Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2009–2010

31 051 Evaluatie Wet bescherming persoonsgegevens

A

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 1 juni 2010

Bij brief van 3 november 2009 heeft de minister van Justitie samen met de minister van Binnenlandse Zaken en Koninkrijksrelaties en mede namens de staatssecretaris van Economische Zaken, het kabinetsstandpunt aangeboden ten aanzien van de bevindingen van de Adviescommissie Veiligheid en persoonlijke levenssfeer (commissie Brouwer-Korf), alsmede de evaluatierapporten van de Wet bescherming persoonsgegevens (Wbp) (TK 31 051, nr. 5). De vaste commissies voor Justitie[1] en voor Binnenlandse Zaken en de Hoge Colleges van Staat/Algemene Zaken en Huis der Koningin[2] hebben in hun vergadering van 2 februari 2010 over dit kabinetsstandpunt gesproken. De leden van diverse fracties hebben daarop inbreng geleverd voor vragen aan de regering.
Deze zijn opgenomen in de brief aan de minister van Justitie en de minister van Binnenlandse Zaken en Koninkrijksrelaties van 19 februari 2010.
De minister van Justitie, minister van Binnenlandse Zaken en Koninkrijksrelaties heeft op 27 mei 2010 gereageerd.

De commissies brengen bijgaand verslag uit van het gevoerde schriftelijk overleg.

De griffier van de vaste commissie voor Justitie,
Kim van Dooren

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

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

kst-31051-A
ISSN 0921 - 7371
's-Gravenhage 2010

BRIEF AAN DE MINISTER VAN JUSTITIE

Den Haag, 19 februari 2010

Bij brief van 3 november 2009 hebt u samen met uw collega van Binnenlandse Zaken en Koninkrijksrelaties en mede namens de Staatssecretaris van Economische Zaken, het kabinetsstandpunt aangeboden ten aanzien van de bevindingen van de Adviescommissie Veiligheid en persoonlijke levenssfeer (commissie Brouwer-Korf), alsmede de evaluatierapporten van de Wet bescherming persoonsgegevens (Wbp) (TK 31 051, nr. 5). De vaste commissies voor Justitie en voor Binnenlandse Zaken en de Hoge Colleges van Staat/Algemene Zaken en Huis der Koningin hebben in hun vergadering van 2 februari 2010 over dit kabinetsstandpunt gesproken. De leden van diverse fracties hebben daarop inbreng geleverd voor vragen aan de regering. Deze vragen treft u in de bijlage[1] bij deze brief aan. Bij het groeperen van de vragen is zoveel mogelijk de opbouw van het kabinetsstandpunt gevolgd.

De leden van de vaste commissies voor Justitie en voor Binnenlandse Zaken en de Hoge Colleges van Staat/Algemene Zaken en Huis der Koningin zien de reactie van het kabinet met belangstelling tegemoet.

Een gelijkluidende brief is verzonden aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties.

De Voorzitter van de vaste commissie voor Justitie,
R. H. van de Beeten

De Voorzitter van de vaste commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat/Algemene Zaken en Huis der Koningin,
L. M. L. H. A. Hermans

[1] Ter inzage gelegd op de afdeling Inhoudelijke ondersteuning onder griffie nr. 145922u.

Bijlage

Reactie op kabinetsstandpunt commissie Brouwer-Korf en evaluatie Wet bescherming persoonsgegevens

1. Inleiding

De leden van de fractie van het CDA hebben met veel instemming kennisgenomen van de instelling door de regering van de commissie Brouwer-Korf die haar diende te adviseren over het zoeken naar de balans tussen veiligheid en de bescherming van de persoonlijke levenssfeer. Ook het op 3 november 2009verschenen kabinetsstandpunt ten aanzien van enerzijds de bevindingen van deze commissie en anderzijds ten aanzien van de evaluatierapporten van de Wet bescherming persoonsgegevens is door deze leden met belangstelling gelezen. De leden van de CDA-fractie beschouwen deze stukken in samenhang met het in april 2007 verschenen rapport «Data voor daadkracht» en het verslag van de expertbijeenkomst over gegevensbescherming die de Eerste Kamer heeft gehouden op 20 maart 2008 (EK 31 200 VI, F). De CDA-fractie heeft voordien al tijdens de behandeling van de begroting van het Ministerie van Justitie van *2006*de aandacht van de regering gevraagd voor het verstoord raken van de balans tussen veiligheid en de bescherming van de persoonlijke levenssfeer en dit is zeer nadrukkelijk gedaan tijdens de Algemene Politieke Beschouwingen van 2008. In het antwoord van de regering is toen gezegd, dat er naar aanleiding van het rapport van de commissie Brouwer-Korf een regeringsstandpunt zou volgen, waarin expliciet op deze problematiek zou worden ingegaan. De leden van de fractie van het CDA hechten er daarom aan het debat nu voort te zetten, aangezien zij het van groot belang achten, dat de regering met een verantwoorde aanpak komt met betrekking tot deze problematiek. Daarbij geldt dat het garanderen van de veiligheid van de burgers evenals het waarborgen van de bescherming van de persoonlijke levenssfeer behoren tot de kerntaken van de overheid.
De leden van de CDA-fractie zullen bij dit overleg met name een aantal vragen stellen met betrekking tot de plannen van de regering om de voorstellen van de commissie BrouwerKorf en de resultaten van de wetsevaluatle, alsmede van de expertmeeting van deze Kamer van 20 maart 2008 In concrete beleidsmaatregelen te implementeren.

De leden van de fractie van de **VVD** hebben kennisgenomen van het kabinetsstandpunt met betrekking tot het advies van de commissie Brouwer-Korf en de evaluatie van de Wet bescherming persoonsgegevens. Zij hebben enkele vragen. Op 16 februari 2009 kondigde de Minister van Justitie aan dat hij in het voorjaar van 2009 een inhoudelijke reactie zou sturen op de evaluatierapporten van de commissie Brouwer-Korf. Die inhoudelijke reactie is pas op 3 november 2009 naar de Tweede Kamer gestuurd. Waardoor is de vertraging van meer dan een half jaar veroorzaakt? Opvallend vinden de leden van de fractie van de VVD dat het kabinet op verschillende punten zijn heil ziet in wetgeving: is nieuwe wetgeving nu inderdaad de aangewezen weg?

De leden van de **PvdA**-fractie hebben met belangstelling kennis genomen van het kabinetsstandpunt over het advies van de commissie Brouwer-Korf en de evaluatierapporten betreffende de Wet bescherming persoonsgegevens. Deze leden hadden vragen en kanttekeningen bij het kabinetsstandpunt.

Het kabinetstandpunt is als volgt opgebouwd:

Samenvatting aan de hand van 4 kernthema's (ruim 2 bladzijden)
1. Inleiding

2. Een nieuwe benadering van persoonsgegevens (aan de hand van de 4 kernthema's in ruim 2 bladzijden)
3. Veiligheid en persoonsgegevens (reactie op de adviescommissie Brouwer-Korf)
4. Bescherming van persoonsgegevens op andere terreinen dan veiligheid
5. Uitgeleide

Deze opbouw heeft tot gevolg dat passages over de kernthema's op 3 plaatsen zijn aan te treffen: in de samenvatting, in paragraaf 2 en in de overige paragrafen. Kan de regering aangeven hoe de discrepantie in de teksten over de al dan niet wettelijke invoering van een klachtrecht op de drie verschillende vindplaatsen is te interpreteren? Wat zijn precies wel en niet de standpunten en voornemens van de regering ter zake?
Reeds in de inleiding en ook op diverse plaatsen elders in de brief komt de verantwoordelijkheid van de professional aan de orde, al dan niet afgezet tegen die van de verantwoordelijke krachtens artikel 1.Wbp. Kan de regering aangeven welke begripsomschrijving en afbakening te hanteren is bij «professional»? Naar verluidt betrof dit in oorsprong hulpverleners maar is dat in de loop van het traject uitgebreid tot veel bredere kringen. Kan de regering hierover uitsluitsel geven?

De leden van de **SP**-fractie hebben met belangstelling het rapport van de commissie Brouwer-Korf en de regeringsreactie daarop gelezen. Het is goed dat de regering zich bewust is van de complexe afwegingen die gepaard gaan in de discussie rond (nationale) veiligheid en privacy. Daarbij kunnen de leden van de SP-fractie zich niet aan de indruk onttrekken dat de regering dit vaak als een zero-sum ziet, waarbij privacy en veiligheid altijd op gespannen voet met elkaar staan. Hoewel dit in een aantal gevallen wel degelijk zo kan zijn, vragen de leden van de SP-fractie zich af of deze trade-off niet al te vaak impliciet door beleidsmakers als vanzelfsprekend wordt verondersteld. Veiligheid kan op terreinen, denk aan pogingen van hackers om met gegevens van burgers kwaad te doen, wel degelijk bevorderd worden door goede waarborging van de privacy van deze burgers. De leden van de SP-fractie hopen dat de regering dit met haar eens is.

Hoewel het vraagstuk van veiligheid en persoonlijke levenssfeer niet beperkt is tot de rechtshandhaving, willen de leden van de fracties van de **SGP** en de **ChristenUnie** hun opmerkingen en vragen vooral richten op de opsporing van strafbare feiten. De leden van deze fracties onderkennen dat wanneer criminele en terroristische groepen steeds meer gebruik maken van moderne communicatiemiddelen en moderne technologie in ruime zin, politie, justitie en veiligheidsdiensten niet achter kunnen blijven. Ofschoon het bieden van veiligheid in een rechtsstaat vanouds een centrale taak van de overheid is, is bij deze leden, gelet op de ontwikkelingen in de voorbije twee decennia, de vraag gerezen of bij burgers en vervolgens in reactie bij de overheid niet een (vorm van) veiligheidsutopie de overhand dreigt te krijgen. Valt bij de zorg voor het gewenste niveau van veiligheid niet een verschuiving van delict naar risico en van repressie naar voorzorg en preventie waar te nemen? Heeft de overheid in meer abstracte zin een toelaatbare grens bepaald ten aanzien van deze verschuiving? Hoe zal er anderzijds blijvend in voorzien worden dat de kern van de persoonlijke levenssfeer – het recht om met rust te worden gelaten en zich van overheidswege onbespied te weten – van burgers die geen wettelijke plichten hebben geschonden, in stand blijft?
Is de regering het eens met deze leden dat het uitgangspunt bij het bieden van veiligheid niet kan zijn dat iedere burger een potentiële verdachte zou kunnen blijken te zijn?

De leden van de fractie van **GroenLinks** zijn ingenomen met het uitgebreide standpunt dat het kabinet heeft geformuleerd ten aanzien van de bescherming van persoonsgegevens. Volgens de aan het woord zijnde leden is het tijd voor reflectie, na een decennium waarin veel wetgeving is aangenomen die opslag en verwerking van persoonsgegevens mogelijk maakt. In de politieke besluitvorming zijn er altijd weer argumenten om persoonsgegevens te verzamelen en uit te wisselen (terrorisme, fraudebestrijding, zware criminaliteit) waarbij het belang van bescherming van persoonsgegevens meestal het onderspit delft. Inmiddels bevat de wetgeving volgens de commissie 5uyver niet meer een balans tussen veiligheid en privacy. De leden van de Groenlinks-fractie beschouwen de kabinetsnotitie daarom als een eerste poging om een nieuw evenwicht te bereiken. Ze zijn verheugd dat het kabinet hierbij de aanbevelingen van de Eerste Kamer ter harte heeft genomen.
In de ogen van de leden van de fractie van GroenLinks is er pas sprake van een balans als burgers zelfbeschikkingsrecht hebben ten aanzien van hun gegevens en ze niet langer zijn overgeleverd aan een onbekende overheid. Vanuit deze optiek zullen de leden de voorstellen beoordelen. Ze onderschrijven het belang dat er voorafgaand aan wetgeving meer wordt nagedacht over privacyeffecten, dat professionals meer ondersteuning krijgen bij de toepassing van de regels (dat vergroot immers ook de uniformiteit), dat burgers beter worden geïnformeerd en dat bedrijven worden geprikkeld tot een beter beleid. Toch hebben de leden van de fractie van GroenLinks een aantal kritische kanttekeningen en vragen naar aanleiding van de hoofddoelstellingen van het kabinet en de uitwerking van deze doelstellingen. Deze leden menen dat een aantal voornemens en doelen met elkaar in strijd is, en dat het doel om de mogelijkheden voor de overheid te verruimen de meeste nadruk krijgt. Zo wil het kabinet dat de uitwisseling tussen opsporing/OM en bestuur wordt vergemakkelijkt zonder de waarborgen duidelijk te formuleren, en wil de regering meer mogelijkheden voor profiling en voor het gebruik van gegevens voor andere doelen dan waarvoor gegevens zijn opgevraagd of bewaard. Deze maatregelen ontnemen burgers het zicht op hun gegevens, terwijl de regering dat juist als hoofddoel heeft aangewezen. Kan de regering ingaan op de vraag hoe de verschillende doelen zich tot elkaar verhouden en op welke wijze ze de belangen tegen elkaar heeft afgewogen?

De leden van de fractie van **D66** hebben kennis genomen van de bevindingen van de Adviescommissie Veiligheid en persoonlijke levenssfeer (commissie Brouwer-Korf) en de evaluatierapporten van de Wet bescherming persoonsgegevens. Deze leden hechten zeer aan de bescherming van persoonsgegevens. Ze stellen vast dat steeds meer burgers zich zorgen maken over de opslag van hun gegevens en het gebruik ervan door overheden en bedrijven. Deze leden delen deze zorgen en zien in de evaluatie van de Wbp, in samenhang met het rapport Brouwer-Korf, gelegenheid om een meer fundamentele discussie over privacybeleid te voeren.

2. Een nieuwe benadering van persoonsgegevens

2.1. Kernthema 1: «Gewoon doen»: meer waarborgen bij de omgang met persoonsgegevens

Met betrekking tot het eerste kernthema onderschrijven de leden van de fractie van **GroenLinks** de noodzaak van het ontwikkelen van open normen in privacywetgeving ten behoeve van de professional, het handhaven van de doelbinding en het aanwijzen van één verantwoordelijke voorafgaand aan de verwerking. Is de regering het met de leden van de GroenLinks-fractie eens dat de invulling met materiële normen een zaak van de wetgever is, en deze keuze niet moet doorschuiven naar

lagere wet- en regelgevers of naar het werkveld? Zou een herijking van artikel 13 van de Grondwet (een volwaardig grondrecht op de bescherming van alle communicatie, inclusief de principes ten aanzien van doel binding, minimalisatie, fair play en een verankering van het recht op privacy zoals in het Handvest voor de Grondrechten is vastgelegd) hier geen richtinggevende functie kunnen hebben? Wel zal duidelijk moeten zijn dat elke sector vraagt om andere afwegingen. Daarom is het goed dat de professional zelf verantwoordelijk blijft. Het is wel de vraag hoever en hoe exclusief het vertrouwen in de professional moet reiken. De professional (bijvoorbeeld de politieagent of de toezichthouder) heeft: toch vooral belang bij het bereiken van zijn doelen, waarvoor hij informatie nodig heeft. Bescherming van persoonsgegevens zal hij dan ervaren als een onwenselijke belemmering. Erkent de regering deze spanning? Is ze bereid om de professionals op te leiden en trainen op een bewuste omgang met persoonsgegevens, en niet te wachten tot zij zelf gebruik maken van een helpdesk?

2.2. Kernthema 2: Robuuster extern toezicht

Het kabinet is voornemens om te komen tot meer of robuuster extern toezicht. Dat doet het kabinet door uitbreiding van de bestuurlijke boetes en externe klachtenregelingen. De leden van de fractie van de **VVD** vroegen zich af of de bestaande klachtenregelingen niet volstaan. Waarom niet meer gebruik maken van het audit instrument zoals de Wet GBA en de Wet politiegegevens die kennen?

Over de versterking van het externe toezicht merkt het kabinet op dat een sterke toezichthouder via zijn bevindingen en uitspraken bijdraagt aan een betere rechtsontwikkeling. Dat is aan de ene kant prima, maar aan de andere kant doet het tekort aan het feit dat privacybescherming juist meer is dan het toepassen van regels. Privacybescherming wordt juist ook geëffectueerd door implementatie van beginselen en regels in techniek en organisatie, in systemen en processen en procedures. Hoe gaat het kabinet die implementatie bevorderen?

Het belang van goede, onafhankelijke controlemogelijkheden wordt door het kabinet onderstreept. Voor de burger is het van belang dat hij niet in de kou staat wanneer op een onjuiste manier met zijn gegevens wordt omgegaan. Kan het kabinet toelichten wat de onafhankelijke toezichthouder kan doen voor een burger op het moment dat een verantwoordelijke op een onjuiste manier met zijn gegevens omgaat? Het uitdelen van een bestuurlijke boete kan weliswaar een belangrijk sanctiemiddel zijn, maar het helpt de individuele burger niet in concrete gevallen.

2.3. Kernthema 3: Minder nadruk op procedures en controle vooraf

In de paragraaf over controle vooraf worden opmerkingen gemaakt over andere noodzakellijkheidstoetsen dan de bestaande bestuursrechtelijke verplichtingen. Dit geldt natuurlijk de uitwerking in de praktijk. Hoe zit het echter met de noodzakelijkheidstoets bij de voorbereiding van nieuwe wetgeving, zo vragen de leden van de fractie van het **CDA** zich af. Is de regering bereid hieromtrent de lijst met criteria te hanteren, die in het verslag van de expertmeeting van 20 maart 2008 van de zijde van het CDA is genoemd en aldaar de instemming van de aanwezige deskundigen heeft verworven (EK 31 200 VI, F)? Ook in de Algemene Politieke Beschouwingen van 2008 is namens het CDA voor deze aanpak de aandacht gevraagd.

