, maar duidelijk is wel dat dit steeds meer gebeurt, ook in relatie tot mensen die nog helemaal niet verdacht zijn, maar wel in een bestand zitten. Vervolgens wordt alles met elkaar vergeleken en dan rollen daar bepaalde zaken uit. Doelt u daarop als u het heeft over de huidige technologische ontwikkelingen?

De heer **Muijen**: Ja. Een concreet voorbeeld. De politie krijgt een melding van een aanrijding. U bent getuige geweest. U wordt gebeld en de politie maakt met u een afspraak. De politie komt vervolgens langs om een getuigenverklaring op te nemen. U als goede burger verleent daar uw medewerking aan. De politieambtenaar die bij u langskomt, kijkt om zich heen en constateert dat u van een student een proefschrift heeft gekregen over iets dat raakt aan pedofilie. De politieambtenaar vindt dat raar, maar misschien ziet hij nog meer in uw interieur dat hem van belang lijkt. De politieambtenaar komt terug op het bureau en muteert een en ander in het systeem, BPS of Multipol, afhankelijk van wat de politie heeft. Hij voegt eraan toe dat hij bepaalde dingen vreemd vond en dat hij dat en dat heeft waargenomen. Hij voegt eraan toe dat het waarschijnlijk niets te betekenen heeft, maar vervolgens is die waarneming wel gekoppeld aan uw naam. Zes maanden later heeft een politieambtenaar in het kader van een ander onderzoek een naam die lijkt op die van u. Dat komt voor, want er gaan getallen rond die erop neerkomen dat de invoergegevens voor 20 tot 30% fout zijn. Vervolgens wordt er met een sleutel gezocht. De politieambtenaar toetst niet de naam «Jansen» in, maar «Jans»? Dan komt ook uw naam te voorschijn, met daarbij die pedofiele verwantschap. Stel dat dit onderzoek ook nog eens betrekking heeft op pedofilie, of kinderporno, dan is de link heel snel gelegd. Dat wil niet zeggen dat u verdachte bent, maar de techniek biedt de mogelijkheid om een breed scala te bekijken. Daar ben ik positief over. Essentieel is wel, maar dat geldt voor politie en justitie, dat de kwaliteit en professionaliteit van het verantwoordelijk bezig zijn met het in de juiste context plaatsen van gegevens overeind blijft. Dat is echter niet altijd het geval.

De heer **Buruma**: U haakt daarmee in feite aan op wat de heer Hustinx aangaf, namelijk dat het kan voorkomen dat er foutief wordt ingevoerd. Misschien gebeurt het ook wel vaker, want u noemde die 20 tot 30%. Ik vind dat niet verbazingwekkend, maar er moet wel verstandig mee worden omgegaan. De agent die de gegevens heeft ingevoerd, schreef er nadrukkelijk bij dat de pedofiliescriptie die hij aantrof niets hoeft te betekenen, maar de volgende agent, een andere, ziet de term pedofilie staan, kijkt naar de naam van de persoon en denkt: «Hm...». Degene die de gegevens heeft ingevoerd, is een ander dan degene die de gegevens gebruikt. Wat voor maatregelen heeft uw organisatie genomen om te voorkomen dat de tweede agent de verkeerde conclusies trekt?

De heer **Muijen**: Het klinkt een beetje plat, maar dat moet gebeuren door het vakmanschap van alle medewerkers binnen het OM, maar specifiek door dat van de officieren van justitie. Je mag van een officier van justitie verwachten dat, als hem of haar gegevens worden aangereikt in de vorm van een proces-verbaal of door middel van een bilateraal gesprek, waarbij niets op papier staat en moet worden vertrouwd op wat de politieambtenaar naar voren brengt, deze op hun juiste waarde worden geschat. Het is mijn ervaring dat de meeste officieren van justitie niet meer blind varen op blauwe ogen, maar echt doorvragen.
Ik meen dat in de meeste gevallen – ik heb niet alle situaties op mijn netvlies – wordt doorgezocht als er onvoldoende context is.

De heer **Buruma**: Dat is mooi, want dit brengt mij bij iemand die naar dit soort zaken onderzoek doet. Ik geloof niet dat zij ook op dit concrete punt onderzoek heeft gedaan, maar zij heeft wel enig zicht op de praktijk van politiewerk in verband met databestanden. Ik heb het over mevrouw De Poot, onderzoekster bij het WODC. Mevrouw De Poot, er wordt gewaarschuwd en natuurlijk worden er wel eens fouten gemaakt. Het is echter de professionaliteit van de politie en het Openbaar Ministerie om hiermee om te gaan. U bent een onafhankelijk onderzoeker, want het WODC is onafhankelijk. Dit neemt niet weg dat u een onafhankelijk onderzoeker bent die de zaken beziet vanuit het oogpunt van het ministerie van Justitie. Het WODC hoort immers bij het ministerie van Justitie. Wat is uw idee? Doet men het zo goed als de heer Muijen suggereert?

Mevrouw **De Poot**: Ik wil hierop twee dingen zeggen. Allereerst voel ik veel voor het idee van de heer Muijen. In feite is informatiegestuurde opsporing niet een andere manier van opsporing dan sinds 1995 gebruikelijk is. Deze informatie komt over het algemeen gewoon van burgers en van politiemensen die iets zien. Het beeld van grote databestanden die zelfstandig aan de slag gaan en via datamining met ideeën komen over mogelijke verdachten, is misschien toekomstmuziek, maar niet de situatie zoals die op dit moment geldt. Informatiegestuurde opsporing gaat nog steeds over burgers die bij de politie komen met informatie en over politiemensen die informatie uit hun verschillende bestanden met elkaar koppelen. Hiermee wil ik niet zeggen dat er geen EMERGO-onderzoek is waarbinnen op een bepaald gebied bestanden aan elkaar gekoppeld worden met een bepaald soort informatie als gevolg. Ik vind het belangrijk te benadrukken dat informatiegestuurde opsporing eigenlijk gewoon over mensenwerk gaat. Telefoontapgegevens van de een worden met de tapgegevens van de ander in contact gebracht. Hieruit kunnen connecties voortkomen waarmee de politie aan de slag gaat.

De heer **Buruma**: Ik denk dat dit een heel goede waarschuwing is. Wij zijn nog helemaal niet zo ver. Aan de andere kant maken Kamerleden juist met het oog op de toekomst wetten en doen aanbevelingen ten aanzien van het beleid in verband met de organisatie van een en ander. Je hoeft maar enkele televisieseries te bekijken om de indruk te hebben dat het gebruikelijk is dat men allerlei bestanden langs elkaar heen knalt. Wij doen dit al met de meldingen van ongebruikelijke transacties en het ZwaCri-systeem. In deze gevallen probeert men conclusies te verbinden aan data. Wellicht gebeurt het niet op grote schaal, maar Kamerleden moeten beoordelen of dit in de toekomst wel op grotere schaal zal gebeuren. Bagatelliseert u de praktijk niet te zeer?

Mevrouw **De Poot**: Wij willen veel meer. Er is hier nog een expert, Wouter Teeuw, die veel meer over de toekomst van dit soort dingen kan vertellen dan ik. Om ongebruikelijke transacties en handelingen in beeld te krijgen, moet je een idee hebben van wat gebruikelijk handelen is en van wat gebruikelijke situaties zijn. Als je alle gegevens over bijvoorbeeld

rij- en belgedrag van heel Nederland samenvoegt, krijg je een overload aan gegevens en heb je als opsporingsinstantie of veiligheidsdienst geen idee meer waar je moet zoeken. De komende tien à vijftien jaar moet worden uitgegaan van een vraaggestuurde opsporing, in de zin van: «in deze situatie zijn wij bang voor dit soort handelingen en in die situatie zijn wij bang voor dit soort mensen». Ik veronderstel dat het nog enige tijd zal duren voordat de data zelf combinaties gaan maken en een persoon naar voren schuiven.

De heer **Hustinx**: In kleinschalige verhoudingen herken ik dit beeld. Informatiegestuurd opsporen is een slogan. Deze heeft alles te maken met infrastructuren die geïnitieerd en ontworpen worden met het oog op het toepassen van grootschalige profilering op risicogedrag.
Een aantal voorbeelden is er al. De discussie met de Verenigde Staten over de uitwisseling van passagiersgegevens gaat uitsluitend daarover. Het gaat niet om het vinden van verdachte individuen, want de identiteiten worden dubbelgecheckt voordat je aan boord gaat. Het gaat om het opsporen van kenmerken die er mogelijk op kunnen wijzen dat iemand een terrorist of iets anders is. Op dit moment ligt er al het voorstel om datgene wat wij in een ongelijke strijd moeizaam in onderhandeling met de Verenigde Staten bereiken, precies zo in Europa te gaan doen. Dat leidt tot wetgeving waarin deze Kamer een rol speelt. De mechanismen die bij de risicoprofilering een rol spelen, hebben niets te maken met fingerspitzengefühl en het professionele gedrag van een diender of een officier van justitie. Waar het op aankomt, is dit: je zal maar in een relevante mate aan het profiel voldoen. Dan heb je een groot probleem.

De heer **Buruma**: Ik zie een Kamerlid van het Europees Parlement.

Mevrouw **In 't Veld** (D66): Een Europees Kamerlid, nou. Als lid van het Europees Parlement heb ik een toch wat andere invalshoek. Wij zitten hier te praten over de vraag hoe wij het in Nederland zouden willen regelen, maar dat is bijna niet meer relevant. Het gaat ook niet om databestanden die worden opgebouwd door de overheid, maar om databestanden die voor commerciële doeleinden worden opgebouwd, door telecomaanbieders, internetaanbieders, banken, verzekeraars, noem maar op. Die zijn over de hele wereld toegankelijk. Over passagiersgegevens hebben wij onderhandeld omdat die daadwerkelijk van Europa naar Amerika worden gestuurd. Alle andere gegevens zijn echter in Amerika toegankelijk voor de Amerikanen, omdat ze onder Amerikaanse jurisdictie vallen. Dat is een van de grote problemen. In Europa hebben de lidstaten nationale wetgeving, maar het heeft geen zin meer om wetten te maken voor een bepaald geografisch gebied als die gegevens over de hele wereld, ook voor de Chinezen, de Indiërs, de Brazilianen, de Australiërs, noem maar op, beschikbaar zijn.

De heer **Buruma**: Je kunt het natuurlijk ook omkeren. Kan onze Nederlandse politie wel de gegevens van Citicorp in Nederland krijgen? Het wereldperspectief is natuurlijk een heel waar perspectief. Een Kamerlid vraagt het woord. Ik laat mij in de discussie snel leiden door wat de Kamerleden willen weten. Dat zeg ik ook tegen alle andere Kamerleden.

De heer **Çörüz** (CDA): De angst is reëel. Professor Jacobs gaf het voorbeeld: stel dat iemand kwaad in de zin heeft met een bepaalde politicus. Ik denk terug aan de tijd van mijn vader. Als je vroeger door rood licht reed of te snel reed, kreeg je zo'n mooie foto. Thuis ontstond dan altijd de discussie over de schaduw rechts naast je. Was dat iemand? Ik geloof niet dat daaruit nu echt veel echtscheidingen zijn voortgekomen. Creëert onze angst niet een beetje zijn eigen weerstand, juist omdat het nieuw is? Op

preventief fouilleren, cameratoezicht – daarover wij gaan praten – of andere ontwikkelingen kwam in het begin precies zo'n reactie.
Een andere opmerking betreft het koppelen. Als je niet koppelt, heb je geen totaalbeeld. Ik wil dat verduidelijken met het voorbeeld van de 22ste kaper bij de aanslag op het World Trade Center. Deze had in veel landen in Europa rondgezworven. Het probleem was dat men geen totaalbeeld had. Op een gegeven moment zat hij ergens in Hamburg, vervolgens vloog hij weer ergens anders heen. Heb je een koppeling niet juist nodig om het totaalbeeld reëel te krijgen?

De heer **Buruma**: Mevrouw Brouwer, dit betreft vooral uw expertise. Delen moet, zegt mijnheer Çörüz.

Mevrouw **Brouwer**: De vraag was aan de heer Jacobs gericht. Ik hoor graag nog zijn reactie hierop. Vooraf maak ik graag een compliment voor dit initiatief van de Eerste Kamer met het Rathenau Instituut. Het is goed dat het parlement zich met deze onderwerpen bemoeit, vooral met het onderwerp «databanken». Heel veel mensen denken dat het al een gelopen race is. Op het gebied van het koppelen van gegevens is al zo veel Europese wetgeving tot stand gekomen. Dat is het onderwerp waarmee ik mij in het bijzonder bezighoud. Het Visuminformatiesysteem en het Europees biometrisch paspoort komen eraan en de verordening voor SIS II is al aangenomen. Het voorstel van maart 2008 van de Europese Commissie over grensbeheer, het «border package», laat echter zien dat er nog heel veel besluiten te nemen zijn. Mijn buurman, de heer Hustinx, reageerde daar al op.
Ik hoop dat deze Kamer en het Europees Parlement alert zullen blijven bij de besluitvorming. Ik ga allereerst in op de vraag over rechtsbescherming. Wat kunnen wij doen dat burgers niet de dupe worden van foute koppelingen en van foute, vervuilde gegevens in de databases? Ik denk dat het heel erg belangrijk is om van tevoren te kijken naar de effectiviteit van de maatregelen die worden voorgesteld: het koppelen van databestanden, het entry/exitsysteem in de border package en het geautomatiseerd controleren van geregistreerde, zogenaamde bonafide reizigers. Deze maatregelen staan allemaal in het voorstel van de Europese Commissie van 12 maart. Ik verbaas mij erover dat de besluitvormers, maar ook de parlementsleden tot nu toe weinig gebruikmaken van en zelfs niet vragen naar evaluaties van bestaande systemen en van de voorstellen.

De heer **Buruma**: Bedoelt u dat het niet nuttig is?

Mevrouw **Brouwer**: Ik was bijvoorbeeld verbaasd over de gang van zaken bij de totstandkoming van SIS II. Wij hebben het er al over gehad dat er te weinig harmonisatie is van de criteria voor de data die wij in de systemen stoppen. Men had dit probleem met de tien jaar ervaring die is opgebouwd met SIS I makkelijk kunnen evalueren. Die evaluatie is er in beperkte mate geweest, maar deze is bijna of niet gebruikt op politiek niveau. Met betrekking tot het doel om terroristen op te sporen, heeft het mij verbaasd dat de Europese Commissie de bevindingen in de zogenaamde «impact assessment» – waarin is gekeken naar de gevolgen van de verschillende voorstellen, nauwelijks mee laat wegen. Zo heeft de Europese Commissie wil voorstellen gedaan voor een elektronische grensbewaking door middel van een EU-paspoort krijgen. Met een geregistreerd reizigerschap zullen EU-onderdanen, als er maar genoeg data worden verstrekt, toestemmming krijgen om langs biometrische poortjes te reizen. Wij hoeven dan dus niet meer gecontroleerd te worden. Wij kunnen met ons paspoort met biometrische chip langs een poortje en worden automatisch ingecheckt.

De heer **Buruma**: Dat is dus handig.

Mevrouw **Brouwer**: Dat lijkt heel handig. In het impact assessment bij dit voorstel staat echter– en daarvan vind je niets terug in het plan van de Commissie – dat het funest en negatief is voor de bestrijding van terrorisme, terwijl in het plan voorop stond dat wij terroristen willen tegenhouden. De aanslagen in Europa zijn gepleegd door EU-onderdanen of door mensen met een legale verblijfstitel in de Europese Unie. Bovendien weten mensen dat zij met zo'n geregistreerd reizigerschap makkelijk de EU binnenkomen zonder persoonlijke controle. Zojuist is gesproken over individueel vakmanschap en fingerspitzengefühl. Met het voorstel van de Europese Commissie wordt de persoonlijke en deskundige controle door grensbewakingsambtenaren weggehaald.

De heer **Buruma**: Geldt hierbij niet wat Hustinx heeft gezegd, namelijk dat je een onderscheid moet maken? Aan de ene kant is er het gebruik van dit soort bestanden om op te sporen; er is iets gebeurd en je gaat zitten zoeken en dan heb je ook dat fingerspitzengefühl nodig. Aan de andere kant is er de weigering om iemand op een flight list te plaatsen omdat hij halal eet. Er bestaat natuurlijk een verschil tussen naar voren gericht, prospectief, handelen, waarbij je gegevens uit lijsten haalt met alle risico's van dien, en het zoveel mogelijk gegevens bij elkaar frutten met het oog op de opsporing van wat reeds is gebeurd. Wat is er nu eigenlijk tegen op het verzamelen en gebruiken van gegevens om catastrofes te voorkomen? Is daarin niet de kernvraag gelegen?

Mevrouw **Brouwer**: Mijn bezwaar betreft de consequentie dat met het voorgestelde systeem de gezochte personen niet worden gestopt en personen die je juist niet wilt tegenhouden mogelijk wel door het gebruik van profilering. Daartegen moet je rechtsmiddelen in stelling brengen. Ik denk dat je, voordat je deze systemen creëert, moet nadenken of je de terroristen die je wilt traceren er met die systemen uithaalt.

De heer **Buruma:** Dat is het voorbeeld van het terrorisme, inderdaad. Ik zie de hand van de heer Jacobs.

