2
Rapport commissie-Brouwer-Korf

Aan de orde is het **beleidsdebat** over **de rol van de overheid bij digitale dataverwerking en -uitwisseling in het kader van het rapport van de commissie-Brouwer-Korf**.

De **voorzitter**:
Ik heet de minister van Binnenlandse Zaken en Koninkrijksrelaties en de staatssecretaris van Veiligheid en Justitie van harte welkom in de Eerste Kamer.
Het woord is aan mevrouw Tan.

De beraadslaging wordt geopend.

□

Mevrouw **Tan** (PvdA):
Mijnheer de voorzitter. Dezer dagen draait in de bioscopen de documentaire Inside Job van Charles Ferguson. De film gaat over de economische crisis die in het voorjaar van 2008 in de Verenigde Staten begon door het instorten van banken als Bear Stearns en Lehman Brothers. Uiteindelijk hebben de bankiers zich met miljoenen dollars verrijkt ten koste van miljoenen gewone mensen. Hun invloed reikt tot in de hoogste kringen van de overheid en de wetenschappelijke wereld. Hoogleraren Economie van Harvard en Columbia University brengen voor hen positieve rapporten uit tegen extreem hoge honoraria. Tot op de dag van vandaag lukt het de overheid niet greep te krijgen op de financiële sector: niet op de bonuspraktijken en niet op de rest. In 2008 publiceerde Jeroen Smit het onthullende en schokkende verhaal over de deconfiture van ABN AMRO in "De Prooi". Vergeleken bij Inside Job is dat kwantitatief gezien qua impact kinderspel, maar inhoudelijk gezien is het in overtreffende trap meer van hetzelfde. Is tegen deze praktijken nog enig kruid gewassen?

De westerse wereld heeft wellicht nog wat te leren van zogenaamde derdewereldlanden zoals China of de landen van de Arabische lente, in plaats van het gebruikelijk arrogante vingertje te heffen richting samenlevingen "die nog het nodige te gaan hebben" voor ze de verheven Westerse standaarden bereiken. Met behulp van nieuwe media blijken burgers van die landen immers de kans te grijpen voor het van onderop aan het wankelen brengen van gevestigde dictaturen. Nieuwe media als vehikel voor democratisering, als remedie tegen oligarchieën van gevestigde regimes bestaande uit old boys networks à la de Inside Job van Manhattan?

Daar is wel moed voor nodig, eens temeer als de openheid en openbaarheid van bovenaf aan banden worden gelegd. In de Nederlandse verhoudingen vergt het een actieve opstelling van bevolking en politiek. Nog onlangs heeft minister Donner bij de dag voor de persvrijheid de journalistieke wereld weer eens de kast op gekregen – dat was niet voor het eerst – door beperkingen op de WOB uit kostenoverwegingen aan te bevelen en daarvoor ook nog een beleefd applausje te krijgen op de Dag van de persvrijheid. Een kunststukje, met daarna ook nog veel publiciteit achteraf van diezelfde journalisten die alsnog kritiek in de media naar voren brachten.

Maar de regering doet er ons inziens wel goed aan, zichzelf te behoeden voor het zich ingraven in het uitgesleten karrenspoor van de bezuinigingen. Hoe noodzakelijk die volgens deze regering ook zijn, als die resulteren in financiële oogkleppen zou dat wel eens onbedoelde tegenkrachten kunnen losmaken, zoals bijvoorbeeld een hausse aan WikiLeaks. Proefballonnen, al dan niet doorspekt met badinerende metaforen over fabricage van worsten, zouden maar zo effecten van de tovenaarsleerling kunnen krijgen.

Het denken en doen in de digitale samenleving kenmerkt zich naar de opvatting van de Partij van de Arbeid door disbalans tussen overheid en instanties enerzijds en de individuele burger anderzijds. Naast dit eendimensionale sudokudenken is meer cryptogramachtige verbeelding aan de macht hoognodig voor het kunnen grijpen van geboden kansen. Voor een beweging van onderop is immers nodig dat de burger meer empowered wordt door een beter besef van kansen en risico's, gevoed door meer transparantie in de informatie daarover. Geen bezuinigingsoogkleppen dus, maar juist ruim baan voor de WOB!

Het parlement heeft hierbij een voortrekkersrol, gesecondeerd door groepen uit de samenleving zoals Bits of Freedom, Privacy First en Ambtenaar 2.0. Naast informatie over wetgeving en overheidsprojecten met inbegrip van die over gegevensbestanden is om te beginnen meer bewustzijn, kennis en informatie nodig over hetgeen aan gegevens is verzameld over individuele burgers en hoe daarmee wordt omgegaan. Ook daarvoor zal de overheid uit de karrensporen van het sudokudenken moeten treden en meer rechter- naast linkerhersenhelft moeten aanspreken. Wat is hierop de visie van de regering?

Immers, naast de ongekende kansen die de digitalisering de samenleving te bieden heeft, zijn er uiteraard ook net zo veel ingrijpende risico's. In de Volkskrant van 7 mei stond het artikel Spion in je broekzak van Sander Heijne. De Duitse politicus Malte Spitz kostte het de nodige moeite, alle gegevens te bemachtigen die het telecombedrijf T-Mobile over hem heeft opgeslagen. Aan de hand van die gegevens was zijn hele leven volledig te reconstrueren. De tussenkop in dit artikel luidde Bij Orwell wist alleen de overheid alles.

Onlangs zijn in de Nederlandse pers verontrustende berichten verschenen over de wijze waarop bijvoorbeeld TomTom en KPN met in hun bestanden opgeslagen gegevens omgaan. Hoe heeft onze overheid het toezicht op bedrijven en de rechten van burgers op inzicht, controle en toegang tot opslag van eigen persoonsgegevens gewaarborgd? Kan de regering daar een visie op geven?

In de Verenigde Staten hebben de senatoren John Kerry van Massachusetts en John McCain van Arizona van de Democratische respectievelijk de Republikeinse partij een initiatiefwetsvoorstel ingediend voor de privacybescherming van consumenten op internet. Alle commotie ten spijt rond een meerderheid in de Eerste Kamer voor de coalitie of niet en de gevolgen daarvan voor dit kabinet, is het toch genoegzaam bekend dat de positie van de Amerikaanse senaat van een gans andere orde is dan die in het Nederlandse bestel. De portee van dit bipartiete initiatief door senatoren van deze statuur is significant voor de politieke lading die deze kwestie in de Verenigde Staten krijgt. Het wetsvoorstel verplicht bedrijven tot: beveiliging van gegevens, het inlichten van consumenten dat hun gegevens worden opgeslagen met een opt-outmogelijkheid, een opt-inverplichting bij gevoelige gegevens als over medische zaken of religie, het bieden van de mogelijkheid aan de consument van toegang tot en correctie van diens verzamelde gegevens, het bieden van de moge-

lijkheid aan de consument om te verzoeken tot het stopzetten van het verzamelen of distribueren van gegevens en het beperken van het verzamelen van informatie over een individu tot het benodigde voor een specifieke transactie voor een specifieke periode.

Is het niet de hoogste tijd dat de regering de wetgeving rond identiteitsmanagement ter hand neemt: de afbakening van rechten en plichten tussen individuen en instanties ten aanzien van profilering en privacy? Wat is hierop de visie van de regering?

De kansen die Web 2.0 aan burgers biedt voor het doorbreken van structuren in combinatie met risico's voor de persoonlijke levenssfeer zijn evenzeer aan de orde bij de digitalisering door de overheid zelve. Wij gaan nu allereerst in op de beantwoording van onze schriftelijke vragen in de kabinetsbrief van 29 april. Vervolgens gaan wij in op de aanbevelingen van de WRR en de vooruitzichten voor de toekomst.

Het dossier waar we het vandaag over hebben, is twee jaar geleden, in 2009 aan de Tweede Kamer aangeboden en een jaar later aan de Eerste Kamer. De fractie van de Partij van de Arbeid heeft onlangs bij schriftelijke vragen van april 2011 vier zeer recentelijk verschenen rapporten betrokken, te weten "Databases. Over ICT-beloftes, informatiehonger en digitale autonomie" en "Check in/Check uit. Digitalisering van de openbare ruimte", beide van het Rathenau Instituut, iOverheid van de WRR en het rapport van de staatscommissie-Thomassen (Staatscommissie Grondwet 2010, nr. 67).

In de kabinetsbrief van 29 april 2011 geeft de regering aan, separaat te zullen reageren op het WRR-rapport dat inderdaad pas op 15 maart jongstleden aan de minister van BZK is aangeboden. Niettemin wil de regering wel verschillende hoofdzaken uit dat rapport in de kabinetsreactie van 29 april behandelen.

De kabinetsreactie als totaal overziende, is de PvdA-fractie vooral getroffen door het gebrek aan urgentiebewustzijn dat daaruit naar voren komt, zeker afgezet tegen de teneur in de zojuist genoemde rapporten. De speech waarmee minister Donner het WRR-rapport in ontvangst nam, was zoals gebruikelijk spitsvondig, maar er was inhoudelijk helaas sprake van een soortgelijk gebrek aan de volgens ons benodigde urgentie.

Het hoofdrapport van de WRR met de titel iOverheid signaleert immers dat de facto en bijna ongemerkt samenhangende informatiestromen het karakter van de overheid domineren, waarmee nieuwe mogelijkheden, maar ook afhankelijkheden en kwetsbaarheden voor zowel de overheid als haar burgers ontstaan. Dit gebeurt terwijl in de dagelijkse praktijk allerminst vanuit een samenhangende visie wordt bestuurd, maar overheidsinitiatieven tot digitalisering met bijbehorende informatiestromen binnen de verschillende sectoren geïsoleerd van elkaar worden ontwikkeld. De WRR stelt dat de overheid alert dient te zijn op de kwaliteit van de informatie – kwaliteit in de zin van karakter, betrouwbaarheid, kenbaarheid, contextualiteit en herleidbaarheid – en op de organisatorische inbedding van informatiestromen. Openheid en transparantie richting burgers is volgens de WRR nodig, zodat zij inzicht krijgen in wat over hen geregistreerd is en ondersteuning beschikbaar is indien correctie noodzakelijk is. Dit laatste is een zeer essentieel punt.

Wat is de reactie van de regering op de in de expertmeeting in deze Kamer van februari jongstleden gesignaleerde foutpercentages in bestanden van onder andere de Belastingdienst? De Rekenkamer gaf in die expertmeeting aan dat een streven van 70% foutloze registratie niet werd gehaald, zonder dat bekend was hoeveel het reële foutpercentage dan wel bedroeg. Deze fouten kunnen burgers enorme overlast bezorgen. Hoe beschermt en ondersteunt de overheid haar burgers hierin?

De WRR verkennende studie nr. 47 "Rolverdeling tussen Overheid en Burger bij Bescherming van Identiteit" door Jelle Attema en David de Nood heeft drie conclusies. Ten eerste, de stelling dat privacy een gepasseerd station is voor burgers wordt door de onderzoeksresultaten ontkracht. Ten tweede, burgers wensen een strakkere regie van de overheid op het gebruik van het burgerservicenummer in het maatschappelijk verkeer. Ten derde, respondenten willen inzage hebben in eigen elektronische dossiers, zodat ze gegevens kunnen corrigeren en kunnen zien wie gegevens bewerkt en inziet. Dit laatste punt, de controle over de toegang tot de eigen gegevens, is zeer essentieel.

Vervolgens stelt de WRR in de epiloog van het rapport dat de overheid niet alleen verantwoordelijk is voor het eigen gebruik van ICT, maar ook voor de ontwikkeling van de informatiesamenleving in zijn algemeenheid, met inbegrip van de informatiemacht van mondiale spelers als Google, Facebook en Apple. In de reactie van 29 april 2011 gaat de regering nauwelijks in op deze rol en verantwoordelijkheid van de overheid en evenmin op mogelijke voornemens om inhoud en vorm te geven aan haar systeemverantwoordelijkheid, terwijl de overheid voor haar burgers dient op te komen ten opzichte van die genoemde private partijen. Evenmin gaat de regering in op de vraag, die we ook schriftelijk gesteld hebben, over het dilemma zoals geformuleerd door John Naughton in het dagblad the Guardian: "Live with the WikiLeakable world or shut down the net, it's your choice".

Niets van dat al, de regering volstaat in het slot van de reactie met een op handen zijnde meldplicht datalekken en de constatering dat Googlezoekopdrachten geen deel uitmaken van de telecommunicatieverkeersgegevens. Dit wekt eens temeer bevreemding afgezet tegen de publieke ophef die bijvoorbeeld is ontstaan door de genoemde praktijken van TomTom en KPN met het doorspelen van gegevens. Kan de regering dan hier en nu, in dit plenaire debat, hier een uiteenzetting over geven?

Op diverse plaatsen wordt in de kabinetsreactie ingegaan op de afweging tussen veiligheid en privacy, uitmondend in de conclusie dat een zorgvuldige afweging plaatsvindt op basis van evenwichtige regelingen met voldoende waarborgen. Hoe denkt de regering echter over de recente bevindingen met de opslag van biometrische gegevens, iets waaraan de Tweede Kamer zo haar conclusies heeft verbonden, en over de steekproef van het CBP naar de gegevensuitwisseling tussen opsporingsdiensten en telecommunicatieaanbieders, waarbij het nodige niet in orde bleek te zijn? Dit geeft de burgers toch gerede aanleiding tot gevoelens van onbehagen? Graag een reactie.

Om te beginnen is naar de mening van de PvdA-fractie meer urgentiebewustzijn op zijn plaats, gelet op de schaal waarop digitalisering van de samenleving inmiddels heeft plaatsgevonden. Professor Corien Prins, lid van de WRR, wees in de expertmeeting in de Eerste Kamer van februari 2011 op de omstandigheid dat de digitalisering over meer gaat dan losse applicaties. Er is volgens professor Prins een gekoppelde, verketende en vernetwerkte wereld ontstaan, waarin de burger wordt geconfronteerd met wel honderd organisaties binnen één dossier waarbij hij moet

aankloppen als er iets niet klopt. Een onderzoek van het CBP naar de vraag in hoeveel databases mensen zitten, wijst uit dat een maatschappelijk weinig actieve persoon toch nog altijd in zo'n 250 databases zit en maatschappelijk actieve individuen zoals wij wel in 1000, 1500 of zelfs meer databases, waar dus nog eens zo'n honderd organisaties achter zitten.

De kabinetsreactie noemt een verkennend onderzoek naar het aantal overheidsdatabases waarin de Nederlandse burger geregistreerd staat, een onderzoek van 2009, dat geen betrouwbare schatting kon geven. Waarom vindt hierover op korte termijn geen nader onderzoek plaats door de regering? Dit is toch ook relevant voor de standpuntbepaling die de regering aankondigt over het rapport van de staatscommissie-Thomassen over een eventuele grondwetbepaling over dit thema? Wanneer is overigens dat standpunt over aanpassing van informatie(grond)rechten naar aanleiding van de digitale ontwikkelingen te verwachten?