2.4. Kernthema 4: Het burgerperspectief

In de regeringsreactie wordt onder Kernthema 4 een verscherping van de beveiliging als voorgenomen maatregel vermeld. De leden van de fractie van het **CDA**vragen zich af aan welke aanpak de regering hierbij denkt. Wordt overwogen de beveiligingsverplichting van de Wet bescherming persoonsgegevens met strafsancties te gaan handhaven?

De regering wil dat de overheid bij opsporing profiteert van technologische mogelijkheden als profiling, zo constateren de leden van de fractie van **GroenLinks.** Ook hier wreekt zich de voor meerdere interpretaties vatbare criteria proportionaliteit en subsidiariteit. Opsporingsautoriteiten komen vaak tot een andere uitkomst dan bijvoorbeeld privacybeschermers of toezichthouders. Nadrukkelijk zou bij elk besluit (net als bij wetgeving) moeten worden onderbouwd wat de noodzaak ervan is (wat ging er mis tot nu toe, en is dit de oplossing?) en hoe effectief de uitwisseling of het gebruik van technologieën is. Profilen zou altijd een wettelijke basis moeten hebben, waarbij ook onbedoelde effecten zoals stigmatisering worden meegewogen.
De regering wil het gebrek aan recht op inzage bij veiligheid compenseren door toezicht van een instantie of rechterlijke toetsing achteraf. Wie laat een besluit tot uitwisseling van gegevens door de rechter toetsen? De burger kan dit niet doen, want die is immers niet op de hoogte van het gebruik van zijn gegevens. Heeft de rechter voldoende handvatten en gegevens om te beoordelen of de uitwisseling noodzakelijk is? Hoe kan een burger erop vertrouwen, als hij zijn gegevens niet krijgt te zien, dat deze worden vernietigd zodra de grondslag verdwenen is? Hoeveel tijdelijke persoonsgegevensbestanden zijn er in Nederland tussen overheidsinstellingen? Welke criteria gelden er voor de vernietiging en wie beslist daartoe?
De regering wil de informatieplicht verbeteren door middel van maatregelen bij de overheid. Zou niet ook het bedrijfsleven moeten worden verplicht tot betere informatieverstrekking aan klanten? De leden van de GroenLinks-fractie onderschrijven de informatieplicht, maar het lijkt toch nog steeds de omgekeerde wereld: burgers moeten er zelf achteraan gaan om te weten te komen wat er met hun gegevens gebeurt. Zou de overheid, dan wel het bedrijfsleven bij de verstrekking van persoonsgegevens door een burger, hem of haar niet meteen op de hoogte moeten stellen van de mogelijke verwerking van zijn gegevens, en hoe dat te volgen is? Dan wordt de inspanning ook voor een deel bij overheid en bedrijfsleven gelegd. En is de regering bereid om het idee van een laagdrempelig loket voor burgers uit te werken? Klachten zouden door de betreffende loketmedewerkers dan bij de juiste organisatie kunnen worden neergelegd, waardoor burgers niet meer van het kastje naar de muur worden gestuurd.

3. Veiligheid en persoonsgegevens

3.1. Het richtinggevend kader van de Adviescommissie Veiligheid en persoonlijke levenssfeer

De commissie Brouwer-Korf bepleit op verschillende plaatsen een versterking van het interne toezicht, te weten zowel bij grondslag 1 («Transparantie, tenzij») als bij grondslag 6 («Zorg voor naleving en intern toezicht»). Wordt deze aanbeveling van de commissie ook door de regering gesteund en zal de regering een dergelijke aanpak ook concreet stimuleren, zo vragen de leden van de fractie van het **CDA**.

Het richtinggevend kader van de commissie moet handreikingen bieden aan de professional bij de juiste afweging van proportionaliteit, zo constateren de leden van de fractie van de **PvdA**. Uitgangspunt is dan: als het nodig is voor de veiligheid moet je delen. Is de regering bekend met het standpunt van prof. mr. E.J. Dommering, hoogleraar Informatierecht aan de UvA, die dit de bijl aan het kernbeginsel van de doelbinding noemt? Naar zijn mening is dit zonder nadere afweging een onderschikking van privacy aan veiligheid. Wat vindt het kabinet van dit standpunt? Zijn geen nadere criteria te formuleren voor de veiligheidsaspecten, zoals soorten en categorieën veiligheidsrisico's die in het geding kunnen zijn, afgezet tegen de mate waarin het delen van persoonsgegevens risico's kan verminderen en de inbreuk op de privacy van (groepen) individuen? Daarin zit toch de proportionaliteit?

De regering concludeert dat de grondslagen voor een goed beleid zoals de commissie die identificeert weliswaar breed toepasbaar zijn, maar «zonder nadere sectorale uitwerking nog geen garantie voor zorgvuldige afwegingen door professional» bieden. De leden van de **SP**-fractie zijn benieuwd of de regering deze grondslagen wel onderschrijft en zo ja, welke concrete stappen zij gaat ondernemen om deze grondslagen ook in de praktijk meer handen en voeten te geven. Zullen er bijvoorbeeld verschillende Privacy Impact Assessment protocollen worden ontwikkeld?

Overheidsinstellingen moeten informatie delen als aan twee voorwaarden wordt voldaan: er is sprake van concrete dreiging jegens de veiligheid van een individu, en informatieuitwisseling kan deze dreiging wegnemen. Dit zijn naar het oordeel van de leden van de fractie van **GroenLinks** bedrieglijk eenvoudige criteria: wat is een concrete dreiging, wat verstaat de regering onder veiligheid en hoe en wanneer beoordeelt ze dat informatie-uitwisseling de dreiging kan wegnemen? Dit vraagt om een nadere invulling van de criteria om misbruik of onnodig veel gebruik (in het kader van indekken) te voorkomen. Is de regering het daarmee eens? En zou deze invulling niet van de wetgever moeten komen? Is de regering het met de leden eens dat dit criterium een breuk vormt met het doelbindingscriterium, dat de regering wil handhaven?

3.2. Evenwicht tussen bescherming van persoonsgegevens en veiligheid: een tweevoudige bescherming

De commissie Brouwer-Korf heeft specifieke aandacht besteed aan de registratie van etniciteit en levensovertuiging en heeft daarbij als voorbeeld de aanpak van Antilliaanse risicojongeren genomen. Het kabinet geeft aan hierop via een aparte brief te reageren. De leden van de fractie van de **VVD** willen graag weten wanneer deze brief kan worden verwacht.

De leden van de fractie van **D66** wensen de evaluatie van de Wbp te betrekken in de discussie over de registratie van bijzondere persoonsgegevens, zoals etniciteit en levensovertuiging. In de juridische literatuur is gewaarschuwd voor de toepassing van etniciteitsregistraties (NJB 2009, 230). Dit gebeurde naar aanleiding van de Antillianenindex. Hierin was sprake van de registratie van herkomstgegevens ten behoeve van lokale Interventie en beleidsinformatie. Ook de registratie van levensovertuiging wordt overwogen als middel tegen radicalisering en polarisatie. De leden van de fractie van D66 hebben hierbij de nodige bedenkingen en vraagpunten. In het licht van de te voeren discussie hebben zij de volgende vragen:

– Onder welke voorwaarden is de regering voornemens om een eventuele registratie van bijzondere persoonsgegevens te beargumenteren?

– Kan de regering aangeven hoe zij bij registratie van persoonsgegevens zal omgaan met het gevaar van stigmatisering?
– Welke argumenten voert de regering aan voor de noodzakelijkheid van deze maatregelen? Dient niet eerst te worden bekeken of het doel van de registratie kan worden bereikt met minder verregaande middelen? Is de Nederlandse regering voornemens om in grote mate gebruik te maken van de «margin of appreciation» waarmee het Europese Hof rekening houdt bij de eventuele toetsing van deze maatregelen aan grondrechten geformuleerd in het EVRM?
– Hoe beziet de regering het gevaar van deze vormen van registratie in het kader van de Richtlijn houdende toepassing van het beginsel van gelijke behandeling van personen ongeacht ras of etnische afstamming (Richtlijn 2000/43/EG, 29 juni 2000, Pb EG L 180/22)?
– Hoe beziet de regering de hiermee samenhangende beperking van artikel 14 EVRM, een artikel dat voorziet in een vrijwaring van discriminatie voor de rechten en vrijheden die in het EVRM zijn neergelegd, zoals in combinatie met artikel 8 EVRM, een artikel dat het recht op respect voor het privé leven garandeert?
– Op welke manier zijn deze maatregelen in overeenstemming te brengen met het door Nederland geratificeerde Twaalfde Protocol bij het EVRM, dat een algemeen discriminatieverbod formuleert? Het Twaalfde Protocol behelst immers een negati-ve verplichting; een algemeen verbod om individuen te discrimineren. Welke objectieve en redelijke rechtvaardigingsgronden liggen ten grondslag aan de overwegingen van het kabinet?

Hoe beziet de regering de risicoanalyse waarover door de commissie Brouwer-Korf in haar rapport wordt gesproken (hoofdstuk 4, p. 11)? Welke waarborgen worden in een risicoanalyse ingebouwd, zodat personen die niet tot de risicovolle gedeelten van een groep behoren, niet worden opgenomen in dergelijke registratiesystemen? Is de regering het met de leden van de fractie van D66 eens dat sprake dient te zijn van een daadwerkelijk risico, of heeft de regering een ander criterium voor ogen? Hoe wordt voorkomen dat een vorm van dataprofiling vaste voet aan de grond krijgt?
In het kader van radicalisering en polarisatie wordt gesproken over het registreren van levensovertuiging van burgers. Wordt onder deze registratie ook verstaan het registreren van concrete politieke ideologieën die door overheidsdiensten als risicovol worden aangemerkt? Deelt de regering de vaststelling van de commissie dat iemands levensovertuiging geen objectief gegeven vormt en de betrouwbaarheid van deze informatie moeilijk toetsbaar is? Brengen juist deze onzekerheden niet met zich dat een aparte juridisch ingeklede en beschermde mogelijkheid van registratie een betere optie is dan het laten bestaan van een leemte?

3.3. Selecteer voor je verzamelt

Op de regel «selecteer voor je verzamelt» geven commissie en kabinet aan dat bij bijzondere omstandigheden uitzonderingen gemaakt kunnen worden. Dan moet er gestreefd worden naar selectie zo kort mogelijk nadat gegevens zijn verzameld en moet «nice to know» verzamelen voorkomen worden. Ook «verdient het aanbeveling» de gegevens te vernietigen wanneer ze niet meer gebruikt worden met het oog op de integriteit van gegevens. Dat vermindert immers de kans dat die op onjuiste wijze gebruikt worden. Kan de regering concreter aangeven welke criteria en waarborgen burger en samenleving hebben in dergelijke gevallen en hoe in toezicht en handhaving is voorzien? De leden van de fractie van de **PvdA** kregen graag een antwoord op deze vraag.

Het criterium «selecteer voordat je verzamelt en houd het sober» klinkt de leden van de fractie van **GroenLinks** zinnig in de oren, maar dit criterium verdient nadere uitwerking en concrete toepassing. In de praktijk blijkt er immers behoefte om zoveel mogelijk gegevens te verzamelen «voor de heb». Teveel Informatie, waarvan maar een fractie bruikbaar is, doet het systeem juist dichtslibben. Medewerkers van Amerikaanse veiligheidsdiensten erkenden recentelijk dat de toenemende opslag van gegevens leidt tot een gebrek aan inzicht: hoe meer je hebt, hoe minder je weet. Ook leidt de toevloed aan informatie tot verlies aan effectieve capaciteit, omdat er veel aandacht moet worden besteed aan zogenaamde vals-positieve gevallen. Op welke manier zal de regering het uitgangspunt van selectiviteit effectueren?

3.4. Transparantie

Wanneer transparantie niet geheel mogelijk is vanwege veiligheidsaspecten kan dat gecompenseerd worden door toezicht en toetsing achteraf door de rechter, zo stelt de regering. Volgens de eerder genoemde professor Dommering (zie paragraaf 3.1) is het streven naar transparantie en integriteit van gegevens in toenemende mate een Illusie door de ondoorzichtigheid van de techniek en de hoeveelheid digitale sporen die Individuele burgers achter laten. Ze komen terecht in talloze databanken waarvan de identiteit en locatie niet te achterhalen zijn, hetgeen de controle op opslag, kwaliteit en verwerking van persoonsgegevens vrijwel onmogelijk maakt. De leden van de fractie van de **PvdA** vragen zich af of de regering het bestaan van de websites www.burgerservicenummer.nl en www.mijnoverheid.nl afdoende acht voor een adequate transparantie voor de burger, mede gezien de uitkomsten van het Regioplan-rapport «Niets te verbergen en toch bang» van januari 2009. Welke aanvullende maatregelen ziet de regering, met inbegrip van nieuwe technologische mogelijkheden als Web 2.0, waarbij niet de dienst, maar de individuele burger centraal staat?

3.5. Integriteit van systemen: privacybescherming door ontwerp

3.5.1. Privacy Impact Assessments

Wil de regering aangeven hoe naar haar oordeel het genoemde Privacy Impact Assessment (PIA) er uit zal zien? De leden van de fractie van het **CDA** gaan ervan uit dat hierbij wordt gedacht aan een uitwerking van het voorstel dat door een lid van de CDA-fractie tijdens de bijeenkomst van 20 maart 2008 is gedaan. Ook zijn de aan het woord zijnde leden benieuwd naar de wijze waarop de regering «aandacht» (zie de bijlage bij TK 31 051, nr. 5) zal geven aan het hanteren van «privacy by design».

Het kabinet wil meer aandacht voor de wijze waarop met persoonsgegevens wordt omgegaan en de waarborgen die daarbij moeten worden vervuld. Daartoe ontwikkelt het kabinet zogenoemde Privacy Impact Assessments. Dit is een toets in de vorm van een risicoanalyse die voorafgaand aan het verzamelen van gegevens toegepast moet worden. Het College bescherming persoonsgegevens heeft dergelijke toetsen reeds ontwikkeld. Is het
kabinet voornemens om gebruik te maken van deze toetsen bij het ontwikkelen van zo'n PIA? Zo nee, waarom, niet? De leden van de fractie van de **WD** kregen graag een nadere toelichting.

De regering stelt in haar reactie op het rapport van de commissie dat zij in de toekomst een «risicoanalyse voorafgaand aan het verzamelen van gegevens» wil laten plaatsvinden. De leden van de **SP**-fractie zijn benieuwd welke criteria daarbij gebruikt zullen worden en hoe uiteindelijk

de afweging zal worden of de verzameling van gegevens wel opweegt tegen de mogelijke bezwaren op het gebied van de privacy. De regering verwijst naar de zogeheten Britse Privacy Impact Assessments, maar de leden van de fractie van de SP zijn benieuwd welke criteria de regering daarin op zal nemen. Hoe ziet het protocol waarnaar de regering in haar reactie verwijst er concreet uit?

De leden van de fractie van **GroenLinks** zijn enthousiast over de introductie van een Privacy Impact Assessment, omdat het zal helpen bij het kunnen beoordelen van wetsvoorstellen. De leden gaan er vanuit dat de assessments openbaar zijn, zodat iedereen ze kan benutten bij commentaar op ontwerpwetgeving, en dat de regering in de toelichting op haar wetsvoorstellen motiveert op welke wijze ze de assessments heeft betrokken in haar besluitvorming.

3.5.2. Kentekenherkenning met camera's (ANPR)

De reactie van de regering houdt in dat wetgeving zal worden voorbereid om de Automatic Number Plate Recognitlon verder te ontwikkelen. Op welke wijze zal dit worden aangepakt en in hoeverre zullen de voorstellen dienaangaande worden ingebed in internationale mogelijkheden tot regulering, zo vragen de leden van de fractie van het **CDA**.

De brief noemt integriteit van systemen met privacybescherming door ontwerp en spreekt van nieuwe technologische mogelijkheden voor privacybescherming met «privacy enhanclng technologies» en authenticatiemogelijkheden bij toegang, beveiliging en aggregatie van gegevens via versleuteling en automatisch opschonen van gegevens. In hoeverre worden deze methoden concreet toegepast, bijvoorbeeld bij het in de brief genoemde systeem voor preventie en opsporing van misbruik van rechtspersonen (wetsvoorstel 31 948), zo wilden de leden van de fractie van de **PvdA** weten. Op verzoek van de regering heeft de commissie immers specifiek aandacht besteed aan automatische kentekenherkenning – Automatic Number Plate Recognitlon (ANPR) – en geconstateerd dat ANPR zonder daadwerkelijke samenhang wordt ingezet. Daardoor worden kennis en ervaring onvoldoende uitgewisseld en blijft de impact van ANPR-systemen op de persoonlijke levenssfeer onderbelicht. Op welke wijze zal dit bij andere toepassingen zoals wetsvoorstel 31 948, maar ook alle andere worden voorkomen en daarmee het risico van vervuilde bestanden met niet actuele informatie die niet alleen onvoldoende effectief zijn maar ook grote risico's inhouden voor ernstige fouten met grote consequenties voor individuen? Een voorbeeld is het niet verwijderen van «no hits» gegevens uit het ANPR. Kan dit in uiterste instantie niet leiden tot situaties als bij de Amerikaanse veiligheidsdiensten rondom de mislukte aanslag boven Detroit?

Cameratoezicht in het publieke domein heeft een hoge vlucht genomen en de neiging tot uitbreiding lijkt continu aanwezig, zo constateren de leden van de fracties van **SGP** en **ChristenUnie**. Staan de regering precieze doeleinden van cameratoezicht voor ogen? Zo ja, welke kunnen dat zijn? Welk doel staat bij de toepassing van camera's ten behoeve van automatische kentekenregistratie voor ogen: het traceren van criminelen en terreurgroepen of het innen van achterstallige parkeerboetes en belastingschulden?