De heer **Jacobs**: Er spelen veel dingen. Ik denk dat wij bezig zijn met een kwalitatieve verandering. U kunt mij niet snel van techniekvijandigheid of van koudwatervrees voor dit soort dingen beschuldigen. Er is een aantal dingen aan de hand – ik ben altijd bang om op dit gebied grote woorden te gebruiken – die gezien kunnen worden als bouwstenen van een politiestaat. Ik denk dat wij daarmee voorzichtig moeten zijn. Wij moeten goed oppassen bij waar wij mee bezig zijn. Ik denk dan aan wat je precies doet met het proactief gebruik van informatie, met datamining en met de centrale opslag van biometrie, waarmee je natuurlijk ook akelige dingen kunt gaan doen die wij in Nederland niet willen. Je kunt een aantal straten afzetten en bij iedereen een vingerafdruk afnemen en vervolgens kijken wat er aan de hand is. Dit roept associaties op die wij in Nederland niet willen. Dit is allemaal niet de bedoeling van dit soort dingen, maar zij zijn er wel mee mogelijk.
Tot nu toe hebben wij natuurlijk in Nederland allemaal brave kabinetten gehad die er goed mee omgaan, maar dat betekent natuurlijk geen garantie voor diezelfde luxe in de toekomst. Je moet het misbruik van al dit soort maatregelen toch echt in de gaten houden.

De heer **Buruma**: Maar waarin zit dan het verschil? Vroeger was het ook al zo dat je een fotootje kreeg met daarop je vader met iemand naast zich. Dat viel dan toch nog wel mee.

De heer **Jacobs**: Daarop wil ik graag ingaan. Voor mijn gevoel speelt de vraag of je wel of niet selectief met gegevens omgaat, hierbij een sleutelrol. Ik druk het zelf altijd graag uit in termen van «select before you

collect»; dat bekt lekker op zijn Engels. Traditioneel selecteer je eerst iemand als verdachte en verzamel je daar vervolgens gegevens over. Dat zijn wij langzamerhand aan het omdraaien. Eerst verzamelen wij van iedereen gegevens en vervolgens kijken wij van wie wij die gegevens nog gaan gebruiken. Dat is een heel fundamentele paradigmawisseling, die sluipenderwijs plaatsvindt. Ik heb daar heel grote moeite mee, want eigenlijk behandel je impliciet iedereen als potentiële verdachte. In Nederland willen wij toch niet zo met elkaar omgaan?

De heer **Buruma**: Ik geef het woord aan mevrouw Van Bijsterveld.

Mevrouw **Van Bijsterveld** (CDA): Ik heb het idee dat tot nu toe vooral de zorgen en de kritische kanttekeningen de overhand hebben bij eigenlijk vrijwel alle deskundigen achter de tafel. Deels wordt er ook gezegd dat het nog niet zover is; het is nog wat verdere toekomstmuziek. Er is heel even ingegaan op de vraag of de systemen als zodanig effectief zijn, maar daarover hebben wij nog niet heel veel gehoord, hoogstens in de zin van dat er verstandig mee omgegaan moet worden omdat er context nodig is. Ik zou ook graag nog iets meer horen over het punt van de overvloed aan gegevens die natuurlijk ook een systeem minder effectief maakt. Eigenlijk ben ik nog het meest benieuwd naar een antwoord op de vraag wat er dan wel moet gebeuren. Hoe moet je nu wel verdergaan? Moet je de bestaande typen van gegevensverzameling en de regulering ervan als uitgangspunt nemen, waarbij je alleen wat selectiever en wat strenger bent en je beter oplet dat er geen fouten gemaakt worden? Of moet je wellicht toch op een heel andere manier nadenken over de vraag hoe om te gaan met dit vraagstuk?

De heer **Buruma**: Dan ga ik eerst naar de heer Muijen. Hij wil iets opmerken. Wat hij wil zeggen, zit misschien al in het verlengde van de vraag van mevrouw Van Bijsterveld.

De heer **Muijen**: Ik wil in ieder geval beginnen met de opmerking dat ik wel positief ben, maar niet vanuit de optiek dat ik een officier van justitie ben die zou vinden dat zo veel mogelijk bevoegdheden moeten worden gegeven en dat wij lak hebben aan de belangen van alle burgers, ook in Europa. Ik wil ook eens gezegd hebben dat met het recentelijk aannemen van de Wet politiegegevens door de Tweede en de Eerste Kamer er, los van de opmerkingen van het College Bescherming Persoonsgegevens, in Nederland toch een wet tot stand is gekomen waarin de Nederlandse cultuur van «wat willen wij nog wel?» is terug te vinden; zo heb ik het althans opgepakt. Heel kort door de bocht: in die wet is het gegeven van, zoals de heer Jacobs zegt, «politie, verzamel maar alles en dan zien wij uiteindelijk wel of er een verdachte overblijft», nadrukkelijk niet aan de orde. In de wet worden natuurlijk begrippen gehanteerd als «niet bovenstallig» en «doeltreffend». Dat soort dingen moet natuurlijk altijd worden teruggebracht tot de menselijke maat; bij grootschalige gegevensverwerking is die menselijke maat vrij vlug zoek.
Ten aanzien van de effectiviteit is al vaker gezegd dat politie en justitie natuurlijk moeten proberen te opereren in een veld waar je de meest vreselijke dingen tegenkomt. Ik zou heel graag alleen maar de gegevens krijgen waarvan ik op voorhand weet dat die tot een succesvolle zaak leiden of tot een succesvol optreden – laten wij dat niet vergeten – in het kader van de openbare ordehandhaving, waarbij het bestuur een nadrukkelijke rol heeft. Maar zo zit het helaas niet in elkaar. Volgens mij zal de toekomst ook leren dat het zo niet in elkaar zal zitten.

De heer **Buruma**: Maar zegt u dan daarmee dat «select before you collect» eigenlijk niet kan? Dus: wij moeten wel 1,8 miljoen telefoon-

gegevens per jaar opvragen, want zonder dat kunnen wij ons werk niet goed doen? Dat aantal is toch juist: 1,8 miljoen telefoongegevens?

De heer **Muijen**: Ik heb uw verhaal daarover wel eens gelezen. Ik ben de laatste die zegt dat het bij die telefoongegevens misschien iets minder kan. Maar dat is een ander issue. Ik vind dat wij zeker selectief moeten zijn, maar ik vind niet dat je zover kunt gaan dat je van tevoren heel driftig selecteert; volgens mij is dat ook niet haalbaar. Het werkt gewoon niet zo. Ik realiseer mij dat dit een schamele opmerking vanuit de praktijk is.

De heer **Buruma**: Dat is natuurlijk wel belangrijk.

De heer **Muijen**: Ik baseer mij op 30 jaar ervaring bij politie en justitie. Los van de bevoegdhedendiscussie, moeten wij – het is mij om het even of dat nu binnen justitie of politie is – natuurlijk een aantal stappen blijven zetten in de ontwikkeling van het privacybewustzijn over het feit dat die persoonsgegevens allemaal mensen betreffen. Dat blijft namelijk wel een probleem.

De heer **Buruma**: Hoe kijkt u naar de vraag van mevrouw In 't Veld? Ik was expres even weggelopen omdat wij het andere lijstje nog niet afhadden, maar haar punt staat natuurlijk wel. Het is inmiddels zo dat het alle kanten opgaat, zeker in het geval van de georganiseerde misdaad en al die DNA-spullen, waar wij het nog over gaan hebben, als daar het Verdrag van Prüm bij wordt gehaald.

De heer **Muijen**: Ik spreek de opmerkingen van mevrouw In 't Veld niet tegen. Natuurlijk moeten wij erkennen dat zeker met criminaliteit de Europese dimensie een dagelijkse realiteit is.

De heer **Buruma**: Wat betekent dat voor de Kamerleden hier in Den Haag?

De heer **Muijen**: Ik wacht even.

De heer **Buruma**: Toch ben ik zo benieuwd wat u te zeggen hebt. Maar goed. Ik geef het woord aan de heer Hustinx.

De heer **Hustinx**: Ik wil wat zeggen over de vraag wat er dan wel moet gebeuren. Het is een positieve insteek waar wij wat mee kunnen. Ik heb er twee opmerkingen over.
Ten eerste geldt voor alle situaties met databanken dat daarop heel consequent de criteria en principes van het gegevensbeschermingsrecht moeten worden toegepast. Dit leidt tot een enorme verbetering in het beheer van de systemen en ook uitwisseling gaat in dat geval een stuk beter. Dat is een les van jaren her, die steeds weer van toepassing is. Wij moeten daar niet relativerend over doen. Het is een onderdeel van het succes wil het goed kunnen aflopen.
Mijn tweede punt betreft de besluitvorming en raakt aan wat zo-even is gezegd. Wij moeten staan op een impact assessment voordat voorstellen worden aanvaard. Ook moeten wij heel close monitoren en de effecten beschouwen als het wordt toegepast. Tot slot moeten wij na verloop van tijd evalueren wat het heeft uitgehaald. In alle projecten die er toe doen, blijkt dit de succesformule.
Ik voeg hier nog een derde opmerking aan toe. Het Visuminformatiesysteem dat de afgelopen jaren op Europees niveau is besproken en dat gebouwd gaat worden in het kader van het gemeenschappelijke visabeleid, wordt gigantisch. Er komen 80 miljoen personen in te staan. Wij hebben daarover een paar jaar geleden een kritische analyse gemaakt. Bijna alle conclusies van die analyses zijn inmiddels verwerkt in de besluitvorming. Je zou kunnen zeggen dat er zo veel aan gedaan is dat er

verantwoord met het systeem kan worden gestart. De andere punten blijven echter gelden. Er zijn dus ook termijnen afgesproken waarop gekeken gaat worden of er een volgende fase kan worden ingevoerd. De besluitvormers, Kamerleden, zouden erop kunnen sturen dat de kwaliteitscriteria op deze manier zowel in de voorstellen als in het gehele tijdstraject gefaseerd bewaakt worden. Het grootste risico is overdrive en overkill: haast, haast, het moet nu en er is geen tijd om het allemaal te bezien. Daar zitten naar mijn mening systematisch de gevaren in.

De heer **Buruma**: Er zijn nu vier mensen die iets willen zeggen, en ook vanachter de tafel wil iemand een opmerking maken. Ik zie mevrouw Westerveld als eerste staan.

Mevrouw **Westerveld** (PvdA): Ik wil iets zeggen naar aanleiding van het betoog van professor Jacobs over wat wij met elkaar niet willen. Ik heb zeer geïnteresseerd geluisterd naar het eerste deel van zijn betoog over bestandsvervuiling en de effecten ervan. Naar mijn idee is het heel belangrijk om heel precies de risico's te formuleren in de discussie over waar wij naartoe gaan en wat voor wetgeving noodzakelijk is. Argumenten als «een samenleving die wij met elkaar niet willen» slaan langzamerhand niet meer aan. Dat heeft ook te maken met alle gebeurtenissen van de afgelopen tijd op dit gebied. Ik roep iedereen op die zich, naar mijn mening terecht, zorgen maakt over dit thema om bij beschouwingen waarin wordt gezegd dat men zulke vergaande regelingen niet wil, aan te geven waarom dan niet. Het kan zijn dat misschien tien of vijftien jaar geleden iedereen vond dat wij dat natuurlijk niet willen, maar dat nu de reactie positiever is. Men vindt dat men niets te verbergen heeft, en ziet geen reden om niet alle huizen af te gaan of om niet alle gegevens eindeloos op te slaan. Voor het maken van beleid is het belangrijk om precies te kunnen zeggen waarom wij iets niet willen.

De heer **Buruma**: Ik ben zo'n provinciaal dat ik eerst het woord geef aan ons Tweede Kamerlid om daarna weer naar de vertegenwoordiger van het Europees Parlement toe te gaan. Het woord is aan mevrouw Azough.

Mevrouw **Azough** (GroenLinks): Mijn vraag betreft de juridische component en is waarschijnlijk bedoeld voor de heer Hustinx.
Gegevensbescherming is een fundamenteel recht van elke burger in Nederland. De nationale staat is daarvoor verantwoordelijk. Mevrouw in 't Veld gaf al aan dat grootschalige uitwisseling van gegevens, ook aan derde landen, op zeer veel verschillende fronten plaatsvindt. In hoeverre kan Nederland als nationale staat nog garanderen dat gegevensbescherming op een goede manier plaatsvindt? Zij gaf al aan dat een en ander zo gedisciplineerd mogelijk moet plaatsvinden. Is dat wel een haalbare kaart? Mijn tweede vraag betreft de commerciële doelstellingen. Ik vind het verbijsterend dat dit punt elke keer uit het oog wordt verloren. Ik vrees dat hier een bepaald gevaar over het hoofd wordt gezien. Zijn daarvan signalen bekend? Welke risico's kan het feit dat die gegevens op internationaal niveau bewaard en toegepast kunnen worden, met zich brengen?

De heer **Buruma**: Kunnen degenen aan wie de vragen gericht zijn, die even vasthouden? Er zijn namelijk nog twee mensen die een vraag willen stellen. Daarna kijk ik even terug. U komt allemaal nog één keer aan de beurt.

Mevrouw **in 't Veld** (D66): Mevrouw Westerveld vroeg waarom wij dit niet zouden moeten doen. Geheel zonder cynisme zeg ik haar dat mijn Oost-Europese collega's heel goed kunnen vertellen waarom wij dat niet moeten willen.
De eerste vraag die wij zouden moeten stellen, die wij altijd maar over-

slaan en waaraan al het andere afgemeten wordt, is, wat nu eigenlijk het doel is. Er wordt altijd gedacht dat het gaat over het vangen van terroristen, of sterker nog, het voorspellen van terroristisch gedrag. Dat doen wij dan met het data minen in enorme databases. De formeel vastgelegde doelstellingen gaan echter vaak veel verder dan terrorisme en gerelateerde criminaliteit. Bij passagiersgegevens bijvoorbeeld gaat het ook over «het voorkomen van infectieziekten en andere risico's», wat die dan ook mogen wezen! Als je de definitie van president Bush van andere risico's aanhoudt, gaat het heel ver. Een klassieker is het in de smiezen houden van politici en van journalisten. Het inreissysteem van Australië dat wij moeten gaan overnemen, wordt bijvoorbeeld ook gebruikt om aspirant-adoptiefouders te screenen, mensen op hiv te screenen of belastingontduikers eruit te halen.
Er is een verschil tussen klassieke opsporingsmethodes en preventief zoeken in grote databestanden. Bij klassieke opsporingsmethodes wordt gericht naar iets gezocht. Natuurlijk moet de informatie dan beschikbaar zijn. Het is een misvatting dat het niet of niet uitsluitend gaat om de overheid die bestanden opbouwt, het gaat juist om het gebruik van bestanden die zijn opgebouwd voor puur commerciële of andere doeleinden. Ik verwijs in dit verband naar Google, naar banken, naar verzekeraars, et cetera. Die bestanden worden gebruikt door de overheid. De Amerikanen en de Chinezen gebruiken onze gegevens. Daarvoor kunnen wij geen regels maken.

De heer **Buruma**: Dit zou uiteindelijk tot een diep fatalisme kunnen leiden. Ik kijk even naar de deskundigen. Ik wist dat dit thema de meeste tijd zou nemen. Ik wil beginnen met mevrouw Brouwer die al in een veel eerder stadium te kennen gaf dat zij nog iets had toe te voegen.

Mevrouw **Brouwer**: Het sluit mooi aan op de vraag van mevrouw Azough over de juridische gevolgen en wat een nationale staat kan doen. Natuurlijk moeten wij ons van te voren afvragen, of het nuttig is en of vreemdelingendiensten of politieambtenaren inderdaad meer data willen. Uit het onderzoek over het Schengeninformatiesysteem blijkt dat ambtenaren niet staan te springen om meer informatie: less is more.
Over de rechtsbescherming van individuen wil ik twee opmerkingen maken. Wij zullen wel moeten. Er worden op verschillende fronten belangrijke uitspraken gedaan waaruit blijkt dat de wetgever rekening heeft te houden met de rechten van individuen. Zowel het Europese Hof van Justitie, als het Hof in Straatsburg voor de mensenrechten als de Duitse constitutionele rechter hebben onlangs nog belangrijke uitspraken gedaan exact over deze onderwerpen. Recent is er een uitspraak geweest van de Duitse constitutionele rechter over het monitoren en automatisch opslaan van kentekens. Dat wil men in Nederland en in Europa ook gaan doen.
Het Duitse Verfassungsgericht heeft hierover gezegd: «het is onconstitutioneel, in strijd met het recht op persoonlijke levenssfeer of het «informationelle Selbstbestimmungsrecht». Het gaat niet alleen maar om privacy en dataprotectie. Opvallend in de huidige discussies is dat je met privacyoverwegingen alleen vaak de strijd verliest wanneer het om de bescherming van veiligheid gaat. In de afweging van veiligheid en privacy vinden wij privacy iets minder belangrijk. Die afweging moet je anders maken; die heeft het Hof van Straatsburg ook anders gemaakt. Alleen als de veiligheid echt aantoonbaar op het spel staat, moet de individuele privacy een stapje terug doen.
Maar er zijn meer rechten in het geding waarvan ik denk en waarvan je ook kunt voorspellen dat ze vaker getoetst zullen worden door de rechter. Ik denk aan het recht op vrij verkeer van EU-burgers in verband met het gebruik van het biometrisch paspoort. De advocaat-generaal bij het Hof van Justitie heeft in haar opinie bij een zaak over dat Europese paspoort,

een procedure waarbij het eigenlijk helemaal niet gaat over dit onderwerp, als extra overweging gezegd dat het Europese paspoort waarbij biometrie wordt opgeslagen mogelijk in strijd is met het recht op dataprotectie van de EU-burgers. Volgende week wordt in een andere zaak het advies verwacht van de advocaat-generaal over de registratie van de EU-onderdanen in het Duitse vreemdelingenadministratiesysteem en de vraag of dit in overeenstemming is met het recht op vrij verkeer van EU onderdanen en de EG Richtlijn inzake de bescherming van persoonsgegevens.