Professor Prins refereerde bovendien aan de constatering in het rapport van de commissie-Brouwer-Korf dat naast handhaving ook advisering en voorlichting cruciaal zijn, onder andere over de interpretatie van essentiële criteria als doelbinding. In de kabinetsreactie bevestigt de regering dat voor de advisering aan de professionals in het kader van het rapport van de commissie-Brouwer-Korf per 1 januari 2012 drie fte's voor het servicecentrum privacy en veiligheid zijn vrijgemaakt. De regering verwacht hiermee voldoende ondersteuning te kunnen bieden. In het voorlopige verslag van februari 2010 heeft de PvdA-fractie onder andere haar zorgen geuit over de uitholling van privacywaarborgen door gebrek aan robuustheid van het toezicht in combinatie met achterblijvende bewustwording bij professionals en burgers, dit mede naar aanleiding van signalen vanuit het CBP. Is er, gelet op de aard en omvang van de problematiek, niet veel meer prioriteit nodig, ook in menskracht en budget, ter bescherming en ondersteuning, niet alleen van professionals, maar ook van individuele burgers? Waar kunnen die burgers terecht bij fouten in de registratie van hun persoonsgegevens in de genoemde massa aan databases en daarmee samenhangende organisaties?

Bij de behandeling van het wetsvoorstel ter invoering van het burgerservicenummer in 2008 heeft de PvdA-fractie met nadruk gevraagd naar een algemeen ex ante toetsingskader voor sectorale regelingen voor de toepassing van het bsn. De regering verwees naar nadere uitwerking in later stadium, ex post dus, in de sectorale toepassingen. In deel II van het WRR-rapport "De staat van informatie" worden de verwijsindex risicojongeren en het epd aan de hand van de beginselen in het toetsingskader langsgelopen en voorzien van op onderdelen zeer kritische kanttekeningen. Het rapport "Databases. Over ICT-beloftes, informatiehonger en digitale autonomie" van het Rathenau Instituut bevat case studies van de ov-chipkaart, het epd, het elektronisch kinddossier, klantenprofielen, het Schengen Informatie Systeem en de GBA. Heeft de regering kennisgenomen van de conclusie? Ik citeer: "Alles bij elkaar genomen schetsen de case studies een vrij onthutsend beeld van wat er in de praktijk kan misgaan bij het gebruik van databases. Deze risico's hangen samen met de keuzes die worden gemaakt over de architectuur van de betreffende database."

In de reactie van 29 april 2011 verwijst de regering naar de komende visie op het WRR-rapport. De PvdA-fractie verneemt graag bij dezen een indicatie van de regering over de urgentie waarmee deze vraagstukken worden ingeschat en opgepakt. De kabinetsreactie vermeldt de toezegging van de toenmalige staatssecretaris van BZK, gedaan op 13 oktober 2010, dat zij over twee jaar zal rapporteren over de mogelijkheid om te komen tot een overkoepelend beoordelingskader. in juli 2007 heeft dezelfde staatssecretaris bij de behandeling van de Wet inzake het bsn in de Eerste Kamer een evaluatie toegezegd over vier jaar, dat is dus juli 2011. Die evaluatie betreft dus ook het toegezegde servicepunt met doorzettingsmacht voor burgers. Op welke wijze is de regering voornemens de werkzaamheden voor die evaluatie en voor het overkoepelend beoordelingskader op elkaar af te stemmen?

Op onze vragen over de bijna spreekwoordelijke overheidsmissers bij grootschalige ICT-projecten is in de kabinetsreactie het antwoord achterwege gebleven op de vraag in hoeverre de centrale positie van de rijks-CIO's als onderdeel van de bureaucratie van de rijksdienst voldoende tegenwicht kan bieden bij de gebruikelijke valkuilen bij grootschalige ICT-projecten in opdracht van de rijksdienst. Ook willen wij graag een antwoord op de vraag over de constatering van de WRR dat geloofwaardige evaluaties zeldzaam zijn, omdat – zo die al plaatsvinden – de discussie blijft steken in de veiligheid van de technologie dan wel de financiële debacles. Is de regering voornemens meer aandacht te geven aan de kwaliteit van evaluaties?

Tot zover de analyse van de WRR. Ik kom nu bij de aanbevelingen van de WRR. De WRR bepleit een paradigmawisseling van een e-overheid naar een iOverheid en wil de spagaat verkennen van de overheid die de dienstverlening aan burgers verbetert enerzijds en tegelijkertijd waakt over grondrechten zoals privacy en autonomie van burgers anderzijds. Is dit niet de gebruikelijke spanning tussen rechten en plichten van individuen en groepen, inclusief publieke en private instituties waarin de overheid als wetgever een ordenende kernfunctie vervult? Ligt dan, toegespitst op nieuwe media, het spanningsveld van de burger niet eerder tussen de behoefte aan profilering, zoals op Facebook en dergelijke, versus die aan privacy en zelfbeschikking? Wat is de visie van de regering?

Concreet komt het WRR-advies neer op het instellen van instituties als een permanente commissie voor de iOverheid, een iPlatform en een iAutoriteit met doorzettingsmacht. Tot verwondering van de PvdA-fractie blijkt hieruit niets anders dan een traditionele top-downbenadering met voorbijgaan aan de elders in het WRR-rapport bepleite betrokkenheid van de samenleving. Waaruit blijkt een meer actieve inbreng van de samenleving, groepen en individuele burgers? Waarom wordt de burger niet veel meer interactief betrokken bij de digitale middelen? Wat is de mening van de regering?

Wat is de meerwaarde van nog meer instanties naast de bestaande zoals het CBP? Komen er andere instrumenten, methoden of werkwijzen? Zo ja, welke dan? Waarom zouden die ineens wel effectief zijn en waarom kunnen die niet worden toegepast door de bestaande instanties? Komt er een herhaling van zetten zoals met de Centra voor Jeugd en Gezin naast de Bureaus Jeugdzorg? In plaats van verbeteringen brengen grote extra investeringen meer belasting voor de dienstverlening volgens het gebruikelijke bestuurlijke Pavlovreactiepatroon. 1. We hebben een probleem dus we stellen nog een instantie in waarmee we aangeven "iets" te doen. Die instantie noemen we autoriteit, taskforce of iets dergelijks en die gaat soortgelijke instanties beconcurreren, waardoor de uitvoering extra en vaak tegenstrijdige instructies krijgt 2. De

instantie krijgt targets, meestal kwantitatief, want kwaliteit is moeilijk meetbaar. Daartoe wordt een informatiesysteem ontwikkeld, want "meten is weten". Jammer genoeg alleen van het kwantitatieve deel van het product. 3. De werkvloer moet bijhouden of de targets worden gehaald. Dus de bureaucratische last wordt groter, temeer als ook protocollen zijn voorgeschreven. De administratieve belasting gaat nog meer ten koste van de beschikbare capaciteit voor de primaire taak. 4. Het systeem van honorering en subsidiëring op basis van kwantitatieve prestaties houdt het risico in van perverse prikkels. 5. De beschikbare informatie leidt tot schijnzekerheid, want de kerninformatie, de kwaliteit en wat de klant daarvan vindt, ontbreekt. 6. De professional komt minder aan het eigenlijke werk toe.

Kortom: de klant gaat er in alle opzichten op achteruit.

Geeft dit niet aan dat het om meer gaat dan de WRR-spagaat tussen dienstverlening en privacy? Naar onze mening is nog onvoldoende het besef doorgedrongen dat de effectiviteit en efficiency van het overheidsfunctioneren als zodanig in het geding is. Herkent de regering het boven geschetste beeld dat de bestaande informatiseringspraktijk de kwaliteit van de dienstverlening aan de burger eerder aantast dan verbetert?

Bij de uitvoerende taak van de overheid is het begrijpelijk dat de automatisering in eerste instantie heeft geleid tot registratie van allerlei gegevens. De nieuwe geavanceerde technologieën maken echter een tot dusverre te weinig toegepaste individuele insteek mogelijk. Het kantelen van algemene databestanden naar op het individu geconcentreerde gegevensverzamelingen biedt een uitweg voor ogenschijnlijk onoplosbare patstellingen vanwege privacy- en veiligheidsrisico's.

Als veel voorkomend probleem bij het systeemontwerp signaleert de WRR de zogeheten "function creep", doelvervuiling tijdens de doorlooptijd bij de ontwikkeling van systemen met als resultaat een onontwarbaar systeem met alle gevolgen van dien voor de praktijk van de uitvoering en de kosten. Een ander veel voorkomend fenomeen is het aanbod dat de vraag creëert. Er is een nieuwe techniek waar een toepassing bij wordt gezocht of er is een bestand ontwikkeld waarvan al te gemakkelijk gebruik gemaakt wordt. Een voorbeeld is het Schengenbestand, waarop naast de oorspronkelijke drie inmiddels zo'n honderd gebruikers zijn aangesloten. Is de regering zich bewust van de risico's van deze koppelingen voor burgers, zeker gelet op de eerder door de Rekenkamer gesignaleerde foutregistraties? Is hier geen strenge effectiviteitstoets vooraf nodig op basis van wettelijke criteria?

Van belang voor de kwaliteit van beleid en praktijk zijn waarborgen voor het opdrachtgeverschap en toezicht in de vorm van instrumenten en instituties. Instrumenten als privacy impact assessment (PIA), privacy by design, privacy enhancing technologies (PET) en gateway reviews zijn de meest gangbare. Over de PIA's hebben wij schriftelijke vragen gesteld die deels zijn beantwoord. In aanvulling daarop de vraag hoe de regering de PIA's en de overige genoemde instrumenten wil inzetten bij de ontwikkelingstrajecten en of de regering een vorm als social impact assessment denkbaar acht? Hoe denkt de regering over versterking van het toezichtinstrumentarium met verplichte openbaarheid bij onderzoek naar praktijken van bedrijven en over hogere sancties, zoals dwangsommen en boetes?

Inzake de instituties geeft de regering aan vooralsnog vast te houden aan de huidige opzet van het CBP. Niettemin wijst het CBP bij voortduring op knelpunten bij de uitvoering vanwege capaciteitstekort. Uit de samenleving komen inderdaad signalen over moeilijke toegang tot het CBP tot op het niveau van Kamerleden van de Eerste Kamer, zoals bij de voorbereiding van de besluitvorming over de slimme meters. Acht de regering het ter versterking van een robuuste toezichtfunctie niet raadzaam de capaciteit van het CBP uit te breiden met meer fte's en daarnaast de taak van het CBP meer toe te spitsen op het toezicht op naleving van de wet? Zou dan het servicecentrum ter ondersteuning van veiligheid en jeugdzorgprofessionals niet moeten worden verbreed naar alle sectoren en naar burgers naast professionals? Uiteraard zijn de drie fte's dan helemaal niet meer voldoende.

Essentieel in de WRR-aanbevelingen is de permanente commissie die jaarlijks rapporteert over de staat van de informatie, met inbegrip van een effectiviteittoets van koppeling en verwerking van persoonsgegevens, inclusief de effectiviteittoets vooraf, en van een evaluatie van lopende, gestrande en afgeronde projecten. Kan de regering aangeven of een dergelijk instituut niet zozeer rechtstreeks aan het parlement rapporteert, maar ook kan worden gepositioneerd als specifiek onderdeel van het onderzoeksbureau van de Tweede Kamer zelf? Meer in het algemeen: zijn genoemde instrumenten niet alleen voor bestaande instituties maar ook voor de Tweede Kamer toepasbaar?

De WRR-aanbevelingen zijn volgens de PvdA-fractie kenmerkend voor de eenzijdige nadruk op de overheid enerzijds en de veronachtzaming van de individuele behoeften en mogelijkheden van de burger anderzijds. Er dient een meer gelijkwaardige wisselwerking te komen tussen de instituties die namens ons werken en de individuen voor wie ze dat doen. Met behulp van Web 2.0 kan de burger de resultaten van democratie en dienstverlening eerder en beter beïnvloeden. Stemmen met de voeten wordt stemmen met de vingers. De burger moet als eerste de beschikking over zijn persoonsgegevens hebben. Het beschikkingsrecht voor instituties daarover moet uitzondering in plaats van regel worden. Is de regering bereid een wetsvoorstel inzake identiteitsmanagement voor te bereiden, mede gebaseerd op het voorstel van de VS-senatoren Kerry en McCain?

Overheidsprojecten moeten standaard zijn voorzien van openbare kosten-batenanalyses, openbaarheid van haalbaarheidsstudies, pilots en onderzoeksrapportages, ondersteuning door externe expertmeetings en onafhankelijk advisering. Publieke betrokkenheid door openheid over opdrachtverstrekking, reikwijdte, inhoud en resultaten van onderzoek en ontwikkeling van door de overheid gefinancierde systemen is een must. Door transformatie naar bottom-up in plaats van top-down kan vanuit de burger tegenmacht ten opzichte van grootmachten in de publieke en private sector worden gegenereerd, met een voortrekkersfunctie van de volksvertegenwoordiging, vooral de Tweede Kamer. Ook particuliere instanties als consumentenorganisaties, mediaprogramma's, zoals Radar, en privacygroepen hebben een aanjaagfunctie. Door de openbaarheid en transparantie van instituties te waarborgen dient de overheid zich te verantwoorden ten opzichte van de burger in plaats van vice versa. Inperken van de WOB is dus uit den boze. Graag een reactie van de regering op deze visie.

Franken

□

De heer **Franken** (CDA):
Voorzitter. Dagelijks laten u en ik digitale sporen achter. Wie, waar, wanneer wij bellen of mailen, wat we kopen – denk aan de barcode – welke tv-programma's wij bekijken, welke medicijnen wij gebruiken: het is bij vele anderen bekend. Soms laten wij die sporen vrijwillig achter, omdat we een tegenprestatie ontvangen of denken te ontvangen als gewaardeerde klant, maar wij weten niet dat we op grond van die informatie in het vervolg misschien juist zullen worden uitgesloten. Wij realiseren ons niet of nauwelijks dat Hyves, Facebook, Twitter en LinkedIn al onze gegevens, meestal geanonimiseerd, gebruiken en verkopen. Ook worden veel sporen ons afgedwongen door de overheid op doorgaans gerespecteerde gronden, maar dan weten wij evenmin wat er in werkelijkheid met "onze" gegevens gebeurt. Men weet ontzettend veel van ons terwijl wij dat zelf niet weten.

De overheid houdt ons in de gaten met passagierslijsten, met controle van ons betalingsverkeer, met blacklists op EU- of VN-niveau en is door middel van de bewaarplicht verkeersgegevens een permanente luistervink. Het CIOT wordt naar het schijnt 300.000 keer per maand bevraagd, dat wil zeggen 10.000 keer per dag. Bedrijven analyseren ons koop- en betaalgedrag en maken daar door middel van statistische bewerkingen profielen van, waarmee men ons een identiteit toekent en eigenschappen toedicht, die wij misschien niet eens zouden willen hebben.

De vraag is: is dat nu zo erg? "Nee", zegt een slinkende groep mensen, "want ik heb niets te verbergen". Dat zei bijvoorbeeld de presentator van een populair BBC-programma – hij stond gisteren in de NRC – en hij maakte zijn eigen rekeningnummer bekend. In een mum van tijd wist iemand zich toegang tot zijn rekening te verschaffen om een maandelijkse afschrijving aan te maken van £500 naar een goed doel. De man is sindsdien van mening veranderd. Ook is de toonzetting in de pers niet meer negatief. Datalekkages zijn nu serieus nieuws in Engeland. Er is zelfs een minister over gestruikeld. Het privacybewustzijn, dat in Nederland tot voor kort bijzonder laag was – 32% in 2008 ten opzichte van een gemiddelde in de Europese Unie van 68% – is beduidend gestegen.

Een recente voorstudie voor het WRR-rapport toont aan dat privacy voor de burger beslist geen gepasseerd station meer is. De respondenten in dat onderzoek geven aan dat zij inzage willen hebben in de elektronische dossiers, zodat ze gegevens kunnen corrigeren en weten wie de gegevens inziet en bewerkt.