Een ingrijpende vorm van het loslaten van het doelbindingscriterium stelt de regering voor ten aanzien van de kentekenregistraties. Wordt bij een ruim gebruik van kentekens geen misbruik gemaakt van gegevens die burgers noodgedwongen prijsgeven, zo vragen de leden van de fractie van **GroenLinks** zich af. Een Burger Service Nummer dragen ze niet op

hun voorhoofd, maar een kenteken kunnen ze niet voor zichzelf houden. De leden van de fractie van GroenLinks vinden dat de regering daar geen ongelimiteerd gebruik van zou mogen maken, maar zich bijvoorbeeld dient te beperken tot handhaving van verkeersregels en ernstige misdrijven. Worden burgers geïnformeerd over (het doel van) de verwerking van hun kenteken, en zo ja, op welke wijze? In het platform dat werkt aan een samenhangende toepassing ontbreekt het College Bescherming Persoonsgegevens (CBP). Waarom hoort dit college daar niet bij? En wat is het advies van het CBP over de wettelijke grondslag?

De leden van de fractie van **D66** stellen vast dat het kabinet een specifiek wettelijk kader tot stand wil brengen om Automatic Number Plate Recognitlon (ANPR) verder te ontwikkelen. Deze leden begrijpen het voordeel van een specifieke wettelijke grondslag, die de werkwijze uniform reguleert en stroomlijnt. Gezien de huidige regionale, incidentele en onsamenhangende werkwijze van ANPR is een eenduidige aanpak logisch. Zij menen dat in de specifieke wettelijke grondslag aandacht zal moeten worden besteed aan uniforme bewaartermijnen van de geregistreerde kentekens en de wettelijke – liefst limitatieve – uitzonderingen daarop. Dit leidt de leden van de fractie van D66 tot de volgende vragen:

– Is de regering in dit verband voornemens om een onderscheid te maken tussen de bewaartermijnen van *immediate hits* en de bewaartermijnen van geregistreerde kentekens waartegen geen concrete en actuele feiten bekend zijn?
– Is de regering voornemens om een «weggooiplicht» in dit systeem op te nemen?
– Maakt de regering hierin onderscheid tussen ANPR ten behoeve van handhaving van de rechtsorde en voor strafvorderlijke opsporingsdoeleinden? Is de regering voornemens om het gebruik van ANPR voor strafvorderlijke opsporingsmethodes aan strengere eisen te onderwerpen?
– Welke waarborgen bouwt de regering in ter bescherming van burgers tegen fouten die gemaakt zijn in gekoppelde systemen, zoals in het systeem van het CJIB? De herkenningssoftware van radarcontroles is immers niet waterdicht. Hoe voorkomt de regering dat burgers verstrikt raken in een bureaucratisch web wanneer sprake is van een onterecht opgelegde bekeuring, die tot gevolg heeft dat ze steeds als *immediate hit* worden geregistreerd?

3.6. Gegevensuitwisseling en veiligheid: een kwestie van belang

De commissie Brouwer-Korf geeft het advies om voor de omgang met persoonsgegevens een aantal grondslagen te hanteren die de aanpak in de praktijk betreffen en niet zozeer tot nieuwe wetgeving aanleiding geven. Toch wordt wel aangegeven om artikel 9 Wbp (de eis van doelbinding) zodanig te wijzigen dat in het belang van de veiligheid een grotere mate van koppeling tussen systemen mogelijk wordt dan thans het geval is. Wat voor (soort) wijziging staat de regering hier voor ogen, zo vragen de leden van de fractie van het **CDA.** Kan de regering aangeven dat het doelbindingsprincipe, dat tot de hoofdbeginselen van de op een Europese Richtlijn gebaseerde Wet bescherming persoonsgegevens behoort, in vorm en wezen geen geweld wordt aangedaan?

In het Stockholm-programma valt ook al te lezen dat er ten aanzien van het doelbindingsbeginsel een relativering zal plaatsvinden. Deze opmerking heeft de leden van de CDA-fractie niet bepaald gerustgesteld. Is de regering zich ervan bewust, dat bij het relativeren van dit principe steeds de term veiligheid wordt gebruikt om tot een uitbreiding van overheidsbevoegdheden te komen, terwijl dit – stap voor stap – tot een zodanige inperking van bepaalde fundamentele rechten van de burger –

met name van de bescherming van de persoonlijke levenssfeer – leidt, dat hierover in toenemende mate irritaties bij de burger ontstaan? De soort en de hoeveelheid van gegevens die de overheid in dit verband verzamelt, leiden tot een steeds sterker wantrouwen van de burger jegens de overheid. De in aantal en intensiteit toenemende discussies over Passenger Name Records (PNR), bewaarplicht verkeersgegevens en cameratoezicht, maar ook over rekeningrijden, Elektronisch patiëntendossier (EPD) en Elektronisch kinddossier (EKD) geven aan dat steeds meer burgers in de overheid de beruchte Big Brother gaan zien, terwijl een zich uitbreidend aantal burgers, teneinde datamining en profilering door middel van grote databestanden te voorkomen, gaat proberen de verzameling van persoonsgegevens te ontgaan en controlemogelijkheden te omzeilen. De burger ziet de proportionaliteit van diverse maatregelen niet (meer). Hoe denkt de regering hieromtrent overtuigend te kunnen opereren, zodat er altijd voldoende draagvlak voor nieuwe maatregelen zal bestaan?

Kan de instelling van een externe vertrouwenspersoon, die door de commissie BrouwerKorf in dit kader wordt voorgesteld om het principe van de doelbinding bij bepaalde koppelingen te controleren, als een reële mogelijkheid worden beschouwd? Hoe stelt de regering zich de realisatie van een en ander voor?

De leden van de fractie van de **WD** hadden enige vragen over het voornemen van het kabinet om artikel 9 Wbp te expliciteren. Artikel 9 Wbp betreft het verenigbaar gebruikprincipe. Dit artikel bevat criteria die bepalend zijn voor het kunnen uitwisselen van persoonsgegevens tussen verschillende verantwoordelijken. Wat wordt de status van dit expliciteren? Wordt er een algemene maatregel van bestuur vastgesteld of een ministeriële regeling? Is het kabinet voornemens om beide Kamers hierbij te betrekken?

De leden van de fracties van **SGP en ChristenUnie** menen dat inbreuken op de privacy slechts zijn toegestaan, mits daar goede redenen voor kunnen worden gegeven. Deelt de regering de opvatting dat de afweging tussen privacy en andere belangen in laatste instantie een politieke, rechtsstatelijk te verantwoorden beslissing behoort te zijn? Meer in het bijzonder met betrekking tot het gebruik van moderne technologie voor opsporings- en veiligheidsdoeleinden rijzen bij genoemde leden vragen over de effectiviteit van deze middelen. Leiden maatregelen als (voortdurende uitbreiding van) DNA-onderzoek, cameratoezicht en datamining in voldoende (proportionele) mate tot opsporing van die categorieën verdachten die men oorspronkelijk, bij instelling van de maatregelen, voor ogen had? Verder vragen deze leden in het bijzonder met betrekking tot datamining in hoeverre er waarborgen bestaan dat beschikbare data betrouwbaar zijn, persoonsverwisseling en identiteitsdiefstal wordt voorkomen. Acht de regering het wenselijk om, gezien de voortschrijdende digitalisering van gegevensbestanden en de koppelingsmogelijkheden daarvan, een strikte begrenzing aan te brengen wat betreft de bevoegdheden van opsporingsdiensten om gegevens bij derden te vorderen?

3.6.1. Verbetering informatie-uitwisseling bij multidisciplinaire samenwerking

Voortbordurend op «indien noodzakelijk voor de veiligheid moet je delen» worden initiatieven opgesomd die illustreren hoe slimmer en effectiever kan worden omgegaan met beschikbare gegevens en hoe informatie-uitwisseling bij multidisciplinaire samenwerking kan worden verruimd (onderaan pagina 17 van het kabinetsstandpunt). Daarbij blijft volgens de

leden van de fractie van de **PvdA** bulten beeld welke privacywaarborgen deze verruimingen bevatten: kan de regering daar concrete bepalingen over aanwijzen in de zes genoemde maatregelen?

Het vervolgens genoemde wetsvoorstel 31 948 ter voorkoming en bestrijding van misbruik van rechtspersonen beoogt een voortdurende, automatische risicogestuurde analyse van de levensloopgegevens van rechtspersonen in te stellen. Deze omvat mede persoonsgegevens van aanverwanten en relaties van bij rechtspersonen betrokken natuurlijke personen. Deze groep familie of naasten van bestuurders van rechtspersonen kan geen gebruik maken van de bevoegdheid de juistheid van de gegevens over hen in het databestand te verifiëren, omdat zij simpelweg geen weet hebben van de omstandigheid daarin voor te komen (zie Van Uchelen in het WPNR van 5 december 2009). Wat is de mening van de regering hierover: op welke wijze kan deze groep burgers gebruik maken van zijn privacyrechten krachtens de Wbp?

De regering noemt vervolgens de ontwikkeling van de Informatie Management Strategie (IMS) in het kader van het Stockholm programma, ter optimalisatie van informatieuitwisseling en voorkoming van wildgroei van juridische Instrumenten, nieuwe processen en ICT-systemen. Meer dan een integrale benadering en de keuze voor tweevoudige bescherming van burgers (dus inclusief bescherming van persoonsgegevens) geeft de regering in het kabinetsstandpunt niet. Kan de regering een nadere toelichting geven op de grondslagen en richtingen bij het ontwerp van de IMS?

De regering zegt in Europees verband te streven naar optimalisering van de voorwaarden voor informatie-uitwisseling, waarvoor aanpassing van de EU-privacyrichtlijn nodig is. Kan de regering preciezer aangeven op welke wijze ze de Privacyrichtlijn wil aanpassen? Heeft de regering met optimalisering een versoepeling van de voorwaarden voor ogen? In het oorspronkelijke regeringsstandpunt inzake het Stockholm Programma stelde de regering ook een «heroverweging van het doelbindingscriterium» voor. Wil de regering dat nog steeds heroverwegen, en wat verstaat ze daar precies onder? Heeft de regering overwogen wat de gevolgen zouden kunnen zijn van een mogelijke verruiming van het doelbindingscriterium of andere voorwaarden voor de rechtsbescherming van burgers, ook in andere lidstaten waar de controle op verwerking (nog) minder goed geregeld is. Is de regering het met de leden van de fractie van **GroenLinks**eens dat dit criterium een van de weinige waarborgen is voor een zorgvuldige omgang met persoonsgegevens, en voor de kennis van burgers van wat er met hun gegevens gebeurt? En is de regering bereid om te pleiten voor een allesomvattende richtlijn, die ook ziet op de bescherming op het gebied van justitie en politie?

3.6.2. Vergemakkelijken uitwisseling toezicht gegevens tussen toezichthouders, politie en OM.

De leden van de fractie van het **CDA**lazen dat wordt voorgesteld de uitwisseling van gegevens tussen toezichthouder, politie en OM te vergemakkelijken. Hoe denkt de regering dit te verwezenlijken? Zal een wijziging van de Algemene wet bestuursrecht (Awb) hiertoe noodzakelijk zijn? Aan welke waarborgen wordt gedacht om te voorkomen dat de koppeling tussen de bij deze organen behorende systemen zal leiden tot wat men wel noemt de *immutable me?*

Eén van de voornemens van het kabinet is het vergemakkelijken van de uitwisseling van toezichtgegevens tussen toezichthouders, politie en OM. Daartoe dient de regering in het voorjaar van 2011 een wetsvoorstel in.

Eén van de constateringen van de Adviescommissie Informatiestromen Veiligheid, zoals verwoord In het rapport «Data voor daadkracht», was dat partijen in het veiligheidsdomein onvoldoende samenwerken ten aanzien van het inwinnen van gegevens, het delen van informatie en het toepassen van nieuwe technologieën. De leden van de fractie van de **VVD**achten het niet waarschijnlijk dat deze samenwerking met een wetsvoorstel wordt verbeterd. Welke maatregelen treft het kabinet om deze vormen van samenwerking daadwerkelijk te verbeteren?

Inzake het vergemakkelijken van uitwisseling van toezichtgegevens tussen toezichthouders, politie en OM geeft de regering aan behoefte te hebben aan nadere advisering over de positie van politie en OM versus bestuur, en over het grensoverschrijdend aspect, zo constateren de leden van de fractie van de **PvdA.** Dit naast de voorgenomen algemene vangnetregeling met betrekking tot het toezicht op de naleving in de Awb. Kan de regering aangeven welke vraagstelling zij voornemens is mee te geven bij de adviesaanvraag aan wetenschappelijke kring?

Een voornemen dat volgens de leden van de fractie van **GroenLinks** breekt met het doelbindingscriterium is het vergemakkelijken gegevensuitwisse1ing tussen toezichthouders, de politie en/of het Openbaar Ministerie en het bestuur. De aan het woord zijnde leden kijken met belangstelling uit naar de adviezen van wetenschappers over de reikwijdte van dit voorstel en de mogelijke wederkerigheid. Op het eerste gezicht achten zij dit voornemen in forse tegenspraak met de doelstelling om de rechtspositie van burgers te versterken met betrekking tot privacy. Ook ten aanzien van de introductie van een vangnetbepaling in de Awb die de uitwisseling regelt als een specifieke regeling ontbreekt hebben de leden van de fractie van GroenLinks huiver. Tenslotte ambieert de regering vanwege het vangnetkarakter een ruime formulering. Heeft de regering inzicht in de (onbedoelde) neveneffecten van een dergelijke vangnetregeling? De leden van de GroenLinks-fractle verzoeken de regering bij de uitwerking van dit idee zorgvuldig te bezien wat de noodzakelijke reikwijdte zou moeten zijn en hoe wordt voorzien in verplichte motivering, toetsingscriteria, weigeringsgronden en de waarborgen voor burgers. Zij gaan ervan uit dat dit voorstel zal zijn voorzien van een Privacy Impact Assessment.

3.7. Organiseren van facilitering, voorlichting en educatie

Voor professionals binnen de overheid wordt een helpdesk ingericht die hen kan helpen bij het nemen van besluiten over wanneer en op welke wijze persoonsgegevens uitgewisseld kunnen worden. Deze helpdesk voorziet daarmee in een belangrijke adviestaak die op dit moment door het College bescherming persoonsgegevens wordt behartigd. Wat betekent dit voor de menskracht van zo'n helpdesk, zo vragen de leden van de fractie van de VVD zich af. Waar wordt de helpdesk gesitueerd? Bij het Ministerie van Justitie?

Wie vallen overigens onder de verzamelterm «professionals»? Vallen daaronder ook departementale ambtenaren die belast zijn met het opstellen van wet- en regelgeving waarbij verwerking, gebruik en bescherming van persoonsgegevens aan de orde is?

Het kabinet wil dat nu op diverse plekken georganiseerde deskundigheid op het gebied van privacy wordt gebundeld en voor een bredere kring toegankelijk wordt gemaakt. De wijze waarop dit gestalte zal krijgen, zal onderdeel uitmaken van het plan van aanpak voor de implementatie van alle in de kabinetsreactie genoemde maatregelen. Is het kabinet bereid de Eerste Kamer inzage te geven in dit plan van aanpak?

Naar de mening van het kabinet heeft rechtsontwikkeling onvoldoende plaatsgevonden en geldt hetzelfde voor de invulling van de open normen van de Wbp. De regering noemt als effectieve maatregel het instellen van de helpdesk Privacy Jeugd en Gezin en helpdesks voor overige professionals binnen de overheid. De nu op diverse plekken georganiseerde deskundigheid op het gebied van privacy wordt gebundeld en voor bredere kring toegankelijk gemaakt als onderdeel van het plan van aanpak ter uitvoering van het kabinetsstandpunt. In aansluiting op eerdere vragen over de afbakening van het begrip «professional» stellen de leden van de fractie van de PvdA de vraag aan de regering of hiermee toereikende maatregelen getroffen zijn voor de niet van de grond gekomen rechtsontwikkeling. Welke overige mogelijkheden zijn te voorzien?

4. Bescherming van persoonsgegevens op andere terreinen dan veiligheid

4.1. Normering en toekomstbestendigheid van de Wbp

Een punt van aandacht voor de Wbp is de vraag of de huidige wetgeving de samenleving nog wel voldoende kan beschermen tegen technologische ontwikkelingen als *radio frequency identification* (RFID), biometrie, internettoepassingen e.d. Wat is de regering – uitgaande van de vigerende Wbp – voornemens vanuit een Integrale aanpak te ondernemen tegen de risico's van voortschrijdende technologische ontwikkelingen, mede binnen EU-kader? Op deze vraag ontvingen de leden van de fractie van de **PvdA** graag een antwoord.

4.2. Het belang van een privacybewuste burger

Het kabinet geeft aan het privacybewustzijn van burgers te willen vergroten, zowel in relatie tot de overheid als met betrekking tot de risico's van een onzorgvuldige omgang met eigen persoonsgegevens, zo constateren de leden van de fractie van de **PvdA**. Welke maatregelen staan de regering concreet en op welke termijn voor ogen, behalve de genoemde campagne «Veilig internetten heb je zelf in de hand»?

4.3. Transparantie

4.3.1 Inzage- en correctierecht

De burger moet door overheidsinstellingen en bedrijven die zijn gegevens verwerken beter worden geïnformeerd. Initiatieven die daaraan een bijdrage leveren, moeten worden versterkt, zo schrijft het kabinet. Welke concrete maatregelen gaat de overheid treffen om die transparantie richting de burger te vergroten? De voorbeelden van www.burgerservicenummer.nl en www.mijnoverheid.nl zijn volgens de leden van de fractie van de **VVD** weliswaar mooi, maar zeggen nog weinig over de concrete maatregelen. Ook wil het kabinet het privacybewustzijn verhogen. Voor de publieke sector krijgt dat een plaats in het persoonsinformatiebeleid van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Kan de regering een toelichting geven op wat het persoonsinformatiebeleid inhoudt? Dit wordt uit de kabinetsreactie niet duidelijk.