De heer **Buruma**: Mag ik heel even onderbreken? Er is een heleboel over te zeggen, maar ik vind één punt heel interessant. U zegt dat het die advocaat-generaal niet om de privacy ging. Het ging kennelijk wel om iets anders. Wat was dat andere?

Mevrouw **Brouwer**: De dataprotectie. Dat zijn de beginselen waar de heer Hustinx al naar heeft verwezen. Die beschermen bredere belangen dan alleen maar privacy. Het non-discriminatiebeginsel is een heel belangrijk recht, juist wanneer je denkt aan de databestanden die vooral op niet-EU-onderdanen worden losgelaten. Ik denk aan het recht op asiel. Het voorgestelde entry/exit-systeem gaat het misschien onmogelijk maken voor erkende of te erkennen vluchtelingen om nog naar Europa te komen. Het zijn meerdere rechten waarvan duidelijk is dat die systemen er inbreuk op zullen maken. Dat is ook de reden waarom de lidstaten en de Europese wetgever worden teruggefloten door de rechters.

De heer **Buruma**: Dank u wel.
Mijnheer Hustinx, ik maakte een opmerking die misschien haast niet beleefd was naar mevrouw In 't Veld, maar haar verhaal wekte bij mij uiteindelijk de indruk dat er toch niks aan te doen is: het rolt allemaal bij die Amerikanen. Dat was de zorg waarvan mevrouw Van Bijsterveldt eigenlijk zegt: gut ja, dat hebben wij al zo vaak gehoord. Dat zei u zo niet, maar zo interpreteer ik uw woorden: die zorgen, dat weten wij nu allemaal wel. Vindt u dat Kamerleden hier nog wel een taak hebben, als wij kijken naar de invloed van al die dingen die er buiten Nederland om plaatsvinden? Ik vat nu een paar van de impulsen samen die ik uit de zaal krijg. Is het niet aan de ene kant het gesomber van de mensen die overal rechtenschendingen zien en aan de andere kant de naïveteit? Wat moeten die Kamerleden hier doen volgens u?

Mevrouw **Quik-Schuijt** (SP): Mag ik een vraag stellen die daarbij aansluit? Wij moeten als Kamerleden iets doen met die wetten. Er komen er weer een paar aan. Is het denkbaar dat je zegt: die gegevensverzameling is nodig, daar kunnen wij niet meer omheen, maar wij gaan regelen hoe je daarmee omgaat? Ik denk er dan aan dat je daarin kunt zoeken als er een aanwijzing is dat iemand ergens van verdacht zou kunnen worden, maar dat je niet in het wilde weg alles gaat koppelen: kijk wat ik nu uit de hoge hoed tover. Zou je dat met wetgeving kunnen regelen?

De heer **Buruma**: Heel goed. Die vraag kunnen wij ook aan de heer Muijen stellen. Die moet hij ook even vasthouden.

De heer **Hustinx**: Wat wij hier horen, is niet zo'n complex en warrig verschijnsel dat wij maar onze handen in de lucht moeten gooien: er komt wat er komt, morgen is er weer een nieuwe dag en er zijn belangrijkere dingen. Nee, Nederland speelt er een rol in mee. Er zijn allerlei openingen waarin wij positie nemen. Dat doen wij in het kader van Europa. Als het gaat om de derde pijler, is de besluitvorming nog steeds bij unanimiteit; in ieder geval blijven meerderheden van belang. Ik geef het voorbeeld van de PNR-overeenkomst met de Verenigde Staten. De discussie over PNR in

Europa is een discussie waarin Nederland 100% medeverantwoordelijkheid draagt.
Volgens mij ligt de aanpak in het midden. Natuurlijk is de werkelijkheid van informatietechnologie buitengewoon belangrijk, dus dat moeten wij goed doen. Het moet in rechte stand houden als bewijs, de verdachte moet het gevoel hebben dat hij eerlijk wordt behandeld, al die zaken zijn een onderdeel van het «aan boord brengen» van de beginselen van dataprotectie. Daarbij gaat het niet alleen om privacy, maar ook om vrijheid van meningsuiting, mobiliteit, transparantie, vertrouwen in de overheid enzovoorts. Dit is gewoon een kernpunt van een behoorlijk gebruik van informatie. Daar spelen beide Kamers een buitengewoon grote rol in, dus zij moeten dat vasthoudend doen. Ik geloof niet dat wij moeten zeggen: al die gegevens zijn er, wij moeten de discussie voeren over de vraag welk gebruik wij ervan maken. Het kan alleen maar goed gaan met de dataprotectie als wij vanaf het moment van verzamelen tot het moment van uitwisselen en vernietigen blijven redeneren.

De heer **Buruma**: Ja, maar dan wordt gezegd dat allerlei bedrijven gegevens aan het verzamelen zijn. Je ziet nu al dat burgers zelf hieraan meedoen door op YouTube de acties van politieagenten weer te geven.

De heer **Hustinx**: Dat snijdt geen hout. Ik zie natuurlijk wel de beperkingen van de Nederlandse en de Europese jurisdictie, maar de bedrijven die in Europa zijn gevestigd, hebben zich aan de Europese regels te houden. Een grote wereldspeler als Google heeft zich aan de Europese regels te houden en zal binnenkort horen wat die regels zijn. Daaraan zijn zij onlangs herinnerd in een discussie over het concurrentierecht. Dus is er een agenda om de grote spelers te disciplineren en waar nodig met de regels te confronteren. Dat is geen fluitje van een cent, maar het is zeker geen verloren strijd.

De heer **Buruma**: Mijnheer Jacobs, u kreeg op een gegeven moment wat tegenwind. Aanvankelijk was het erg overtuigend wat u zei, maar toen men besefte dat er een verband is tussen veiligheid en privacy, veranderde dat.

De heer **Jacobs**: Wij moeten een visie ontwikkelen, aangezien een aantal cruciale zaken aan het veranderen is. Daarom ben ik blij met dit debat. Vanuit mijn ict-achtergrond benadruk ik dat de inrichting van ict-systemen een politieke beslissing is. Op welk niveau zet je de gegevens neer en wie mogen erbij? Het is belangrijk dat de politiek daarbij het voortouw houdt. Verder is het belangrijk de waarde van de techniek te relativeren. Als je te veel op de techniek vertrouwt, word je kwetsbaar en lui, waardoor je bepaalde dingen niet meer ziet. Deze week zagen wij het met de pasjes, waarmee onze kwetsbaarheid duidelijk wordt. Het is belangrijk bepaalde afspraken te maken over datamining. Is het niet redelijk om hier af te spreken dat de AIVD mag data minen en de politie niet? Datamining is proactief gebruik van gegevens, wat de inlichtingendiensten in een zeer beperkte context wel mogen, maar de politie reageert reactief, zij creëert geen nieuwe gegevens. Een heel duidelijk voorstel.
Deze discussie gaat wel degelijk over wat voor samenleving wij willen, wat het tot een heel interessante discussie maakt. Om enigszins gechargeerd daar stelling over in te nemen: in een dictatuur is het voor veel mensen veiliger dan in een democratie. In een democratie lopen allerlei mensen los en wild rond. Dat creëert risico's. Daar hebben wij het nu wel over. Met dit perspectief wil ik afsluiten.

De heer **Buruma**: Mijnheer Muijen, er is ook een vraag aan u gesteld.

De heer **Muijen**: Ik wil krachtig ondersteunen dat het geen ontwikkelingen zijn die zo maar over ons heen vallen. Op Europees en Nederlands niveau wordt door de politiek een ambitie geformuleerd, die wij uitvoeren. Dat betekent dat je daar toch wel het nodige mee kunt doen.
Ik wil graag de vrijheid nemen om een advies te geven. Ik zou het buitengewoon van belang vinden als in de discussie de focus niet alleen ligt op terreurbestrijding. Ik heb af en toe het gevoel dat het woordje «terreur» de panacee is voor allerlei soorten volgende uitvoeringen. Als wij kijken naar de ambitie die bijvoorbeeld op lokaal, provinciaal en rijksoverheidsniveau wordt geformuleerd als het gaat om criminaliteitsbestrijding, moet je constateren dat 85% van alle aanhoudingen die in Nederland door de politie plaatsvinden door de surveillancedienst worden gedaan. Dat betekent dat wij behoefte hebben aan fatsoenlijke criminaliteitsbeeldanalyses, die op regionaal en lokaal niveau voor het bestuur, maar ook voor politie en justitie aangeven wat er speelt.
Mijn laatste opmerking betreft de Wet politiegegevens. Daar ging het de geachte spreekster zojuist om. Wij hebben in deze wet precies datgene geregeld wat u graag wilt, namelijk getrapte bevoegdheden bij een verdere verwerking van de gegevens. Als je na basale gegevensverwerking een stapje hoger wilt gaan, moet aan een aantal extra voorwaarden worden voldaan, zelfs met individuele toestemming van een bevoegde functionaris.

De heer **Buruma**: Dank u wel. Mevrouw De Poot, zijn er nog nabranders van uw kant?

Mevrouw **De Poot**: De heer Jacobs haalde mij de woorden uit de mond, toen hij een strikte scheiding maakte tussen de opsporings- en informatiebelangen. Ik vind het heel belangrijk dat de AIVD als het gaat om onze belangen op het punt van veiligheid en informatie de mogelijkheid heeft om meer dingen te zien en te doen, dan wanneer het gaat om opsporing door de politie. Er is gesproken over «op basis van een aanwijzing gaan zoeken». Op het moment dat de politie op basis van aanwijzingen gaat zoeken, krijgt men met mensen te maken die niet echt verdachte zijn en die dus ook geen rechtsbescherming genieten, althans niet op dezelfde manier als een verdachte, die met allerlei rechtswaarborgen omkleed is. Een probleem daarbij is dat op het moment dat je te veel op basis van aanwijzingen als politieorganisatie allerlei gegevens gaat verzamelen, men zich toch op het terrein gaat van de AIVD gaat begeven. Zelfs op dat moment ben ik terughoudend. De politieorganisatie heeft het recht om dat te doen, maar men moet zich dan wel realiseren wat dat betekent. Ik heb het sterke vermoeden dat de politie heel snel probeert om iemand tegen wie zij een aanwijzing hebben, echt verdachte te maken. Op het moment dat dat niet lukt moet men misschien zeggen: «hij gaat weer terug naar de AIVD, want het is ons pakkie-an niet». Die strikte scheiding vind ik erg belangrijk.

De heer **Buruma**: Dat wordt overigens ook binnen de criminele-inlichteneenheden onderkend. Het probleem is dat politie zich ook met terreurbestrijding moet bezighouden. Dat vinden zij vaak vervelend.

Mevrouw **De Poot**: Ik wil graag nog iets zeggen over de efficiency en effectiviteit van het gebruik van allerlei gegevensbestanden. Het is heel interessant, maar ook buitengewoon ingewikkeld om de effectiviteit van dat soort dingen na te gaan. Hoe kun je namelijk de effectiviteit van allerlei antiterrorismemaatregelen meten? Als er geen aanslagen zijn geweest, is het dan effectief geweest?

De heer **Buruma**: Dat is een belangrijke opmerking naar aanleiding van wat eerder werd gezegd over het belang van de impactanalyses.

Dames en heren, ik wist dat dit het zwaarste onderwerp zou zijn. Daarom heb ik het expres laten uitlopen. Nu heb ik mijzelf echter wel in de problemen gebracht. Over zeven minuten hebben wij pauze. Ik zou eerst de heer Munnichs nog het woord willen geven over het volgende onderwerp, cameratoezicht. Daarna kunnen wij dan een kopje koffie of thee drinken en er alvast over nadenken. Dan worden de vragen nog toegespitster.
Ik ben even kwijt welke deskundigen straks na de pauze blijven zitten, maar ik dank hen allemaal alvast voor hun deskundige inbreng.

Casuspositie II: Cameratoezicht

De heer **Munnichs**: Voor alle duidelijkheid: wij hebben de volgorde van de tweede en derde sessie omgedraaid. Wij gaan nu dus in op het cameratoezicht en daarna volgt het dna-onderzoek.
Gemeenten maken steeds vaker gebruik van camera's om de veiligheid te vergroten en het toezicht op de openbare orde te verbeteren. Zij worden vooral ingezet in uitgaanscentra en winkelcentra en rond stations. Dit toezicht is aan een aantal regels gebonden. Het is alleen toegestaan als andere middelen niet effectief zijn. Het middel dient overeen te stemmen met het doel en de inbreuk op de privacy moet zo klein mogelijk zijn. Het toezicht moet voor burgers kenbaar worden gemaakt en personen hebben recht op inzage en correctie van beelden.
Het aantal camera's is de afgelopen jaren flink toegenomen. Veel gemeenten hebben ook verdere plannen op dit gebied. Eigenlijk vormen de camera's een steeds alledaagser verschijnsel. Wij weten al bijna niet meer beter. Toch kunnen ook op dit punt een aantal vragen worden opgeworpen, die vooral betrekking hebben op de effectiviteit. Evaluatieonderzoek naar de effecten van cameratoezicht wijst uit dat er maar weinig over de effectiviteit kan worden gezegd. Gelet op het aantal camera's dat al wordt gebruikt, is dat een opmerkelijke conclusie, maar tegelijkertijd is dit verklaarbaar. In de eerste plaats zijn doelen van het cameratoezicht vaak vrij algemeen geformuleerd: vergroten van de veiligheid en toezicht op de openbare orde. Dat maakt deze doelen moeilijk meetbaar.
In de tweede plaats laten de misdaadcijfers een gemengd beeld zien van het effect van cameratoezicht. In een aantal gevallen nemen de misdaadcijfers af, in andere nemen zij juist toe. Dat kan trouwens samenhangen met het feit dat door cameratoezicht meer wordt gezien en meer wordt geregistreerd.
Ten derde maakt cameratoezicht vaak deel uit van een pakket aan maatregelen, waardoor onduidelijk is welk effect aan camera's kan worden toegeschreven. Al met al lijkt het er nog het meest op dat cameratoezicht uitgaansgeweld niet tegengaat, maar mogelijkerwijs wel een positief effect heeft op straatroof en auto-inbraak. In ieder geval vergroot het de pakkans na een incident.
Ook over het effect op de subjectieve veiligheid, de vraag hoe veilig mensen zich voelen, bestaat discussie. Wel kan cameratoezicht over het algemeen rekenen op een groot publiek draagvlak. Daarbij moet wel weer worden aangetekend dat burgers lang niet altijd weten wanneer ze worden gefilmd. Het ligt dus allemaal heel genuanceerd.
Nieuwe ontwikkelingen als intelligent cameratoezicht staan volop in de belangstelling. Camera's kunnen worden uitgerust met bewegingsdetectie, bewegingsanalyse, agressiedetectie en gezichtsherkenning. Onze Nationaal Coördinator Terrorismebestrijding verwacht slimme camera's in te kunnen zetten voor het voorkomen van terreuraanslagen. Zo zouden camera's patronen van afwijkend gedrag kunnen herkennen. Veel van de toepassingen staan echter nog in de kinderschoenen. Bewegingsanalyse en gezichtsherkenning kampen nog met de nodige problemen, zeker op drukke punten. Een kleine foutmarge in een druk station kan al tot veel vals-positieve meldingen leiden.

Een tweede ontwikkeling is het koppelen van camerabeelden aan databestanden. Er wordt al geëxperimenteerd met automatische nummerplaatherkenning, gekoppeld aan politieregisters en databestanden met niet betaalde boetes of openstaande belastingschulden. Dergelijke toepassingen zijn ook een vorm van datamining. De vraag is natuurlijk hoever je met dat soort toepassingen wil gaan.
Wij staan dus wellicht nog maar aan het begin van allerlei ontwikkelingen op het gebied van cameratoezicht. Voor een doordacht gebruik ervan lijken in ieder geval twee zaken van belang, zaken die ook terugkomen in de stellingen. Ten eerste lijkt er meer helderheid nodig over de doelstellingen van cameratoezicht. Moet het vooral dienen om kleine criminaliteit, volumecriminaliteit terug te dringen? Moet het vooral de pakkans na een misdrijf vergroten of kan het ook daadwerkelijk helpen bij het voorkomen van terreuraanslagen, zoals de heer Joustra zou willen. Ten tweede zullen wij meer inzicht moeten krijgen in de effectiviteit van cameratoezicht, bijvoorbeeld door meer en beter evaluatieonderzoek.