Het is dus zeker belangrijk om als burger zo veel mogelijk een afweging te maken waar en wanneer je sporen achterlaat. Ik moet daarbij vaak denken aan een roman uit de jaren dertig van de vorige eeuw: "Der Mann ohne Eigenschaften". Nu krijgt een burger, die wel eigenschappen heeft, er een of meerdere opgeplakt, die hij of zij niet wil. Erger is nog wanneer iemand anders zich jouw identiteit toe-eigent. Dat is niet zo moeilijk. "Spoofing" heet dat in het jargon. Ik wil graag van de bewindslieden horen wat zij tegen deze gedragingen in onze "geketende netwerken" denken te ondernemen en wel tegen de achtergrond, dat identiteitsfraude in de Verenigde Staten wordt gezien als de snelst groeiende vorm van misdaad. Ik kom er straks nog even op terug.

Vandaag wil ik spreken over het vinden van een balans tussen het overheidsbelang tot dataverzameling en -verwerking ten behoeve van voornamelijk veiligheid en preventie enerzijds en de inbreuk op het recht op eerbiediging van het privéleven en de bescherming van persoonsgegevens anderzijds. Aan dit onderwerp zijn door de CDA-fractie in de algemene politieke beschouwingen van 2008 al beschouwingen gewijd. Wij spreken hier over de werking van twee grondrechten: de artikelen 7 en 8 van het Europese Handvest met analoge bepalingen in artikel 8 EVRM en artikel 10 van de Grondwet. Beperkingen op deze rechten voor de burger zijn mogelijk, maar die moeten aan strikte voorwaarden voldoen.

Ik zal eerst trachten de schuivende panelen van de twee gebieden aan te geven. Daarna zal ik ingaan op de stukken die de beide bewindspersonen ons als antwoord op onze vragen hebben toegestuurd, waarin een aantal maatregelen wordt voorgesteld. Overigens mijn dank voor de toezending van deze stukken. Ten slotte leg ik een aantal aandachtspunten en suggesties voor, die onder meer zullen uitmonden in een motie met betrekking tot het wetgevingsproces.

Er is al veel geschreven en ook veel geregeld met betrekking tot de verhouding tussen veiligheid en de bescherming van de persoonlijke levenssfeer. De uitgangspunten voor de privacybescherming zijn neergelegd in de Wbp van 2001, die is gebaseerd op een richtlijn van 1995. De hoofdlijn betreft de informatie aan en de toestemming van de betrokkene, zijn inzage- en correctierecht en de doelbinding. Dat laatste wil zeggen dat alleen onder bepaalde voorwaarden gegevens mogen worden gebruikt buiten het domein waarvoor zij zijn verzameld. Deze uitzonderingen zijn:
- het voorkomen, opsporen en vervolgen van strafbare feiten;
- de bescherming van belangrijke financiële en economische belangen van de staat;
- de bescherming van de betrokkene of de rechten en vrijheden van anderen.

Van deze uitzonderingsmogelijkheden is in een hele serie wetten gebruik gemaakt. Een groot aantal daarvan dateert al van vóór 9/11, maar ook daarna zijn er stelselmatig nieuwe of meer uitgebreide bevoegdheden voor politie en Openbaar Ministerie bijgekomen. Daar spelen natuurlijk maatschappelijke ontwikkelingen een rol. Ik denk aan de toename van de georganiseerde criminaliteit, de toename van de bevolkingsdichtheid met als gevolg minder sociale controle, alsmede technologische ontwikkelingen waardoor datamining en profilering mogelijk zijn gemaakt. Wij kunnen echter – en in het Rathenaurapport staat het nog eens netjes op een rij – in de uitbreiding van wetgeving een aantal trends onderscheiden.
- Politieonderzoek wordt steeds vaker uitgebreid tot personen op wie zelf geen verdenking rust. Nu is het zelfs zo dat iedere Europeaan een verdachte is, omdat zijn communicatiegegevens onder het bereik van de opsporingsinstanties worden gebracht.
- Politioneel onderzoek krijgt in toenemende mate de vorm van een verkenning, waarin op basis van risicoprofielen potentieel verdachte groepen worden gevolgd.
- Bestaande wettelijke beperkingen die gelden voor het gebruik van bepaalde onderzoeksmethoden worden verlicht.
- Opsporingsdiensten krijgen meer mogelijkheden om zelfstandig onderzoek te verrichten zonder dat de toestemming van een rechter-commissaris voor ingrijpende maatregelen nodig is.

- Opsporingsdiensten kunnen in toenemende mate beschikken over persoonsgegevens afkomstig van andere (semi)overheidsdiensten, die voor andere dan opsporingsdoeleinden zijn verzameld.
- Opsporingsdiensten dwingen steeds vaker andere partijen tot medewerking aan onderzoek.

Nu zijn al die maatregelen op zich best verdedigbaar, althans verklaarbaar, maar er is geen overzicht meer. Wij bevinden ons op een "slippery slope". Er worden steeds nieuwe bevoegdheden geschapen, terwijl de grenzen van de bestaande bevoegdheden nog niet echt zijn verkend. Hoe moet het nu verder gaan of moet het überhaupt nog wel verder gaan?

Wij verwachten binnenkort de "slimme" camera's, die zelfstandig afwijkingen van tevoren vastgestelde patronen kunnen herkennen. De wachter wordt een onverbiddelijke robot. Met RFID kun je mensen overal en altijd volgen. De zelfdenkende computers doen hun intrede. Deze computers nemen zelfstandig beslissingen. Moeten wij dan de opsporingsbevoegdheden – op voorhand – weer gaan uitbreiden? Zal er meer "function creep", toe-eigening van bevoegdheden in strijd met de doelbinding, worden gecreëerd? Is het mislukken van de centrale opslag van vingerafdrukken niet een nieuwe les, dat naast het epd, waar de autorisatie het knelpunt bleek, nu door de ontoereikende verificatie het totale systeem nog niet rijp was? Het gaat dan niet alleen om de techniek, maar vooral om de organisatie. Daar mag toch geen basis liggen voor de uitoefening van opsporingsbevoegdheden? Ik houd hiermee een pleidooi voor zowel techniekonafhankelijke wetgeving als voor grote terughoudendheid ten opzichte van het scheppen van nieuwe bevoegdheden. Graag de mening van de bewindslieden hierover.

Ik sprak al even over het gevaar van identificatiefraude. Er is recentelijk onderzoek gedaan naar de kennis, de houding en het gedrag van burgers ten aanzien van de voorkoming van identiteitsfraude. Het blijkt, dat de burgers er niet zoveel van weten. Zij hebben behoefte aan informatie daarover en voelen zich medeverantwoordelijk. Immers, veel gevallen zijn te voorkomen. Ziet het kabinet hier een taak door het aanbieden van "slachtofferhulp avant la lettre" en door strafbaarstelling van bepaalde gedragingen?

Wil de minister of de staatssecretaris medewerking verlenen om encryptietechnieken te bevorderen en daardoor herroepbare privacy in brede zin mogelijk te maken? In het boek Check in/Check out van het Rathenau Instituut is beschreven hoe een betrouwbare digitale identiteit kan worden opgebouwd met een machtiging aan de politie om onder bepaalde voorwaarden in kennis te worden gesteld van de sleutel. De collega's van de PvdA-fractie hebben hiernaar gevraagd, maar er is op deze, naar mijn mening voor de toekomst uitermate belangrijke vraag nog geen antwoord gegeven.

In de paragraaf Visie van de regering gaan de bewindspersonen gedegen in op de vraagstukken die het maken van profielen met zich kan brengen. Ik heb daar toch nog enige vragen over. We moeten ervan uitgaan dat ICT-toepassingen allesbehalve neutraal zijn. Onder invloed van de inzet van technologie gaat de overheid, zoals iedere gebruiker, anders handelen en functioneren. Natuurlijk worden er al veel langer grote hoeveelheden gegevens verzameld. Nu gaat het erom uit de berg van verzamelde gegevens de relevante informatie te vergaren. Daarvoor worden beelden van burgers, typeringen van consumenten of categorieën van klanten gemaakt. In de publieke sfeer wordt die identiteit benut voor een specifiek doelgroepenbeleid: fraudebestrijding, jeugdbeleid, huiselijk geweld enzovoort. De vraag is nu hoe dynamisch deze geconstrueerde digitale identiteiten zijn. Bestaat de mogelijkheid om profielen aan te passen en veranderde identiteiten te wissen? Is er een recht om te worden vergeten, of is wie eens steelt inderdaad voor altijd een dief?

Deze typeringen kunnen bovendien multifunctioneel worden ingezet, met als gevolg dat er samenwerkingsvormen tussen overheidsorganen ontstaan en het principe van doelbinding wordt veronachtzaamd. Bovendien ligt function creep hierbij voor de hand. Juridisch rijzen hier ook nog vragen: wie is dan de in de Wbp voorgeschreven verantwoordelijke voor de gegevensbescherming? En hoe staat het met de mogelijkheid tot inzage en correctie voor de "Mann mit zugeschriebenen Eigenschaften"?

Waar, zoals bij de hantering van de Wbp, belangen moeten worden afgewogen, is het voor de praktijk nuttig om criteria aan te reiken die daarbij kunnen helpen. De commissie-Brouwer-Korf heeft voor de afwegingen met betrekking tot gegevensverwerking in het veiligheidsdomein een richtinggevend kader aangeboden voor de feitelijke omgang met persoonsgegevens. Het gaat om de grondslagen die de personen die de betreffende afweging moeten maken bij hun keuzes moeten hanteren. Deze criteria dienen serieus te worden genomen.

Daarnaast verdient een leidraad voor de wetgever aandacht. Dan gaat het niet zozeer om het departementale document dat de titel draagt "Leidraad afstemmen van wetgeving op de Wet bescherming persoonsgegevens", overigens een prima leer- en handboek voor wetgevingsambtenaren. Het gaat om noodzakelijke aandachtspunten voor de wetgever die aan de orde moeten komen bij beslissingen inzake privacygevoelige wetgevingsprojecten. We hebben in deze Kamer in maart 2008 daarover tijdens een expertmeeting gediscussieerd en toen Kamerbreed tezamen met alle aanwezige deskundigen geconcludeerd dat ieder wetsvoorstel waarbij de bescherming van de persoonlijke levenssfeer een rol kan spelen, getoetst moet worden aan de volgende vijf criteria.

Als eerste noem ik de noodzaak, effectiviteit en hanteerbaarheid van de maatregel. Vooral die noodzaak is niet zo vanzelfsprekend als het lijkt. Het gaat erom dat je gegevens alleen mag verzamelen en verwerken omdat het moet en niet omdat het kan. Het tweede criterium is de proportionaliteit: de inbreuk mag niet groter zijn dan strikt noodzakelijk is. Het derde aandachtspunt gaat over de resultaten van een privacy impact assessment. Hierdoor wordt vooraf onderzocht welke risico's de maatregel met zich meebrengt. Vier: effectief toezicht en controle. Het laatstgenoemde begrip is hierbij niet opgevat in de Angelsaksische zin van beheersen ("to control"), maar van de Franse benadering "contre rôle", waarbij het gaat om tegenspel, onder meer te realiseren door audits door de onafhankelijke toezichthouder. Ten slotte het vijfde aandachtspunt: de beperking van de geldigheidsduur door een horizonbepaling, of in ieder geval een evaluatiebepaling.

Wij stellen voor dat er in de memorie van toelichting van de in aanmerking komende wetsvoorstellen tot uitdrukking wordt gebracht hoe er aan deze toetsingscriteria is voldaan, net zoals dat gebeurt bij het nemen van andere vaste stappen in het wetgevingsproces. Het komt ons opportuun voor om deze conclusies thans in een motie vast te leggen. Ik kom in de tweede termijn met de motie

omdat ik nog op zoek ben om deze zo breed mogelijk gedragen te doen zijn.

Een van de toetsingscriteria die ik zojuist besprak, de privacy impact assessment, is in de schriftelijke ronde ook ter sprake gekomen. De regering heeft geantwoord dat zij initiatieven vanuit het bedrijfsleven voor het ontwikkelen van PIA's ondersteunt, maar geen voorstander is van het verplicht voorschrijven van het gebruik van PIA's in de wetgeving. Als argument voert de regering aan dat een dergelijke verplichting zou leiden tot een onevenredig zware financiële belasting van het bedrijfsleven.

Wij zijn het hiermee niet eens. Het gaat nu om een oriënterend onderzoek dat het departement dient te verrichten. Van het bedrijfsleven zal in een enkel geval misschien worden gevraagd een vragenlijst in te vullen. Het gaat hier niet om een milieueffectrapportage waarvoor een serie deskundigen uitgebreide studies moet verrichten. Bovendien is het afwijzende antwoord niet in lijn met de begeleidende brief waarin de beantwoording van de Kamervragen wordt aangeboden. In de brief staat namelijk onder punt j dat een onderzoek zal worden gedaan "naar de mogelijkheid om de Awb te benutten voor het delen van toezichtgegevens en de mogelijkheden voor het gebruik van PIA's". Daarnaast staat in de notitie Privacybeleid op pagina 13 dat het wetsvoorstel ANPR een goede gelegenheid vormt om, in mijn woorden, als proeftuin te dienen. Aansluitend: privacy by design wordt, terecht, door de regering aanvaard. Het ministerie van EL&I heeft TNO gevraagd daar onderzoek naar te doen. Kan de minister of de staatssecretaris een indruk geven van de vraagstelling voor en vormgeving van dit onderzoek?

In het kader van de Europese en internationale ontwikkelingen wil ik aandacht vragen voor cloudcomputing. Deze vorm van dataverwerking maakt een ongekende flexibiliteit en schaalbaarheid mogelijk en biedt daarom zeer gunstige economische perspectieven. Er bestaan echter twijfels over de privacywaarborgen en de toegankelijkheid van data, waardoor de maatschappelijke acceptatie en het brede gebruik van clouddiensten stagneert. Ziet de regering kans om maatregelen te treffen waardoor aan de gebruikers de zekerheid wordt gegeven dat zij over "hun" gegevens kunnen beschikken en dat zij zonder al te veel moeite kunnen overstappen naar een andere leverancier, zoals dat ook in de telecommunicatiesector met de nummerportabiliteit is geregeld? De gebruikers zouden er ook op moeten kunnen vertrouwen dat hun data die bij cloudcomputing her en der worden verspreid, goed zullen worden beveiligd en niet zullen worden misbruikt.

Daarnaast zijn er nog veel vragen met betrekking tot de aansprakelijkheid van de ISP's, het toepasselijke recht en de individuele toegang, correctie en verwijdering. Ziet de regering een middel om desondanks deze economische gangmaker te faciliteren? Naar ik aanneem – maar ik vraag voor de zekerheid nog even een bevestiging – ondersteunt de regering de netneutraliteit en zal zij zich met kracht tegen iedere vorm van filtering verzetten.

Ten slotte. Ondanks het feit dat wij een schriftelijke ronde hebben gehad, zijn er nog veel vragen. Ik zal me desondanks beperken tot een laatste opmerking met het verzoek om commentaar daarop van de beide bewindslieden. Als uitgangspunt voor de benadering van informatiegrondrechten kies ik het adagium "kennis is vrij". Dat betekent dat in beginsel alle informatie vrij is. Informatie beheersen, zoals dictators gewoon zijn te doen door media te verbieden, past in een verouderd, hiërarchisch informatiemodel. Nu heeft iedereen een mobieltje en is zelf verslaggever. Dat leidt tot twee veranderingen. In de eerste plaats wordt de aandacht verplaatst van de verwerking van data, processing of data, naar het datagebruik en de consequenties daarvan voor de burgers, zoals het manipuleren van identiteiten.