Burgers maken weinig gebruik van het inzage- en correctierecht en van informatiebronnen over registraties van hun persoonsgegevens door onvoldoende bekendheid met mogelijkheden en feitelijkheden, zo constateren de leden vande fractie vande **PvdA**. Voor de publieke sector krijgt bewustmaking van de burger een plek in het persoonsinformatiebeleid van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Inzagerecht moet worden ondersteund door klachtrecht. Maar de regering geeft aan geen wettelijke regeling voor de private sector te willen voorschrijven, aangezien het georganiseerd bedrijfsleven en consumentenorganisaties dat beter onderling kunnen regelen. Verwacht de regering na de teleurstellende resultaten tot nu toe dat dit voldoende is voor een daadwerkelijke verbetering?

De leden van de fracties van **SGP** en **ChristenUnie** vragen of burgers naar de opvatting van de regering over voldoende, adequate, toegankelijke bezwaar- en/of beroepsmogelijkheden beschikken indien zij fouten in registraties of foutieve interpretatie van gegevens constateren, ook wanneer een geschil in deze niet tot een rechtszaak leidt.

In het kabinetsstandpunt (TK 31 051, nr. 5, p, 23) inzake het rapport van de commissie Brouwer-Korf wordt geconstateerd dat geen specifieke verplichtingen bestaan om informatie over de gebruikswijzen te verschaffen. Deze leemte doet volgens de leden van de fractie van **D66** af aan de verplichting tot transparantie. Is de regering voornemens om een dergelijke voorziening in de Wbp te introduceren?
Tevens is het kabinet voornemens om het inzagerecht te ondersteunen met een facultatief klachtrecht (p. 23). De leden van de fractie van D66 vragen zich af waarom voor een facultatieve variant van klachtrecht wordt gekozen. Waarom wordt niet voor de invoering van een algemeen klachtrecht gekozen? Is effectuering van het inzagerecht niet van dusdanig belang dat een algemene wettelijke regeling gerechtvaardigd is?

4.4. Bijzondere aandacht voor de beveiliging van persoonsgegevens

Ondanks dat zich tot nu toe geen grote problemen hebben voorgedaan wijst de regering op ernstige incidenten in het Verenigd Koninkrijk en Duitsland en op de vraag of de huidige wetgeving voldoende bescherming biedt. Naast een privaatrechtelijke sanctie als de onrechtmatige daad, dan wel strafbaarheid van overtreding van de geheimhoudingsplicht noemt de regering een aantal andere mogelijkheden zoals:
– Verzwaring van de bestaande verplichting tot dataminimalisatie, beperking van bewaartermijnen, het instellen van wettelijke opschoonverplichting;
– Het sanctioneren van de beveiligingsverplichting in de WbP;
– Een meldingsplicht voor ernstige doorbraken van beveiligingsmaatregelen.

Kan de regering aangeven of, hoe en zo ja, wanneer deze mogelijkheden zullen worden omgezet in concrete maatregelen? De leden van de fractie van de **PvdA** ontvingen graag een antwoord op deze vraag.

Beveiligingseisen worden aangescherpt. De regering denkt aan het verzwaren van de plicht tot dataminimalisatie, bijvoorbeeld door een wettelijke opschoonverplichting, of sanctioneren van de beveiligingsverplichting, gecombineerd met versterkte handhaving. Tot slot denkt de regering aan een meldplicht voor doorbraken in een beveiligingssysteem. De leden van de fractie van **GroenLinks** zijn van mening dat de dataminimalisatie, versterkte handhaving en een meldplicht voor doorbraken in een beveiligingssysteem elkaar goed aanvullen, en daarom alle drie moeten worden ingevoerd. Daarnaast zijn de leden voorstander van een periodieke hackproof bij grote systemen (ook voorafgaand aan de invoering), en bepleiten ze het minimaliseren van het aantal centrale databestanden.

4.5. Het College bescherming persoonsgegevens

4.5.1. Cbp als wetgevingsadviseur

De commissie Brouwer-Korf heeft een scheiding tussen de adviesfunctie met betrekking tot wetgeving en de toezichts- en handhavingsfunctie van het CBP bepleit. De regering heeft volgens de leden van de fractie van het **CDA** op goede gronden dit advies niet overgenomen, aangezien de Privacyrichtlijn een dergelijke adviesfunctie voor de toezichthouder voorschrijft. Is de regering echter bereid om toch in de organisatie van het CBP een vorm van scheiding tussen deze functies mogelijk te maken?

4.5.2. Toezichthoudende taak van het Cbp

De regering pielt in haar reactie op de voorstellen voor een robuuster extern toezicht, zo constateren de leden van de fractie van het **CDA**. Dit moet worden gerealiseerd door het toekennen van sancties, zoals het toepassen van bestuursdwang, het opleggen van een last onder dwangsom, alsmede het opleggen van een bestuurlijke boete. Tot op heden kan het CBP deze sancties alleen benutten bij het niet naleven van een aantal formele verplichtingen, zoals het niet naleven van de meldplicht. Is de regering van plan het in de evaluaties gemelde nalevingstekort nu te gaan bestrijden door ook ten aanzien van materiële bepalingen van de WBP dergelijke sancties mogelijk te maken?

De commissie Brouwer-Korf adviseert zorg te dragen voor robuust extern toezicht en handhaving en acht de combinatie van die taken door het CBP met adviserende en toetsende taken ongewenst. De regering heeft er begrip voor dat het CBP de maatschappelijke advisering wil laten vervallen, maar wil de algemeen informerende rol via de website en de rol als wetgevingsadviseur handhaven. De leden van de fractie van de **PvdA** hebben gerede twijfel over de aanbevolen robuustheid van het toezicht zolang versterking van het CBP in kwantitatief en kwalitatief opzicht achterwege blijft. Immers vanuit het college zelf komen regelmatig signalen in die richting, zoals onlangs in de EPD-expertmeetlng van de Eerste Kamer op 12 december 2009. Kan de regering aangeven waarom geen maatregelen in die richting zijn aangekondigd?

De regering noemt volgens de leden van de fractie van **GroenLinks** te billijken redenen voor het voorstel om de adviserende en handhavende taak te scheiden. Tegelijkertijd stelt ze dat de versterking van handhaving budgettair neutraal moet verlopen. Wat is hiervan de reden? De verwerking van persoonsgegevens heeft een enorme vlucht genomen. Dat moet gepaard gaan met een toename van middelen voor het CBP. Het op peil houden van de handhaving zou dus al meer middelen vergen, en de door de regering gewenste versterking noopt tot een extra investering. Hoe denkt de regering anders te komen tot het terugdringen van het nalevingstekort? De invoering van een bestuurlijke boete betekent immers niet dat er minder handhaving nodig is. De regering constateert dat er weinig rechterlijke uitspraken zijn, maar heeft ze onderzocht wat hiervan de oorzaken zijn? Houdt deze beperkte jurisprudentie niet ook verband met de gebrekkige informatievoorziening aan burgers over de gegevensverwerking (informatie over gegevensverwerking door veiligheidsdiensten gebeurt helemaal buiten het gezichtsveld van burgers), of met het feit dat de lage organisatiegraad van consumenten belemmerend kan werken voor de toegang tot de rechter? Is de regering bereid om te onderzoeken of de toegang tot de rechter met betrekking tot privacybescherming wel voldoende gewaarborgd is, en welke maatregelen deze toegang kunnen vergroten? En heeft de regering zicht op de rechtsbe-

scherming ten aanzien van internationale gegevensstromen, of de noodzakelijke verbeteringen daarin?
Is de regering tevreden over de rol van het College Bescherming Persoonsgegevens? Heeft de regering de indruk dat het College hier prioriteit bij legt? Wordt deze taak van het College uitgebreid, en krijgt het ook een rol bij de Privacy Impact Assessments?
De leden van de fractie van GroenLinks stemmen in met het overlaten van de invoering van klachtenregelingen door de sectoren zelf, maar vinden het onaanvaardbaar dat als een consumentenorganisatie daar niet in slaagt, de burgers in de kou staan. Waarom niet het initiatief enkele jaren aan de samenleving overlaten, maar met een horizonbepaling: vanaf 2014 wordt het wettelijk verplicht?

De leden van de fractie van **D66** constateren dat de regering een heroverweging van de taken van het College Bescherming Persoonsgegevens overweegt (p. 25–26). Hierin blijft het CBP fungeren als wetgevingsadviseur. Daarnaast wil het CBP nadrukkelijker gaan handhaven in plaats van adviseren. In dit kader merkt de regering op dat hiervoor prioritering van taken noodzakelijk is, aangezien uitbreiding van de middelen geen reële optie is. In de praktijk blijkt sprake van een nalevingstekort en behoefte aan advisering door het CBP. Deze leden vragen zich in dat licht af waarom uitbreiding van de middelen geen reële optie wordt genoemd. Begrijpen deze leden het goed dat een stevige handhaving «aan de hand van aansprekende voorbeelden» een beter nalevingsgedrag moet veroorzaken? Deze leden vragen zich af of hierbij de proportionaliteit van de handhaving niet in het geding komt. Er moet toch immers niet slechts sprake zijn van een «daad stellen» om aandacht te genereren, maar van een vaste handhavingslijn die uniform wordt toegepast.
De leden van de fractie van D66 stellen met instemming vast dat de regering de mogelijkheid overweegt om bezwaar en beroep open te stellen tegen bevindingen van het Cbp (p. 27). Dit geeft burgers en maatschappelijke organisaties de mogelijkheid om zich te mengen in de toepassing en rechtsontwikkeling van de Wbp.

4.6. Ruimhartiger vrijstellingsbeleid t.a.v. de meldplicht

Het kabinet merkt op dat de wet de mogelijkheid zou kunnen bieden bedrijven en verantwoordelijken meer vrijheid ten opzichte van de verplichtingen van de Wbp te verlenen, bijvoorbeeld door een vrijstelling van de meldplicht bij het Cbp te verlenen. Het kabinet koppelt daaraan de verplichting tot het vaststellen van een privacybeleid en het aanstellen van een functionaris voor de gegevensbescherming (FG). Het voorbeeld van de vrijstelling van de meldplicht bij het Cbp is volgens de leden van de fractie van de **VVD** ongelukkig nu al wettelijk is geregeld dat verantwoordelijken die een FG hebben aangesteld hun verwerkingen niet hoeven te melden bij het Cbp, maar dat kunnen beperken tot melden bij de FG.

4.7. Bevorderen van zelfregulering

De evaluatierapporten laten zien dat nog maar weinig gebruik wordt gemaakt van het aanstellen van een functionaris voor de gegevensbescherming (FG) of het opstellen van sectorale gedragscodes. Wanneer wel een FG is aangesteld, heeft dat een belangrijk positief effect op de kwaliteit van de gegevensbescherming binnen de organisatie. Het kabinet ambieert echter niet om het gebruik van gedragscodes of het aanstellen van FG's dwingend te gaan voorschrijven. Het kabinet ziet meer in het door middel van wetgeving stimuleren van het gebruik van deze middelen. Zien de leden van de **VVD**-fractie het verkeerd dat deze middelen al in de wet zijn opgenomen, maar desondanks toch weinig

worden toegepast? Wat gaat het kabinet doen om de toepassing te stimuleren?

Naar analogie van compliance officers bij governance wordt in het kabinetsstandpunt ter bevordering van zelfregulering gewezen op functionarissen voor de gegevensbescherming (FG) of privacy officersbij zeer grote bedrijven. De regering onderschrijft de positieve werking van het aanstellen van deze functionarissen maar wil die niet dwingend voorschrijven. Bovendien wordt gewezen op de verhouding tussen FG en toezichthouder: versteviging van de laatste mag naar de mening van de regering de positie van de interne toezichthouder niet verzwakken. Verwacht de regering dat met deze insteek voldoende tempo in het proces zal komen, gelet op de ervaringen tot nu toe met het instellen van FG's en met zelfregulering in het algemeen, inclusief corporate governance? Is niet meer druk op de private sector geboden? Zal een effectief robuust extern toezicht de positie van de interne FG niet juist versterken? De leden van de fractie van de **PvdA** ontvingen graag een reactie van de regering.

De leden van de fractie van **GroenLinks** begrijpen het voorstel om de interne controle bij bedrijven en organisaties te versterken, via de stimulans van een vrijstelling van de meldplicht of een voorafgaand onderzoek. Hiermee zou het interne toezicht en het privacy bewustzijn op de werkvloer kunnen verbeteren, wat waarschijnlijk effectiever is dan mogelijke handhaving van buitenaf. Onderkent de regering echter ook het risico dat de aanstelling van een privacyfunctionaris het verantwoordelijkheidsgevoel van andere werknemers» kan doen verminderen? Of een dergelijke «privatisering» van de privacybewaking positief te beoordelen is, hangt af van de effectiviteit. Dat zal centraal moeten staan bij een evaluatie van een dergelijke verschuiving van verantwoordelijkheden. Daarnaast zal externe druk nodig blijven om de interne alertheid in leven te houden. Denkt de regering aan een rapportageverplichting, zodat het CBP kan blijven volgen hoe het beleid wordt toegepast? Als dat tegenvalt, zou de vrijstelling moeten komen te vervallen. De leden van de fractie van GroenLinks onderstrepen de voorwaarden van de regering dat de verruiming niet in strijd is met de richtlijn en dat het de handhavingsbevoegdheden niet doorkruist.

5. Uitgeleide

In de slotparagraaf geeft de regering aan betere uitwisseling ten behoeve van veiligheid in combinatie met meer waarborgen, ondersteund door stevige handhaving als de kern van het kabinetsstandpunt te zien, naast juridische stimuleringsmaatregelen en praktische handreikingen. De leden van de **PvdA**-fractie vernemen graag van de regering een reactie op hun zorg dat diverse waarborgen voor de privacy zoals vastgelegd in de Wbp te zeer en te ongenuanceerd worden aangetast en ondergeschikt gemaakt aan de veiligheid, en in het verlengde daarvan op de verontrusting dat de compensatie voor de burger in toezicht en handhaving twijfelachtig blijft zolang de robuustheid niet beter wordt gewaarborgd en de bewustwording van professionals en burgers niet meer aandacht krijgt.

Kan de regering aangeven of en hoeverre nieuwe technologische toepassingen worden meegenomen in de beleidsontwikkeling terzake, niet alleen langs de in het kabinetsstandpunt genoemde lijnen, maar ook via meer vanuit de individuele burger opgezette toepassingen met Web 2.0? Deelt de regering de indruk dat er gebrek is aan expertise in de technologische mogelijkheden en risico's in alle lagen en sectoren van de samenleving tot in de top van de departementen? Zou de regie niet van de regering moeten uitgaan dat die kennis zou worden gebundeld en van daaruit gecommuniceerd? Is daarvoor niet een goed voorbeeld van hoe

het beter kan het «Bericht aan het Parlement» van het Rathenau Instituut van oktober 2008, een toegankelijke beschrijving van de situatie, inclusief risico cases, uitmondend in heldere beleidsmatige aanbevelingen?

De leden van de **SP**-fractie zijn benieuwd in hoeverre bestaande wetgeving en wetgeving die op dit moment in de Eerste Kamer ligt actief aan de criteria die de regering in haar reactie noemt getoetst zullen worden. De leden van de SP-fractie denken daarbij vooral aan de Wet verbetering mogelijkheden van de inlichtingen- en veiligheidsdiensten onderzoek te doen naar en maatregelen te nemen tegen» terroristische en andere gevaren met betrekking tot de nationale veiligheid (30 553). Zal de regering de grondslagen van de commissie Brouwer-Korf ook toepassen op dit wetsvoorstel? En zal het wetsvoorstel ook het eerder genoemde Privacy Impact Assessment ondergaan?

Gegeven de – op zich zelf wenselijke – samenwerking tussen de lidstaten van de Europese Unie ter bestrijding van criminaliteit en het daarmee gepaard gaande Europese informatienetwerk, vragen deze leden van de fracties van **SGP** en **ChristenUnie** of er naar de opvatting van de regering toereikende waarborgen bestaan dat registraties op de juiste rechtsgrondslag berusten en of er gesproken kan worden van een evenwaardig, uniform stelsel voor gegevensbescherming, bijvoorbeeld bij de uitwisseling van gegevens uit nationale DNA-databanken.
De leden van de fracties van SGP en ChristenUnie vragen verder, zowel met het oog op nationale als Europese voorstellen tot (verdere) uitbreiding van opsporings- en veiligheidsmaatregelen, of daarbij continu het cumulatief effect van deze maatregelen op de bescherming van de privacy in ogenschouw wordt genomen en of dit in het verleden een argument is geweest om van een geïnitieerde maatregel af te zien.

De leden van de fractie van **D66** vragen aandacht voor de beveiliging en bewaking van persoonsgegevens wanneer een bedrijf failleert. Deze leden hebben vernomen dat het voorkomt dat persoonsgegevens, na executoriale verkoop van bedrijfscomputers, in handen komen van onbevoegde derden. Bescherming van de privacy moet volgens de leden van de fractie van D66 steeds onder de aandacht blijven, ook wanneer een bedrijf onder leiding staat van een curator. Is de regering voornemens dit punt extra onder de aandacht te brengen bij de beroepsgroep?