De heer **Buruma**: Dames en heren. Volgens het programma mogen wij ons nu een moment terugtrekken voor een kopje thee. Ik hoop dat ik u over een minuut of vijftien in deze zaal terugzie om over dit thema verder te spreken. Wees gerust: ik zal dan niet alleen proberen om de discussie korter te houden, maar ook om een verbinding te leggen met het punt dat de heer Munnichs noemde, het koppelen van databestanden aan cameratoezicht. Cameratoezicht is namelijk een even belangrijk onderwerp als de ontwikkeling van bijvoorbeeld de RFID-chips. Daardoor worden namelijk allerlei koppelingen mogelijk. En dat raakt weer aan het thema waarvoor deze middag is bedoeld.
Tot over een kwartier! De bijeenkomst wordt vijftien minuten geschorst.

De heer **Buruma**: Dames en heren. Wij hebben zojuist de inleiding gehoord van de heer Munnichs tot het onderwerp cameratoezicht. Nu is een drietal nieuwe deskundigen bij de heer Muijen aangeschoven. Ik stel hen kort aan u voor. Rechts van de heer Muijen zit de heer Teeuw van het Telematica Instituut. Links van de heer Muijen zit de heer Kohnstamm, de voorzitter van het College Bescherming Persoonsgegevens en naast hem zit mevrouw Dekkers van het onderzoeksinstituut Regioplan, die het nodige onderzoek heeft gedaan naar cameratoezicht in de praktijk.
Wij discussiëren opnieuw aan de hand van twee stellingen, die vooral bedoeld zijn om de discussie op gang te brengen. Wij weten allemaal dat er veel meer camera's zijn dan wij kunnen tellen. Ik las ergens dat er in Rotterdam alleen al, los van de particuliere dingen, 140 straatcamera's waren, en nog een eindeloos groter aantal in de metro's. En dat is alleen nog maar in de stad Rotterdam. Wat moeten wij daar nou mee? Hoe moeten wij daartegenaan kijken?
Ik wil u vooral uitnodigen om het thema cameratoezicht ook te beschouwen als een illustratie van de totaalverzameling die begint te ontstaan, al die kleine partjes van allerlei soorten gegevens die op elkaar kunnen worden aangesloten. Worden zij wel op elkaar aangesloten? Zijn daar nog bepaalde voorwaarden aan verbonden? Kunnen er dingen mee misgaan? Hoe werken zij? Hoe slim zijn zij? Dat is ook het punt waarmee ik begin: hoe slim zijn die camera's? Soms krijg je de indruk dat wij veel kunnen, alleen weet ik niet of dat betekent dat wij ook veel doen. Ik weet zeker dat de heer Teeuw ons een korte uiteenzetting kan geven over de werking van cameratoezicht. Ik denk dat wij allemaal vooral geïnteresseerd zijn in de intelligente camera's. Er zijn steden die ze hebben en er zijn steden die ze niet hebben. Waarom moeten wij aan de intelligente camera's en zijn die

dan uiteindelijk ook zelfontbrandend of blijven de camerabeelden ons tot in lengte van jaren achtervolgen als wij een keer door een prostitutiebuurt hebben gelopen?

De heer **Teeuw**: U stelt een vraag over de technologie. Ik ben voor de opbouw van mijn betoog uitgegaan van de stellingen. Daar ga ik dan ook op in. Wij moeten oppassen dat wij het cameratoezicht niet als doel gaan zien in plaats van als middel. Cameratoezicht is en blijft een middel. Dat vond ik ook mooi in de stelling dat cameratoezicht dient om zowel kleine criminaliteit als nieuwe terreuraanslagen te voorkomen. De heer Munnichs heeft in de inleiding al prima gezegd dat in geweldsdelicten en emotie camera's weinig helpen. Bij zaken als overlast blijken zij preventiever te werken. De stelling dat cameratoezicht criminaliteit helpt voorkomen, is vergelijkbaar met de stelling dat de mobiele telefoon criminaliteit helpt voorkomen, of het breedbandnetwerk dat de beelden vervoert. Cameratoezicht is een middel; het proces van de politie is leidend. De technologie ondersteunt dat.
Effectiviteit wordt vaak gemeten in subjectieve en objectieve veiligheid. Deze is echter ook af te meten aan de effectiviteit van de politie. Er zijn voorbeelden bekend van verdachten die bekennen omdat gesuggereerd wordt dat alles door camera's is opgenomen terwijl dat niet het geval is. De effectiviteit van camera's is gelegen in het feit dat met minder mensen meer zaken in de gaten kunnen worden gehouden. Daardoor is preventief optreden mogelijk.
Ik kom hiermee te spreken over de processen, waarbij ik terugkom op de voorgaande discussie over koppeling. Een camera is een sensor, zoals je heel veel sensoren hebt, bijvoorbeeld geluid. Je kunt allerlei databanken koppelen om de informatiepositie te verbeteren. Het meten van de kwaliteit van de informatiepositie is heel lastig. Wij voeren zelf een project uit om erachter te komen of camerabeelden van een crisissituatie een operationeel team helpen om een beter advies te geven aan een beleidsteam. Hoe kun je dat meten? Je zou dubbele metingen moeten doen, in een experimentgebied en in een controle gebied. Het is daarnaast ook lastig, want cameratoezicht wordt in Nederland niet los ingezet, maar als een van de maatregelen in een heel pakket.
De intelligentie van de camera moet altijd worden geplaatst in de context van het gebruik. Er kan heel veel, vooral in geconditioneerde omstandigheden. Als de belichting goed is en er niet te veel mensen in beeld zijn, is er veel mogelijk met de beelden, zoals het detecteren, volgen of classificeren van objecten. Intelligentie in de zin van «wat gebeurt er nu?» is een ingewikkelder verhaal.

De heer **Buruma**: Ik heb het volgende beeld bij een intelligente camera: als er drie jongens bij elkaar staan op een straathoek, staat de camera uit. Als een van de jongens plotseling met stemverheffing begint te roepen of wanneer hij een bepaalde grimas op zijn gezicht heeft waardoor hij er boos uitziet, begint de camera te lopen. Misschien zie ik het wat simpel, maar is dat nu ongeveer een intelligente camera, of is het iets anders?

De heer **Teeuw**: Die grimas kun je natuurlijk niet zien als de camera uit staat. Het geluid heeft te maken met het feit dat je twee sensoren hebt, één voor geluid en één voor beeld. Het beeld laat je pas lopen als je in het geluid agressie detecteert. Er zijn bedrijven die erin gespecialiseerd zijn om het geluid selectief te benaderen en agressie eruit te halen. Op dat moment kun je de camera laten lopen. De vraag is nu, hoe selectief je gegevens gaat verzamelen. Verzamelen wij alles en gaan wij achteraf analyseren, of gaan wij selectief verzamelen? Daarin speelt technologie een rol. Het klassieke proces van opsporing is: data verzamelen, analyseren en objectiveren, gevolgd door bewijsvoering en veroordeling. Door de technologie en de innovatie gaan die fasen in elkaar overlopen. De

camera maakt al een analyse van het geluid en op basis van die analyse wordt het vorige proces, het verzamelen van data, aangestuurd. Dat geldt in zijn algemeenheid en niet alleen voor de camera's. Neem bijvoorbeeld forensisch sporenonderzoek. Met lab-on-a-chip onderzoek kun je ter plekke al bloedsporen analyseren en vervolgens gerichter data verzamelen. De processen gaan dus veranderen en daar moet wellicht rekening mee gehouden worden in de wetgeving.

De heer **Buruma**: Als je vaststelt dat een bepaalde toonhoogte agressief is, neem je in feite al een beslissing over de vraag of je iets gevaarlijk vindt? Is dat wat u bedoelt met het door elkaar heen lopen van de fasen?

De heer **Teeuw**: In een forensisch proces worden er sporen verzameld. Die gaan naar een forensisch laboratorium en dat leidt tot een bewijsvoering. Die processen gaan veel sneller online, doordat je ter plekke de sporen kunt analyseren. Op basis daarvan kun je gerichter zoeken. Dit kun je vertalen naar de camera's. De vraag is dan, of er al een beslissing wordt genomen op zo'n moment. In hoeverre gaan alle fasen door elkaar lopen?

De heer **Buruma**: In feite betekent dit dus dat de wetgever er rekening mee moet houden dat de man achter de camera in de controlekamer heel vroeg in allerlei procedures bij wijze van spreken beslissingen zit te nemen die vroeger de officier van Justitie nam.

De heer **Teeuw**: Die processen gaan veel meer iteratief lopen. In het rapport van de commissie-Bosma wordt er ook meer een cyclisch verhaal in plaats van een lineair verhaal getoond.

De heer **Buruma**: Hoe lang is het eigenlijk normaal dat de gegevens van die camera's worden bewaard?

De heer **Teeuw**: Die vraag kunt u beter aan een jurist stellen.

De heer **Buruma**: Nee, ik ben gewoon benieuwd naar hoe lang het feitelijk normaal is om dergelijke gegevens te bewaren. Als je zoiets opneemt, wordt er dan telkens een nieuw bandje in gedaan?

De heer **Teeuw**: In de praktijk is het een paar dagen.

De heer **Kohnstamm**: Bij fietsenstallingen in sommige gemeentehuizen korter dan de politieke rel wellicht wenselijk had geacht.

De heer **Buruma**: Mijnheer Kohnstamm, u kunt dit vast aanvullen. Ik krijg de indruk dat erover wordt nagedacht en dat de apparatuur er is. Het verandert de gang van zaken wel een beetje. Er zullen meer beslissingen in een eerdere fase worden genomen.
De tweede vraag ging over nut en noodzaak. Mevrouw Dekkers gaat daar hopelijk zo meteen ook nog iets over zeggen. Nu was de heer Kohnstamm al even aan het woord, dus ik geef hem hierover ook graag het woord. U hebt natuurlijk ook gekeken naar wat er feitelijk gebeurt. Denkt u dat de kosten de baten waard zijn, gezien hetgeen in die gemeenten in de praktijk gebeurt? Dit bedoel ik niet alleen in termen van geld, maar ook in termen van waar u goed in bent: bescherming van persoonsgegevens. Hoe kijkt u aan tegen het verschijnsel camera's, die nieuwe camera's, dus de smartcamera's en tegen de vraag of de wetgever daar al dan niet iets mee moet?

De heer **Kohnstamm**: De wetgever heeft er onlangs, overigens met de wijziging van de Gemeentewet, een en ander over vastgelegd. Daar is een termijn van vier weken in opgenomen. De essentie blijft dat je het doel

waarmee je het doet, verschrikkelijk helder moet formuleren. Dat bleek ook uit de stellingen van het eerste panel. Als je dat nalaat, kun je aan het einde van de rit de effectiviteit bijvoorbeeld helemaal niet meer meten. Je kunt dan ook niet bepalen of het überhaupt van begin af aan zinvol is geweest. Naarmate je dat doel formuleert, kun je smartcamera's beter inzetten. Ik heb mij laten vertellen dat patroonherkenning nog een betrekkelijk ingewikkelde aangelegenheid is, bijvoorbeeld omdat de junk die op zoek is naar een autoradio, hetzelfde patroon aan de dag legt als de man die moet controleren of het parkeergeld wel is betaald. Dit kan tot misverstanden aanleiding geven. In Groningen is een «smart»of slim apparaat werkzaam. Er wordt alleen maar gefilmd als het geregistreerde geluid daar aanleiding toe geeft. Als ik voor een draaiende camera in elkaar getremd word, gebeurt er niets, dus in mijn ogen is dat niet erg effectief. De essentie moet dus zijn dat als die camera gaat draaien omdat er een alarmerend geluid is, er ook iemand is die ernaar kijkt en effectief kan ingrijpen om ervoor te zorgen dat de onverlaten verder van mij afblijven of om ervoor te zorgen dat er iemand komt om mij te helpen. Het is dus ontzettend moeilijk om over die punten in het algemeen iets te zeggen. De ontwikkelingen gaan wel heel hard. Dat zit hem precies in de koppeling van cameratoezicht aan andere gegevens, om het zo maar te zeggen. Het eerste panel heeft de CatchKen al genoemd. Het idee daarvan is dat je echt iedereen filmt en dat er achter die camera allerlei opsporingsgegevens over kentekens zitten. Er zijn drie categorieën. Ik houd het kort. De eerste methode betreft mensen die verdacht zijn met een bepaalde auto. Dan is het raar om een agent op de Utrechtsebrug neer te zetten en al die nummers te laten noteren om na te gaan of er iets aan de hand is. Dat is niet effectief; het is veel handiger om dat te koppelen aan gegevens die er zijn en om die mensen, zodra zij de Utrechtsebrug over zijn, in de kraag te vatten. De tweede methode is inmiddels ook hier en daar uitgeprobeerd. Die betreft veelplegers, draaideurcriminelen. Zij vormen een gigantisch probleem voor iedereen die daarmee te maken heeft en ook voor mensen die daar overigens niets mee te maken hebben.
Mag je nu kentekenbewijzen van draaideurcriminelen aan zo'n apparaat koppelen en hen vervolgens ook aan het einde van de Utrechtsebrug stoppen of hen volgen om te zien of er iets aan de hand is? Mijn rechtsgevoel zegt mij dat dit niet zomaar kan omdat het niet gezegd is dat een veelpleger altijd veelpleger zal blijven. De cijfers wijzen voor sommigen wel een beetje in die richting, maar dan nog vind ik dat de wetgever aan zet is. Dan moet, bij wijze van spreken, als bijkomende straf worden bepaald dat je gegevens wel aan de CatchKen mogen worden gekoppeld. Het derde punt, waar zojuist ook aan werd gerefereerd en waarover het Bundesverfassungsgericht net een uitspraak heeft gedaan, is dat je niet iedereen mag filmen en dus niet een grote databank mag bouwen van iedereen die in mijn voorbeeld over de Utrechtsebrug komt. Zeker in Amsterdam gebeurt er van alles wat geen daglicht kan velen, maar het is niet zo dat iedereen die naar Amsterdam komt daarmee ook verdacht is. Ik zou het dus ook vreemd vinden als wij die kant op gaan, door persoonsgegevens op te slaan als er geen begin van verdenking is. Een kentekenbewijs is uiteindelijk heel gemakkelijk te retraceren tot een persoon en is daarmee gelijk te stellen aan een persoonsgegeven.

De heer **Buruma**: Als die CatchKen alle kentekens filmt, gaat het toch niet om personen, maar alleen om auto's? Dus er is niets op tegen om die beelden op te slaan. Gaat het niet om iets anders dan om privacy? Is dit niet het onderwerp waarover wij eerder spraken? Hoe zit het in dit verband bijvoorbeeld met mensen die ten onrechte al in zo'n systeem staan? Komen fouten in deze systemen voor? Of is de informatie keihard? Het laatste zou je denken van filmbeelden, want ik loop in de rosse buurt of ik loop er niet. Fouten kun je daarmee niet maken, dus waarom zouden wij eigenlijk moeilijk doen? Dat was een van de belangrijkste punten uit

het eerste verhaal. Voor de privacy maakt het toch niet uit of men mijn nummerplaat filmt? Maakt men eigenlijk wel fouten met die films?

De heer **Kohnstamm**: Als men alleen maar nummerplaten filmt voor de leuke plaatjes en daar verder niets mee doet is dat geen probleem. Wanneer men de gegevens terugvoert op naam, adres en woonplaats van de eigenaar van het kentekenbewijs, is het kentekenbewijs indirect een persoonsgegeven, al is dat juridisch niet correct. Het gaat niet om het kenteken als zodanig maar om het feit dat men daarmee al heel snel bij een persoon terecht kan komen. De kwaliteit van de gegevensbestanden is in bijna alle gevallen relevant voor de bescherming van persoonsgegevens, voor non-discriminatie en voor het tegengaan van schade en vertrouwen in elkaar, maar net zo relevant voor de opsporing en vervolging. Het hele probleem dat keihard op ons af gaat komen – dit heeft misschien niet direct met cameratoezicht te maken, maar wel met de sessie van vanmiddag – van identiteitsfraude en identiteitsdiefstal heeft alles te maken met de integriteit van de informatie die in de datawarehouses zit.
Er zijn twee zaken waarover niemand tot nu toe echt iets kan zeggen. Niemand weet welke bulkgegevens nu door de geweldsmonopolist worden gebruikt. Verder weet niemand hoe effectief data mininig en alles wat daarmee samenhangt is. Dit brengt mij bij het laatste antwoord – waar ik wel om moest lachen – van mevrouw De Poot, dat de effectiviteit van antiterrorismewetgeving niet te meten is omdat er in Nederland te weinig terroristische aanslagen zijn. Bij meer aanslagen zouden wij die wel kunnen meten. Ik geef haar woorden heel vals weer, maar dit is wel het probleem. Ik heb het ook wel eens hier en daar gelezen. Het probleem van de effectiviteitsmeting is dat wij niet weten wat ermee gebeurt en dat wij daarmee ook niet de volgende stap kunnen zetten door de volgende keer nog eens beter na te denken.

De heer **Buruma**: Misschien kan mevrouw Dekkers ons over die effectiviteit nog iets naders vertellen. Zij heeft daar onderzoek naar gedaan en zij weet hoe veel misdaden worden opgelost dankzij de camera's en hoeveel camera's er lopen waarmee nooit iets gebeurt.