Daarnaast zien we een verschuiving van privacy als individueel afweerrecht in de richting van collectieve doelen zoals autonomie, sociale cohesie en gelijke behandeling. De oorzaak daarvan vormen de technologische veranderingen van web 2.0. Wij zien privacy van "the right to be let alone", het afweerrecht dat het privédomein beschermt, overgaan naar "the right to act alone", een actierecht. Dat betekent: ik bepaal zelf mijn profiel. Anders gezegd: er bestaat een collectief georganiseerde bescherming van persoonsgegevens met daarnaast het recht om individueel de wijze van gebruik van de eigen persoonsgegevens te bepalen. Het optreden van de twitteraar en Facebookadept moet daartoe dan ook worden gefaciliteerd. In deze zin wordt privacy, evenals de vrijheid van meningsuiting, een voorwaarde voor een vrije en democratische samenleving. Graag verneem ik de visie van de regering op deze ontwikkeling.

□

Mevrouw **Slagter-Roukema** (SP):
Voorzitter. Ik voer mede namens de Partij voor de Dieren het woord, dus dat scheelt in de tijd. Daardoor wordt mijn bijdrage misschien iets langer, maar in totaal zal het iets korter worden.

Een debat zoals we vandaag voeren met de minister van Binnenlandse Zaken en Koninkrijksrelaties en de staatssecretaris van Veiligheid en Justitie heeft als grootste valkuil dat het te veel gaat uitwaaieren. Hierdoor wordt over veel zaken iets gezegd maar komt er vervolgens weinig uit als het om afspraken en resultaten gaat. Toch is een debat als dit nodig, verwijderd van de hectiek van alledag, gevoerd in een omgeving waar de politiek uiteindelijk misschien wel het eindoordeel velt, maar waar ook plaats is voor bezinning en reflectie, plaats voor een inhoudelijk debat. Het is de mening van mijn fractie dat het hoog tijd is om ons te bezinnen op de stand van zaken met betrekking tot de balans tussen bewaken van de veiligheid en het recht van de burger op bescherming van zijn persoonlijke levenssfeer.

Ter voorbereiding op dit debat heb ik me laten leiden door de bevindingen van de adviescommissie veiligheid en persoonlijke levenssfeer oftewel de commissie-Brouwer-Korf, de evaluatierapporten van de Wet bescherming persoonsgegevens en de brief en notitie van 29 april van beide bewindslieden over privacybeleid. Het was prachtig dat wij die op tijd hebben gekregen, waarvoor mijn hartelijke dank aan de bewindslieden. Daarnaast heb ik de publicaties van het Rathenau-instituut over databases, over ICT-beloften, informatiehonger en digitale autonomie en de recente publicatie van de Wetenschappelijke Raad voor het Regeringsbeleid over de iOverheid gelezen.

Tot slot waren er in het voorbereidingstraject op dit debat twee expertbijeenkomsten op 20 maart 2008 en op 21 februari 2011 met deskundigen op het gebied van veiligheid en privacy. In beide bijeenkomsten zijn veel zaken aan de orde geweest die voor het debat van vandaag van groot belang zijn. Omdat de verslagen openbaar zijn, hoop ik dat de bewindslieden ook zelf kennis hebben genomen van de discussies en dat niet alleen aan hun amb-

tenaren hebben over gelaten. Ik ben overigens wel heel erg verheugd door het grote aantal ambtenaren op de tribune. Dat geeft het belang van dit debat aan.

Eigen observaties en eigen ervaringen zijn belangrijk bij het vormen van een mening en bij het voeren van discussies over een zo belangrijk onderwerp als wij vandaag behandelen. Over ervaringen gesproken: de ervaringen van deze Kamer met de gang van zaken rondom het wetsvoorstel 31466, dat beoogde te komen tot een landelijk epd, zijn mijns inziens bijzonder leerzaam voor het debat van vandaag.

Vorige week had de commissie voor VWS van de Eerste Kamer een mondeling overleg met minister Schippers. In dit overleg werd zowel teruggekeken op het proces als ook vooruitgekeken. Wat valt er te leren van het verloop van dit grote digitaliseringsproject dat door de overheid met zo veel ambitie is neergezet en dat tot nu toe 300 mln. kostte? Ook van dit overleg komt overigens een openbaar verslag.

We hebben met elkaar geconstateerd dat de trein die zou moeten leiden tot een landelijk epd gaandeweg de behandeling van het wetsvoorstel een andere bestemming, een ander doel en een andere vorm heeft gekregen. Er is function creep opgetreden. Het systeem was te grootschalig en daardoor ook moeilijk te beveiligen. Het is begonnen met een valse start doordat het ministerie van VWS de vorige minister op pad stuurde met een foute en misleidende introductiebrief en er was veel te weinig aandacht voor de kwaliteit van de gegevens.

Tot onze vreugde heeft minister Schippers de commissie beloofd om op korte termijn een commissie in te stellen die als opdracht krijgt om de rol van veld en politiek in dit hele proces te analyseren en te evalueren, om – ik zeg het nog maar eens – ervan te leren. Ik verwacht dat de conclusies van de commissie niet alleen leerzaam zijn voor het ministerie van VWS, maar dat het leermomenten voor alle ministeries zal bevatten. Ik ben benieuwd naar het commentaar van de bewindslieden.

In het plenaire debat dat op 15 maart jongstleden met de minister van VWS gevoerd is, heb ik een aantal randvoorwaarden genoemd waaraan digitaliseringsprojecten van de overheid, als grootste speler op het gebied van veiligheid en de belangrijkste verwerker van persoonsgegevens, getoetst dienen te worden. Ze zijn gedestilleerd uit hetgeen de commissie-Brouwer-Korf heeft aanbevolen en wat de deskundigen in de expertmeetings hebben opgemerkt. Ze kleuren de bril waarmee mijn fractie ernaar wil kijken. Ik zal die kort schetsen. 1. Van te voren moeten bestuurlijke keuzes worden gemaakt. Het doel moet duidelijk omschreven en afgebakend zijn. Er dient een beoordelings- en afwegingskader te zijn en er moet gewaakt worden voor function creep. 2. Privacyaspecten moeten vanaf het begin in het design worden meegenomen, evenals privacy impact assessments tijdens de ontwikkeling. 3. Toezicht in de ontwerpfase en transparantie en verantwoording in de verschillende uitvoeringsfasen moeten wettelijk verplicht zijn, evenals externe onafhankelijke audits. De slager moet niet zijn eigen vlees willen keuren. 4. De positie van de burger dient versterkt te worden. In jargon, ik citeer hier de heer Kohnstamm: transparantie, toestemming, informed consent, recht op inzage, correctie, afscherming en verzet inclusief gezamenlijk optreden in rechten van consumer collective redress. 5. Compleetheid van gegevens is niet te garanderen. Houd systemen daarom kleinschalig: select before you collect. 6. Het stellen van deadlines zet de ontwikkeling van een groot ICT-project makkelijk onder druk. Politiek, minister en ICT-industrie moeten waken voor een complexiteitsspiraal waarmee ze elkaar in een wurggreep houden.

Zoals de bewindslieden natuurlijk al gemerkt hebben, kom ik zo langzamerhand meer in de buurt van de documenten die onder hun verantwoordelijkheid zijn geproduceerd. Ik zal de genoemde punten langslopen en van opmerkingen voorzien.

In de eerste plaats: het doel moet duidelijk omschreven en afgebakend zijn. Er dient een beoordelings- en afwegingskader te zijn. Tijdens het debat in juli 2007 over wetsvoorstel 30312, de invoering van het BSN, heeft de staatssecretaris van BZK deze Kamer toegezegd te komen met een voorstel voor een overkoepelend beoordelingskader. Uit latere correspondentie en ook uit de beantwoording van de vragen die in de aanloop naar het debat van vandaag zijn gesteld, blijkt dat het nog niet zo'n vaart loopt met de productie van het gevraagde en toegezegde kader. Collega Tan wees daar ook al op.

Het argument dat er op dit moment geen basis bestaat om te komen tot een dergelijk kader omdat er momenteel geen nieuwe wetgeving of wetgevingswijzigingen zijn ingediend, lijkt mijn fractie niet erg valide. Een beoordelingskader, een kader waaraan je toetst, dient toch ex ante vervaardigd te worden? Er ligt toch genoeg materiaal op basis waarvan in ieder geval een ontwerpkader gemaakt kan worden?

Ik verwijs daarbij naar hetgeen collega Franken heeft benoemd tijdens de plenaire behandeling van het wetsvoorstel BSN in de zorg. Hij maakte onderscheid tussen algemene, wettelijke normen en standaarden voor koppeling van bestanden en een gelaagd normenkader, toe te spitsen per sector. Hierin zijn ondergebracht: transparantie en doelbinding; nut en noodzaak met effectiviteit en hanteerbaarheid; proportionaliteit van te nemen maatregelen; kosten, baten, prognose van het gebruik; privacy impact assessments – ik zal dat vanaf nu maar PIA noemen, uitgesproken op zijn Nederlands omdat dat leuker bekt dan de Engelse uitspraak en doet denken aan een nieuwsgierig aagje – periodieke controle op vervuiling van de bestanden; een horizonbepaling.

Graag hoor ik een toelichting van de bewindslieden op het gebrek aan actie op dit punt, waarbij ik ook aanteken dat, zolang niet duidelijk is hoe de overheid zelf omgaat met digitale dataverzameling en -uitwisseling, het ook moeilijk voor de burger is om de overheid erop aan te spreken. Dat maakt burger en overheid kwetsbaar.

De Staatscommissie Grondwet, de commissie-Thomassen, adviseerde zelfs om in een grondwettelijke bepaling over het recht op de bescherming van persoonsgegevens, het principe van doelbinding vast te leggen. Dit zou betekenen dat een precies doel moet worden aangegeven voor de verwerking van gegevens en dat degene die gegevens verwerkt, zich moet houden aan het doel waarvoor hij gegevens heeft verzameld.

Ook tijdens de expertmeeting van 21 februari is het belang van doelbinding nog eens duidelijk neergezet. We waren het er met elkaar over eens dat gegevens verzameld voor een specifiek doel slechts voor een ander doel gebruikt mogen worden, mits dat doel verenigbaar is met het oorspronkelijke doel. Dat vereist dat het doel duidelijk omschreven is, dat het transparant is en met argumenten omkleed en het liefst per wet geregeld.

Een belangrijke reden om eventueel de specifieke doelbinding te doorbreken, zou kunnen zijn, zoals de bewindslieden vermelden in de brief van 29 april, in situaties

waarin het vitaal belang daartoe dringend noodzaakt. Dergelijke situaties worden gedefinieerd als een onmiddellijke of dreigende aantasting van leven of gezondheid van betrokkene of een derde. Wij begrijpen dat het hierbij gaat om een wijziging van de Wet bescherming persoonsgegevens en vragen een toelichting van de bewindslieden. Mijn fractie is voor privacy by design en niet voor mission creep by design, zeker niet als dit by law dreigt te worden ingevoerd.

Mogelijk kunnen de bewindslieden zich bij hun beantwoording laten inspireren door de gang van zaken rond de centrale opslag van vingerafdrukken in het kader van de Ppw en daarbij ook de overweging meenemen dat onder het mom van veiligheid – centraal opslaan van vingerafdrukken dient de veiligheid – een andere veiligheid geschaad kan worden: vingerafdrukken bevatten bijzonder kwetsbare persoonlijke gegevens.

Ik wil de bewindslieden oproepen om kritisch te blijven. Een term als vitaal belang is multi-interpretabel en afhankelijk van de achtergrond van degene die hem hanteert. Eén van de redenen dat het landelijk epd-wetsvoorstel sneuvelde, was juist dat het doel in de loop van de tijd veranderde.

Mijn tweede punt. Privacy aspecten moeten evenals PIA's vanaf het begin in het design worden meegenomen, voorafgaand aan en tijdens de ontwikkeling. De bewindslieden melden ten aanzien van verplichte PIA's dat het kabinet op dit moment onvoldoende reden ziet om het gebruik van PIA's in wetgeving voor te schrijven. De verwachting is dat de kosten niet opwegen tegen de baten en het zou met name voor het midden- en kleinbedrijf leiden tot een onevenredig zware verplichting. Wel zal bij de ontwikkeling van het wetsvoorstel voor automatische nummerplaatherkenning – collega Franken wees hier ook al op en noemde het een proeftuin – ervaring worden opgedaan met het in kaart brengen van de effecten van de voorgenomen maatregelen op de persoonlijke levenssfeer. Die zouden van nut kunnen zijn voor het ontwikkelen van PIA's voor eventuele nieuwe gegevensverwerkingen op het gebied van het ministerie van Veiligheid en Justitie.

Mijn fractie hoopt dat de conclusie van die exercitie zal zijn dat een PIA in ieder geval voor alle overheidsactiviteiten verplicht moet worden gesteld en openbaar moet zijn. Het is toch opvallend dat in de rest van Europa PIA's veel gebruikelijker zijn dan bij ons. Met een assessment komen de risico's rond de bescherming van persoonsgegevens indringend en openbaar op het netvlies. Daarmee kan dan bij het design rekening gehouden worden. Mij trof de opmerking van professor Bart Jacobs in het artikel over het epd in de Rathenaupublicatie: "architecture is politics". De ICT-architectuur die gekozen wordt, geeft een goed beeld van de onderliggende machtsverhoudingen. Bij veel ontwerpen is de positie van patiënten, cliënten of burgers niet groot. De gebruiker, de verzamelaar, bepaalt in de meeste gevallen de architectuur.

Dat is een extra reden om het design kritisch te beschouwen en kennis van de kansen en belemmeringen van privacy by design breed te verspreiden. Want wat is de reden dat privacy bij design in ons land nog niet breed wordt toegepast, ondanks dat het een goede manier is om privacybescherming concreet vorm te geven in informatiesystemen waarin persoonsgegevens worden verwerkt? Kunnen de bewindslieden in dit kader toelichten met welke opdracht TNO is begonnen aan een onderzoek naar privacy by design en wanneer de resultaten van dit onderzoek zijn te verwachten?

Mijn punten drie en vier. Toezicht in de ontwerpfase en transparantie en verantwoording in de verschillende uitvoeringsfasen moeten wettelijk verplicht zijn. De opmerkingen die te maken hebben met toezicht en transparantie en ook die te maken hebben met het daarna genoemde punt van versterking van de positie van de burger raken beide aan de taken en bevoegdheden van het College bescherming persoonsgegevens. Mijn fractie is blij met de meeste voorstellen tot wijziging van de Wbp zoals vermeld in de brief van 29 april, voorstellen die ook kunnen rekenen op instemming vanuit het CBP zelf. De voorzitter Jacob Kohnstamm vertelde ons tijdens de laatste expertmeeting dat hij zich soms voelde als een lam in plaats van de door hemzelf gewenste leeuw. Ik heb enige moeite om de heer Kohnstamm als een leeuw te visualiseren, maar het zijn zijn woorden.