BRIEF VAN DE MINISTER VAN JUSTITIE, MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 27 mei 2010

Bij brief van 19 februari 2010 (kenmerk 145922u) hebben de vaste commissies voor Justitie en voor Binnenlandse Zaken en de Hoge Colleges van Staat/Algemene Zaken en Huis der Koningin van uw Kamer een aantal vragen aan de regering voorgelegd over het kabinetsstandpunt ten aanzien van de bevindingen van de Adviescommissie Veiligheid en persoonlijke levenssfeer (commissie Brouwer-Korf), alsmede de evaluatierapporten van de Wet bescherming persoonsgegevens.

Namens het kabinet geef ik in deze brief mijn reactie op de door de verschillende fracties gestelde vragen. Bij de beantwoording van de vragen is de opbouw van het kabinetsstandpunt gevolgd.

1. Inleiding

De leden van de fractie van de VVD wijzen erop dat het kabinetsstandpunt pas op 3 november 2009 naar de beide Kamers is verstuurd terwijl bij de aanbieding van het onderzoeksrapport «Wat niet weet, wat niet deert. Evaluatieonderzoek Wbp» op 16 februari 2009 was aangekondigd dat het kabinet nog in het voorjaar van 2009 zou komen met een inhoudelijke reactie op de evaluatie van de Wet bescherming persoonsgegevens (Wbp) en het rapport van de Adviescommissie Veiligheid en persoonlijke levenssfeer (commissie Brouwer-Korf). Deze leden vragen naar de reden van de vertraging van de toezending van het kabinetsstandpunt.

Het kabinet heeft in zijn brief van 3 november 2009 uiteengezet hoe het te werk is gegaan bij het formuleren van zijn aanpak. Daarbij zijn niet alleen de in het standpunt genoemde rapporten gebruikt, maar is ook een aantal maatschappelijke organisaties over de te nemen maatregelen geconsulteerd. Hier bleek uiteindelijk meer tijd mee gemoeid te zijn dan oorspronkelijk was gepland.

De leden van de VVD-fractie vinden het opvallend dat het kabinet op verschillende punten zijn heil ziet in wetgeving. Deze leden vragen of nieuwe wetgeving de aangewezen weg is.

Het kabinet heeft een mix van voorstellen gedaan, variërend van nieuwe wetgeving tot praktische voorzieningen en handreikingen. De in het vooruitzicht gestelde wetsvoorstellen zijn nodig om de doelen te realiseren die het kabinet met de voorgestelde aanpak voor ogen staat, zoals een versterking van de handhaving en een vermindering van de administratieve lasten.

De leden van de PvdA-fractie hebben een aantal vragen gesteld die verband houden met de redactie van de brief van het kabinet. Deze leden constateren dat als gevolg van de opbouw van de brief passages over kernthema's op meerdere plaatsen zijn aan te treffen. In het bijzonder wijzen zij naar de verschillende passages over de introductie van een klachtrecht. Zij zien een discrepantie in de teksten en vragen het kabinet precies aan te geven wat de voornemens ter zake zijn. Daarnaast vragen zij het kabinet om een nadere omschrijving van het begrip «professional».

Het kabinet kiest voor een andere benadering van gegevensbescherming en baseert deze op een viertal kernthema's, te weten (1) meer aandacht

voor waarborgen bij de omgang met persoonsgegevens, (2) robuuster extern toezicht, (3) minder nadruk op procedures en controle vooraf, en (4) het burgerperspectief.
Deze benadering geldt in principe voor alle sectoren in de samenleving. Tegelijkertijd is het kabinet zich er van bewust dat het verzamelen en gebruiken van persoonsgegevens in het veiligheidsdomein deels leidt tot andere uitkomsten dan in andere domeinen. De rol van de burger is in dit domein wezenlijk anders dan het geval is binnen andere terreinen. Dit komt naar voren in de beperkte keuzevrijheid van de burger om zelf te kiezen of zijn persoonsgegevens worden verwerkt, maar ook in de af te wegen belangen: de overheid heeft tot taak de bescherming van de veiligheid van de burgers. Zo wordt transparantie als één van de grondslagen voor een zorgvuldige omgang met persoonsgegevens op het terrein van veiligheid op een andere manier ingevuld dan daarbuiten. In het kabinetsstandpunt wordt een onderscheid gemaakt tussen verwerkingen van persoonsgegevens binnen en buiten het veiligheidsdomein. Dit heeft tot gevolg dat een onderwerp als transparantie op meerdere plekken in de brief aan de orde komt.

Wat betreft de introductie van een klachtrecht verwijs ik graag naar paragraaf 4.3.1 van deze brief waarin de meer specifieke vragen van de leden van de PvdA-fractie over dit onderwerp worden beantwoord.
Met het begrip «professional» doelt het kabinet op die functionarissen die werkzaam zijn in de hulpverlening en in het veiligheidsdomein.

De leden van de SP-fractie zijn van mening dat in een aantal gevallen privacy en veiligheid op gespannen voet met elkaar kunnen staan, maar dat op een aantal terreinen veiligheid wel degelijk bevorderd kan worden door een goede waarborging van de privacy van burgers. Deze leden vragen of het kabinet het met haar eens is.

Ik kan deze opvatting van de SP-fractie volledig onderschrijven. In het openbare debat worden privacy en veiligheid vaak als uitersten gezien, alsof het een keuze betreft tussen het één of het ander. Dat is wat mij betreft niet het geval. Beide zijn essentiële waarden van onze rechtsstaat. Bij beide gaat het om de bescherming van de burgers. Dit uitgangspunt vormt ook de basis van het kabinetsstandpunt.

De fracties van de SGP en de ChristenUnie wijzen op een aantal trends in het sociaal-veiligheidsbeleid. Daarbij is een verschuiving zichtbaar van delict naar risico en van repressie naar voorzorg en preventie. Deze leden vragen zich af of ten aanzien van deze ontwikkeling niet een toelaatbare grens moet worden bepaald, die garandeert dat de kern van de persoonlijke levenssfeer – het recht om met rust te worden gelaten en zich van overheidswege onbespied te weten- van burgers die geen wettelijke plicht hebben geschonden, in stand blijft.

In beginsel heeft iedereen het recht met rust te worden gelaten en zich onbespied te weten. Dit recht is niet absoluut net zoals het streven naar veiligheid niet onbegrensd is. Het gaat er om dat zowel bij het werken aan veiligheid als bij de bescherming van de persoonlijke levenssfeer waarborgen voor een vrije ruimte voor de burger worden geëerbiedigd, zoals zo treffend staat verwoord in het rapport van de commissie Brouwer-Korf.

De leden van de fractie van GroenLinks constateren dat het kabinet de uitwisseling van gegevens tussen opsporing en OM en het bestuur wil vergemakkelijken zonder dat de waarborgen duidelijk zijn en zij constateren dat het kabinet meer mogelijkheden wenst voor het gebruik van gegevens voor andere doeleinden dan waarvoor de gegevens zijn

opgevraagd of bewaard. Deze maatregelen ontnemen burgers volgens de leden van deze fractie het zicht op hun gegevens, terwijl het kabinet dat juist als hoofddoel heeft aangewezen. Deze leden vragen het kabinet in te gaan op de vraag hoe de verschillende doelen zich tot elkaar verhouden en op welke wijze zij de belangen tegen elkaar heeft afgewogen.

Ik wijs er allereerst op dat het in het kabinetsstandpunt uitgesproken voornemen om een ruimere mate van het delen van gegevens tussen politie en OM enerzijds en bestuursorganen anderzijds te bevorderen nog nader moet worden uitgewerkt en dat daarbij ook aandacht wordt gegeven aan de positie van de burger in zijn hoedanigheid van betrokkene.
Dat neemt niet weg dat daarover in abstracto wel reeds iets kan worden gezegd. Het verwerken van gegevens, waaronder begrepen persoonsgegevens, moet worden aangemerkt als een normaal beleidsinstrument van de overheid. Dat het verwerken van persoonsgegevens onder omstandigheden tot een inmenging in het privé-leven kan leiden, staat niet principieel in de weg aan het gebruik van dit beleidsinstrument. Een andersluidende visie zou er immers toe leiden dat de overheid het gebruik van ICT voor haar taken principieel zou worden ontzegd. Dat geldt ook voor de omstandigheid dat de voortschrijdende technische ontwikkelingen op ICT-gebied het gemakkelijker en kosteneffectiever, dan vroeger het geval was, maken om reeds door de overheid voor uiteenlopende doelen verwerkte gegevens met elkaar in verband te brengen.
Uiteraard vergt het gebruik van dit beleidsinstrument een zorgvuldige afweging tussen de betrokken belangen. De afwegingen tussen de belangen van een rechtmatige en doelmatige uitvoering en handhaving van wettelijke voorschriften en de opsporing en vervolging van strafbare feiten enerzijds en de positie van de burger anderzijds liggen in abstracto als volgt. De overheid oefent haar taken op het eerder genoemde gebied mede uit in het belang van verwerkelijking van de grondrechten van de burgers. Daarbij gaat het onder meer om het recht op leven en het recht op vrijheid en veiligheid van de persoon van de burger. Burgers kunnen aanspraak maken op de bescherming door de overheid van deze rechten jegens hen die deze rechten door hun gedrag schenden. Het gebruik van persoonsgegevens ten behoeve van de verwerkelijking van deze rechten kan ertoe leiden dat een zekere inmenging in het privé-leven van de burger onvermijdelijk is. Dit is echter niet noodzakelijkerwijs ongerechtvaardigd, aangezien een inmenging in dat recht onder omstandigheden er juist op is gericht de burger te beschermen tegen hen die geen enkel respect tonen voor het recht op leven of veiligheid van de persoon.
Dat wil uiteraard niet zeggen dat bij de regeling van een inmenging in concreto het recht op bescherming van het privé-leven van de burger van verwaarloosbaar belang is. In concreto zal de noodzakelijke belangenafweging nader moeten worden verricht, waar nodig onder het stellen van beperkende voorwaarden bij het verwerken of verder verwerken van persoonsgegevens. In alle gevallen behoort daaraan een behoorlijke wettelijke regeling ten grondslag te liggen.
Ik zie daarvoor twee verschillende varianten. Primair zal in de daarvoor in aanmerking komende bijzondere wetgeving een zo precies mogelijke regeling moeten worden opgenomen van de doeleinden van gegevensverwerking, de voor die verwerking verantwoordelijke, en doeleinden van verdere verwerking van de verzamelde gegevens en de partijen die daartoe zijn gerechtigd. In de sociale zekerheidwetgeving en de vreemdelingenwetgeving zijn daarvan al voorbeelden aan te treffen. Ik stel mij voor dat vergelijkbare wetgeving ook tot stand kan komen op andere terreinen. Deze wetgeving wordt vastgesteld in aanvulling op en niet in afwijking van de Wet bescherming persoonsgegevens. De waarborgen van de Wbp blijven op de gegevensverwerking onverkort van kracht. Dat wil zeggen dat de voor de verwerking verantwoordelijke bestuursorganen

verplicht zijn eigener beweging aan de burger bekend te maken voor welke doeleinden zijn gegevens worden verwerkt of verder worden verwerkt. De rechten van inzage, correctie en -onder omstandigheden – verzet kunnen daarbij normaal worden uitgeoefend.
Naast de bijzondere wetgeving is het denkbaar dat ook de Algemene wet bestuursrecht wordt aangevuld met een vangnetbepaling – een regeling die geldt wanneer de bijzondere wetgever geen specifieke regeling heeft getroffen – voor de verdere verwerking van gegevens in de sfeer van de uitoefening van toezichthoudende en handhavende taken. Zoals aangegeven in het kabinetsstandpunt zal nog nadere studie naar een dergelijke mogelijkheid noodzakelijk zijn. Een dergelijke regeling zou, voor zover zij betrekking heeft op persoonsgegevens, overigens evenmin afbreuk kunnen doen aan hetgeen geregeld is in de Wbp. Transparantieverplichtingen van de overheid blijven dan ook gewoon gelden, uiteraard voor zover het niet betreft de opsporing en vervolging van strafbare feiten. Ook kunnen de rechten van inzage, correctie en – onder omstandigheden – verzet worden uitgeoefend.

2. Een nieuwe benadering van persoonsgegevens

2.1. Kernthema 1: «Gewoon doen»: meer waarborgen bij de omgang met persoonsgegevens

De vraag van de leden van de fractie van GroenLinks of het kabinet het eens is met de opvatting van deze leden dat de invulling van de privacywetgeving met materiële normen een zaak van de wetgever is, kan bevestigend worden beantwoord. Of artikel 13 van de Grondwet daarin een richtinggevende functie kan hebben, valt te bezien. Momenteel doet de staatscommissie Grondwet onderzoek naar de grondrechten in het digitale tijdperk, waarbij zij onder andere artikel 13 Grondwet betrekt. De staatscommissie Grondwet komt voor 1 oktober a.s. met haar advies.

De leden van de GroenLinks-fractie vragen of het kabinet erkent dat er zich een spanning kan voordoen bij de professional die een afweging moet maken tussen enerzijds het bereiken van zijn doelen waarvoor hij informatie nodig heeft en anderzijds de bescherming van persoonsgegevens die hij dan als een onwenselijke belemmering zal ervaren. Deze leden vragen of het kabinet bereid is om professionals hierin op te leiden en niet te wachten tot zij zelf gebruik maken van een helpdesk.

Het kabinet heeft in zijn reactie op het rapport van de commissie Brouwer-Korf en de evaluatie van de Wbp aangegeven dat een helpdesk zal worden ingericht voor professionals die zich in de praktijk geconfronteerd zien met afwegingen over veiligheid en de bescherming van de persoonlijke levenssfeer. De keuze voor een helpdesk is een uitwerking van één van de adviezen van de commissie, waarin zij aangeeft dat ondersteuning van professionals hard nodig is. Het zwaartepunt zal komen te liggen bij het ondersteunen van de professionals op -bij voorkeur- sector- of organisatieniveau. Het doel hiervan is ervoor te zorgen dat de zelfredzaamheid van organisaties of sectoren structureel toeneemt. Het verhogen van het kennisniveau van professionals vormt één van de speerpunten. Dat kan bijvoorbeeld door het stimuleren van voldoende aanbod van opleidingen. Hoe de faciliterende rol van de helpdesk precies zal worden vormgegeven, wordt momenteel uitgewerkt in een plan van aanpak dat in juni 2010 in een interdepartementaal overleg zal worden vastgesteld.

2.2. Kernthema 2: Robuuster extern toezicht

De leden van de VVD-fractie vragen zich naar aanleiding van het voornemen van het kabinet om de sanctionering van de Wbp met bestuurlijke boetes uit te breiden en het inrichten van externe klachtenregelingen te bevorderen af of de bestaande klachtenregeling niet volstaat. Deze leden vragen waarom niet meer gebruik kan worden gemaakt van het auditinstrument, zoals geregeld in de Wet politiegegevens en in de Wet GBA.

Naar aanleiding van de evaluatie van de Wbp heb ik de conclusie getrokken dat er sprake is van een nalevingstekort van de Wbp. Dat nalevingstekort uit zich op allerlei verschillende wijzen. Zo lijkt er in de afgelopen jaren slechts in een relatief gering aantal gevallen sprake te zijn van geschillen over de verwerking van persoonsgegevens die aan de rechter zijn voorgelegd. Een van de redenen daarvoor lijkt te zijn dat de verwerking van gegevens niet steeds tot op geld waardeerbare geschillen leidt, waarbij partijen een eigen afweging kunnen maken over de investering in tijd en geld die nu eenmaal is gemoeid met het voorleggen van een geschil aan de rechter. Inrichting van een laagdrempelige informele klachtprocedure kan dan een zinvol alternatief zijn voor de weg naar de rechter. In de sfeer van de overheid bestaat deze procedure al. De klachtprocedure, geregeld in hoofdstuk 9 van de Algemene wet bestuursrecht, biedt voor dit type geschillen uitkomst. Voor de private sector bestaan dergelijke geschillenregelingen nog niet in algemene zin. De gevallen waarin met toepassing van hoofdstuk 3 van de Wbp gedragscodes zijn vastgesteld, laat ik buiten beschouwing. Ik wil de inrichting van dergelijke geschillenregelingen in de private sfeer bevorderen.
De leden van de VVD-fractie wijzen terecht op de waarde van het auditinstrument. Waar de Wet politiegegevens en de Wet GBA dit instrument voor specifieke gegevensverwerkingen introduceren, beoog ik ook in de Wbp een regeling van dit instrument op te nemen, zij het niet als verplichtend instrument, maar als vrijwillige maatregel. Een partij die gebruik maakt van dit instrument zou bevrijd kunnen worden van bepaalde administratieve lasten.

De leden van de VVD-fractie wijzen erop dat privacybescherming ook wordt geëffectueerd door implementatie van beginselen en regels in techniek en organisatie, in systemen en processen en procedures. Deze leden vragen hoe het kabinet die implementatie gaat bevorderen.

In navolging van de commissie Brouwer-Korf onderstreept het kabinet het belang van privacy-by-design: bescherming door ontwerp. Privacy-by-design houdt voor het kabinet in dat risico's voor privacy en de daaraan verbonden achterliggende waarden, zoals vrijheid van meningsuiting, mobiliteit en autonomie van de burger, al vanaf het beginstadium van betekenis zijn bij het maken van afwegingen rond nieuwe wetgeving of het inrichten van systemen. Technologische ontwikkelingen bieden vervolgens kansen om waarborgen voor een correct gebruik van persoonsgegevens vorm te geven bij de inrichting van systemen.
Het uitvoeren van Privacy Impact Assessments is een concrete mogelijkheid om privacyrisico's bij de ontwikkeling van nieuw beleid of nieuwe systemen te identificeren. Het College bescherming persoonsgegevens heeft (mede) het initiatief genomen om de methodiek van Privacy Impact Assessments te ontwikkelen. Het streven is dat dit model nog deze zomer gereed is.