Mevrouw **Dekkers**: Ik had gehoopt hier een eenduidig antwoord te kunnen geven, in de trant van «het werkt wel» of «het werkt niet», maar zo simpel is het niet. Mevrouw De Poot heeft daarnet ook al gezegd dat effectiviteit heel moeilijk te meten is.
Het komt ook, doordat gemeenten het cameratoezicht over het algemeen slecht evalueren. Ruim de helft van de gemeenten heeft het cameratoezicht nog nooit geëvalueerd. De kwaliteit van de evaluaties die wel zijn uitgevoerd, is niet altijd even goed, maar voor zover daarover uitspraken kunnen worden gedaan, is het beeld erg wisselend. De criminaliteit neemt soms toe, maar soms ook af. Er is in die zin geen eenduidig beeld, maar de constatering van een toename van de criminaliteit is niet per definitie negatief, omdat er meer ogen op straat zijn en omdat de aangiftebereidheid stijgt. Daardoor wordt een deel van de verborgen criminaliteit zichtbaar. Merkwaardig is wel dat er zo gemakkelijk wordt overgestapt op het inzetten van cameratoezicht. De verwachtingen van de effectiviteit daarvan liggen hoog, maar gelet op het gebrek aan kennis over een en ander is dat merkwaardig. In Engeland is men heel erg ver met cameratoezicht, maar ook daar is de kennis nog behoorlijk beperkt.
Ik wijs nog wel op de ontwikkeling van het koppelen van het cameratoezicht dat onder het private en onder het publieke regime wordt toegepast. Daar wordt steeds meer naar toe gegaan. Stel dat in een winkel een camera is opgesteld. Als daarmee een bepaald incident wordt waargenomen, wordt dat op een andere manier bekeken dan een incident dat via de camera op straat wordt waargenomen. Van verschillende kanten hoor

ik regelmatig dat men het vreemd vindt dat de informatie via de camera uit de winkel niet kan worden gebruikt voor het aansturen van de camera op straat. Soms is die informatie niet eens bekend, maar als dat wel het geval zou zijn, zou iemand daarna door de camera op straat in de gaten kunnen worden gehouden. In die zin zou je wat dat betreft een koppeling kunnen krijgen.

De heer **Buruma**: Dat is heel handig. Als ergens een overval is en de snuiter rent naar buiten, zou je willen dat een camera aanfloept om de persoon te kunnen volgen. Waarom gebeurt dat nu niet? Komt dat door de wetgeving, of door de manier waarop dit is georganiseerd?

Mevrouw **Dekkers**: Dat komt door de wetgeving. Er is sprake van twee wettelijke regimes die strikt gescheiden zijn. Je hebt een uitkijkruimte voor de publieke beelden en een uitkijkruimte voor de private beelden. Soms zijn ze wel samengebracht in een en dezelfde uitkijkruimte, maar de regimes zijn strikt gescheiden. Er is sprake van twee verschillende harddisks waarop de beelden worden opgenomen.

De heer **Buruma**: Welk voordeel heeft die scheiding? Het klinkt alsof er alleen maar nadelen zijn.

De heer **Kohnstamm**: Het gaat gewoon om twee verschillende bevoegdheden. Daarom moet je heel erg oppassen wat je met de gegevens doet en wie daar iets mee doet. De winkelier heeft een andere bevoegdheid dan de burgemeester in het kader van de openbare orde.

De heer **Buruma**: Dat begrijp ik. Ik snap ook heel erg goed dat er op dit moment verschillende wettelijke regimes zijn. Een van de redenen waarom wij hier zitten, is echter dat al die wetten door elkaar lopen en dat het heel ingewikkeld en onoverzichtelijk is. Het feit dat sprake is van verschillende wettelijke regimes zou een voorbeeld kunnen zijn van een nadeel. Voordat de Kamerleden roepen dat dit moet worden aangepakt, wil ik eerst horen waarom dat niet zou moeten.

De heer **Kohnstamm**: Het gebeurt in de praktijk al. Neem Schiphol. Daar heeft men één camerasysteem voor de afhandeling van de bagage, het tanken van vliegtuigen en al dat soort zaken. Er is dus één front office, maar daar achter zitten allerlei back offices waar met verschillende verantwoordelijkheden naar de beelden wordt gekeken. Vervolgens wordt daar iets mee gedaan door degenen die daarvoor zijn ingehuurd. Als je dat fatsoenlijk regelt, als iedereen dat weet, als het doelgericht is, is daar niet zo gek veel op tegen. Je moet er ontzettend voor oppassen om publiek en privaat door elkaar te laten lopen, want dan gaan de geweldsmonopolist en de tanker van de vliegtuigen ineens door elkaar lopen.

De heer **Muijen**: Ik snap de opmerking dat het wenselijk is dat je, als je de winkel verlaat, in de openbare ruimte wordt opgevangen door een camera die je dan weer volgt, maar het uitgangspunt is dat je je in de openbare ruimte in beginsel onbevangen moet kunnen bewegen. Wij hebben alleen een regeling voor het gemeentelijk cameratoezicht in de openbare ruimte. Dat is vooral voor het handhaven van de openbare orde. Daar moet je niet veel verder in gaan.

De heer **Buruma**: Als ik goed geïnformeerd ben, hebben tien van de elf grote steden met meer 150 000 inwoners deze camera's. Dit betekent dat de beslissing of je camera's wilt of niet op gemeentelijk niveau ligt. Begrijp ik het goed dat u niet zegt dat eigenlijk nationaal geregeld moet worden dat er overal camera's komen?

De heer **Muijen**: Dat zou mijn antwoord zijn. Ik benader het even heel simpel. Als men het op lokaal niveau noodzakelijk vindt nadrukkelijker te kijken naar de openbare orde... U weet wellicht dat het wordt uitgevoerd door de politie. De politie kijkt uit. Overigens is mijn stellingname dat online moet worden uitgekeken. De Gemeentewet biedt de mogelijkheid om niet online uit te kijken en de beelden dus naderhand te bekijken. Het moet wel tot actie leiden. Dit is een belang van de openbare orde. In uw vraag zit een beetje verborgen hoe men er bij justitie tegenaan kijkt. Ik moet u zeggen dat ik er wel blij mee ben. Stel dat u in elkaar wordt getremd, mijnheer Buruma, en het wordt opgenomen, dan krijgt de politie het filmpje dat vervolgens als digitale bijlage bij het proces-verbaal gevoegd. Wij krijgen het via de politie aangeleverd in digitale vorm. Tijdens de zitting kunnen wij het de ontkennende of de bekennende verdachte voorhouden. Het is altijd heel bijzonder om te laten zien onder welke omstandigheden dit aftuigen heeft plaatsgevonden. Persoonlijk, als officier van justitie, ben ik dus blij met deze techniek.

De heer **Teeuw**: Ik zei al dat ik geen jurist ben, maar daarom kan ik ook een vraag stellen. Als techneut vind ik het volgende merkwaardig. Er is cameratoezicht dat onder artikel 151c van de Gemeentewet valt. Het moet door de gemeenteraad, het moet het laatste middel zijn, enzovoort. Daarnaast is er nog de Politiewet, artikel 2, voor mobiel cameratoezicht. Hierbij hoeft de gemeente alleen maar geïnformeerd te worden. Sommige mobiele camera's kunnen erg lang op dezelfde plek staan. Verder is er ook nog het private cameratoezicht. Deze camera's hangen ook aan de buitenkant. Officieel moet alles wat buiten de voordeur valt, afgeplakt worden, maar ik kan zo een foto sturen uit Enschede waarop zes camera's te zien zijn die bij elkaar hangen en waarvan niemand weet welke camera van wie is. Mijn stelling is dat dit vroeg of laat bij elkaar gaat komen.

De heer **Buruma**: Mevrouw Dekkers, hebt u nog een slotopmerking? Anders gaan wij naar het onderwerp DNA toe. U hebt misschien nog iets op het oog waarvan u zegt: dit is er aan de hand in verband met de camera's, dat moeten de Kamerleden weten en daaraan moeten zij iets gaan doen.

Mevrouw **Dekkers**: Wat ik nu zie in het onderzoek dat wij doen, is dat er een neiging is om steeds meer naar die koppeling te gaan. Het is wel heel erg aantrekkelijk om gebruik te maken van alle resources die je hebt om die ene boef op straat te kunnen pakken. Ik denk dat wij met ons allen er heel goed over moeten nadenken hoever wij hierin willen gaan.

De heer **Buruma**: Dat is in feite ook een beetje wat de heer Teeuw al suggereert zijn opmerking over die zes camera's.
Omwille van de tijd – de sessie over het onderwerp DNA wordt nu heel kort – wil ik de sprekers bij deze sessie hartelijk danken. Bij een van de volgende sessies zien wij de heer Kohnstamm nog terug.
Ik verzoek de spreker van het Rathenau Instituut om zijn betoog zo kort mogelijk te houden.

Casuspositie III: DNA-profielen

De heer **Brom**: Binnen het opsporingsapparaat bestaan hoge verwachtingen van het gebruik van DNA-onderzoek. Dat is niet verwonderlijk, want vergeleken met bijvoorbeeld vingerafdrukken biedt DNA-onderzoek grote voordelen. DNA-sporen zijn makkelijker te vinden, ze bevatten meer informatie en ze hebben een groter onderscheidend vermogen. De Raad van Hoofdcommissarissen verwacht dan ook dat DNA-onderzoek het oplossingspercentage van misdrijven fors helpt opschroeven. DNA-bewijsvoering lijkt erg betrouwbaar, oftewel men zegt: een DNA-profiel liegt niet.

Daarom wordt er flink geïnvesteerd in DNA-onderzoek. Maar er zijn ook enkele aandachtspunten.
Ten eerste is forensisch bewijs zelden 100% waterdicht. Dat geldt ook voor DNA-materiaal. Afhankelijk van de kwaliteit van het materiaal zijn er foutmarges. Bovendien moet er een relatie gelegd worden tussen spoor en delict. Zo kunnen inbrekers bewust een dwaalspoor uitzetten door haar van iemand anders achter te laten. Maak dat maar eens duidelijk in de rechtzaal. Kortom, dichten wij aan DNA-bewijs niet te veel zekerheid toe? En hebben opsporingsambtenaren en rechters voldoende kennis om de onzekerheden goed te interpreteren?
Er is ook een tweede aandachtspunt, namelijk de trend om steeds grotere databanken met DNA-profielen aan te leggen. Daar zijn ze weer, de databanken. De voor de hand liggende gedachte hierbij is: hoe groter de databank, hoe groter de kans dat het profiel van een dader erin voorkomt. Met een grotere databank hebben wij echter ook het risico van een grotere kans op een mismatch, een vals positieve match, met het gevaar van een ongegronde verdenking. Dat is voor de verdachte én voor de rechtsstaat een probleem. Bovendien vormt dit een belasting van het opsporingsapparaat. Hierbij doet zich dus eveneens de effectiviteitsvraag voor.
Het derde aandachtspunt wordt gevormd door de trend om bij steeds lichtere vergrijpen DNA-materiaal af te nemen. In 1994 werd het toegestaan voor zware misdrijven en sinds 2001 mag het al voor misdrijven met een maximumgevangenisstraf van vier jaar. Daaronder vallen woninginbraken en winkeldiefstallen. Dit komt onder andere door de technologische vooruitgang. Afname is nu veel minder invasief. In 1994 was bloedprikken nog noodzakelijk; nu is een beetje wangslijm voldoende.
Welk doel dienen databanken? Ook die vraag hebben wij eerder gehoord. De recente uitbreiding van het Verdrag van Prüm maakt deze vraag urgent. Dit verdrag regelt de uitwisseling tussen EU-staten van DNA-informatie van verdachten. Grensoverschrijdende criminaliteit moet hiermee bestreden worden. Is het opslaan van gegevens van winkeldiefstalplegers hiervoor zinnig? Vang je daarmee wie je wilt vangen? Daarbij komt de vraag van de rechtsbescherming. Bij de uitwisseling van DNA-profielen in EU-verband is de positie van burgers in het geding. Verschillende EU-lidstaten hanteren verschillende criteria voor opname in een DNA-databank. Ook dit hebben wij in de eerste sessie al gehoord. Er is geen uniform stelsel voor gegevensbescherming. Het lijkt dat het voor burgers onduidelijk is waar zij hun recht kunnen halen bij onterechte verdenking.
Er is kortom voldoende reden om de discussie voort te zetten. Daartoe hebben wij een aantal stellingen geformuleerd. Hierin komen twee zaken aan de orde: de bewijskracht van het DNA-materiaal en het doel van de opslag van DNA-profielen in de databanken.

De heer **Buruma**: Ik nodig graag uit: professor Broeders, hoogleraar criminalistiek aan de Universiteit Maastricht, mevrouw De Poot, die al eerder het woord heeft gevoerd, mevrouw Van der Ploeg, lector infonomie aan de Hogeschool Zuyd en de heer Hustinx.
Mijnheer Broeders, ik laat de anderen rustig zitten, maar u kunt alvast vertellen waarom het zo zou kunnen zijn dat DNA toch niet zo zeker is als wij vast allemaal denken, of althans zoals ik zelf dacht. Ik kan mij iets voorstellen bij een boef die in een zwembad de haren uit een putje haalt en deze rondstrooit. Dat begrijp ik, maar in zijn algemeenheid is DNA-materiaal toch keihard?

De heer **Broeders**: DNA is inderdaad een middel dat een groot onderscheidend vermogen heeft, zoals al in de inleiding werd opgemerkt. In de inleiding is eveneens gezegd dat de herkomstbepaling slechts één aspect is. Je kunt met een groot onderscheidend vermogen vaststellen of celmateriaal van een bepaalde persoon afkomstig is, maar dan rijst onmiddellijk

de tweede vraag: bij welke activiteit is dat celmateriaal vrijgekomen? In strafrechtelijke zin maakt het nogal wat verschil of het gaat om verkrachting dan wel om consensueel seksueel contact. Daarmee zijn wij meteen op het derde niveau, dat van de delictgerelateerdheid. Wij kunnen vaststellen dat celmateriaal op een bepaalde plaats aanwezig is, maar de vraag is vervolgens nog: hoe is het er gekomen? De derde vraag is of het om een delict gaat. Die drie vragen moeten niet door elkaar worden gegooid.
Het onderscheidend vermogen is inderdaad heel erg groot. Dat was het zeker in het begin. Toen wij begonnen met DNA-onderzoek, had je een heleboel bloed nodig en vrij veel sperma om daarvan als het ware een prachtig profiel te maken. Tegenwoordig kunnen wij door de toegenomen analysemogelijkheden ook met een heel slechte sporen werken. Daarvan krijg je heel moeilijke profielen, in de zin dat het profielen zijn waarin het materiaal van een aantal personen aanwezig is. De Schiedammer parkmoord was daarvan eigenlijk het eerste voorbeeld. Daarbij is een techniek gebruikt, low copy number DNA-analyse, waarbij je al van tevoren weet dat je heel slecht materiaal hebt en dat je dus inderdaad grote problemen zult krijgen met de interpretatie van die profielen. Je weet immers niet of de pieken die je ziet echte pieken zijn of artefacten. In die zin is DNA-bewijs zowel boterzacht als spijkerhard.

De heer **Buruma**: Ik heb gelezen dat het NFI sinds 1 januari werkt met robots om dit soort DNA-onderzoek te doen. In het eerste jaar streeft men ernaar om naar ik meen 35 000 van die DNA-profielen te maken en uiteindelijk moeten dat er 80 000 per jaar worden. Bestaat er geen grote kans dat daarin allemaal fouten gaan ontstaan?

De heer **Broeders**: Ik denk dat wij een onderscheid moeten maken. Er zijn referentieprofielen, die afkomstig zijn van het wangslijmvlies van personen die veroordeeld zijn of van verdachten. Ik denk dat je deze profielen heel goed gerobotiseerd kunt bewerken. Daarbij kunnen natuurlijk altijd fouten gemaakt worden. Overigens, robotiseren en automatiseren zijn eigenlijk dé manier om fouten te voorkomen. Fouten ontstaan meestal als mensen zoals u en ik dingen overschrijven van het ene briefje op het andere. Het is natuurlijk wel belangrijk dat je het aan het begin echt goed automatiseert. Dat is ook al een aantal malen gezegd vandaag. Ik denk dat het probleem hem zit in de interpretatie van het sporenmateriaal van het plaats delict.

De heer **Buruma**: Je moet dus vooral investeren in technische recherche?

De heer **Broeders**: Natuurlijk moet je daar ook in investeren. Het begint inderdaad bij de vraag waar je het materiaal gaat verzamelen. Zodra je profielen hebt, krijg je inderdaad de vraag hoe je de profielen interpreteert. Op dat gebied moet nog een heleboel wetenschappelijk onderzoek gedaan worden. Bij de FSS in Engeland, zo'n beetje de baanbreker op het gebied van DNA-onderzoek, heeft men het programma Pendulum List Searching ontwikkeld. Dit is een geautomatiseerd programma, waarmee je kunt uitrekenen welke profielen kunnen hebben bijgedragen aan een complex van mengprofielen. Je krijgt zo alle mogelijkheden onder elkaar en kunt dan, misschien met verstand, daarnaar kijken en bepalen welke profielen je serieus neemt. Vervolgens kun je naar je databank kijken enzovoort. Deze tak van sport is echter nog in ontwikkeling.

De heer **Buruma**: Ik begrijp dat mevrouw De Poot onderzoek heeft gedaan, ook naar wat er in Engeland gebeurt. Daaruit komt naar voren dat het allemaal niet zo succesvol is als wij denken dat het is. Misschien heb ik het echter te snel gelezen.