Een volwassen CBP moet kunnen beschikken over voldoende sanctiemogelijkheden, die ook nog afschrikwekkend zijn. Afschrikwekkend is kennelijk een Neelie Kroesachtige boete. De toezichthouder vraagt om meer budget en meer bevoegdheden. Hij vraagt om een verplichting tot materiële en formele samenwerking met collega-toezichthouders en hij wil graag verplicht worden tot het openbaar maken van zijn onderzoeksbevindingen. Ik vond het saillant om te horen dat de toezichthouders in een kort geding op zeker moment zelf moesten strijden om de onderzoeksgegevens openbaar te krijgen. Wat is de stand van zaken ten aanzien van de ontwikkeling van het wetsvoorstel? Gaat de regering ook iets doen met de nuttige adviezen van het CBP?

In dit kader vraag ik nogmaals naar de beantwoording van de vraag door mijn fractie gesteld tijdens de voorbereiding van dit debat. Het betreft de vraag naar de dubbele petten van het CBP, een positie waarvan de voorzitter zelf aangaf dat hij dat het ongemakkelijk vond. Mijn fractie vindt dat de beantwoording van onze vraag niet adequaat was. Het CBP combineert taken die volgens de trias politica niet bij elkaar horen. Hij is toezichthouder en handhaver, is betrokken bij beleidsvorming en adviseert het kabinet over wetgeving. Daarnaast geeft hij voorlichting aan burgers en aan bewerkers en behandelt hij klachten. De bewindslieden melden op onze vraag dat het CBP volledig vrij is in zijn prioriteitsstelling. Dat was niet de vraag. Daarom nogmaals en nu nog duidelijker gesteld: is de regering met de heer Kohnstamm en met mijn fractie van mening dat de taken van het CBP strijdig met elkaar kunnen zijn? Als de bewindslieden dat ook vinden, wat gaan ze er dan aan doen?

Mijn fractie is overigens van mening dat de regering in het commentaar op het WRR-rapport over de iOverheid vooral ook moet ingaan op de opmerkingen die gaan over het gebrek aan ICT-kennis bij overheid en toezichthouder en dan niet alleen van de techniek, maar ook hoe techniek kan ingrijpen in de persoonlijke levenssfeer. Wil de toezichthouder goed kunnen functioneren, dan is betere kennis dringend geboden. Graag een indicatie in welke richting de bewindslieden denken dat het toezicht zich zal moeten gaan ontwikkelen: als een aparte ICT-toezichthouder, of als een uitbreiding in taken, kennis en budget van het CBP?

Het vijfde punt. Compleetheid van gegevens is niet te garanderen. Houd systemen daarom kleinschalig, select before you collect. De relatie tussen kleinschaligheid en effecten op de veiligheid van de persoonlijke levenssfeer

wordt in de beantwoording van een vraag van deze fractie door de bewindslieden ontkend. Dat is jammer, want juist de grootschaligheid en complexiteit van het ontwerp landelijk epd, naast het feit dat de kwaliteit van de gegevens – in dit geval gegevens de gezondheid betreffende, gegevens die vaak subjectief en multi-interpretabel zijn – maakten dat er te grote beveiligingsrisico's werden gecreëerd en maakten dat het wetsvoorstel werd verworpen.

Het principe van select before you collect moet uitgangspunt zijn als men aan digitale dataverzameling begint. Niet alles moet wat kan. Het risico is ook groot dat men dan door de bomen het bos niet meer ziet. Ter relativering: de verzamelwoede is pas echt losgebroken na de gebeurtenissen in september 2001. Sindsdien zijn met name de Verenigde Staten de drijvende kracht geweest achter het idee dat naarmate je meer verzamelt, je eerder dingen te weten komt. Toch duurde het tien jaar voordat ze uitvonden waar Osama Bin Laden zat, onder de neus van het Pakistaanse leger en op enkele kilometers afstand van de Pakistaanse hoofdstad waar het stikt van de Amerikaanse veiligheidsfiguren. Maar wel zonder internet en zonder mobieltje, dus onzichtbaar voor alle databases.

Met de toename van een aantal bewerkingsslagen op informatie, het aantal betrokken functionarissen en de betrokken werkprocessen neemt bovendien de kans toe dat de juistheid en volledigheid van de informatie wordt aangetast. Hiervoor zijn geen adequate maatregelen te treffen. Zijn de bewindslieden met mijn fractie van mening dat ook de iOverheid betrouwbaar dient te zijn en dus beleid niet moet bouwen op wankele gegevens? Dat voedt het wantrouwen van de burgers. De kwaliteit van de gegevens wordt door de mens bepaald, is mensenwerk, en is afhankelijk van de mate van objectiviteit die mogelijk is. Die verschilt per categorie. Eenmaal fout aangeleverd, gaan de gegevens een eigen leven leiden en is correctie bijna onmogelijk, in ieder geval niet als de overheid niet eens zicht heeft op de aantallen – gekoppelde – databanken.

In dit kader blijft de vraag relevant hoe groot het aantal databanken is waarin de overheid gegevens van de burgers verwerkt en hoeveel koppelingen er zijn. Ik vind het bijzonder om te vernemen dat het niet doenlijk is deze vraag te beantwoorden. Kunnen de bewindslieden aangeven of zij met mijn fractie van mening zijn dat alles op alles gezet moet worden om dat inzicht wel te verkrijgen, ook al is het arbeidsintensief en ook al moeten er langdurig inspanningen worden verricht? Dat kan toch geen argument zijn?

Het laatste punt dat ik wil bespreken, is dat het stellen van deadlines de ontwikkeling van een groot ICT-project gemakkelijk onder druk zet. "Politiek, minister en ICT-industrie moeten waken voor een complexiteitsspiraal, waarmee ze elkaar in een wurggreep houden", verzuchtte een van de deelnemers aan de expertmeeting. Er kan, zoals gezegd, ICT-technisch heel veel: dataverzameling, datamining, cloud computing, profilering. Mijn collega Franken voegde er net nog twee dingen aan toe die ik nog niet kende. Zo gaat het natuurlijk maar door. Risico's kunnen in kaart gebracht worden, hele groepen kunnen als risico gekwalificeerd worden en uiteindelijk gaan wij als datapakketten onze weg. Het elektronisch kinddossier is daar een heel goed en ook heel slecht voorbeeld van.

Dat brengt mij de opmerking: bewindslieden houdt de menselijke maat, de vrijheid en waardigheid in het oog; er is geen enkel bewijs dat onze samenleving door alle dataverzamelingen en -koppelingen veiliger is geworden. En voor de andere kant van de medaille is al helemaal weinig oog. In hoeverre speelt de overheid met al deze gekoppelde databestanden criminelen in de kaart?

Het is tijd voor bezinning en een pas op de plaats. Ik verwees er al naar aan het begin van mijn bijdrage. Waarom niet eens de rug rechtgehouden, ook als de politiek – daaronder versta ik zowel parlement als regering – weer mogelijkheden bepleit tot uitbreiding van systemen, uitbreidingen waar die systemen niet voor waren bedoeld?

Ik zou zeggen: bewindslieden, lees het rapport van de WRR en kom terug met een degelijke analyse en een stappenplan. Met een deltaplan tegen het gevaar van een datasnoodramp, om Marc Chavannes uit de NRC van 10 april 2011 te citeren.

Voorzitter. Tot slot. Het is belangrijk dat de politiek, regering en parlement, zich naast de voordelen terdege ook van de grote risico's van het almaar opslaan van gegevens bewust is. Minstens zo belangrijk is het dat het publiek beseft wat er allemaal gedaan kan worden met vergaarde persoonlijke gegevens en daardoor ook zorgvuldig met de eigen gegevens omgaat. Om dat laatste te ondersteunen heeft de schrijver en voormalig rechtbankgriffier Ton Theunis zich verdiept in de warrige wereld van het dataverzamelen en datakoppeling. Het resultaat daarvan is het voortreffelijke boek De kluizenaar, dat ik voor mij heb liggen. Overigens heeft de SP-fractie in het Europarlement hem daarin ondersteund. Wij ontdekten dat zelf ook redelijk laat. Het eerste exemplaar was terecht voor Jacob Kohnstamm van het CBP. Maar dit boek, dat nu het einde van zijn commerciële cyclus nadert, hoort zeker ook in de boekenkasten te staan van de hier aanwezige bewindslieden. Als het te moeilijk is om alle rapporten te lezen, is er misschien wel tijd voor deze thriller. Het gaat immers ook over hun verantwoordelijkheden. Ik geef het hun daarom vandaag graag als een spannende versie van hetgeen waarover wij hier vandaag met elkaar debatteren, wat misschien iets minder spannend is. Ik zie de reactie op mijn inbreng met belangstelling tegemoet.

□

De heer **Holdijk** (SGP):
Voorzitter. Ik zou willen beginnen met aan de samenvatting van het rapport van de WRR over de iOverheid het volgende te ontlenen.

"De alomtegenwoordige inzet van informatie- en communicatietechnologie (ICT) door de overheid heeft ervoor gezorgd dat deze niet langer meer zoals een e-overheid, gericht op dienstverlening en gebruikmakend van techniek, kan worden gekarakteriseerd. In de dagelijkse praktijk is veeleer een iOverheid ontstaan.

De beleidsplannen voor de e-oveheid – gericht op de (interne) bedrijfsvoering, de dienstverlening van de overheid en op de techniek zelf – ademen stuk voor stuk een groot vertrouwen in de ICT als middel om de overheid effectiever, klantvriendelijker, toegankelijker, kwalitatief beter en voorbereid op de toekomst te maken. In toenemende mate wordt ICT enthousiast binnengehaald door beleid en politiek voor zowel de complexe administratieve opdracht van de overheid, als de aanpak van urgente maatschappelijke uitdagingen, zoals terrorisme, veiligheid, mobiliteit en goede en betaalbare zorg.

Het technovertrouwen van politiek en beleid vertaalt zich in grote ambities met ICT, niet alleen in technische, maar zeker ook in beleidsinhoudelijke zin."

Holdijk

Het is een bekende ontwikkeling en het zijn voor ieder bekende verschijnselen, waaraan ook negatieve aspecten verbonden zijn. Steeds meer informatie wordt vastgelegd, bewaard, gekoppeld en hergebruikt, ook buiten de oorspronkelijke context, met het risico van foute interpretaties en conclusies. Burgers worden zo soms jarenlang vastgepind op informatie uit het verleden. Ik noem slechts het ekd. De overheid haalt "overal en nergens" gegevens vandaan en dan moet de betrokkene maar aantonen dat het fout is, om maar niet te spreken van datalekken, vervuilde of verouderde informatie. Informatiestromen trekken zich bovendien tegenwoordig niets meer aan van de grenzen tussen publiek, semipubliek en privaat.

Een technisch systeem, dat bedacht en bedoeld is om mens en samenleving te dienen dreigt, zoals meer gebeurt, hen te gaan overheersen. Dat blijkt bijvoorbeeld wanneer er een fout zit in de informatie die de overheid over de burger heeft. Dan kan men eindeloos bezig zijn om herstel te bewerkstelligen. Ook de overheid wordt geconfronteerd met systemen die steeds complexer worden en in die complexiteit vastlopen – ik noem slechts de Belastingdienst en de politie – waardoor deze niet meer beheersbaar is.

Natuurlijk zijn de positieve effecten van de ICT-ontwikkeling te waarderen. Wij behoeven ook niet bij voorbaat uit te gaan van kwade bedoelingen en wij doen dat ook niet. Veel vaker zullen het gemakzucht en kostenoverwegingen zijn die misbruik en oneigenlijk gebruik in de hand werken.

Het is een waagstuk om als digibeet of, zoals het tegenwoordig wel wordt genoemd, als "digitaalimmigrant" aan een debat als dit deel te nemen. Enige bescheidenheid is daarom gepast. Nochtans stel ik er prijs op om namens de fracties van SGP en ChristenUnie nog enkele opmerkingen naar voren te brengen.

Aan de schriftelijke voorbereiding van dit debat als zodanig hebben onze fracties niet deelgenomen, wel aan de reactie op het rapport van de commissie-Brouwer-Korf over veiligheid en de persoonlijke levenssfeer. Op die thematiek zal ik mijn bijdrage thans toespitsen. Weliswaar staat de relatie overheid-burger centraal, maar deze is van asymmetrische aard. Het is daarom dat wij menen dat de weerbaarheid van de burger moet worden vergroot, bijvoorbeeld bij het verwerken van persoonsgegevens in de vorm van datamining of profilering. Ik denk onder andere aan medische gegevens. Voor ons zijn aanvaarde principes bij de omgang met persoonsgegevens ter bescherming van de burger onder andere het volgende drietal. 1. Het recht op uitdrukkelijke, voorafgaande en volledig geïnformeerde toestemming bij gebruik en hergebruik, door wie ook. 2. Elk gebruik van persoonsgegevens dient strikt noodzakelijk en doelgebonden te zijn. 3. De burger heeft te allen tijde recht op inzage, correctie en eventuele verwijdering van zijn persoonsgegevens.

Nogmaals, dit zijn vrij algemeen aanvaarde principes die wij hier nog eens willen onderstrepen. Ik heb uit de stukken op kunnen maken dat het kabinet gelukkig niet stilzit, maar, zoals gewoonlijk, loopt de ontwikkeling van de technische mogelijkheden soms ver en geruime tijd op wet- en regelgeving vooruit. Dat is een gegeven waar niets aan te veranderen is. Daarbij komt dan nog dat gegevens steeds meer wereldwijd verspreid worden of raken, hetgeen veel internationale afstemming vergt.

Ik zou naar de thematiek van veiligheid en privacy terugkeren. Wij zijn met de regering van oordeel dat de bescherming van de persoonlijke levenssfeer en de zorg voor veiligheid van samenleving en individu niet per definitie en noodzakelijkerwijs tegengestelde belangen zijn. Het zijn echter wel belangen die telkens weer met uiterste zorgvuldigheid tegen elkaar moeten worden afgewogen. In de recente Notitie privacybeleid van het kabinet wordt erkend dat de wetgever de burger dient te beschermen tegen negatieve aspecten van de informatiesamenleving op het punt van de bescherming van de persoonlijke levenssfeer. Er worden ook concrete initiatieven op dit terrein aangekondigd. Een wijziging van de Wet bescherming persoonsgegevens moet leiden tot een verdere informatiebeveiliging en bescherming van persoonsgegevens. Bij de afweging van beide genoemde belangen behoren wettelijke maatregelen, die voorzien dienen te zijn van een transparante toets aan de grondrechten. Bij volgende initiatieven zal steeds wel minimaal moeten worden voorzien in een evaluatiebepaling. Een horizonbepaling noemt de regering echter niet meer dan een optie, en wel voor die gevallen waarin dat gelet op de mate en de aard van inmenging in de grondrechten enerzijds en de te plegen investeringen in ICT anderzijds gerechtvaardigd is. Die opmerking heeft bij mij wel de wenkbrauwen doen fronsen.

De afweging van deze beide belangen lijkt niet zonder meer gerechtvaardigd. De afweging van deze beide belangen vraagt wat ons betreft nog wel om een nadere verduidelijking en argumentatie. Voor ons is het de vraag of het hier nog wel gaat om afweegbare belangen. Men kan wel af willen wegen, maar men kan niet alles tegen elkaar afwegen. Wat bedoelt de regering met de aansporing als het over die horizonbepaling gaat om in dezen terughoudendheid te betrachten?