De leden van de VVD-fractie vragen het kabinet toe te lichten wat de onafhankelijke toezichthouder kan doen voor een burger op het moment dat een verantwoordelijke op een onjuiste manier met zijn gegevens omgaat.

Burgers kunnen bij het College bescherming persoonsgegevens (Cbp) een klacht indienen over een organisatie die onzorgvuldig met hun persoonsgegevens omgaat. Zij kunnen het Cbp ook vragen te bemiddelen. De ervaring leert dat een rapport van bevindingen vaak voldoende is om een klacht naar tevredenheid af te ronden. Volgt de verantwoordelijke het advies van het Cbp niet op dan kan de burger de zaak aan de rechter voorleggen. Daarnaast wil het kabinet de totstandkoming van sectorspecifieke klachtregelingen stimuleren.

2.3. Kernthema 3: Minder nadruk op procedures en controle vooraf

De leden van de CDA-fractie vragen of het kabinet bereid is bij de voorbereiding van nieuwe wetgeving de lijst te hanteren die in het verslag van de expertmeeting door de leden van deze fractie is genoemd.

Ik kan mij voor het overgrote deel goed vinden in de criteria die gehanteerd kunnen worden bij de voorbereiding van regelgeving waarin gegevensverwerking als beleidsinstrument is opgenomen, zoals voorgesteld door de leden van de CDA-fractie in het verslag van de expertmeeting waarop deze leden doelen (Kamerstukken I 2007/08, 31 200 VI, F). Op het Ministerie van Justitie wordt gewerkt aan de totstandkoming van een leidraad voor het afstemmen van wetgeving op de Wbp. In die leidraad zal worden verwezen naar de criteria die door deze leden zijn voorgesteld, met de aantekening daarbij dat de Eerste Kamer aan de desbetreffende punten bijzondere aandacht pleegt te schenken bij de beoordeling van de haar voorgelegde wetsvoorstellen. Ten aanzien van één criterium kan ik de leden van de CDA-fractie niet volledig volgen. Het lijkt mij, niet alleen uit het oogpunt van het belang van gegevensverwerking, maar ook uit het oogpunt van verstandig wetgevingsbeleid, geen vanzelfsprekendheid dat elk wetsvoorstel waarin gegevensverwerking als beleidsinstrument regeling vindt een horizonbepaling moet bevatten. Dat zou inhouden dat na verloop van tijd elke wet waarin gegevensverwerking wordt geregeld door enkel tijdsverloop zijn gelding verliest. Daartegen bestaan bezwaren. Te denken valt aan de naleving van Europeesrechtelijke verplichtingen. Verder vergt gegevensverwerking doorgaans de nodige investeringen in ICT-voorzieningen. Die investeringen zijn niet lonend wanneer de rechtsgrondslag voor het gebruik daarvan vervalt. Ook kan het routinematig gebruik van horizonbepalingen leiden tot een overmatig beroep op de wetgevingscapaciteit van ministeries. Het komt mij voor dat een goed doordacht gebruik van evaluatieverplichtingen een zinvol alternatief vormt voor het criterium dat door de leden van de CDA-fractie is voorgesteld.

2.4. Kernthema 4: Het burgerperspectief

De leden van de CDA-fractie merken op dat het kabinet verscherping van de beveiliging van persoonsgegevens als voorgenomen maatregel vermeldt. Deze leden vragen aan welke aanpak het kabinet hierbij denkt. Zij vragen of wordt overwogen de beveiligingsverplichting uit de Wbp met strafsancties te gaan handhaven.

In paragraaf 4.4 van het kabinetsstandpunt is uiteengezet welke aanpak van de verscherping van de beveiligingsplicht mij voor ogen staat. Ik zie daarvoor drie mogelijke maatregelen. In de eerste plaats kan een verplichting tot dataminimalisatie worden overwogen. Dat zou in concreto

een aanpassing van artikel 10 van de Wbp kunnen betekenen. Een alternatief daarvoor zou kunnen zijn dat de overheid, bedrijven en instellingen in het kader van hun transparantieverplichtingen expliciet aandacht moeten schenken aan bewaartermijnen en het lot van persoonsgegevens na afloop van de bewaartermijn. Een opschoonverplichting zou een aanvullende maatregel kunnen zijn. Een keuze uit deze maatregelen zal ik maken na overleg met de daarvoor in aanmerking komende partijen.
In de tweede plaats kan het naleven van de beveiligingsverplichting worden gesanctioneerd met een punitieve sanctie. Die keuze komt wat mij betreft nadrukkelijk in beeld, omdat de sanctionering van de materiële bepalingen in de Wbp hoe dan ook een van de centrale wetgevingsvoornemens uit het kabinetsstandpunt is. Ik denk daarbij overigens niet aan strafrechtelijke, maar aan bestuursrechtelijke sancties, op te leggen door het College bescherming persoonsgegevens, zulks in overeenstemming met de kabinetsnota «keuze sanctiestelsels» (Kamerstukken I 2008/09, 31 700 VI, D).
In de derde plaats zal er een meldplicht voor ernstige doorbraken van beveiligingsmaatregelen worden opgenomen in de Wbp. Dit heb ik reeds toegezegd aan de Tweede Kamer in het algemeen overleg dat op 3 februari 2010 plaatsvond naar aanleiding van het kabinetsstandpunt.

De leden van de fractie van GroenLinks constateren dat het kabinet het gebrek aan recht op inzage bij veiligheid wil compenseren door toezicht van een instantie of rechterlijke toetsing achteraf. Deze leden hebben een aantal vragen over hoe dit in de praktijk gestalte zal krijgen.

Het is inderdaad zo dat het belang van de veiligheid met zich mee kan brengen dat in voorkomende gevallen geen volledige transparantie naar de burger kan worden gegeven over de verwerking van zijn persoonsgegevens. Wanneer dit het geval is, is het van groot belang dat de zorgvuldigheid en rechtmatigheid van deze verwerking kunnen worden gewaarborgd. Ik wil daarbij opmerken dat de verwerking en bescherming van persoonsgegevens niet optimaal worden gewaarborgd wanneer er uitsluitend een toetsing achteraf plaatsvindt.
Het is tevens van belang dat toezicht voorafgaand en tijdens de verwerking van persoonsgegevens plaatsvindt.
In het kabinetsstandpunt worden drie toezichtvormen genoemd. Deze zijn iteratief van aard.
Allereerst vind ik het van belang dat de rol van de externe toezichthouder wordt verstevigd. Dit uitgangspunt is dan ook een kernthema van het standpunt. In de brief zijn verschillende maatregelen aangekondigd die de handhavingsmogelijkheden van het Cbp versterken. Onafhankelijk toezicht vindt ook plaats door de Commissie van Toezicht betreffende de Inlichtingen- en veiligheidsdiensten (CTIVD). Ten tweede heb ik in de brief aangegeven dat een zorgvuldige verwerking van persoonsgegevens zeer gediend is met de inrichting van intern toezicht. Intern toezicht ziet op de dagelijkse kwaliteit van de afwegingen die door de professionals in de praktijk worden gemaakt. Binnen het veiligheidsdomein is intern toezicht ook daadwerkelijk ingericht. Een voorbeeld hiervan is de aanwezigheid van privacy officers bij de verschillende politiekorpsen.
Tot slot noem ik de rechterlijke toetsing van de verwerking van persoonsgegevens. Wanneer gegevens worden uitgewisseld of verwerkt, kan door de rechter achteraf de rechtmatigheid van de verwerking worden getoetst. Wanneer sprake is van een onrechtmatig gebruik, kan dit onder andere leiden tot bewijsuitsluiting of het niet-ontvankelijk verklaren.

De leden van de fractie van GroenLinks onderschrijven de informatieplicht maar constateren dat burgers er zelf achteraan moeten gaan om te weten te komen wat er met hun gegevens gebeurt. Deze leden vragen of de overheid dan wel het bedrijfsleven de burger niet meteen op de hoogte

zou moeten stellen van de mogelijke verwerking van zijn gegevens, en hoe dat te volgen is.

De Wet bescherming persoonsgegevens geeft betrokkenen een inzage-, en correctierecht (artikel 35 en 36 Wbp). In artikel 33 en 34 van de Wet bescherming persoonsgegevens is tevens de informatieplicht geregeld. De informatieplicht schrijft voor dat de burger actief geïnformeerd dient te worden bij doorgifte van gegevens aan derden.
Het inzage-, en correctierecht voor de Gemeentelijke Basisadministratie is apart geregeld in de wet GBA (artikel 79 en 82 Wet GBA). De burger kan bij zijn gemeente inzage verzoeken om te zien welke persoonsgegevens zijn verwerkt in de GBA en andere gemeentelijke registers. Tevens kan de burger zijn gemeente verzoeken een schriftelijk bewijs af te geven van de opgeslagen persoonsgegevens in de GBA. Dit schriftelijke bewijs is het zogeheten *afschrift.* De burger heeft tevens het recht zijn gemeente te vragen waar eventuele persoonsgegevens vandaan komen in het geval de burger deze gegevens niet zelf heeft verstrekt. Indien van toepassing kan de burger zijn gemeente verzoeken tot correctie, aanvulling, geheimhouding of verwijdering van de gegevens die zijn opgeslagen in de GBA.

De overheid bevordert de transparantie naar de burger toe op vele manieren. Mede door middel van het gebruik van internet. Op de website www.burgerservicenummer.nl kan de burger zien welke organisaties welke soort gegevens uitwisselen met behulp van het burgerservicenummer (BSN). Via www.mijnoverheid.nl wordt voor de burger inzichtelijk gemaakt hoe bepaalde gegevens zijn opgenomen in de GBA. Ook kan de burger een aantal gegevens raadplegen die het kadaster en de RDW over hem hebben opgeslagen. Niet alle gegevens van deze overheidsorganisaties zijn al via mijnoverheid.nl voor de burger ontsloten. De reden hiervoor is dat het technisch nog niet mogelijk is om al deze gegevens te ontsluiten. Mijnoverheid.nl levert daarmee een bijdrage aan de transparantie voor de burger.
De leden van de GroenLinks-fractie vragen of het kabinet bereid is om het idee van een laagdrempelig loket uit te werken.

Binnen de overheid zijn er reeds diverse loketten ingericht om vragen ten aanzien van persoonsgegevens te beantwoorden.
- Burgers kunnen terecht bij het College bescherming persoonsgegevens voor uitleg over de Wet bescherming persoonsgegevens, o.a. door het raadplegen van de website www.mijnprivacy.nl.
- Burgers kunnen zich in eerste instantie wenden tot de gemeente bij vragen over registratie in de GBA.
- Burgers kunnen daarnaast te allen tijde terecht bij elk overheidsorgaan (anders dan de gemeentelijke dienst) om te vragen hoe zij voor hun eigen organisatie en doeleinden persoonsgegevens verwerken.
- Naast de website www.burgerservicenummer.nl bestaat er ook een BSN-punt. Bij het BSN-punt kunnen burgers terecht met vragen over de omgang met het BSN en wanneer er een fout wordt geconstateerd in het BSN of in daaraan gekoppelde gegevens.
- Postbus 51 vervult een belangrijke rol ten aanzien van identiteitsfraude. Sinds december 2008 is het Centraal Meldpunt Identiteitsfraude (CMI) opgericht. De doelstelling van het CMI is burgers die te maken hebben met identiteitsfraude of met een fout in de registratie van persoonsgegevens hulp te bieden, te adviseren en te informeren. Ook wordt door het CMI aan de burger informatie verstrekt over hoe identiteitsfraude zoveel mogelijk kan worden voorkomen.

3. Veiligheid en persoonsgegevens

3.1. Het richtinggevend kader van de Adviescommissie Veiligheid en persoonlijke levenssfeer

De leden van de CDA-fractie vragen of het kabinet de op verschillende plaatsen in het rapport van de Commissie-Brouwer-Korf bepleite versterking van het intern toezicht op gegevensbescherming steunt en deze aanpak ook concreet zal stimuleren.

De aanbeveling van de Commissie Brouwer-Korf om het interne toezicht op de gegevensverwerking te versterken kan ik onderschrijven. Ook uit de evaluatierapporten van de Wbp blijkt dat wanneer een bedrijf of instelling is overgegaan tot de aanstelling van een functionaris voor de gegevensbescherming het bewustzijn van de noodzaak van gegevensbescherming en het niveau van die bescherming toenemen. Toch blijkt ook dat de drempel voor het aanstellen van een functionaris voor de gegevensbescherming vrij hoog is. Dat valt waarschijnlijk terug te voeren op de formele positie die deze functionaris heeft. Ik overweeg daarom om in de Wbp naast de regeling voor de functionaris voor de gegevensbescherming alternatieve toezichtsmechanismen te gaan regelen. Er zou dan gedacht kunnen worden aan een privacyfunctionaris zonder specifieke bevoegdheden, aan het toepassen van privacy-audits of het toepassen van Privacy Impact Assessments. Inzet van een of meer van deze instrumenten zou op vrijwillige basis kunnen plaatsvinden in ruil voor meer vrijheid ten opzichte van verplichtingen van de Wbp. Introductie van dergelijke systemen zal echter alleen kunnen plaatsvinden wanneer maatschappelijke partijen en het Cbp zich daarin kunnen vinden.

De leden van de SP-fractie vragen of het kabinet de door de commissie geformuleerde grondslagen voor een zorgvuldige omgang met persoonsgegevens onderschrijft en welke concrete stappen worden gezet om deze grondslagen ook in de praktijk meer handen en voeten te geven.

Het kabinet onderschrijft de grondslagen van het richtinggevend kader die de commissie heeft ontworpen. In de kabinetsreactie heeft het kabinet aangegeven op welke wijze het kabinet deze wil toepassen, onder andere door het ontwikkelen en uitvoeren van Privacy Impact Assessments en de inrichting van een helpdesk.

De leden van de fractie van GroenLinks zijn van mening dat de door het kabinet uitgesproken noodzaak om gegevens tussen overheidsinstellingen uit te wisselen afhankelijk wordt gemaakt van twee bedrieglijk eenvoudige criteria, zijnde de concrete dreiging jegens de veiligheid van een individu en de zekerheid dat informatie-uitwisseling deze dreiging kan wegnemen. Deze leden vragen wat moet worden verstaan onder een concrete dreiging, wat moet worden verstaan onder veiligheid en hoe moeten worden beoordeeld of informatie-uitwisseling de dreiging kan wegnemen. Zij vragen of een nadere invulling van deze criteria nodig zal zijn, en of die invulling niet van de wetgever moet komen. Zij vragen verder of dit niet een breuk vormt met het doelbindingsbeginsel dat het kabinet zegt te willen handhaven.
De leden van de fractie van de PvdA wijzen in dit verband op het standpunt van prof. mr. E.J. Dommering die heeft gesteld dat het hoofdbeginsel van het richtinggevend kader van de commissie Brouwer-Korf: «als het nodig is voor de veiligheid moet je delen», zonder nadere afweging de bijl zet aan het kernbeginsel van de doelbinding.

Deze vragen van de leden van de fractie van GroenLinks geven mij aanleiding in te gaan op de formulering van artikel 9 van de Wbp. In dat

artikel is een algemene regeling neergelegd van de zogeheten verdere verwerking van persoonsgegevens. Onder verdere verwerking van persoonsgegevens wordt verstaan het verwerken van persoonsgegevens voor een ander doel dan het doel waarvoor zij oorspronkelijk zijn verzameld. Verdere verwerking van persoonsgegevens wordt door artikel 9 van de Wbp zeker niet principieel uitgesloten. Integendeel, de hoofdregel van die bepaling komt erop neer dat de verantwoordelijke voor een bepaalde verwerking zelf moet beoordelen of een bepaalde verdere verwerking verenigbaar of onverenigbaar is met het voor de oorspronkelijke verwerking geformuleerde doel. Dat is dus geen uitzondering op het doelbindingsbeginsel, maar juist een regeling die – ook in zijn huidige formulering – beoogt om een maatschappelijk volstrekt noodzakelijke flexibiliteit aan te brengen bij de verwerking van persoonsgegevens. De wetgever heeft de verantwoordelijke een aantal criteria meegegeven om die beoordeling te maken. Die criteria zijn open en abstract geformuleerd, en moeten door de verantwoordelijke nader worden ingevuld. Dit type normstelling is in de context van de Wbp overigens normaal. De Wbp beoogt immers een regeling te bieden voor een onbepaald aantal verwerkingen van persoonsgegevens van de meest uiteenlopende soorten. Een dergelijke regeling moet noodzakelijkerwijs open en abstract geformuleerd zijn.
Naast de vorenbedoelde hoofdregel kent artikel 9 van de Wbp nog twee andere regels, namelijk een verruiming van de mogelijkheden voor verdere verwerking voor doeleinden verband houdend met historische, statistische en wetenschappelijke doeleinden en een verbod op de verwerking (en verdere verwerking) van persoonsgegevens wanneer een geheimhoudingsplicht uit hoofde van wet, ambt of beroep daaraan in de weg staat.

Een aanvulling van artikel 9 Wbp met een afzonderlijke grondslag voor de verdere verwerking van persoonsgegevens ten behoeve van de veiligheid van het individu zou, nog los van de concrete formulering van een dergelijke grondslag, eerder als een verduidelijking en nadere concretisering van een reeds bestaande regeling moeten worden gezien, dan als een vage, voor velerlei uitleg vatbare constructie, waarvoor de leden van de GroenLinks-fractie wellicht vrezen. Een dergelijke constructie moet twee problemen oplossen. In de eerste plaats moet duidelijk zijn dat er een rechtvaardiging moet bestaan voor de verstrekking van persoonsgegevens, bijvoorbeeld wanneer het vitaal belang van een betrokkene dat vergt. In de tweede plaats moet duidelijk zijn dat bij de inroeping van dat belang in concreto een bestaande geheimhoudingsplicht buiten toepassing kan blijven.