Mevrouw **De Poot**: Dat is wel een beetje kort door de bocht. Wij hebben inderdaad het gevoel dat wij met behulp van DNA veel meer zaken opgelost krijgen. De mogelijkheden zijn echter beperkt. De meeste zaken die de politie oplost, worden niet aan de hand van DNA opgelost. Dit wil zeggen dat de politie de daders niet vindt aan de hand van DNA. Meestal is de rol van DNA wel heel erg belangrijk als bewijsmateriaal achteraf, als de dader op een andere manier gevonden is.

De heer **Broeders**: Ik wil hierbij een kleine kanttekening maken. Ik denk dat mevrouw De Poot haar uitspraak vooral baseert op de studie die zij een aantal jaren geleden gedaan heeft. Er is een belangrijk onderscheid te maken tussen kapitale delicten, waarbij je de verdachte inderdaad niet vaak vindt door DNA-onderzoek, en het project volumecriminaliteit dat in Nederland en in Engeland, als twee van de weinige landen, goed draait. Daarbij wordt DNA-onderzoek als integraal opsporingsmiddel ingezet. Grote aantallen inbraken worden hierbij gerelateerd.

De heer **Buruma**: Even voor uw kennis: dat haalt de 7% van alle opgeloste inbraken niet. Ik denk dus dat je «grote aantallen» tussen aanhalingstekens moet zetten.

De heer **Broeders**: In absolute zin zijn het grote aantallen, in relatieve zin kennelijk niet. Niettemin gaat het om substantiële aantallen, waarbij je plaatsen delict kunt linken. Daarmee kom je wel degelijk uit bij verdachten.

De heer **Buruma**: Dan moet je dus wel gegevens in je bestand hebben.

Mevrouw **De Poot**: Diezelfde kanttekening wilde ik ook al maken. Je moet de gegevens altijd relateren aan het ophelderingspercentage bij een bepaalde delictcategorie. Dit onderzoek is gedaan in Engeland, waar de databank op dat moment al behoorlijk groot was. Er zaten miljoenen DNA-profielen in de databank. Inbraken zaten inderdaad rond de 7%, maar een heleboel andere delicten zaten dus veel en veel lager. Hierdoor was het ophelderingspercentage, het percentage van alle opgehelderde delicten en de delicten waarbij DNA een rol had gespeeld, 1,5%.

De heer **Buruma**: Mevrouw Van der Ploeg, u hebt ook onderzoek gedaan naar DNA en naar biometrie. U verneemt dit soort ontwikkelingen. Kennelijk worden er steeds meer gegevens opgeslagen. Een enkele keer denk ik wel eens: komt niet sluipenderwijs iedereen in de DNA-bank terecht? Hoe kijkt u daar tegenaan? Hoe kijkt u tegen deze ontwikkeling aan?

Mevrouw **Van der Ploeg**: Engeland is in dit verband een heel mooi voorbeeld. In Engeland duikt regelmatig het pleidooi op om de hele bevolking dan maar in de databank te stoppen, omdat dit de effectiviteit zou verhogen. Ik denk dat wij een grote terughoudendheid moeten betrachten. Wij moeten de criteria niet steeds maar oprekken om de databank gevuld te krijgen, ook al gaat het om volumediefstal. Ik zie het belang ervan om dit soort dingen goed aan te kunnen pakken, vanuit het perspectief van de politie enzovoort. Niettemin denk ik dat wij op dit terrein een grote terughoudendheid moeten betrachten. Het feit dat je in zo'n database terechtkomt, markeert je in zekere zin toch als een verdachte. Iemand komt daar in een bepaalde sociale categorie terecht en dat heeft gevolgen voor hem.

De heer **Buruma**: Dat is niet het geval als iedereen daarin zit, vanaf het moment dat een hielprik is afgenomen.

Mevrouw **Van der Ploeg**: In zekere zin behandel je dan de hele samenleving structureel als verdachte. Daar moet je natuurlijk in zekere zin ook

niet naar toe willen. Een ander aspect van met name DNA en biometrie betreft het feit dat het bij de DNA-discussie heel vaak gaat over de rechten van de verdachte en over lichamelijke integriteitskwesties – die discussie schijnt al gevoerd te zijn – omdat men dan met name focust op een moment van afname van lichaamsmateriaal. Dan is het inmiddels een kwestie van: oké, er is geen bloedprik meer nodig, een beetje wangslijm is voldoende; dat is toch allemaal zo ernstig niet en aan die paar haren ligt het ook allemaal niet. Ik wil er toch op wijzen dat wat wij hier voor ons zien, toch een vorm van informatisering van het lichaam is. Het brengt mogelijk een heel nieuwe vorm van mogelijke schendingen van integriteit van het lichaam met zich mee. Ik bedoel daarmee dat wij juist door digitaliseringsprocessen die zich richten op het menselijk lichaam, als het ware een vertaling zien van lichamelijke kenmerken en van het menselijk lichaam in digitale informatie, die dan eenmaal opgeslagen ook eindeloos beschikbaar blijft voor analyse, opsporing en wat al niet meer. Daarmee krijg je dus als het ware de mogelijkheid van een virtueel lichamelijk onderzoek, waarbij de desbetreffende persoon zich op een heel andere plaats en in een heel andere tijd kan bevinden en wat ook eindeloos in de tijd herhaald kan worden. Daarmee worden op een heel nieuwe manier integriteitskwesties aan de orde gesteld.

De heer **Buruma**: Dit is toch een beetje vaag voor mij. Wat betekent dit nu concreet? Bedoelt u te zeggen dat als je wangslijm bewaart, daar dan ander onderzoek op losgelaten wordt?

Mevrouw **Van der Ploeg**: Dat is ook nog een kwestie. Wat bewaar je nu precies? Wordt er alleen een digitaal bestandje bewaard, of worden ook nog de biologische samples bewaard? Daarover bestaat ook vaak onduidelijkheid. Wanneer je weer terug kunt grijpen op het biologisch materiaal, dan zijn er nog weer andere vragen te stellen.

De heer **Buruma**: Dat bedoelde u kennelijk niet. Wat bedoelt u dan?

Mevrouw **Van der Ploeg**: Ik bedoel te zeggen dat juist met die technologie en die digitaliseringsprocessen het lichaam als het ware andere bestaansvormen aanneemt, in een digitale vorm. Daarmee bestaat het lichaam als het ware als informatie. Er wordt ook gezegd: DNA is wat je bent en DNA is informatie. Over ons lichaam leren wij steeds meer te denken in termen van informatie. Dat lichaam krijgt andere bestaansvormen. Daarmee ontstaan nieuwe risico's voor de integriteit van dat lichaam.

De heer **Buruma**: Mijnheer Muijen. Nieuwe risico's, maar ook nieuwe kansen. U wilt vast gewoon een DNA-databank in Nederland.

De heer **Muijen**: Dat klopt.

De heer **Buruma**: Dat is handig: boeven vangen.

De heer **Muijen**: Ik kan alleen maar aangeven hoe het in onze praktijk werkt. Wat ik persoonlijk vind van de vraag of wij iedereen in Nederland in een databank moeten stoppen, is niet zo relevant.
Ondanks het feit dat 7% niet veel is, wil ik toch het volgende erover zeggen. In de praktijk komt de politie ter plaatse en constateert dat er ingebroken is en dat er een sigarettenpeuk ligt. Die peuk wordt onderzocht en uit dat onderzoek blijken twee goede profielen te halen te zijn; daaruit kan geconcludeerd worden dat er vermoedelijk twee verdachten hebben staan wachten en aan diezelfde sigaret hun genot hebben ontleend. Maar aan die profielen hangt geen naam. Doordat die databank beschikbaar is en wij het profiel daarin laten vergelijken, komt er een soortgelijk profiel

uit met daarbij een naam. Dat betekent dat het eerste bovenregionale rechercheteam, dat een paar jaar geleden is gestart, zo'n 350 woninginbraken heeft kunnen oplossen. Dat wil overigens niet zeggen dat dan 350 keer een hit in die databank gedaan wordt. De opsporing komt in dat geval verder om de hoek kijken. Dat is dus het nut van een DNA-databank. Ik ben persoonlijk daar erg tevreden over; los van de technische onvolkomenheden, want het moet wel allemaal goed zijn. In de praktijk valt mij op dat wij bij de DNA-hits die het Openbaar Ministerie worden gemeld, in de slag moeten met de politie om voldoende opsporingscapaciteit te krijgen voor een zaak, waarvan ik niet zeg dat die op voorhand rond is, maar die zeker wel voldoende aanleiding biedt om te onderzoeken. Wij hebben heel veel moeite om die onderzoeken te «slijten».
Ik weet niet hoe het misverstand elke keer weer in de wereld komt, maar ik zie dat in de stukken staat: «Opsporingsambtenaren en rechters hechten te veel waarde aan de bewijskracht.»; officieren van justitie worden niet vermeld. Ik weet in ieder geval dat bij de discussie over een kale bewijskracht het voor rechters niet op die manier geldt en dat het zo ook nooit wordt benaderd. Dat misverstand blijft echter bestaan.

De heer **Buruma**: Ik onderschrijf uw laatste opmerking blind, voor zover een voorzitter iets mag onderschrijven. Er is echter nog wel één ding. U merkte op: krijg je het wel gedaan? Dat was een heel spannende opmerking. In mei aanstaande – daarbij richt ik mij tot de heer Hustinx, maar een kleine opmerking van uw kant wil ik daarover nog wel horen – worden alle onopgeloste zaken waarvan profielen bestaan, via het Verdrag van Prüm uitgezet naar de rest naar Europa.
Ik las op de website van het NFI dat men verwacht dat daar 2000 tot 3000 zaken uit zullen rollen. Welnu, welke agent is hiervoor beschikbaar? Wordt het niet haast virtueel wat er aan mogelijkheden tot onze beschikking staat, terwijl wij daar tegelijkertijd helemaal geen gebruik van maken? Is het wat dat betreft allemaal wel de moeite waard?

De heer **Muijen**: Dat is een terechte vraag. Vooraf moet je je die vraag zeker stellen, in overleg met de Nederlandse politie en andere opsporingsinstellingen die er daarbuiten nog zijn. Het moet wel degelijk aan de voorkant geregeld worden, anders blijft het of te lang op de plank liggen, of gebeurt er simpelweg niets meer. Het is een reële vraag, waar wij met zijn allen een antwoord op moeten vinden.

De heer **Broeders**: Wij hebben dit verschijnsel in Engeland gezien. De eerste cd-rom die door Nederland naar Engeland is gestuurd, heeft daar een jaar op het bureau van een ongetwijfeld heel belangrijke man gelegen zonder dat de cd-rom gebruikt werd. Het ding heeft nog net niet in een pub gelegen. In Engeland heeft men natuurlijk nogal wat cd-roms met allerlei belangrijke gegevens daar achtergelaten.

De heer **Buruma**: Inderdaad. Omwille van de tijd heb ik een vraag aan de heer Hustinx. Het Verdrag van Prüm is natuurlijk een enorm punt. Ik heb in Privacy International gelezen dat men het ons erg verwijt dat wij graag wilden dat er in Europees verband samenwerking is, en dat soort dingen. Ik begreep niet helemaal wat er tegen zou zijn. Is de heer Hustinx er wel voor of is hij het met de mensen van Privacy International eens? Zitten er eigenlijk bezwaren aan het Verdrag van Prüm of is het, zoals de heer Muijen opmerkte, wel handig en moet er hooguit op de capaciteit worden gelet?

De heer **Hustinx**: Het Verdrag van Prüm was misschien wel een verstandig project, maar het was bedoeld als proef in een klein aantal landen, zeven, die met elkaar ervaringen zouden gaan uitwisselen op dit nieuwe gebied. Er heeft een onverantwoorde versnelling plaatsgevonden. Binnen

een half jaar tot een jaar is dat kleinschalige proefproject tot een megaproject van 27 landen uitgegroeid. Daarbij gaan brokken vallen. Dat heeft alles te maken met het feit dat de praktijken en de ervaringen in die zeven landen, maar zeker in die 27 landen, heel verschillend zijn. Dat betekent dat wij de diversiteit die er daardoor gaat ontstaan, weerspiegeld zullen zien in allerlei onderzoeken.
Het is al een paar keer vermeld dat Engeland wereldkampioen is op het gebied van DNA-profielen. Onder die 27 landen zijn er echter ook die nog nooit iets met DNA gedaan hebben. De spelregels van het Verdrag van Prüm voorzien nu in het verplicht instellen van DNA-databases. Dat is dus een Europees besluit dat in de politiek rond is. Tegelijkertijd is men bezig er implementatieregels over af te spreken. De versnelling die daar wordt afgesproken zou ons zorgen moeten baren, want die heeft alles in zich wat wij in de eerste sessie over databanken als funest hebben aangemerkt. Er zou dus eens moeten worden gekeken hoe twee landen met verschillende spelregels hier verstandige resultaten kunnen boeken.
De Duitsers hebben hun voorzitterschap van de EU gebruikt om te zeggen dat zij in de eerste maand met Oostenrijk 2000 gevallen hebben uitgewisseld, moordenaars, kinderverkrachters enzovoort. Dat is onweerstaanbaar. Er is geen minister die daar weerstand aan kan bieden. Toen is het binnen drie maanden besloten.

De heer **Buruma**: Kunnen wij er nog iets aan doen? Nee toch?

De heer **Hustinx**: Jawel. Als ik het goed heb begrepen, heeft Nederland het Verdrag van Prüm geratificeerd. Dat geldt voor de zeven landen die ermee begonnen, de Benelux, Duitsland, Oostenrijk, Spanje en Frankrijk. Verder komt er dus een kaderbesluit aan. Wij zouden nog eens heel goed kunnen kijken naar de implementatie daarvan.

De heer **Buruma**: Ik geef het woord aan mevrouw Strik.

Mevrouw **Strik** (GroenLinks): Ik heb twee vraagjes. Het ene ging meer over het ontwikkelen van technologie; mevrouw Van der Ploeg kan er misschien antwoord op geven. Er is net al aangegeven dat er in de toekomst wellicht meer mee kan worden gedaan. Ik heb er niet zo heel veel verstand van, maar ik kan mij voorstellen dat je straks veel meer uit DNA-materiaal kunt lezen dan nu. Kun je dat dan ook doen met het materiaal dat nu wordt afgenomen? Is op de een of andere manier te garanderen dat het niet mogelijk is, ofwel in technologische zin of via de wet? Ik vraag een heel concreet wetgevingsadvies van de heer Hustinx. In de inleiding werd al over het belang van rechtsbescherming gesproken. Aan de orde is nu het Kaderbesluit bescherming persoonsgegevens voor de derde pijler voor politiële en strafrechtelijke samenwerking. Wij moeten binnenkort beslissen of wij daarmee instemmen. Wat betreft doelbinding worden er heel veel uitzonderingen gemaakt op de doelvereisten. Je mag best in een aantal opzichten afwijken van het doel. Bovendien is het vrij arbitrair wanneer je het kunt overdragen aan een derde land. Een lidstaat kan zelf bepalen of dat een voldoende effectief beschermingsniveau biedt. Moeten wij hiermee akkoord gaan? Of zou het slimmer zijn om te zeggen: die derde pijler bestaat nog maar een jaar; over een jaar zijn er geen pijlers meer? Is het dan niet veel slimmer om de Richtlijn bescherming persoonsgegevens, richtlijn 46, zodanig uit te breiden dat politiële en strafrechtelijke samenwerking daaronder kan vallen? Dan hebben wij een eenduidig systeem. Dat is beter voor de rechtszekerheid. Zou dat kunnen en zou dat wenselijk zijn?

De heer **Hustinx**: De tweede vraag is heel belangrijk en heel strategisch. Laat ik er feitelijk over zijn. Ik heb over dat voorstel van de Commissie drie adviezen uitgebracht met allemaal zeer bruikbare suggesties. Die zijn

nagenoeg niet opgenomen in het voorstel dat er nu ligt. Doordat nu de eenstemmigheidsregels gelden, is er een soort zoeken naar een aanvaardbaar minimum ontstaan. Het effect van die twee mechanismen is dat het voorstel dat er nu ligt ontoereikend is in allerlei opzichten en op zijn best een eerste begin zou kunnen zijn. Het is niet voldoende om het in Prümkader goed te laten aflopen, het is niet voldoende om allerlei andere dingen te doen die wij nodig hebben. Eigenlijk is het op zijn best een eerste stap. De rest is een politieke afweging. Ik zou zelf het medebeslissingsrecht van het Europees Parlement een interessante modaliteit vinden – inderdaad, over een jaar zijn de spelregels anders – om ervoor te zorgen dat dit buitengewoon belangrijke project via de kop of de staart veel beter wordt dan het nu is.

De heer **Buruma**: Er is ook een vraag gesteld aan mevrouw Van der Ploeg.

Mevrouw **Van der Ploeg**: Gevraagd is wat je uit DNA kunt halen. Belangrijk daarbij te bedenken is dat mensen altijd hebben gezegd dat DNA-fingerprints stukjes DNA betreffen die niet echt coderen voor eigenschappen van mensen. Dat is voor het grotere gedeelte junk-DNA dat niet echt codeert voor eigenschappen. Dat is wel altijd ten opzichte van de huidige stand van wetenschap en techniek. De voortgang in dit soort technologische ontwikkelingen is snel. Ook kan men nu verschillende dingen uit DNA halen wat eerst niet kon. Met name in relatie tot dat soort DNA-banken en opsporing zijn nu allerlei onderzoeksprojecten gaande om steeds meer uit het DNA te halen dat op een crime scene is gevonden, bijvoorbeeld de haarkleur, de ogenkleur en de etniciteit, om van daaruit te werken naar daderprofielen. Dat geeft aan dat datgene wat op een gegeven moment uit DNA kan worden gehaald altijd relatief is ten opzichte van de huidige stand van technologie en wetenschap. Die zijn in ontwikkeling, dus je kunt er heel moeilijk vaste uitspraken over doen. Die ontwikkelingen zijn nu al zichtbaar.