Het kabinet kondigt ook een nader wetenschappelijk onderzoek aan naar de mogelijkheden om in de Algemene wet bestuursrecht een voorziening op te nemen om toezichtgegevens – waaronder persoonsgegevens – op structurele basis te kunnen uitwisselen tussen toezichthouders, de politie en het OM. Dat daarbij in het bijzonder geheimhoudingsverplichtingen maar ook justitiële onderzoeksbelangen aandacht verdienen, ligt voor de hand. Een vraag voor ons is echter wel om welke toezichthouders het zou moeten gaan. Moet wat dat betreft niet gedifferentieerd worden? Hoe uitgebreid is het veld van toezicht op de burger niet geworden! Hoe wordt doelbinding in dit verband verzekerd en bewaakt? Daarom zouden wij de noodzaak willen onderstrepen om inhoudelijke criteria te formuleren waaronder het recht op bescherming van persoonsgegevens in concreto moet wijken voor het belang van de veiligheid. Onderkent de regering die noodzaak? De heer Franken heeft hierover veel uitgebreider gesproken, maar ik hoop dat ook de regering de noodzaak daarvan onderkent.

Ten slotte nog een opmerking over het zogenaamde recht om vergeten te worden. Thans is krachtens de Wet bescherming persoonsgegevens de verantwoordelijke degene die bepaalt welke gegevens om welke reden voor welke termijn bewaard mogen worden. Bewaartermijnen moeten volgens ons transparanter worden. Onze hoop is gevestigd op de Mededeling van de Europese Commissie van 4 november 2010 die een grotere zeggenschap van de burger over de eigen gegevens aankondigt. Daartoe behoort het verplicht wissen van persoonsgegevens na afloop van een – bekend gemaakte – bewaartermijn of na het intrekken van de toestemming voor verwerking door betrokkene.

Holdijk

Voorzitter. Met deze enkele fragmentarische opmerkingen willen onze fracties graag deze eerste termijn besluiten en zien wij met belangstelling naar een reactie van de regering uit.

□

Mevrouw **Dupuis** (VVD):
Voorzitter. Er is veel gezegd waar mijn fractie het mee eens kan zijn. Toch zal ik proberen namens mijn fractie in grote lijnen het liberaal perspectief weer te geven.

Wij spreken vandaag over een klassiek probleem in een 21ste-eeuwse jas. Het thema is voor liberalen een politiek kernprobleem, en in zekere zin zelfs de oorzaak en aanleiding van het ontstaan van het liberalisme, namelijk de verhouding burger-overheid. Kon het klassiek liberalisme nog volstaan met de formulering van vrijheidsrechten van de burger, vandaag komt er een lastige dimensie bij: de potentiële voordelen en bedreigingen van gebruik van ICT door de overheid met het oog op de privacy van de burger. Klassieke grondrechten, waar wij in het Westen voor gaan, ook niet-liberalen, vragen in het licht van de informatie en communicatietechnologie om een nieuwe bezinning en een nieuwe uitwerking. Mijn fractie doet daaraan graag mee. Daarbij vragen wij aandacht voor de bijzondere positie van de overheid, die enerzijds de privacy van burgers dient te beschermen, maar anderzijds onderdeel is van het probleem: de overheid zelf levert volgens al onze bronnen een niet geringe bedreiging van de privacy op.

Ons uitgangspunt bij dit debat betreft de vraag: is de privacy van de burger bij de Nederlandse overheid in goede handen en dan op twee manieren: beschermt de overheid de burger voldoende, en is de overheid zelf een voldoende betrouwbare speler? Bij de beantwoording van deze vragen hebben we ons gebaseerd op drie verschillende soorten bronnen. 1. Bestaande wetgeving, zoals vanzelfsprekend de Grondwet, artikel 10, de Wet bescherming persoonsgegevens, het EVRM, artikel 8 en de Europese richtlijn nummer 95. 2. De behandeling van en discussies rondom al of niet ingevoerde wetgeving op deelgebieden van de samenleving, zoals het ekd, het epd, en het eld. 3. Een groot aantal rapporten, die door de andere woordvoerders zijn genoemd en die ik kortheidshalve nu niet meer zal noemen.

Bij deze inleiding behoren ten slotte nog twee observaties. De eerste is dat bij de bespreking van de vraag of de privacy van de burger in goede handen is bij onze overheid, twee zaken om te beginnen nodig zijn: kennis van de feiten – hetgeen lang niet altijd simpel is – en de capaciteit tot het maken van morele en politieke afwegingen, hetgeen al even lastig is. Ik verwijs in dit verband graag naar wat de heer Holdijk zojuist gezegd heeft over belangenafweging.

De tweede observatie is dat het hier inderdaad om morele afwegingen gaat, maar dat deze term werkelijk nergens te vinden is in de door mij geziene vele literatuur en gehoorde debatten. Hoe kunnen wij, vraagt mijn fractie, over principiële morele zaken spreken, zoals de privacy van de burger, als wij niet eens inzien dat het hier om morele aangelegenheden gaat? Door dit niet onder ogen te zien missen we ook de kans om ten aanzien van deze morele of ethische kwesties op de geëigende wijze te argumenteren. Dit is natuurlijk een opmerking voor de liefhebbers.

Het eerste antwoord op de vraag of de privacy van de burger in goede handen is bij deze overheid is niet eenduidig. Uiteraard is er wetgeving en is duidelijk dat de overheid, althans sommige afdelingen op sommige departementen, zich bezighoudt met de bescherming van privacy van de burger. In dit verband noem ik allereerst de zeer recente notitie van Justitie over het privacybeleid van deze regering. De notitie gaat in op een aantal zeer relevante thema's en kondigt diverse maatregelen aan. Met veel in deze nota kan de VVD-fractie instemmen, al zou het allemaal nog wel een stuk daadkrachtiger kunnen. Waarom niet meteen een privacy impact analyse vereisen voor alle grootschalige elektronische dossiers van de overheid en van andere instanties? De regering zegt voorts "grootschalige verwerkingen van persoonsgegevens nadrukkelijker dan voorheen het geval is te willen toetsen op effectiviteit". Ja, eindelijk. Dit is wel een stap vooruit, maar het had allang gemoeten, want het heeft echt ontbroken en het ontbreekt nog, bijvoorbeeld bij het ekd, het epd – dat er nu niet meer is – en het eld. Ik kom hier nog op terug.

De nota pleit voorts voor een meldplicht van datalekken, en kondigt aan dat de regering gaat werken aan verdere sanctionering van overtredingen van de Wet bescherming persoonsgegevens en veel meer. Ook wordt gekeken naar de uitwerking van Europese dataprotectieregels en andere zaken. De overheid is, kortom, bezig met de privacybescherming van de burgers, althans, zij uit de intentie daartoe in deze notitie. Nu nog de daden. Er is zeker nog aanvullende wetgeving nodig, zoals alle woordvoerders hiervoor betoogd hebben, opdat de overheid haar beschermende functie optimaal kan invullen.

Dan de tweede kwestie, namelijk de vraag in hoeverre de overheid zelf onderdeel is van het probleem. Wat dit betreft hebben we kunnen zien hoe zonder voldoende onderbouwing qua doelstelling, effectiviteit, en bescherming van zeer persoonlijk gegevens van burgers, een elektronisch kinddossier is opgetuigd, waarbij steeds duidelijker wordt dat je wel kunt proberen veel gegevens te verzamelen, maar dat het bijhouden van de gegevens, het beheer en de interpretatie ervan cruciaal zijn voor de kans van slagen van zo'n project. Het ziet er naar uit dat aan deze laatste punten veel te weinig aandacht is geschonken bij het ekd. Helaas heeft het parlement in de Tweede noch in de Eerste Kamer dit ekd gestopt.

Mevrouw **Slagter-Roukema** (SP):
Voorzitter. Ik heb een vraag aan mevrouw Dupuis. Ik ben het met haar eens dat we tegen het ekd hadden moeten stemmen, maar kan zij analyseren waarom wij toen wel voorgestemd hebben? Ik heb het nog eens nagekeken en ...

Mevrouw **Dupuis** (VVD):
De fractie van de VVD heeft tegengestemd, als enige. Dus ik kan moeilijk analyseren wat uw beweegredenen geweest zijn.

Mevrouw **Slagter-Roukema** (SP):
Excuus, dan heb ik dat over het hoofd gezien. Misschien is het dan nu niet zo relevant als ik vertel waarom wij voorgestemd hebben. In mijn herinnering had het er vooral mee te maken dat het elektronisch kinddossier geplaatst werd in een wetsvoorstel waarin de rest best wel goed was en dat wij heel lang gesproken hebben over de vraag hoe we zo'n belangrijk punt konden onderbrengen

in een wet, waarmee wij als het ware een schaap met vijf poten creëerden.

Mevrouw **Dupuis** (VVD):
Dat is het bekende probleem. Daar hebben we het vaker over gehad. De VVD-fractie was als enige tegen, tot ons grote verdriet.

Wat betekent dit nu? De VVD-fractie dringt er bij de regering alsnog op aan om het ekd te toetsen aan de eisen die de regering zelf stelt in genoemde nota, en aan de eisen van het WRR-rapport. Zoals bekend, is het epd verworpen en ligt het eld nog in deze Kamer voor ter behandeling. Ook dit dient naar de mening van de VVD-fractie te worden getoetst op door de regering zelf genoemde criteria. De vraag is natuurlijk of de regering dit gaat doen. Wij zouden dat absoluut noodzakelijk vinden. Voor dit moment stellen we vast dat de overheid bij al deze drie dossiers naar de mening van de VVD-fractie zich geen adequate behoeder van de privacy van de Nederlandse burger heeft betoond.

Wat is er dan mis? Als wij het goed zien, is de overheid te lichtvaardig en te naïef aan de slag gegaan met genoemde dossiers. Ook was sprake van tunneldenken. Dit gold volgens de vele analyses en commentaren ten minste de volgende punten: de te behalen doelstelling was onvoldoende verkend en geformuleerd, het kwaliteitsbehoud en dus onderhoud van de data was onvoldoende geregeld, de veiligheid en de positie van de burger als controleur van de opslag van zijn eigen gegevens was onvoldoende uitgewerkt en het toezicht en de verantwoordelijkheid daarvoor waren niet transparant. Ook – en dat is ernstig – lijkt de overheid weinig of niets te willen weten van expiratietermijnen en wordt zo "het recht om vergeten te worden" volledig uitgehold. Eigenlijk zeggen alle deskundigen steeds hetzelfde: de doelbinding ontbreekt, er is te weinig aandacht voor dataminimalisatie, de toegang tot en controle van de burger van zijn eigen gegevens is problematisch en over structureel toezicht wordt te weinig nagedacht. Mevrouw Corien Prins van de WRR wijst er op dat een manier van redeneren nodig is, waarbij van een werkelijke afweging van belangen – zie ook de heer Holdijk – van de burger sprake is, veel explicieter dus, en met aandacht voor bovengenoemde aspecten. Dit geldt in de ogen van de VVD-fractie a fortiori voor databestanden waarbij er van de overheid uit sprake is van een verplichting voor burgers om daarin te worden opgenomen.

Wat moet er gebeuren? Er is al veel genoemd, maar de VVD heeft nog een aantal andere zaken. Volgens de VVD fractie is belangrijk dat, zoals de commissie-Brouwer-Korf ook aangeeft, een empowerment plaatsvindt van professionals die betrokken zijn bij de opslag van privégegevens van burgers. Wetgeving alleen is niet voldoende. Het gaat om een alom aanwezig besef bij de vele dienaars van de overheid en bij anderen die bezig zijn met het ontwerpen en gebruiken van grootschalige elektronische datasystemen, dat zij niet de eigenaar zijn van de gegevens van burgers, maar de burgers zelf. Bij aanwezigheid van dit besef zou een uitglijder als het ministerie van VWS maakte in november 2008 niet hebben plaatsgevonden. Toen werd door het departement zelfs contra legem gehandeld, namelijk tegen de WGBO, door alle burgers domweg mee te delen dat er een epd zou komen, waarin 24 uur per dag op alle plaatsen in Nederland ieders medische gegevens toegankelijk zouden worden voor hulpverleners.

Het gaat om awareness, om een attitude die er had moeten zijn en die er toen niet was. Hoe uitgebreid, effectief, en waterdicht wetgeving ook zou worden, altijd dient er het besef te zijn inzake het eigenaarschap van privégegevens van burgers en van respect voor grondwetsartikel 10. Dat is er niet voor niets. Hoe denkt de regering dit besef te vergroten bij ambtenaren?

Concreet zou de VVD-fractie graag zien dat de departementen die werken aan een grootschalige dataopslag zich veel meer zouden blootstellen aan kritiek van buitenaf en niet krampachtig hun eigen vermeende gelijk zouden willen halen. Aan benepen geesten is geen behoefte. Wees open, wees dienstbaar aan de rechten van de burgers en niet aan de inperking daarvan.

De VVD-fractie zou zich ook kunnen voorstellen dat het College bescherming persoonsgegevens meer het karakter krijgt van een ICT-autoriteit. Wat is de mening van de regering hierover?

Ten slotte vraagt de VVD-fractie aandacht voor de aanbevelingen van het WRR-rapport iOverheid. Het is om te beginnen zeer spijtig dat de recente notitie van de overheid die wij bespraken met de aanbevelingen nog niets doet. Ik neem aan dat het woordje "nog" hier op zijn plaats is. Is dat zo, vragen wij de regering? De aanbevelingen zijn samen te vatten onder de formulering: van e-overheid naar iOverheid, een mooie, maar vooral betekenisvolle vondst. De WRR geeft hiermee aan dat de overheid zich veel meer bewust dient te zijn van haar eigen rol als informatieoverheid. Ik citeer graag bladzijde 194 van het WRR-rapport iOverheid: "De paradox van de iOverheid bestaat erin dat de overheid een iOverheid opbouwt waar ze zelf het bestaan niet van afweet. Het ontbreken van een politiek besef 'een iOverheid' te zijn, maakt dat deze in feite geen natuurlijke begrenzing heeft." De VVD-fractie raadt de regering aan om de volgende 40 bladzijden uit dit rapport goed te lezen en uit het hoofd te leren. Het gaat om tal van zeer constructieve aanbevelingen waardoor de beide rollen van de overheid, namelijk beschermer zijn van de privacy enerzijds en een goed functionerend en veilig onderdeel zijn van de informatiewerkelijkheid anderzijds, optimaal kunnen worden ingevuld. Ik hoor hierop gaarne het commentaar van de regering.

□

De heer **Staal** (D66):
Voorzitter. De leden van de D66-fractie zijn vanzelfsprekend geïnteresseerd in de ontwikkelingen en nieuwe mogelijkheden op het gebied van digitale informatieverwerking en communicatie. De fractieleden delen de mening van diverse experts dat het gebruik van informatiesystemen intussen noodzakelijk is geworden voor het functioneren van de overheid. Naast het nut en de noodzaak voor de overheid hebben bedrijfsleven en burgers ook baat bij de door informatietechnologie gefaciliteerde mogelijkheden. Dit neemt echter niet weg dat de potentiële kracht van deze technieken diverse en aanzienlijke risico's met zich brengt. De afgelopen jaren is dit door problemen met verschillende overheidsprojecten duidelijk geworden. Een recent en veelzijdig voorbeeld hiervan is de problematiek rond de ov-chipkaart. Men bleek niet alleen betrekkelijk snel in staat te zijn om de beveiliging te omzeilen, maar ook werd duidelijk dat de privacy van reizigers in het geding was doordat men via de kaart de reiziger als het ware kon volgen.