Uiteraard is de aanvulling van artikel 9 Wbp te zijner tijd zaak voor de wetgever, zoals ook in het overzicht van de kabinetsvoornemens is aangegeven, dat als bijlage[1] bij het standpunt is gevoegd. Bij eerdere gelegenheden, onder meer bij de aanbieding van het rapport van de werkgroep «Herijking toezichtsregelgeving» (Kamerstukken II 2008/09, 31 700, VI, nr. 70), heb ik reeds aangegeven dat er alle aanleiding kan zijn om in bijzondere regelgeving, in aanvulling op de Wbp, terzake een nadere regeling te treffen. Een dergelijke nadere regeling biedt het voordeel dat deze beter kan worden toegesneden op de doeleinden van gegevensverzameling en verdere verwerking.

3.2. Evenwicht tussen bescherming van persoonsgegevens en veiligheid: een tweevoudige bescherming

De leden van de fractie van D66 hebben een aantal vragen gesteld tegen de achtergrond van de lopende maatschappelijke discussie over de registratie van herkomstgegevens en van levensovertuiging. De leden van

[1] Ter inzage gelegd op de afdeling Inhoudelijke ondersteuning onder griffie nr. 145922.01

de VVD-fractie vragen wanneer de door het kabinet hierover toegezegde brief kan worden verwacht.

Het kabinet heeft de Tweede Kamer toegezegd een standpunt over registratie van herkomst te formuleren. Het voortouw voor dit standpunt ligt bij de Minister voor Wonen, Wijken en Integratie. De kern van de vraag is of het huidige kader van wetten en regelingen enerzijds voldoende ruimte biedt om verwerking van bijzondere persoonsgegevens over etnische herkomst mogelijk te maken als dit noodzakelijk is voor het uitvoeren van beleid op het gebied van zorg, hulpverlening, bestrijding van criminaliteit en overlast door leden van specifieke groepen en, anderzijds voldoende waarborgen biedt om aantasting van de privacy en stigmatisering op grond van herkomst te voorkomen. Het huidige demissionaire kabinet zal geen standpunt over dit onderwerp meer innemen.

Ter voorbereiding van het toegezegde kabinetsstandpunt is er onder twintig gemeenten een verkenning gehouden naar de noodzakelijkheid van registratie van herkomst in de uitvoeringspraktijk. De uitkomsten van deze verkenning zijn gereed en zullen worden betrokken bij een eventueel door een nieuw kabinet te formuleren standpunt.
Daarnaast bestaat er bij burgemeesters van enkele grote steden de behoefte aan nadere voorzieningen om ook bijzondere persoonsgegevens te kunnen registreren als middel tegen radicalisering en polarisatie. Thans wordt door het Ministerie van BZK verkend of, en zo ja onder welke voorwaarden, de Verwijsindex Risicojongeren ook bruikbaar is op het terrein van polarisatie en radicalisering.

3.3. Selecteer voor je verzamelt

De leden van de fracties van de PvdA en GroenLinks vragen het kabinet om de grondslag «selecteer voor je verzamelt en houd het sober» nader uit te werken en aan te geven hoe deze grondslag in de praktijk zal worden geëffectueerd.

In het model voor een Privacy Impact Assessment zullen nadere criteria worden opgenomen die behulpzaam zijn bij de toepassing van deze grondslag in een concrete situatie.

3.4. Transparantie

De leden van de fractie van de PvdA constateren dat individuele burgers terecht komen in talloze databanken waarvan de identiteit en locatie niet te achterhalen zijn, hetgeen de controle op opslag, kwaliteit en verwerking van persoonsgegevens vrijwel onmogelijk maakt.

Deze leden vragen zich af of het kabinet het bestaan van de websites als www.burgerservicenummer.nl en www.mijnoverheid.nl voor een adequate transparantie voor de burger afdoende acht. Voorts zijn deze leden benieuwd welke aanvullende maatregelen het kabinet ziet, met inbegrip van nieuwe technologische mogelijkheden als Web 2.0.

Ten aanzien van de vraag of genoemde websites afdoende zijn om transparantie te bieden voor de burger kan het volgende worden opgemerkt. Via de website www.mijnoverheid.nl kan de burger een aantal van zijn GBA-gegevens inzien. Ook kan de burger een aantal gegevens raadplegen die het kadaster en de RDW van hem of haar hebben opgeslagen. Niet alle gegevens van deze organisaties zijn via deze website voor burger ontsloten. De reden hiervoor is dat het technisch nog niet mogelijk is om al deze gegevens te ontsluiten.

Ten aanzien van het gebruik van Web 2.0 is het kabinet in beginsel positief gestemd. Het kabinet verkent daarom de mogelijkheden hiervan, onder andere om de interactie met burgers te kunnen verbeteren. Het kabinet is zich er echter terdege van bewust dat Web 2.0 nog geen gemeengoed is in onze samenleving. Hoewel een steeds groter wordende groep burgers de mogelijkheden van Web 2.0 al weet te benutten, is er nog steeds een grote groep burgers die daar niet toe in staat is. Het kabinet vindt het daarom op dit moment niet opportuun om concrete Web 2.0 toepassingen in te zetten in het kader van verbeteren van de transparantie rond het gebruik van persoonsgegevens.

3.5. Integriteit van systemen: privacybescherming door ontwerp

3.5.1. Privacy Impact Assessments

De leden van de fracties van CDA en SP vragen het kabinet hoe een Privacy Impact Assessment eruit zal gaan zien. De leden van de VVD-fractie vragen of het kabinet voornemens is daarbij gebruik te maken van reeds door het College bescherming persoonsgegevens ontwikkelde toetsen. De leden van de GroenLinks-fractie pleiten ervoor de uitkomsten van een assessment openbaar te maken, zodat iedereen ze kan benutten bij commentaar op ontwerpwetgeving.

Een Privacy Impact Assessment (PIA) heeft tot doel zoveel mogelijk effecten op de persoonlijke levenssfeer te identificeren bij het ontwikkelen van nieuwe regelgeving of van nieuwe systemen. Het hanteren van een PIA verschaft inzicht in de aanwezige risico's of eventuele nadelige effecten van voorgenomen regelgeving of systemen.

Het is van belang om dit inzicht in een vroegtijdig stadium te verkrijgen, zodat al meteen met risico's en nadelige gevolgen rekening kan worden gehouden, waar dat mogelijk is. Het kabinet wil bevorderen dat de uitvoering van een PIA onderdeel wordt van de praktijk.

Zoals ik paragraaf 2.2 in antwoord op vragen van de VVD-fractie aangaf, heeft het College bescherming persoonsgegevens het initiatief genomen om samen met een aantal partners, waaronder VNO-NCW, een model PIA te maken. Het streven is om dit model nog deze zomer gereed te hebben.

Het kabinet is niet van plan om het gebruik van PIA's verplicht te stellen. Wel wil het kabinet de verantwoordelijken stimuleren om zelf voorafgaand aan een verwerking de risico's daarvan in een PIA te onderzoeken, deze risico's zelf openbaar te maken en daarbij aan te geven welke maatregelen zij hebben genomen om deze risico's weg te nemen.

3.5.2. Kentekenherkenning met camera's (ANPR)

De leden van de PvdA-fractie vragen het kabinet op welke wijze bij de toepassing van gegevens als voorzien in het wetsvoorstel tot *wijziging van onder meer boek 2 van het Burgerlijk Wetboek en de Wet documentatie vennootschappen in verband met het vervallen van de verklaring van geen bezwaar en het verbeteren en uitbreiden van de controle op rechtspersonen met het oog op de voorkoming en bestrijding van misbruik van rechtspersonen* (Kamerstukken I 2009/10, 31 948, A) methoden worden toegepast als privacy by design en op welke wijze bij de voorziene toepassing van dit wetsvoorstel rekening wordt gehouden met de impact van gegevensverwerking op de persoonlijke levenssfeer van betrokkenen en het voorkomen van de risico's die voortvloeien uit het gebruik van vervuilde bestanden.

Ik geef er de voorkeur aan de vragen die specifiek betrekking hebben op het door de leden van de PvdA-fractie genoemde wetsvoorstel te beantwoorden bij gelegenheid van de memorie van antwoord. Het is mij niet ontgaan dat de leden van deze fractie in het door de Kamer uitgebrachte verslag over dat wetsvoorstel dezelfde vragen hebben gesteld.

De leden van de fracties van SGP en ChristenUnie constateren dat cameratoezicht in het publieke domein een hoge vlucht heeft genomen en dat de neiging tot uitbreiding continu aanwezig lijkt. Deze leden vragen welke doeleinden het kabinet bij de toepassing van automatische kentekenherkenning voor ogen staat.

Automatische kentekenherkenning (ANPR) is een programma waarmee camera's worden gebruikt om kentekens van voertuigen vast te leggen. Het vastleggen van deze kentekens gebeurt met het doel deze te vergelijken met een vooraf samengesteld selectiebestand. In dit selectiebestand staan kentekens die nader onderzoek behoeven.
De politie zet ANPR in voor de handhaving van de openbare orde en de opsporing van strafbare feiten. Daarbij maakt zij gebruik van vergelijkingsbestanden van gesignaleerde personen, gestolen voertuigen en openstaande boetes. De politie zet ANPR tevens in bij de aanpak van de drugsrunnersproblematiek en de bestrijding van mobiel banditisme.
ANPR wordt ook toegepast door andere overheidsinstanties. De belastingdienst gebruikt ANPR-gegevens voor controle op diverse belastingen. De VROM-inspectie past ANPR samen met de politie toe bij controles op afvaltransporten. De Inspectie Verkeer en Waterstaat gebruikt ANPR voor controle van het taxivervoer en voor controle op rij- en rusttijden. Rijkswaterstaat gebruikt ANPR voor het in kaart brengen van verkeersstromen.

De leden van de fractie van GroenLinks vragen naar de kenbaarheid van het gebruik van ANPR en de wijze waarop de burgers worden geïnformeerd over (het doel van) de verwerking van hun kenteken.
Daarnaast vragen deze leden naar de reden waarom het College bescherming persoonsgegevens (Cbp) niet in het ANPR platform vertegenwoordigd is en wat het advies van het Cbp is over de wettelijke grondslag.

Het kabinet streeft naar een meer uniforme toepassing van ANPR. Praktische voorzieningen zoals automatische opschoning, uniformiteit van programmatuur, autorisatieniveaus en voorlichting aan het publiek, inclusief de mogelijkheid tot inzage, zullen nader worden geregeld.

Het Cbp neemt geen deel aan het ANPR platform om potentiële rolconflicten te voorkomen.
Het Cbp heeft zijn zienswijze over de huidige wettelijke grondslag van het gebruik van ANPR door de politie neergelegd in richtsnoeren. In deze richtsnoeren geeft het Cbp aan dat automatische kentekenherkenning op grond van de Wet politiegegevens voor de uitvoering van de dagelijkse politietaak onder voorwaarden mag worden toegepast. Alleen de «hits»(dat zijn de kentekens die in de automatische vergelijking leiden tot een match met een kenteken in het vergelijkingsbestand) mogen worden bewaard.

De leden van de fracties van CDA en D66 hebben vragen gesteld over het voornemen van het kabinet om een specifiek wettelijk kader voor ANPR tot stand te brengen.

Mijn ambtsvoorganger van Binnenlandse Zaken en Koninkrijksrelaties en ik hebben onze voornemens ten aanzien van het wettelijk kader voor ANPR nader uiteengezet in een brief aan de Tweede Kamer (Kamerstukken II 2009/10, 31 051, nr. 6). Deze brief is vervolgens aan de orde geweest in het eerder genoemde Algemeen overleg van 3 februari jl. Wij hebben bij die gelegenheid toegelicht dat voorrang zal worden gegeven aan het opstellen van een wettelijke regeling voor het gebruik van ANPR voor de strafrechtelijke handhaving en voor bepaalde toepassingen in de bestuursrechtelijke sfeer. In dit traject zullen nog keuzes worden gemaakt ten aanzien van de specifieke doeleinden, de te bewaren categorieën van gegevens en de te hanteren bewaartermijnen. Ik streef ernaar dit wetsvoorstel kort na de zomervakantie bij de Tweede Kamer in te dienen.

3.6. Gegevensuitwisseling en veiligheid: een kwestie van belang

De leden van de CDA-fractie vragen welke wijziging van artikel 9 van de Wbp de regering voor ogen staat om in het belang van de veiligheid een grotere mate van koppeling van systemen mogelijk te maken. Zij vragen aan te geven of het doelbindingsprincipe, als een van de hoofdlijnen van de EU-richtlijn, met een dergelijke constructie geen geweld wordt aangedaan.

Voor het antwoord op deze vraag verwijs ik de leden van de CDA-fractie graag naar het antwoord dat ik gaf op de gelijkluidende vraag van de leden van de fractie van GroenLinks.

De leden van de CDA-fractie hebben een aantal vragen gesteld over, wat zij noemen de relativering van het doelbindingsbeginsel. Zij vragen of de regering zich ervan bewust is dat de relativering van dit beginsel steeds de term veiligheid wordt gebruikt om tot een uitbreiding van de overheidsbevoegdheden te komen, terwijl dit stapsgewijs leidt tot een inperking van de fundamentele rechten van de burger – het recht op bescherming van de persoonlijke levenssfeer daaronder met name begrepen. Deze leden stellen dat deze bevoegdheidsuitbreiding en beperking van rechten in toenemende mate leidt tot irritatie bij de burger en een groeiend wantrouwen jegens de overheid. Deze leden wijzen in dit verband op een aantal lopende ontwikkelingen, zoals de verzameling van passagiersgegevens, de bewaarplicht van verkeersgegevens, cameratoezicht, rekeningrijden, het elektronisch kinddossier en het elektronisch patiëntendossier. Deze leden vrezen dat door de stapeling van deze maatregelen burgers in toenemende mate zullen proberen deze verwerkingen te ontgaan en de overheid controlemogelijkheden zullen willen ontzeggen. Naar deze leden stellen ziet de burger de proportionaliteit van deze maatregelen niet meer. Zij vragen het kabinet dan ook hoe het denkt overtuigend te kunnen opereren zodat er een voldoende draagvlak voor nieuwe maatregelen zal blijven bestaan.

Waar het op neerkomt is dat als gevolg van de voortschrijding van de technische ontwikkelingen op ICT-gebied de verwerking van persoonsgegevens gemakkelijker, kosteneffectiever, en inderdaad ook grootschaliger kan plaatsvinden dan een decennium geleden. Burgers en bedrijfsleven profiteren daarvan bij het realiseren van hun eigen ontplooiingsmogelijkheden. Dat de technische ontwikkelingen ook leiden tot een uitbreiding van de mogelijkheden tot verdere verwerking van persoonsgegevens is daaraan inherent. Dat leidt op zichzelf nog niet tot de slotsom dat daarmee het doelbindingsbeginsel voorwerp van verregaande relativering is geworden. Het leidt er wel toe dat de betekenis en uitwerking van het doelbindingsbeginsel in het licht van de lopende herziening van het Europese kader voor gegevensbescherming aandacht verdient. De vraag is vervolgens wat de houding van de overheid – die immers zorgdraagt

voor de verwerkelijking van grondrechten, waaronder ook het recht op bescherming van de persoonlijke levenssfeer – moet zijn ten opzichte van die nieuwe mogelijkheden. Ik zie in de omstandigheid dat het op de weg van de overheid ligt om zorg te dragen voor de verwerkelijking van grondrechten van de burgers geen principiële reden om af te zien van hetgeen de techniek te bieden heeft. Integendeel, zou dat worden nagelaten, en zou de overheid het gebruik van ICT moeten worden ontzegd, dan zou de overheid juist tekortschieten bij de vervulling één van haar kerntaken, de verwerkelijking van grondrechten.
Daaraan is ook een Europese dimensie verbonden. Als richtlijn nr. 95/46/EG een ruimte van vrij gegevensverkeer binnen de Europese Unie creëert, waarvan burgers en bedrijven dagelijks profiteren, is het niet meer dan passend dat de Europese Unie in de sfeer van de rechtshandhaving het beschikbaarheidsbeginsel hanteert als uitgangspunt bij de regulering van de gegevensstromen binnen de EU.
De optimale garantie van deze grondrechten van het recht op leven en het recht op veiligheid van de persoon, kan onder omstandigheden een inmenging in het privé-leven van de burger vergen. Daarbij moet worden bedacht dat de overheid bescherming beoogt te bieden tegen de activiteiten van individuen die zich doorgaans weinig gelegen laten liggen aan de waarden die tot uitdrukking worden gebracht in de grondrechten op leven, veiligheid van de persoon én bescherming van het privé-leven. Dit alles doet niets af aan de verplichting die voortvloeit uit het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en de Grondwet om bij inmengingen in het privé-leven zorg te dragen voor een solide wettelijke grondslag die voldoet aan de eisen van kenbaarheid en voorzienbaarheid, en een overtuigende toets van de voorziene inmenging aan de noodzaak in een democratische samenleving in een van de in het EVRM genoemde doelen en de beginselen van proportionaliteit en subsidiariteit. Dat zal moeten gebeuren op ieder afzonderlijk onderwerp waarbij gegevensverwerking aan de orde is als instrument van overheidsbeleid. Dergelijke onderwerpen zullen zich in de nabije toekomst veelvuldig voordoen. De opsomming van onderwerpen in de vragen van de leden van de CDA-fractie geeft al aan dat dit het geval is. Ik ontken ook niet dat het op sommige van deze onderwerpen lastig is gebleken een voor eenieder overtuigende motivering van voorstellen te formuleren. Het blijft ook in de komende jaren een uitdaging dit goed te blijven doen. Anders dan de leden van de CDA-fractie neem ik echter geen toenemende neiging onder brede lagen van de samenleving waar om gegevensverwerkingen te ontgaan of zich daartegen te verzetten.