De heer **Buruma**: Dank u allen zeer. Hier is nog veel meer over te zeggen, maar wij moeten nu naar het slotdebat. Dat zal worden ingeleid door een korte beschouwing van een van de autores intellectualis van deze bijeenkomst, de heer Franken.

Slotdiscussie

De heer **Franken** (CDA): Voorzitter, dames en heren. De beschikbare nieuwe technologie is prachtig, het is doorgaans een vooruitgang voor de samenleving. De vraag is alleen, hoe die nieuwe technologieën verantwoord moeten worden ingezet. Wij hebben vanmiddag drie thema's behandeld om die zoektocht naar de balans tussen veiligheid en privacy enigszins vorm te geven, maar nu komt concreet met dit panel naar voren hoe wij moeten handelen. Er zijn hier vertegenwoordigers van beide Kamers van de Staten-Generaal aanwezig, die met de regering beslissingen moeten nemen over de toekenning van de bevoegdheden ten aanzien van het handelen met die nieuwe technologieën. Daar zijn prachtige rapporten over verschenen. *Data voor daadkracht* is een mooi rapport, waarmee nog weinig is gedaan. Verder heeft het Rathenau-instituut er van alles aan gedaan. Laatst heeft u een interessante zaterdag kunnen doorbrengen in het Glazen Lichaam in Rotterdam, waarover breed is gerapporteerd. Wat moeten wij hiermee doen? Welke criteria voor de afweging bij de toekenning van nieuwe bevoegdheden moeten wij hanteren?
Big Brother is het schrikbeeld. Ik geloof dat niet heel veel mensen het boek van George Orwell hebben gelezen. Dit is overigens een pseudoniem van Arthur Blair. Big Brother is het schrikbeeld, maar wij hebben al

wel een Big Mother. Immers, voor onze bestwil worden er allerlei vrijheden ingeperkt. In hoeverre moeten wij onder de vleugels van die Big Mother blijven en in hoeverre mag dat worden uitgebreid? Help ons nu die criteria te formuleren. Ik geef er vijf, die u mag afbranden, afschieten of onderlijnen, maar u mag ze ook uitbreiden of vertienvoudigen, hoewel het laatste niet werkbaar zal zijn. Geef ons werkbare criteria.

1. Noodzaak, met effectiviteit en hanteerbaarheid daarbij;
2. proportionaliteit;
3. een privacy impact assessment, waarbij ik verwijs naar Canada, waar vooraf mogelijke problemen moeten worden geanalyseerd, dus in het stadium van wetgeving, zodat wij dan proberen daarmee vooruit te kijken;
4. de mogelijkheid van controle, maar dan niet in de Angelsaksische zin van beheersing, maar in de zin van contre rôle, tegenspel, wat zou kunnen door audits door onafhankelijke organen, of door rechtsbescherming;
5. een horizonbepaling, zodat er een review na korte tijd komt.

De heer **Buruma**: Dank u wel mijnheer Franken. Volgens mij is dit een goed moment om de heer Bosma aan het woord te laten, de voorzitter van de commissie die het rapport *Data voor daadkracht* het licht heeft doen zien.
Mijnheer Bosma, u hebt in uw rapport laten zien hoe ontzettend veel er op dit moment al wordt gedaan met gegevens en gegevensbestanden. Als u de Kamers moet informeren en u ziet dit lijstje over noodzaak en proportionaliteit, hoe beoordeelt u die dan in het licht van de gegevens die al bij elkaar geharkt zijn en de huidige gegevensstromen?

De heer **Bosma**: Voordat ik die vraag beantwoord, wil ik mijn positie markeren. Doordat ik bijna naast hem zit, lijkt het er nu een beetje op dat ik een medestander van de heer Kohnstamm zou zijn, maar dat is niet zo. Er mag geen enkel misverstand over bestaan dat ik een voorstander ben van het koppelen van gegevens. Dergelijke koppelingen moeten wel aan een aantal voorwaarden voldoen, voorwaarden die gebaseerd zijn op ijver en intelligentie.
In Nederland worden veel te veel gegevens gestapeld, zonder dat goed is nagedacht over de effectiviteit daarvan. Wij doen wel alsof wij hierover hard nadenken, maar in feite doen wij dat niet. Gevolg is dat wij met een verzameling gegevens soms niet het resultaat bereiken dat wij voor ogen hadden. Dat is het punt intelligentie.
Er is echter ook ijver nodig, want het moeten wel correcte gegevens zijn. Daarover is vandaag terecht veel gezegd, want dat is essentieel. Je moet correct beginnen en correct doorwerken. Dat betekent dat men gedisciplineerde ijver tentoon moet stellen. Als iedereen zich dat voor ogen houdt, is de privacy in mijn ogen geen probleem. Ik ben daarom ook niet tegen koppeling. Er moet echter wel een noodzaak zijn om een koppeling aan te brengen en die kan er alleen zijn als je vooraf hebt nagedacht over wat je wilt bereiken met de gegevens die je verzamelt. Ik probeer het woord doelbinding te vermijden en daarom houd ik het er maar op dat je intelligent moet opsporen.
Natuurlijk is proportionaliteit van belang. Het heeft geen enkele zin om gegevens te gaan verzamelen onder het motto: dan hebben we ze maar. In het verleden is gewerkt met gebrekkige onderzoeksmethodieken, maar het is toch frappant dat ik op de vraag of iemand gegevens nodig had en, zo ja, voor welk doel, het antwoord kreeg: «dat laatste weet ik nog niet, maar ik wil ze wel graag hebben, want dan heb ik ze maar». Deze houding is schering en inslag in het Nederlandse opsporingsapparaat.

De heer **Buruma**: Daarmee bevestigt u eigenlijk wat de heer Jacobs eerder zei en wel: «select before you collect». Dat laat echter onverlet dat

mensen zullen zeggen: maar je weet vooraf vaak niet waarom je bepaalde gegevens nodig zult hebben.

De heer **Bosma**: Ik ben minder streng dan hij hoor.

De heer **Buruma**: Dat is duidelijk. Maar kan iemand wel van tevoren bepalen wat hij eigenlijk wil weten? Zegt men niet vaak achteraf dat het heel handig zou zijn geweest om over bepaalde gegevens te beschikken. Zo denkt de gemiddelde politieambtenaar er waarschijnlijk wel over.

De heer **Bosma**: Dat begrijp ik wel, maar ik ken ook andere voorbeelden. Ik wijs er in dit verband op dat het verschil tussen criminaliteit en terrorisme vervaagt en daarmee het verschil tussen de opsporingsdiensten en de AIVD. Daarom wordt het in mijn ogen alleen maar belangrijker dat mensen nadenken over de vraag waarvoor ze bepaalde gegevens nodig hebben. Officieren van justitie en opsporingsdiensten denken dan ook steeds meer na over het type gegevens dat ze nodig hebben om bijvoorbeeld fraude en milieucriminaliteit op het spoor te komen. Er is wel degelijk sprake van proactief gebruik van gegevens als men van tevoren bepaalt wat men gaat doen als een bepaald type container de haven binnenkomt.

De heer **Buruma**: U beoordeelt het dus niet eendimensionaal? U zegt dus niet bij zware delicten bestaat hiervoor wel de noodzaak, maar bij lichte niet? En: bij terrorisme wel, maar bij georganiseerde misdaad niet? De enige vraag die voor u telt, is de vraag of het zin heeft.

De heer **Bosma**: Ja.

Mevrouw **Ten Horn** (SP): Mijnheer Bosma, volgens u moet er een noodzaak zijn om gegevens te verzamelen. Over twee weken behandelt de Eerste Kamer het burgerservicenummer in de zorg. Men zegt dat de kwaliteit van de zorg en dan vooral de kwaliteit van de acute zorg verbetert als men databestanden kan koppelen. Denkt u dat er in dit geval een echte noodzaak is om bestanden te koppelen?
De heer Hustinx zei dat 20 tot 30% van de gegevens vervuild is. U zei net dat het essentieel is dat gegevens kloppen. Hoe groot acht u de kans dat de uitkomst van het koppelen van die gegevens uiteindelijk eerder tot doden leidt dan tot verbetering van de kwaliteit van de zorg?

De heer **Bosma**: Ik kan u een antwoord geven over uw vraag over het BSN, maar dan wil ik wel eerst melden dat ik in het bestuur van Nictiz zit. Het zou oneerlijk zijn om dat niet te vertellen bij mijn beantwoording. Ik ben ervan overtuigd dat koppeling nodig is. Er is een absolute noodzaak om dat te doen. Ik kan dat wel uitleggen, maar laten wij er niet al te diep op ingaan. Als je met succes een elektronisch patiëntendossier in de lucht wil brengen en een medicatiedossier, is het gebruik van het BSN nodig. Dat is absoluut onvermijdelijk. U vroeg hoeveel fouten daarin gaan kruipen. Van de correctheid van GBA-gegevens, wordt je niet al te vrolijk. Het is wel beter geworden in een stad als Amsterdam, die ik toevallig heel goed ken uit een vroeger leven, maar het is nog steeds niet echt in orde. Wij moeten proberen om te voorkomen dat met het BSN gebeurt wat met het sofinummer is gebeurd, namelijk dat dit vergaand vervuild raakt. Daar moet u als parlementslid absoluut interesse in hebben. U zou zo nu en dan te horen moeten krijgen of dat inderdaad gebeurt. Ik denk dat dit de enige manier is om dat te doen. Het parlement moet van tijd tot tijd een overzicht krijgen waaruit is af te lezen dat de nauwkeurigheid een punt van aandacht blijft en dat deze niet slechter wordt, hopelijk zelfs iets beter. Dat is de enige manier om er controle op te houden, op afstand. Dat is controle in de zin die de heer Franken beschreef.

De heer **Buruma**: U bent niet vrolijk over de kwaliteit van wat er is opgeslagen.

De heer **Bosma**: Ik kom uit dat vak, dus ik weet wel ongeveer hoe dat zit.

De heer **Buruma**: Ik weet dat uit een steekproef naar gegevens van 700 gevangenen bleek dat er van 46 verkeerde data beschikbaar waren.

De heer **Bosma**: Dat viel mij nog mee, moet ik zeggen.

De heer **Buruma**: Het is prettig om dat te horen, althans verhelderend. De vraag is hoe dat kan worden verbeterd, maar die ga ik aan iemand anders stellen. Mijnheer De Vries, wat vindt u van wat u hebt gehoord? Uw blik is die van de terrorismebestrijding. De neiging zou zijn om te vermoeden dat u als terrorismebestrijder op het standpunt staat dat er zo veel mogelijk moet worden gekoppeld, dat er zo min mogelijk gedoe met privacy moet zijn en dat er wel een beetje moet worden gelet op de kwaliteit van de gegevens omdat u anders uw werk niet kunt doen. Zie ik dat juist of ligt dat in de antiterreurwereld een beetje anders? Wij weten dat er tussen Europa en de Verenigde Staten bijvoorbeeld verschillen van mening bestaan op dit terrein.

De heer **De Vries**: U stelt nu ongeveer vier vragen in één, dus ik kies er een enkele uit. Wij moeten ons blijven realiseren dat terroristen altijd de bedoeling hebben om overheden te provoceren tot een overreactie en de vrijheden die deze overheden zelf zeggen te willen verdedigen te ondermijnen. Zo'n reactie van de overheid wekt immers protest op in de samenleving en daarmee is het nuttige effect van de aanslag drie keer zo groot als de aanslag alleen. Er moet worden gewaakt voor overreactie, dus moet worden gelet op burgerlijke vrijheden. Anders ben je namelijk niet bezig met de strijd tegen terrorisme. Burgerlijke vrijheden zijn een onderdeel van effectiviteit en geen belemmering ervan.

De heer **Buruma**: Dit betreft dus ook de privacy impact assessment van Franken?

De heer **De Vries**: Ik denk dat de vijf punten van Franken allemaal belangrijk zijn. Ik had er zelf twee opgeschreven toen ik hier naartoe kwam, namelijk de horizonbepaling en de controle. De belangrijkste is de controle. Beide Kamers kunnen naar mijn mening veel meer doen aan het houden van toezicht op de uitvoering van regelgeving. Hoe werkt het eigenlijk in de praktijk? Hebt u daar wel een overzicht van? Ik stel het niet als retorische vraag. Het viel mij op dat minister Ter Horst in aanbiedingsbrief of de dankbrief bij het rapport-Bosma zei dat nader onderzoek eigenlijk helemaal niet nodig is omdat er in Nederland een samenhangend stelsel van privacybescherming bestaat. Dat stelde zij. Ik heb de adstructie van die stelling in haar brief niet aangetroffen. Dat zou mij als Kamerlid toch wel geweldig interesseren. Wat is dan dat samenhangende stelsel en klopt die stelling eigenlijk wel? Ik denk dat de Kamer daar veel scherper op moet inzoomen.
Er is bijvoorbeeld vandaag weer heel losjes gesproken over datamining. Ik heb het gevoel dat er nogal wat verschillende interpretaties van dat begrip door de zaal zoemden. Ik zou als Kamerlid wel eens willen weten hoeveel datamining er plaatsvindt in Nederland, wie dat precies doet, waarvoor het gebeurt en wat de effectiviteit ervan is. Als die vragen niet in een openbare zitting kunnen beantwoord, zijn er vertrouwelijke overlegvormen. Ik denk dat controle op de AIVD en op de politie buitengewoon belangrijk is.
De vraag van de dag was van mevrouw Strik. Zij heeft een buitengewoon belangrijk punt aangeroerd. Als wij in Europees verband willen voor-

komen dat er gaten vallen in de privacybescherming met betrekking tot vraagstukken van veiligheid en terrorismebestrijding, moeten op Europees niveau harde criteria worden opgesteld, inclusief toezichtmechanismen. Het onverstandigste dat de wetgever kan doen, is toestaan dat elke lidstaat zelf beslist welke gegevens hij aan derde lidstaten beschikbaar stelt en welke niet. Daarmee ontstaan gaten in de bescherming van Europese burgers waar het gaat om het leveren van informatie door een of ander Europees land aan bijvoorbeeld de Verenigde Staten.
Het beste dat je kunt doen, is de ontwerpkaderverordening voorlopig tegenhouden, wachten op het nieuwe verdrag, insisteren bij de Europese Commissie op een voorstel met inhoudelijke criteria die voor de hele Europese Unie bindend zijn en die dan met gekwalificeerde meerderheid – desnoods tegen de stemmen van bepaalde lidstaten in – door het Europees Parlement en de Europese Raad laten vaststellen. Dan heb je bovendien controle door het Europees Hof van Justitie.

De heer **Buruma**: Dat is een heldere aanbeveling. Even wachten en uiteindelijk een gekwalificeerde meerderheid in Europa. Het gaat uit van een beeld dat je als Europa iets kunt regelen.
Mevrouw Prins, gaat de praktijk niet veel sneller? Is het niet zo, dat Europa wel iets kan willen regelen en dat het misschien ook wel beter is dat Europa regelt dan dat Nederland zelf iets gaat doen, maar is het eigenlijk niet al gepasseerd? Vindt, ook onder de officiële grenzen door, al niet zo veel datakoppeling plaats dat wij helemaal niets meer hoeven te regelen? Kunnen wij hier dus eigenlijk wel naar huis gaan?