Staal

De praktijk heeft, naast dit voorbeeld, een rijke collectie aan potentiële risico's met dergelijke systemen tentoongespreid. De risico's beperken zich niet enkel tot systemen of producten van de overheid. Ook als gebruikgemaakt wordt van gelijksoortige systemen, producten of services uit de commerciële sector bestaan deze risico's. Intussen is er een situatie ontstaan waarbij een groeiend aantal multinationals gericht bezig is met het opzoeken van de grenzen van het recht op privacy. Deze bedrijven hebben hun verdienmodel ingericht op het vergaren van informatie die in de privésfeer geplaatst kan worden. Vorige week donderdag kwamen telecomproviders KPN en Vodafone in opspraak door het gebruik van deep packet inspection, waarbij de communicatie tussen een mobiele telefoon en het internet tot in detail door een derde, buitenlandse, partij geanalyseerd werd. In de tussentijd is gebleken dat de situatie mogelijk minder ernstig is dan aanvankelijk gedacht werd. Het College bescherming persoonsgegevens gaat desalniettemin onderzoek doen naar de betrokken bedrijven.

De leden van onze fractie achten deze ontwikkelingen zorgwekkend. Bovendien is het gebruikers vaak niet bekend is dat dit soort technieken toegepast wordt, terwijl het gebruik ervan mogelijk een aanzienlijke inbreuk maakt op de privacy van de eindgebruiker. Het is een duidelijk voorbeeld van de noodzaak om dit debat niet te beperken tot de wijze waarop de overheid met eigen informatiestromen omgaat, maar ook van gedachten te wisselen over de rol van de overheid in de informatiesamenleving. De adviezen van commissie-Brouwer-Korf geven een aantal goede aanknopingspunten voor privacybewust handelen door overheid. Het principe select before you collect is bijvoorbeeld bij een nieuw ICT-project een goed uitgangspunt. De adviezen zijn echter voornamelijk gericht op stroomlijning van het overheidshandelen binnen projecten. De fractie van D66 merkt op dat het bij dit debat ook moet gaan over de grote lijnen. Welke visie heeft de regering op de huidige informatiemaatschappij? Het recente nieuws uit de telecomsector is een voorbeeld van de noodzaak om een visie op de in dit opzicht veranderende samenleving te ontwikkelen. Hoewel de nadruk van het debat voornamelijk bij de verwerking en uitwisseling van informatie door de overheid zelf zal liggen, heeft de overheid volgens onze fractie ook een systeemverantwoordelijkheid. Hier kom ik later op terug.

Ten tijde van de expertmeeting in februari was het onderzoek van de Wetenschappelijke Raad voor het Regeringsbeleid helaas nog niet beschikbaar. Intussen is dit wel het geval. Het onderzoek is op een aantal punten kritisch en roept belangrijke vragen op. Het meest fundamentele punt van het rapport is het signaleren van een gebrek aan bewustzijn bij de overheid als het gaat om de fundamentele verandering van de maatschappij en zichzelf. De maatschappij is volgens het rapport de afgelopen jaren geïnformatiseerd. Naast dat gebrek aan bewustzijn constateert de raad dat informatietechnologie voornamelijk wordt gezien als een middel om beleidsdoelen te bereiken, terwijl deze technologie in korte tijd meer is geworden dan slechts een middel. Intussen beheerst het in aanzienlijke mate het karakter, de mogelijkheden en de kwetsbaarheden van de overheid. Het enthousiasme waarmee informatietechnologie door beleidsmakers gebruikt wordt, heeft geleid tot een wirwar van systemen, producten en services, waarbij the big picture uit het oog verloren is. De fractie van D66 vindt dat deze twee elementen centraal moeten staan in het debat over de relatie tussen de overheid en informatieverwerking en de toekomst daarvan.

In het rapport wordt geconcludeerd dat de huidige situatie mede is ontstaan door een ongefundeerd vertrouwen in de ICT als probleemoplosser. Door gebrek aan besef een informatieoverheid te zijn, ontstaat wildgroei. De afwezigheid van een institutioneel kader dat verantwoordelijkheid draagt voor alle informatietechnische innovaties bij de overheid, is de oorzaak daarvan. Tijdens de expertmeeting is het concept van een nieuwe toezichthouder, autoriteit of chief information officer ter sprake gekomen. De leden van de fractie van D66 zijn van mening dat enkel een nieuwe externe toezichthouder weinig toegevoegde waarde heeft. De fractie deelt de mening van de raad dat het in de eerste plaats noodzakelijk is om het besef te creëren een informatieoverheid te zijn. Het is van belang dat nieuwe systemen, producten en services met dit in gedachten ontworpen worden. Een institutioneel kader zou daar in belangrijke mate aan kunnen bijdragen. Het zou de verantwoording kunnen dragen voor de privacy impact assessments. Het is echter van belang dat het nieuwe kader ook over algemene bevoegdheden zoals advies, coördinatie en evaluatie beschikt.

Het feit dat informatiesystemen de grenzen van beleidsterreinen overschrijden, geeft al blijk van de noodzaak tot centrale coördinatie. De leden van mijn fractie denken dat een aanzienlijk deel van de problemen, die de in de aanloop naar dit debat besproken zijn, gebaat zou zijn bij een gecentraliseerd kader voor informatieverwerking. Tijdens de expertmeeting is een aantal modaliteiten besproken, waaronder de mogelijkheid van een CIO binnen een departement of een externe toezichthouder die mogelijk naast het CBP zou komen te staan. De wijze waarop is vooralsnog van ondergeschikt belang. Wanneer de overheid de transformatie naar een zelfbewuste informatieoverheid heeft gemaakt, zullen bepaalde elementen, zoals privacy by design, vanzelfsprekend zijn. De leden van de fractie van D66 zijn van mening dat twee elementen van bijzonder belang zijn bij het realiseren van dit institutionele kader. Ten eerste is het essentieel dat er oog is voor het beleidsterreinoverschrijdende en mogelijk interdepartementale karakter van projecten. Daarnaast deelt de fractie de mening van het Rathenau Instituut dat voor advisering en evaluatie van informatiesystemen gegronde kennis van informatietechnologie noodzakelijk is. Het institutionele kader dient dan ook te beschikken over deze capaciteiten.

Als het kader op centrale wijze wordt ingericht, levert dat een aantal voordelen op. Ten eerste zal bij centrale evaluatie van informatiesystemen een probleem als function creep zich in mindere mate manifesteren doordat de werking van alle informatiestromen en systemen op centraal niveau inzichtelijk worden gemaakt. Het is op die manier eenvoudiger om een systeem te toetsen aan bijvoorbeeld doelbinding. Daarnaast kan bijvoorbeeld geadviseerd worden over de kwaliteit van gegevens bij de intentie om gekoppelde data te gebruiken voor een bepaald beleidsdoel. Ten derde wordt de door de experts geschetste complexiteitsspiraal doorbroken door een institutioneel kader dat begrip heeft van ICT en de doelen van een project. Derhalve kan een dergelijk instituut een betere inschatting maken van de benodigde functionaliteit en deze met het oog op function creep verder te begrenzen. Verder wordt, door het instellen van dit kader, een eerste stap gemaakt in het erkenningsproces van de informatisering van de overheid. Bovendien maakt een

dergelijke aanpak het mogelijk om ook andere valkuilen die samenhangen met het ICT-gebruik door de overheid in kaart te brengen. Het maakt het bijvoorbeeld eenvoudiger om het geheugen van de overheidsinformatie te beheren als een instituut inzicht heeft in alle systemen. Deelt de regering de overtuiging dat een dergelijk instituut noodzakelijk is voor de transformatie naar een overheid die zich bewust is van de nadruk die op informatiestromen is komen te liggen? Hoe kijkt de regering aan tegen het verschil tussen het realiseren van oplossingen op projectbasis versus oplossingen op een structurele manier? Kan de regering zich verenigen met een nieuw institutioneel kader of is zij van mening dat de eerder genoemde zaken ook voldoende gewaarborgd zijn door het versterken van het bestaande kader? Daarnaast vragen de leden van mijn fractie zich af of de overheid de bestaande realiteit voldoende meeweegt bij de ontwikkeling van nieuwe en het beheer van oude informatiesystemen?

De leden van de D66-fractie hebben bovendien een vraag over de schaal van systemen. Tijdens het debat over het elektronisch patiëntendossier is de schaal van het systeem uitvoerig ter discussie gesteld. Enerzijds geldt: hoe grootschaliger een systeem des te groter ook de daaruit voortvloeiende risico's op het gebied van beveiliging en privacy. Anderzijds leiden veel kleine systemen tot problemen van beheersbaarheid en controle. Kan de minister aangeven hoe de regering deze afweging maakt? Tot slot op dit punt vragen de leden van de fractie van D66 of en, zo ja, hoe gevolg wordt gegeven aan de aanbevelingen uit het rapport van de WRR?

De leden van mijn fractie erkennen de noodzaak van privacy impact assessments. Tijdens de expertmeeting gaf de heer Kohnstamm van het College bescherming persoonsgegevens aan dat bij de ontwikkeling van een standaardmodel voor deze assessments de werkgeversorganisaties de onderhandelingen hebben verlaten. Kan de minister aangeven wat de huidige status is van de ontwikkeling van deze model assessments? Kan de regering voorts ingaan op de vraag of deze modellen al toepassing vinden in de praktijk en, zo ja, hoe en in welke fase van het ontwerp van nieuwe systemen producten of diensten deze worden toegepast?

De leden van de D66-fractie delen de mening van de WRR dat de samenleving net als de overheid aan het informatiseren is. Het grote verschil tussen de ontwikkelingen bij de overheid en de rest van de samenleving is de snelheid waarmee dit gebeurt. De fractieleden hechten veel waarde aan waarborging van de privacy in de samenleving. Uit het rapport "Niets te verbergen, maar toch bang" van het CPB komt naar voren dat burgers na zich te hebben geïnformeerd over privacyrisico's het gedrag ten aanzien hiervan aanpassen. De leden van de fractie van D66 vernemen graag van de regering op welke wijze de overheid van plan is om de burger verder te beschermen tegen de informatiehonger van bedrijven zoals Google, Microsoft en Facebook. Mijn fractie is van mening dat mede gezien het internationale karakter van de problematiek, de meest voor de hand liggende oplossing van het vraagstuk is: het vergroten van het besef van de burger ten aanzien van de privacyproblematiek. Deelt de regering deze opvatting? Zo ja, heeft zij concrete plannen om hier een actievere rol in te spelen dan tot nu toe het geval was? De WRR spreekt in haar rapport over het belang van het recht op het wissen of "vergeten" van informatie. Kan de regering dit vanuit internationaal perspectief toelichten?

Tot slot signaleert de D66-fractie een nieuwe ontwikkeling op het gebied van dataverwerking: cloud computing. Het betreft een nieuw gebruik van de computer waarbij vrijwel alle data van een gebruiker naar de zogenaamde "cloud", dat wil zeggen het internet, verplaatst wordt. Hoe kijkt de regering vanuit het oogpunt van privacy tegen deze nieuwe ontwikkeling aan?

Wij zien de antwoorden van de regering met belangstelling tegemoet.

□

Mevrouw **Strik** (GroenLinks):
Voorzitter. Gedurende de afgelopen vijftien jaar lijkt onze bezorgdheid over de privacy te zijn omgeslagen in onbekommerdheid. In datzelfde tempo is de inbreuk erop verder toegenomen. Sindsdien heeft de overheid op Europees en nationaal niveau een scala aan bevoegdheden vergaard om persoonsgegevens op te eisen en uit te wisselen. Vooral de aanslagen van september 2001 hebben een onstilbare informatiehonger bij de regeringen teweeg gebracht. Daarom zijn onze telefoon- en internetgegevens en onze banktransacties opvraagbaar voor justitie. Zelf zijn we te traceren via onze mobiele telefoon. Als we willen vliegen, moeten we voor lief nemen dat de overheid ons lichaam scant en de luchtvaartmaatschappij onze persoonsgegevens overdraagt aan de autoriteiten van het land van bestemming. Om de dader niet te missen, volgt de overheid iedereen. En zo zijn we geruisloos allemaal in het verdachtenbankje terechtgekomen.

Niets meer voor jezelf kunnen houden, is een vorm van vrijheidsverlies. Dreigt juist dat opdringerige veiligheidsbeleid ons niet te verstikken? Waar beginnen veiligheid en vrijheid onbehaaglijk te schuren? Waar ligt de grens tussen een betere dienstverlening en bescherming van onze persoonsgegevens? Burgers willen zelf die grens bepalen. De overheid moet haar bevoegdheden aanwenden om ons daartoe in staat te stellen. Dat vergt een ingrijpende koerswijziging. Op dit moment kunnen burgers zich niet tot één verantwoordelijke wenden, want de potentiële schenders vertegenwoordigen alle aspecten van de overheid, de samenleving en het bedrijfsleven. Zijn ze aan te spreken op hun handelen door burgers? Er zijn veel dwarsverbanden en uitruilen, maar is er ook een regisseur? Om burgers greep op hun eigen data terug te geven, zal de overheid en dus ook de politiek de regie moeten gaan nemen om ons grondwettelijk recht op bescherming van onze persoonsgegevens te waarborgen. Dat vergt regie op normering, transparantie, voorlichting, toezicht en handhaving.

Het is nog niet zo gemakkelijk om die regie zodanig te voeren, dat de daaraan ten grondslag liggende normering klip-en-klaar is voor iedereen. Praktisch altijd wordt wetgeving gemaakt op basis van een afweging van belangen. Het belang van de Staat bij de bescherming van de openbare orde of het belang van de burger bij zijn veiligheid hebben een bepaald gewicht, net zoals het belang bij het zelfbeschikkingsrecht over de eigen gegevens of bij rechtsbescherming. Het is echter allang niet meer zwartwit veiligheid versus privacy. Efficiency speelt een rol bij de dienstverlening, in de gezondheidszorg en in het bedrijfsleven. Ook daar zijn onze gegevens geliefd om het consumentengedrag te doorgronden en het aanbod van de producten nog passender te maken. Het belang van het bedrijfsleven dus. De gegevens die bedrijven verzamelen, komen allemaal weer beschikbaar voor de opspo-

ring, kortom voor de veiligheid. De heer Franken heeft de normen die wat ons betreft bij de toets van ontwerpwetgeving als uitgangspunt moeten dienen, die voortvloeiden uit onze expertmeeting van 2008, zojuist opgesomd. Wij steunen dan ook graag de motie die hij vanavond zal indienen.

Een toets voorafgaande aan een wetgevingsvoorstel, aan noodzaak, effectiviteit en hanteerbaarheid, en proportionaliteit, is alleen mogelijk als we inzicht hebben in het effect van ontwerpwetgeving op onze privacy. Een privacy impact assessment is dus een conditio sine qua non voor een zorgvuldige afweging tussen het belang van de bevoegdheden, gegevens en het belang van burgers bij de bescherming van persoonsgegevens. Waarom kiest de regering ervoor om nu eerst onderzoek te doen naar de mogelijkheid van het gebruik van privacy impact assessments? Ook de regering zelf zou die gegevens op tafel moeten willen hebben alvorens een afweging te maken. Een assessment maakt het ook mogelijk dat onbedoelde effecten tijdig boven water komen, zodat ontwerpwetgeving daarop kan worden aangepast. De regering noemt het kostenaspect in relatie tot het niet verplicht stellen, maar voor een PIA bij wetgeving is alleen de overheid verantwoordelijk. Een verwijzing naar het arme midden- en kleinbedrijf is dan niet op zijn plaats. Heeft de regering eraan gedacht dat een PIA ook bijzonder kostenbesparend kan werken? Wetgeving kan nog tijdig worden aangepast in plaats van aan het eind van een traject. De vele miljoenen die verloren zijn gegaan met het voorbereidingstraject van het elektronisch patiëntendossier hadden wellicht kunnen worden bespaard als alle effecten meteen op tafel hadden gelegen. Een PIA is ook een goede gelegenheid voor een onderbouwde reactie op adviezen van officiële adviesorganen. Momenteel zien we te vaak dat ook zeer kritische commentaren van de EDPS of het CBP zonder veel argumenten in de wind worden geslagen. Dat past niet in een democratische rechtsstaat.