Mevrouw **Prins**: Mijn antwoord op die vraag zou «neen» luiden. Het was een van mijn misvattingen. Ik heb een lijstje misvattingen dat ik graag met u wil delen.
Hans Franken is mijn promotor. Hij heeft ons een vraag voorgelegd over de criteria. Ik meen dat ik in ieder geval vanuit mijn bijzondere wetenschappelijke relatie met hem zou moeten proberen om op die vraag een antwoord te geven. Ik ben het van harte met hem eens. Ik meen dat alle vijf criteria cruciaal zijn, zeker in relatie tot hetgeen de heer De Vries zojuist heeft aangevuld. Ik meen dat het laatste punt op de lijst, de horizonbepaling, een heel belangrijk instrument zou kunnen worden.
In een interview met de Groene Amsterdammer dat dit weekeinde verschijnt, heb ik daar toevallig op gewezen. Ik meen dat het cruciaal zou kunnen zijn en dat wij er nader onderzoek naar moeten doen.
Dan wil ik graag terug naar mijn misvattingen. Ik zal het kort houden. Ik ben het eens met alle criteria, maar ik denk dat deze vervolgens in een bepaalde context moeten worden beoordeeld. Het is cruciaal dat iedereen weet wat de context van nu en de toekomst is. Dit zijn mijn zes misvattingen.
De eerste misvatting is dat het niet langer om privacy als een waarde op zichzelf gaat. De heer Hustinckx heeft er eerder vandaag al op gewezen dat er zoveel meer achter ligt. Ik meen dat wij af moeten van de dichotomie in de zin dat het om privacy en veiligheid gaat. Het gaat om veel meer. De grote uitdaging die ik – ook voor mijzelf – zie en die ook bijvoorbeeld de commissie-Brouwer ziet, is om tot een brug tussen privacy en veiligheid te komen en naar de achterliggende belangen te kijken. De discussie moet, naar mijn mening, dus niet meer over het woordje «privacy» gaan. Dat is misvatting nummer 1. Het gaat om vrijheid, autonomie, waardigheid, afhankelijkheid, kwetsbaarheid en het ideaal van de democratische rechtstaat. Om er maar een paar te noemen.
Misvatting nummer 2 is dat het om simpele gegevens, een zelfstandig doel, afzonderlijke systemen en afzonderlijke maatregelen gaat. Neen. Dat is een volstrekte misvatting. Ik meen dat dit vanmiddag is aangetoond en dat beide Kamers hierin een cruciale rol zouden kunnen spelen. Niemand heeft het echte overzicht van het geheel. Wij hebben vandaag een lijstje

maatregelen onder ogen gekregen, maar er is veel meer. Wij moeten kijken naar de combinatie van het geheel. Mevrouw Van der Ploeg heeft daaraan nog een element toegevoegd. Wij hebben het nu veelal over heel simpele gegevens. Inmiddels hebben wij het ook over DNA en genetische gegevens. In Nederland bestaan inmiddels vele weefselbanken, die ook wel biobanken worden genoemd. Van ons allemaal zit er materiaal ergens in die biobanken. Het kan een bloedbank zijn of een databank met donormateriaal. In een aantal andere landen stelt men zich inmiddels op het standpunt dat feitelijk lichaamsmateriaal een persoonsgegeven is. Dat geldt dus niet alleen voor informatie over het bloed, maar ook voor het bloed zelf. Dat betekent dat het binnen de reikwijdte van de Wbp valt. Zo ver gaan wij in Nederland niet. Het College heeft dat inmiddels ook uitgesproken. Toch, de tendens gaat in de richting van het oprekken van het begrip «persoonsgegeven». Het gaat om veel meer dan simpele gegevens en individuele systemen. Het gaat om het geheel.

Misvatting nummer 3 is dat het om individuen gaat. Het gaat niet langer uitsluitend om onze persoonlijke gegevens, maar om de wijze waarop wij als groep van mensen worden getypeerd. Datamining is een voorbeeld. Wij hebben het eerder over profielen gehad. Het gaat niet meer om losse gegevens van individuele mensen. Het gaat om typen mensen, typen burgers, typen consumenten, typen patiënten, et cetera. Daarop maken wij het profiel en daarop handelt de maatschappij. Dat wordt alleen maar meer. Het individu, de context en de scheiding tussen de deze twee zullen steeds meer vervagen.

Misvatting nummer 4 is dat een scheiding bestaat tussen norm en handhaving. Als wij de technologie gaan inzetten, verpakken wij de norm in de technologie en handhaven wij dus ook door middel van de technologie. Norm en handhaving worden daarmee in toenemende mate één.

Deze technologie is echter niet transparant. Er is nauwelijks verantwoording over af te leggen. Technologie wordt vaak, ook in kabinetsplannen, gepresenteerd als een black box. Wat mij betreft moet daarvoor aandacht zijn. Dit schaar ik onder de controle en dit is wat de heer De Vries aankaart. Transparantie is cruciaal. Ik heb vorig jaar in een bundel voor de Nationale ombudsman geschreven dat dit in de toekomst een van de belangrijkste punten zal zijn, wanneer normen en handhaving in de technologie worden verdisconteerd.

Ik kom op de vijfde misvatting. Men vroeg mij of hieraan nationaal niets meer te doen valt. Misschien is dit voor een deel zo. Ik zie echter nog steeds vergaande nationale ontwikkelingen zoals die rond het elektronisch kinddossier. Ik hoorde gisteren dat hierover op de website van de overheid staat dat er in dit dossier informatie staat over mensen «van min negen maanden tot ver na de dood». Gegevens over min negen maanden staan dus al in een elektronisch kinddossier en dit wordt nu op nationaal niveau opgezet. Verder is er het BSN in de zorg. Inmiddels wordt er ook voor een nationale biobank gepleit. Ook op nationaal niveau kunnen wij veel. Hier ligt dus zeker een rol.

Ik kom ten slotte op misvatting zes, namelijk dat de politiek hieraan nauwelijks iets zou kunnen doen. Ik ontken dit, maar ik ben uiteraard geen politicus. Soms vraag ik mij af of er niet eens een parlementaire enquête hierover moet worden gehouden. Toetsing aan de Grondwet is wellicht ook een optie, kijkend naar de ontwikkeling in Duitsland. Dit zijn echter twee vergaande opties die wellicht nog niet in beeld komen. Maar, het lijkt mij zinnig als de politiek eens actief onderzoekt wat er feitelijk gebeurt en hoe het zit met de effectiviteit. Een onderzoek naar het totaalplaatje is mijns inziens cruciaal, want niemand heeft dat beschikbaar. Ik vind ook nog steeds dat er een discussie moet worden gevoerd over de financiering van toezicht. De bijeenkomst vandaag bewijst wederom dat de druk op privacy toeneemt. Juist daarom is het belangrijk om adequate instrumenten voor het toezicht en een adequaat functionerende en goed gefinancierde toezichthouder ter beschikking te hebben. Als er onvoldoende

geld beschikbaar is, is er geen sprake van een onafhankelijke, maar van een aan de band gehouden en kort gehouden toezichthouder.

De heer **Buruma**: Dank u wel. Dit was een indrukwekkend verhaal. Ik ben bijna sprakeloos. Toch ga ik door naar de volgende sprekers, die wat mij betreft de laatste twee sprekers zijn. Eigenlijk zijn wij namelijk al over onze tijd heen.
Er is zojuist als het ware een oproep gedaan: wij kunnen iets doen en moeten beter controleren. De vijf punten van de heer Franken zien er goed uit. Mijnheer Van Brummen, ik wil u over een klein dingetje nog iets vragen, namelijk over de noodzaak en de effectiviteit. Is het nu allemaal wel zo effectief? Vraagt de politie niet meer informatie dan ze kan gebruiken? Overspelen wij onze hand? Als wij het lijstje bekijken, moeten wij dan toch niet iets met bijvoorbeeld de ernst van het delict of de urgentie van wat er gaat gebeuren, nog los van alle discussies over privacy? Als er morgen ergens een aanval kan zijn, moet je natuurlijk iets doen, zelfs bij een lichte aanwijzing. Kunt u in die hoek aanknopen bij het lijstje van de heer Franken? Misschien kunt u ook uw andere indrukken geven.

De heer **Van Brummen**: Ik geef u een praktijkvoorbeeld, want dat maakt dit punt mijns inziens het meest helder. Er werd gesproken over 700 gedetineerden, van wie er ongeveer vijftig een identiteit hadden waarbij vraagtekens konden worden geplaatst. Dit heeft ertoe geleid dat men binnen justitie heeft gezegd dat men toe wil werken naar een integer persoonsbeeld. Dat betekent dat men in de strafketen altijd weet of men werkelijk te maken heeft met de juiste persoon. Aan het begin van het strafketenproces zal dan een vingerafdruk worden afgenomen, die het hele proces een rol blijft spelen.. Bij elke volgende stap wordt gecontroleerd of de desbetreffende persoon werkelijk is wie hij zegt te zijn. Dat leidt ertoe dat je de organisatie hierop moet voorbereiden en dat het vingerafdrukkensysteem opnieuw moet worden ontworpen. Het betekent ook dat je in gevangenissen, bij rechtbanken, bij rechter-commissarissen, op ieder politiebureau, bij Halt-bureaus en bij de reclassering voor de taakstraffen, de mogelijkheid moet hebben om te controleren op vingerafdrukken. Dit doen wij dus allemaal op grond van de identiteitsvragen die mogelijk in de genoemde 7% van de gevallen spelen.
Daar kun je heel goed het lijstje met de criteria van Franken tegenaan houden, die je kunt afvinken. Ik voeg hieraan de vraag toe die mij door het hoofd schoot toen deze vijf criteria passeerden. Als wij nadenken over wat wij willen en als wij voor die balansvraag staan, moeten wij ons ook de vraag stellen of de organisatie op orde is om het te kunnen doen. Die vraag passeert bijna nooit. Ik denk dat het heel verstandig zou zijn dat altijd de controlevraag gesteld wordt of de organisatie op orde is. Als wij zien wat er op dit moment aan de orde is bij justitie, politie en het Openbaar Ministerie hoeft die vrees voor datamining er nog helemaal niet te zijn. Dat is iets wat wij niet doen omdat wij er nog niet aan toe zijn. De organisatie daarvoor is er nog niet. Dat geldt ook voor heel veel andere vragen die spelen. De organisatie is nog niet zo ver op orde dat wij daar al aan toe zijn. Wij staan pas aan de vooravond van het opbouwen van een informatieorganisatie binnen de politie, binnen de regiokorpsen en bij het KLPD.
Dat maakt het zoeken naar afwegingen en een balans heel boeiend. Ik zou dus de controlevraag stellen of de organisatie op orde en eraan toe is, of zij het aan kan en wat zij ermee gaat doen, en zien hoe die vraag beantwoord wordt. Daarop zou ik mede de vraag naar de balans afstemmen.

De heer **Buruma**: Toch doet het heel vreemd aan dat u nu zegt dat wij met datamining nog niet zo ver zijn. Aan de andere kant wordt er vanuit de politie voortdurend geroepen dat wij bezig zijn met information lead

policing. Het zijn altijd grote woorden door wij horen. Moeten wij die dan toch wat relativeren?

De heer **Van Brummen**: Jazeker zou ik die relativeren, want er zijn in Nederland regiokorpsen van de politie die überhaupt nog geen informatieorganisatie hebben. Dus laten wij ook niet denken dat wij al in een fase zitten waar wij nog niet zijn.

De heer **Buruma**: Het laatste woord is wat mij betreft aan de heer Kohnstamm. U hebt nu heel veel gehoord. U had heel veel daarvan natuurlijk wel eens eerder gehoord. Maar niettemin zijn hier allerlei punten naar voren gekomen, zoals die op het lijstje van de heer Franken. Vindt u dat lijstje genoeg of moet er meer bij?

De heer **Kohnstamm**: Ik ben het zeer eens met het lijstje van Franken. Ik hoop dat de heer Franken het mij niet euvel duidt dat ik daar nu niet op inga. Ik noem twee andere punten uit de eerdere sessie die sterk een rol spelen. Welke bulkgegevens worden nu gebruikt? Wij weten het niet. Er is geen politiek of ander onderzoek naar gedaan. De heer Bosma is gedechargeerd en er is geen opvolger gekomen, dus wij zullen het voorlopig ook niet weten. De tweede vraag is wie waar welke experimenten doet met datamining en profilering. Laten wij daarover een discussie voeren. Laat dat tenminste zo transparant zijn als het kan.
Bij sommigen van u heeft een boekje op tafel gelegen, waarvan er nog meer zijn. Wij hebben op 1 november 2007 samen met de ministeries van Binnenlandse Zaken en Justitie een symposium over veiligheid en privacy georganiseerd. De speeches die daar zijn gehouden staan in dat boekje afgedrukt. Ik raad het u aan, omdat het sterk aansluit bij de discussie van vandaag.
Op het gevaar af dat dit een politieke opmerking is van een toezichthouder, sluit ik af met de opmerking dat ik mij gegeven de discussie van vandaag ernstig zorgen maak over de wijze waarop de evaluatie van de Wet Bescherming Persoonsgegevens wordt aangepakt. Ik zeg het wat gechargeerd, maar die gaat helemaal langs de lijn van «heeft de wet lasten teweeg gebracht?» Ik kan u het antwoord daarop voorspellen. Ja, dat was ook het noodzakelijke effect, misschien niet in deze omvang, maar dat staat als een paal boven water.
Als je het conglomeraat waarover wij het vandaag hebben gehad, op de een of andere manier onder controle wilt hebben, in die zin dat er normen en waarden in worden aangegeven, moet je niet alleen naar de lasten kijken. Je moet dan doen wat de wetgever in artikel 80 van de WBP heeft neergelegd, namelijk dat bij de evaluatie moet worden bekeken of het voor burgers en samenleving, gegeven de technologische ontwikkelingen sinds de totstandkoming van de WBP, afdoende is. Die vraag wordt op geen enkele wijze geadresseerd in de evaluatieopdracht die door het WODC, naar ik aanneem gedekt door de minister, is afgegeven. Dat betekent dat wij aan het eind van het jaar op basis van het onderzoek zullen constateren dat sprake is geweest van lasten, achter de WBP aankomend, maar dat er nog geen begin van een antwoord is gegeven op de vragen die wij vandaag centraal stellen en die wat mij betreft het primaat zouden moeten hebben van het denken over hoe de persoonsgegevens worden beschermd; ik heb het niet over de privacy. Het gaat over veel meer dan dat. Dat wilde ik nog heel graag even kwijt.

De heer **De Vries**: Nog een kleine nabrander. Het enige dat ontbreekt in het lijstje van de heer Franken, maar je kunt het er impliciet in lezen, is dat je die vijf criteria niet alleen binnen Nederland moet hanteren. Een van de meest uitdagende vragen voor de beide Kamers heeft betrekking op de schakel tussen de nationale rechtsorde en de Europese rechtsorde. Ik hoop dat de Kamers daar nog eens over willen nadenken.

De discussie vandaag heeft in het teken gestaan van de gevaren van het verzamelende, analyseren en delen van informatie. Ik deel die analyse en die zorg, maar vergeet niet dat er in Europa nog altijd eerder te weinig informatie wordt gedeeld dan te veel. Ook daar zou ik graag aandacht voor willen vragen van de beide Kamers. Wij praten niet alleen over de bescherming van persoonsgegevens, maar ook over het nuttig gebruik van gegevens om de grensoverschrijdende criminaliteit beter aan te pakken. Dat is een apart onderwerp, maar het vergt meer aandacht.

De heer **Buruma**: Dames en heren, ik vat de discussie vanmiddag in drie zinnen samen. Wij hebben prachtige speeches en toelichtingen gehoord waarop nog veel meer moet kunnen worden doorgegaan.
De eerste zin. Sprekend over gegevensbescherming, databanken en dat soort dingen concludeer ik dat, naast de privacykwesties, de kwaliteit van het materiaal ontzettend belangrijk is. Daar moet je niet te luchtig over doen. De tweede zin. De Kamerleden moeten niet in die zin naar de Europese en wereldregelgeving kijken dat zij het gevoel krijgen dat ze hier hooguit achteraan kunnen hobbelen. De heer Hustinx heeft nog benadrukt hoezeer vanuit Nederland stappen voorwaarts kunnen worden gezet, maar je moet er goed over nadenken hoe je kunt beïnvloeden wat er in Europa gebeurt. Daarnaast zijn er heel veel dingen die binnen Nederland kunnen plaatsvinden.
Het lijstje van Franken werd tamelijk omarmd, zou je kunnen zeggen. Er ligt meer achter de privacy, zoals mevrouw Prins ook al zei. De kwaliteit van het materiaal is één ding, Europa is zeker van belang, maar bedenk wel dat niemand echt overzicht heeft van wat er allemaal speelt. Dat heeft mevrouw Prins ook nog gezegd. Ik denk dat wij dat vast moeten houden. Maar wij kunnen wel iets. U ook! En dan «het lijstje van Franken» dat waarschijnlijk voortaan altijd zo zal heten.
Dames en heren, wij kunnen deze middag afsluiten. Ik geef het woord graag terug aan de plaatsvervangend voorzitter van de commissie.

De heer **Franken**: Mies Westerveld heeft mij zojuist gevraagd om haar te vervangen. Ik ben dus een vervanger in de tweede graad. In die hoedanigheid wil ik u allen bijzonder bedanken voor uw aanwezigheid en voor uw bijdragen. De Kamer heeft niet besloten om een nieuw rapport te vragen. Er zijn al veel rapporten en die lezen wij natuurlijk braaf en trouw. Het ging nu echt om een interactieve gedachtewisseling waarin wij zelf ook met vragen konden komen – het debat is daardoor enigszins gestructureerd – maar waar wij ook concrete aanknopingspunten uit hoopten te kunnen destilleren. U hebt u bijdrage daartoe geleverd. Reuze veel dank daarvoor! Ik dank uiteraard ook onze dagvoorzitter die onvermoeibaar heeft geacteerd op dit speelveld. Ik dank de mensen van het Rathenau instituut die ons hebben geholpen om deze dag vorm te geven. De Kamer is daarvoor niet geëquipeerd. De Tweede Kamer heeft 150 leden met 650 fte ondersteuning. Wij hebben 75 leden en 47,5 fte ondersteuning. Wij moesten daarom naar buiten. Het Rathenau instituut is zo vriendelijk geweest om ons hierbij te helpen. Ik ga u niet meer allemaal individueel bedanken. Ik denk dat het effectiever is om dat tijdens de borrel te doen. Dan mag ik nog even bij u langslopen. U wil ik allemaal graag spoorslags naar de borrel doen geleiden, maar niet eerder dan nadat ik ook de medewerkers van de vaste commissie van Justitie van deze Kamer uitdrukkelijk heb bedankt voor al het extra werk dat zij gedaan hebben om deze middag mogelijk te maken.

Sluiting 17.25 uur.