De regering zegt wel toe om de voorgenomen maatregelen nadrukkelijker te gaan toetsen aan effectiviteit en transparantie. Betekent dit ook dat wij dit herkenbaar en toetsbaar zullen terugzien in de ontwerpwetgeving? Voor medewetgevers is het van belang om dezelfde toets te kunnen doen als de regering. Ook het voornemen tot een evaluatie of horizonbepalingen gaat in de goede richting. Waarom heeft de regering het in dit verband over "of-of"? Is het niet logischer om de horizonbepaling vergezeld te laten gaan van een evaluatie op een bepaald tijdstip ruim voorafgaand aan het aflopen van de horizonbepaling? Het gaat om de stok achter de deur voor een zorgvuldig tegen het licht houden van nut en noodzaak, maar ook om een waarborg dat ondeugdelijke wetgeving niet automatisch doorloopt. Ik hoor hierop graag een reactie van de regering.

Wat is de wenselijke normering? De WRR heeft de kern te pakken met de conclusie dat het gaat om regie op informatiestromen, niet alleen op applicaties. Wat willen we weten als overheid en waarom? Welke informatie willen we koppelen en met welk beleidsdoel of politiek doel? Alleen vanuit die inhoudelijke uitgangspunten is het mogelijk om selectief te zijn. Daarom zal de regering zich bij een wetsvoorstel eerst moeten afvragen of de inbreuk op de privacy noodzakelijk is. Verkeren we in problemen omdat we een bepaalde wettelijke bevoegdheid nog niet hebben? Onderbouw dat dan met feiten en laat zien wat wordt opgelost met extra bevoegdheden en data.

Dat vraagt om een kritisch blik van iedereen: departementen, politiek en uitvoerders. De neiging naar meer en meer mogelijkheden is groot, omdat we dat verwarren met daadkracht, maar het kan zich evengoed tegen ons keren. Het onderzoek "doelwit Europa" naar aanslagen of half gelukte aanslagen laat zien dat de politie de meeste plegers al in het vizier had, gewoon via het ambachtelijke opsporingswerk. Het gevaar van een onbeperkte hoeveelheid gegevens beschikbaar stellen, is dat nog meer data en bevoegdheden juist het ambacht verzwakken en er nog meer langs elkaar heen wordt gewerkt. We creëren heel veel hooibergen waarin de politie mag gaan zoeken.

Hetzelfde zien we gebeuren bij het elektronisch kinddossier. Er zijn nu zo immens veel als risicokinderen getypeerde kinderen opgenomen in de databanken, dat gerichte hulpverlening onmogelijk wordt of preventiemaatregelen ondoenlijk te nemen zijn. De profilering is te grof, waardoor we ons doel voorbij schieten. Bovendien leidt het tot stigmatisering en onrechtvaardige uitsluitingen, bijvoorbeeld als iemand te boek komt te staan als wanbetaler omdat hij een bepaalde postcode hebt en ergens één keer een rekening te lang open heeft laten staan.

Hetzelfde gebeurt als data voor te veel verschillende doelen worden gebruikt. Zo is het Schengen Informatie Systeem gestart om de grenscontroles effectiever te. maken. Nu mogen opsporingsdiensten ook voor strafrechtelijke doeleinden gebruikmaken van de databanken. Dat betekent dat migranten vaker voorkomen in databanken waar politie en justitie vrij over kunnen beschikken. Het valt te bezien of dit gebruik niet indruist tegen de uitgangspunten die het EHRM heeft neergelegd in de Marperzaak, omdat het onschuldige migranten kan stigmatiseren. Met profilering is het gevaar voor stigmatisering nog nadrukkelijker aanwezig. Het Hof heeft in deze zaak nadrukkelijk op de grote verantwoordelijkheid voor overheden gewezen bij het gebruik van nieuwe technologieën. Zij dienen de juiste balans te vinden. Opspoorders in de voorhoede dienen tevens privacybeschermers in de voorhoede te zijn.

Tot zover mijn vragen en opmerkingen over de wenselijke normering, maar wat is de feitelijke normering? Wij zien dat de techniek uiteindelijk nog steeds de norm is; een groot contrast met de wijze waarop dit kabinet bijvoorbeeld met gentechnologie omgaat, zeker als het gaat om menselijke cellen. Dan is het van belang, eerst een ethische discussie te voeren en op basis daarvan grenzen te stellen. Zo niet bij privacy: elke nieuwe mogelijkheid die een nieuwe techniek biedt, zullen we uiteraard toepassen. Zonde om niet te gebruiken! De "waaromvraag" sneuvelt te vaak onder dit enthousiasme. Tegelijkertijd weten we inmiddels dat de privacy vooral afhangt van de wijze waarop mensen met die techniek omgaan. Aan wie verstrek je het mandaat om in een databestand te kijken? Maakt iemand fouten bij de invoering? Vallen de gegevens in verkeerde handen? De menselijke factor is een zwakke schakel en die kunnen we beter wantrouwen.

We moeten ons tegen onszelf beschermen, zo beschouw ik het uitgangspunt select before you collect. Eerst weten wat je waarom nodig hebt en dan de wetgeving en de toepasselijke technieken zo ontwerpen, dat er ook geen andere informatie wordt opgeslagen of bewaard. Dit is het zogenaamde zero knowledge-uitgangspunt. Je moet wel eerst een cursus Engels volgen voordat je je het privacydebat eigen kunt maken. Dat alles betekent een zorgvuldige afbakening al in het stadium van het ontwerp van de wetgeving. Dat verkleint tevens de kans

dat gegevens voor een ander doel worden gebruikt en wat ons betreft is dat winst, want een ander doel verdient een nieuw debat in de Staten-Generaal; een doordachte, welbewuste keuze. Bovendien kan gebruik van gegevens voor een ander doel dan de wet oorspronkelijk in voorzag, alleen met instemming van de persoon zelf. Dat is iets anders dan een wet ergens publiceren en er dan van uitgaan dat iedereen op de hoogte is gebracht. Bovendien moet er een gegronde reden voor zijn. Deze twee criteria betekenen per definitie dat datamining uit den boze is.

Toch blijkt in de praktijk keer op keer dat datamining en profilering worden toegepast, evenals het zogenaamde function creep, het gebruik van gegevens voor een ander doel. Hier worden burgers ongemakkelijk van. Je hebt geen greep op je gegevens, je weet zelfs niet in wiens handen ze zijn en waarom. Graag hoor ik klip-en-klaar van de regering welke grenzen zij stelt ten aanzien van het omgaan met bulkgegevens, bijvoorbeeld in een databank, los van het doel waarvoor ze zijn opgeslagen. En welke waarborgen biedt de regering om deze grenzen te bewaken? De regering illustreert meteen ook zelf hoe lastig het is om selectiviteit te betrachten. Wegens doorslaand succes zou de automatische nummerplaatherkenning (ANPR) moeten leiden tot nieuwe wetgeving om kentekens voor meerdere doelen te kunnen gebruiken. Kan de regering aan de hand van dit voorbeeld nu eens uitleggen waarom het geoorloofd is om kentekens op grote schaal te gebruiken voor het volgen van bestuurders met een geheel ander doel dan waarvoor de nummerplaatherkenning ooit bedoeld was? En kan ze daarbij een vergelijking trekken met de beslissing om niet verder te gaan met proeven voor de kilometerheffing, omdat dit de privacy te veel zou aantasten? Die maatregel zou zorgen voor 15% minder auto's op de weg en volgens de toenmalige regering, maar ook het Rathenau Instituut, was de privacy bijzonder goed gewaarborgd. In de woorden van de toenmalige minister Eurlings: "U zou banger moeten zijn voor uw gsm dan voor het kastje in uw auto."

Soms gloort er een begin van inzicht dat we niet op de weg van eindeloos vergaren van data verder moeten. Een centrale databank voor de vingerafdrukken komt er voorlopig niet. Graag hoor ik van de regering hoe dit debat verder verloopt en wat er gebeurt met onze biometrische gegevens die inmiddels al zijn afgenomen. Zijn die gegevens veilig? Worden ze vernietigd? Dat laatste lijkt mij de meest logische weg. Graag informatie daarover.

Een zwaluw maakt nog geen zomer. Ook dit kabinet lijkt weer te barsten van energie om data van ons te verkrijgen en te gebruiken voor zijn politieke ambities. De regering wil bijvoorbeeld instanties verplichten om data te delen als het noodzakelijk is voor de veiligheid. Dit is dus een plicht voor professionals om te breken met het doelbindingsprincipe. We hebben met name de afgelopen jaren gezien hoe subjectief het begrip "veiligheid" is. Dus hoe ziet de regering dit voor zich? Wie mag bepalen of het nodig is? Het zijn die instanties zelf die deze afweging moeten maken.

In het kader van zelfbescherming en uniformiteit juicht onze fractie dan ook het idee van de helpdesk toe, waarbij professionals worden geadviseerd over hun omgang met data. De vraag is wel onder wie die helpdesk zou moeten fungeren. Wat ons betreft, wordt een dergelijke helpdesk breed ingericht, ook voor burgers en het bedrijfsleven. Zo kan er een centraal expertisecentrum ontstaan met een eenduidige advisering, wie de hulpvrager ook is. Als we burgers weer meer greep op hun gegevens willen geven, zullen we moeten beginnen met meer transparantie en overzicht moeten scheppen. Dat betekent een herkenbare plek met functionarissen die vragen beantwoorden en adviseren, maar tegelijkertijd de doorzettingsmacht hebben om gegevens te corrigeren of verwijderen, ten aanzien van alle departementen en uitvoeringsinstanties. Hoe kijkt de regering hier tegenaan? Wat ons betreft, zou de commissie die de WRR voorstelt om jaarlijks de ontwikkelingen in de informatiestromen tegen het licht te houden en de Kamer en de regering daarover te adviseren, ook aan dit expertisecentrum gekoppeld kunnen worden. Dan zou een goede basis kunnen vormen voor haar bevindingen. Vanuit het burgerperspectief is de transparantie nog ver onder de maat. Naast een dergelijk expertisecentrum zou de wettelijke informatieplicht moeten worden versterkt en ook de mogelijkheden voor recht op inzage, bezwaar of klachten moeten worden versterkt.

Dan het toezicht. Burgers krijgen hun regie echter niet terug met een helpdesk en een aansprakelijke met doorzettingsmacht. De overheid dient daarvoor zelf uit de mist te treden: laten zien wat ze weet van ons en wat ze daarmee doet. Het begint dus met inzage te krijgen in de registratie door de overheid en het gebruik van de gegevens. Zoals ik al bij aanvang zei: de overheidsregie moet zich ook uitstrekken over de private sector. Bepaal doelstellingen en randvoorwaarden en organiseer toezicht. De regering stelt voor om het externe toezicht te verstevigen, maar wel meer achteraf in te zetten. Het interne toezicht bij bedrijven zou versterkt worden door middel van privacyofficieren. Het aantrekkelijke hiervan is dat wellicht het bewustzijn en de verantwoordelijkheid van bedrijven zelf hierdoor worden vergroot. De normen worden van binnenuit opgebouwd, maar hoe voorkomen we het risico dat het beperkt blijft tot zo'n privacyofficier? En dient die officier niet ook de belangen van het bedrijf daar tegenover af te wegen?

De bedrijven zouden zelf belang moeten krijgen bij een zorgvuldig gebruik van gegevens van hun klanten. Dat hebben wij gezien bij het bedrijf TomTom. Toen burgers ervan op de hoogte kwamen dat hun gegevens aan justitie werden verstrekt om snelheidsovertredingen te kunnen vaststellen, realiseerde de eigenaar van TomTom zich dat het bedrijf voorzichtiger moest zijn met het uitwisselen van gegevens. Als de overheid meer voorlichting geeft aan burgers over de wijze waarop het bedrijfsleven omgaat met data, kan de interne druk om zorgvuldigheid te betrachten worden vergroot. Een doelmatig toezicht zit niet alleen in hoge boetes, maar onze fractie acht het wel van groot belang dat het CBP die boetes kan uitdelen. De leeuw moet inderdaad een beetje eng worden.

De overheid zou erop moeten toezien, bij zichzelf en het bedrijfsleven, dat de technologie vooral benut wordt om ons te beschermen tegen ongewenst gebruik van onze gegevens. Meer privacy by design dus en daar mag een financieel belang nooit iets aan afdoen. Regie door de overheid betekent ook regie over de rol van toezichthouders. Het antwoord van de regering op de vraag over de rol van het CBP is tot nu toe nogal ontwijkend. Wij ondersteunen een versterkende rol van wetgevingsadvies en toezicht op de naleving van die wetten. De advisering van bedrijven en uitvoerende instanties zien wij liever in een andere hand, wat het CBP vrijheid geeft in zijn toezichthoudende taak. Wellicht dat het CBP bij het kwijtraken van deze taak wel voldoende capaciteit krijgt. Dat zou zeer nauwgezet moeten worden uitgezocht.

Strik

Ten slotte: het wordt steeds duidelijker dat niemand meer het overzicht heeft. En de overheid zou het wel moeten willen hebben om enigszins grip te houden en sturing te geven. Wij als volksvertegenwoordigers dienen het burgerrecht serieus te nemen en een gevoel van urgentie te ontwikkelen ten aanzien van de onmacht die veel burgers voelen bij de technologische ontwikkelingen. Privacy gaat om veel meer dan om het kunnen afschermen van je persoonsgegevens. Het heeft met vrijheid te maken, waardigheid, autonomie, maar ook de democratische rechtsstaat. De door de WRR voorgestelde commissie die jaarlijks rapporteert over die ontwikkelingen en ons aanspreekt op onze verantwoordelijkheid, zou dat gevoel van urgentie kunnen versterken. Maar uiteindelijk draait het om de politieke wil. Ik ben blij met het gevoel van urgentie dat ik vanochtend heb gehoord. Laten we onze wetgevingstoets gewetensvol verrichten en geen genoegen nemen met vage wettelijke criteria, controle houden op normering die in lagere regelgeving wordt neergelegd, Europese ontwerpwetgeving becommentariëren en implementatiewetgeving kritisch toetsen op de strikte noodzaak. Als we consistent zijn, zal de regering gedwongen zijn om onze uitgangspunten al bij aanvang van het wetgevingsproces ernstig te nemen.

De beraadslaging wordt geschorst.

De vergadering wordt van 12.40 uur tot 13.45 uur geschorst.

De **voorzitter**:
De ingekomen stukken staan op een lijst die in de zaal ter inzage ligt. Op die lijst heb ik voorstellen gedaan over de wijze van behandeling. Als aan het einde van de vergadering daartegen geen bezwaren zijn ingekomen, neem ik aan dat de Kamer zich met de voorstellen heeft verenigd.

(Deze lijst is, met de lijst van besluiten, opgenomen aan het einde van deze editie.)