De leden van de VVD-fractie hebben enige vragen over de voorgenomen uitbreiding van artikel 9 van de Wbp. Zij vragen wat de status wordt van het expliciteren van de mogelijkheid om gegevens ten behoeve van de veiligheid te kunnen delen. Deze leden vragen voorts of er een algemene maatregel van bestuur of ministeriële regeling zal worden vastgesteld en of het kabinet van plan is beide Kamers bij de voorbereiding daarvan te betrekken.

Voor het antwoord op deze vraag verwijs ik de leden van de VVD-fractie allereerst graag naar het antwoord dat ik gaf op de gelijkluidende vraag van de leden van de fractie van GroenLinks. In aanvulling op dat antwoord kan ik deze leden geruststellen. Een aanvulling van artikel 9 van de Wbp zal op het niveau van de formele wet plaatsvinden. Het ligt niet in mijn bedoeling om dat te doen in de vorm van het vaststellen van een delegatiegrondslag om een en ander op het niveau van de algemene maatregel van bestuur of ministeriële regeling te regelen.

De leden van de fracties van SGP en ChristenUnie vragen of het kabinet de opvatting deelt dat de afweging tussen privacy en andere belangen in laatste instantie een politieke, rechtsstatelijk te verantwoorden beslissing behoort te zijn. Daarnaast stellen zij vragen over de effectiviteit van moderne technologie (o.m. DNA) die wordt ingezet voor opsporings- en veiligheidsdoeleinden, alsmede of de inzet van die middelen voldoet aan de doelstelling die voor ogen stond bij de invoering ervan.

Ik kan de opvatting van de leden van de fracties van SGP en ChristenUnie in dezen onderschrijven.
De inzet van moderne technologie past binnen het (voortdurend) streven om de kwaliteit van het werk van de politie, i.c. door technologische vernieuwingen, te optimaliseren. Het is tegen de achtergrond van de inzet van (extra) middelen, maar ook in relatie tot de inbreuk die bepaalde maatregelen op de privacy kunnen hebben, van belang om te weten of de beoogde effecten, zoals grotere effectiviteit en efficiency, ook inderdaad wordt bereikt. Door begeleiding met evaluatief onderzoek van de invoering van nieuwe technologieën, alsmede van bestaande praktijken, kan worden gewaarborgd dat in de praktijk zoveel mogelijk kansrijke, effectieve methoden worden toegepast.
Specifiek over DNA is een onderzoek «Sporen met DNA» uitgevoerd, dat bij brief van 25 juni 2008 is aangeboden aan de Voorzitter van de Tweede Kamer (TK 2007-2008, 31 415, nr. 2). Dit onderzoek was gericht op de effecten van de wettelijke verruiming van de mogelijkheden van DNA-onderzoek in strafzaken die met ingang van 1 november 2001 in werking was getreden. Op andere terreinen vonden en vinden er eveneens dergelijke onderzoeken plaats.

De leden van de fracties van SGP en ChristenUnie vragen met betrekking tot datamining in hoeverre er waarborgen bestaan dat beschikbare data betrouwbaar zijn en of het kabinet het wenselijk acht om een strikte begrenzing aan te brengen wat betreft de bevoegdheden van opsporingsdiensten om gegevens bij derden te vorderen.

Ik acht een begrenzing van de bevoegdheden van opsporingsdiensten wenselijk en ik kan de leden van de fracties van SGP en ChristenUnie in die zin geruststellen dat het Wetboek van Strafvordering ook grenzen stelt, te weten in de artikelen 126 nc tot 126 ni. Voor het vorderen van gegevens bij derden in het kader van een verkennend onderzoek bij terrorisme geldt een aparte regeling in artikel 126 hh Sv.

3.6.1. Verbetering informatie-uitwisseling bij multidisciplinaire samenwerking

De leden van de PvdA-fractie vragen het kabinet naar aanleiding van een opsomming van maatregelen die illustreren hoe informatie-uitwisseling bij multidisciplinaire samenwerking kan worden verruimd en de concrete bepalingen in deze maatregelen aan te wijzen waarin de privacywaarborgen zijn opgenomen.

Er zijn verschillende manieren om in een regeling of maatregel de privacy van degene wiens gegevens worden verwerkt, te waarborgen. Dat kan door middel van wetgeving gebeuren, bijvoorbeeld op de manier die is voorgesteld in het meergenoemde rapport van de Werkgroep herijking toezichtregelgeving. Dat kan door in de maatregel zelf regels op te nemen waarbinnen informatie-uitwisseling vorm kan krijgen, zoals bijvoorbeeld een convenant.

Een voorbeeld is het bestuurlijk akkoord inzake de geïntegreerde decentrale aanpak van de georganiseerde misdaad. Dit akkoord beschrijft expliciet het geldende juridische kader voor gegevensuitwisseling, waaronder de relevante bepalingen uit de Wet politiegegevens (art. 20), de Wet bescherming persoonsgegevens (art. 8 sub e en f, en art. 9) en specifieke bepalingen uit de Algemene wet inzake rijksbelastingen. Daarnaast is bij het bestuurlijk akkoord ook nog een «checklist waarborging naleving Wet bescherming persoonsgegevens regionaal samenwerkingsverband» gevoegd.

Een apart geval is de voorgenomen wijziging van artikel 13 van het Besluit justitiële gegevens. Daarmee wordt beoogd bestuursorganen die een besluit moeten nemen dat onder de werking van de Wet BIBOB valt, in staat te stellen justitiële gegevens op te vragen met betrekking tot een aanvrager van een vergunning of subsidie. Thans is die mogelijkheid nog beperkt tot de verlening van vergunningen op grond van een beperkt aantal wetten, waaronder de Drank- en Horecawet. Het betreft dus een uitbreiding van deze bevoegdheid naar alle branches die onder de Wet BIBOB vallen of komen te vallen. Met deze maatregel wordt beoogd dat bestuursorganen sneller een besluit kunnen nemen en in gevallen waarin op basis van justitiële gegevens een vergunning moet worden geweigerd dat wordt gedaan zodat niet meer dan noodzakelijke informatie over de vergunningaanvrager en zijn zakelijk samenwerkingsverband wordt ingewonnen. Eenzelfde doel heeft het verstrekken van strafvorderlijke informatie door het Openbaar Ministerie. Dat is, onder in de wet en richtlijnen van het Openbaar Ministerie genoemde voorwaarden in alle gevallen mogelijk, behoudens de gevallen waarin de Wet BIBOB van toepassing is.

De leden van de PvdA-fractie wijzen op het wetsvoorstel *wijziging van onder meer boek 2 van het Burgerlijk Wetboek en de Wet documentatie vennootschappen in verband met het vervallen van de verklaring van geen bezwaar en het verbeteren en uitbreiden van de controle op rechtspersonen met het oog op de voorkoming en bestrijding van misbruik van rechtspersonen* (Kamerstukken I 2009/10, 31 948, A). Deze leden menen dat familieleden of andere naasten van bestuurders van rechtspersonen geen gebruik kunnen maken van de bevoegdheid de juistheid van de gegevens over hen in het databestand te verifiëren, omdat zij simpelweg geen weet hebben van de omstandigheid daarin voor te komen. Deze leden vragen wat de mening van het kabinet daarover is. Zij vragen op welke wijze deze groep burgers gebruik kan maken van zijn privacyrechten krachtens de Wbp.

Ik geef er de voorkeur aan de vragen die specifiek betrekking hebben op het door de leden van de PvdA-fractie genoemde wetsvoorstel te beantwoorden bij gelegenheid van de memorie van antwoord. Het is mij niet ontgaan dat de leden van deze fractie in het door de Kamer uitgebrachte verslag over dat wetsvoorstel dezelfde vragen hebben gesteld.

De leden van de fractie van de PvdA vragen het kabinet een nadere toelichting te geven op de grondslagen en richtingen van de Informatie Management Strategie (IMS) die in het kader van het Stockholm programma is ontwikkeld.

Het IMS staat voor een strategie voor het beheer van rechtshandhaving-informatie die de bevoegde autoriteiten nodig hebben om de interne veiligheid van de EU te waarborgen. Deze strategie beoogt niet te bepalen welk soort informatie moet worden opgeslagen en/of uitgewisseld, maar voorziet in een methode (het «hoe») om ervoor te zorgen dat besluiten over de noodzaak van het beheren en uitwisselen van gegevens en

besluiten over de manieren om dat te doen, worden genomen op een coherente, professionele, efficiënte en kosteneffectieve wijze die begrijpelijk is voor de burgers en de professionele gebruikers. Onderdeel van deze strategie is dat nieuwe operationele behoeften inzake gebruik en uitwisseling van informatie samen beoordeeld moeten worden met de juridische eisen voor bescherming van persoonsgegevens en voor beveiligingsnormen. Andere eisen zijn dat adequate maatregelen inzake gegevensbescherming daadwerkelijke en regelmatige operationele controles moeten inhouden en bij inbreuken moeten zorgen voor passende sancties die effectief worden opgelegd. Verder betekent deze strategie dat er mechanismen voor systematische evaluatie en systematisch toezicht moeten worden ontwikkeld om de kwaliteit en het effect van de gegevensbeschermings- en gegevensbeveiligingsmaatregelen te beoordelen.

Het IMS is op 30 november 2009 door de JBZ-Raad aanvaard. Er is nu een actieplan in uitvoering die dit proces van de nodige instrumenten moet voorzien. Eén daarvan is de ontwikkeling van een dataprotectie impact assessment voor dit domein.

De leden van de GroenLinks-fractie houden het kabinet voor dat het in Europees verband zegt te streven naar optimalisering van de voorwaarden voor informatie-uitwisseling, waarvoor aanpassing van de EU-privacyrichtlijn nodig is. Deze leden vragen het kabinet preciezer aan te geven op welke wijze zij de privacyrichtlijn aangepast zou willen zien. Zij vragen of de regering met bedoelde optimalisering een versoepeling van de voorwaarden voor ogen heeft. Deze leden vragen verder of het kabinet nog steeds van mening is dat het doelbindingscriterium moet worden heroverwogen en zo dat het geval is, wat daaronder dan moet worden verstaan. Zij vragen voorts of het kabinet heeft overwogen wat de gevolgen zouden kunnen zijn van een verruiming van het doelbindingscriterium of andere voorwaarden voor de rechtsbescherming van burgers, vooral in andere lidstaten waar de controle op de verwerking van gegevens nog minder goed is geregeld dan in Nederland. Zij vragen het kabinet dan ook of het met deze leden van mening is dat dit criterium een van de weinige waarborgen is voor een zorgvuldige omgang van hun gegevens en de kennis van wat er met hun gegevens gebeurt. Zij vragen het kabinet tenslotte of het bereid is te pleiten voor een alomvattende richtlijn die ook ziet op het gebied van justitie en politie.

Inderdaad ben ik van oordeel dat de mogelijkheden tot het uitwisselen en delen van gegevens binnen de sfeer van de overheid in Nederland en binnen de EU tussen de overheden van de lidstaten een belang is dat thans onvoldoende zelfstandig tot uitdrukking komt in richtlijn nr. 95/46/EG. Ik heb er daarom bij de Nederlandse inbreng voor de herziening van de richtlijn voor gepleit dat dit belang te zijner tijd afzonderlijke erkenning krijgt. Ik heb er daarbij op gewezen dat ik dit juist van belang acht in verband met de bescherming van grondrechten, maar dat ik daarbij steeds van mening ben dat een inmenging in het grondrecht op bescherming van het privé-leven een adequate wettelijke (of Europeesrechtelijke) grondslag behoeft die vergezeld gaat van een behoorlijke toets aan het EVRM en het Handvest van de grondrechten. Uiteraard ben ik bereid mijn inbreng terzake te overleggen. Bijgaand[1] treft u deze aan. Ik heb niet het standpunt ingenomen dat het doelbindingscriterium moet worden her*overwogen*. Gebruik van het woord «heroverweging» wekt ten onrechte de suggestie dat dit criterium zou kunnen worden afgeschaft. Dat bepleit ik niet. Wat ik wel heb bepleit in de Nederlandse bijdrage voor het Stockholm-programma is her*oriëntatie* van het doelbindingscriterium (Kamerstukken I 2008/09, 23 490, ER, bladzijde 6).

[1] Ter inzage gelegd op de afdeling Inhoudelijke ondersteuning onder griffie nr. 145922.01

De EU is volgens artikel 67, eerste lid, van het Verdrag betreffende werking van de Europese Unie (VWEU) één ruimte van veiligheid, vrijheid en recht, waarin de grondrechten van de lidstaten worden geëerbiedigd. Dat betekent in mijn visie dat gegevens die zijn verzameld ten behoeve van rechtshandhavingsdoeleinden in beginsel steeds moeten kunnen worden uitgewisseld met andere lidstaten uit de Europese Unie, wanneer in een andere lidstaat de behoefte aan het ontvangen van de desbetreffende gegevens wordt uitgesproken in verband met andere rechtshandhavingsdoeleinden. Voorwaarde daarbij is dat er dan wel sprake moet zijn van een adequaat niveau van gegevensbescherming, passend bij de aard van de desbetreffende gegevens. Dat kan een algemene regeling zijn, zoals bijvoorbeeld richtlijn nr. 95/46/EG of kaderbesluit nr. 2008/977/JBZ. Dat kan ook een specifieke regeling zijn, zoals bijvoorbeeld kaderbesluit nr. 2009/315/JBZ met betrekking tot inlichtingen uit de strafregisters.
Die heroriëntatie van het doelbindingsbeginsel komt hierop neer dat niet behoeft te worden aanvaard dat het voor de overheden op nationaal én op Europees niveau moeilijker zou moeten zijn dan het voor bedrijven en burgers is om onderling gegevens uit te wisselen. Wel geldt onder alle omstandigheden dat er een behoorlijke wettelijke of Europeesrechtelijke grondslag moet zijn, wil gegevensuitwisseling aanvaardbaar zijn. Als die grondslag er is, dan hoeft niet te worden gevreesd voor een tekortschietend niveau van gegevensbescherming in Nederland en in het land van bestemming van de gegevens. Ook overigens wijs ik de leden van de fractie van GroenLinks erop dat de gelding van richtlijn nr. 95/46/EG en kaderbesluit nr. 2008/977/JBZ garandeert dat in de hele EU sprake is van een adequaat niveau van gegevensbescherming, met inbegrip van onafhankelijk toezicht en rechtsbescherming.
Het is niet juist te suggereren dat het doelbindingscriterium één van de weinige waarborgen is voor de verantwoorde verwerking van persoonsgegevens. Het is juist één van de vele waarborgen, naast andere waarborgen als de transparantieverplichting, de rechten van inzage en correctie en toezicht en rechtsbescherming.
Ik ben zeker niet op voorhand tegenstander van een richtlijn gegevensbescherming die zich mede uitstrekt over de gegevensverwerking in de sectoren rechtshandhaving, opsporing en strafvervolging. Ik wacht terzake met grote belangstelling eventuele voorstellen van de Europese Commissie af.

3.6.2. Vergemakkelijken uitwisseling toezichtgegevens tussen toezichthouders, politie en OM

De leden van de fracties van CDA, PvdA en GroenLinks hebben een groot aantal vragen gesteld over het voornemen om de uitwisseling van gegevens tussen toezichthouders, politie en OM te verbeteren. De leden van de CDA-fractie vragen hoe het kabinet denkt dit te verwezenlijken. Zij vragen of een wijziging van de Algemene wet bestuursrecht daartoe noodzakelijk is. Zij vragen verder aan welke waarborgen wordt gedacht om te voorkomen dat de onderlinge koppeling van gegevensbestanden tussen deze organen zal leiden tot een wat deze leden aanduiden als «immutable me».

De leden van de fractie van de PvdA vragen het kabinet aan te geven welke vraagstelling zij voornemens is mee te geven aan de adviseurs uit wetenschappelijke kring bij het verkennen van de mogelijkheid tot formulering van een vangnetbepaling in de Algemene wet bestuursrecht.

De leden van de fractie van GroenLinks kijken met belangstelling uit naar de adviezen van wetenschappers over de mogelijkheid voor het formuleren van een vangnetbepaling voor de uitwisseling van toezichtgegevens in de Awb. Zij achten dit op het eerste gezicht in tegenspraak met de

stelling van het kabinet dat de rechtspositie van de burgers met betrekking tot privacy moet worden verbeterd. Zij spreken huiver uit ten aanzien van een dergelijke vangnetbepaling. Zij vragen of de regering wel voldoende inzicht heeft in de onbedoelde (neven) effecten van een dergelijke regeling. Zij verzoeken het kabinet dan ook bij de uitwerking van dit idee nader te bezien wat de noodzakelijke reikwijdte zou moeten zijn en hoe wordt voorzien in verplichte motivering, toetsingscriteria, weigeringsgronden en waarborgen voor de burgers. Zij gaan er bovendien vanuit dat een dergelijk voorstel wordt voorzien van een Privacy Impact Assessment.

Van de overheid in zijn hoedanigheid als toezichthouder en rechtshandhaver verwacht de samenleving steeds meer dat deze zijn taken effectief en efficiënt uitvoert op een wijze die burgers en bedrijven die niets valt te verwijten zo min mogelijk belast. Dat brengt met zich dat toezichthouders, bestuursorganen, politie en OM gedwongen zijn samen te werken. Er is in dit opzicht geen andere keuze. Het gaat dan niet om samenwerkingsverbanden van toezichthouders, bestuursorganen, politie en OM voor het overige slechts te laten werken met de informatiepositie die zij op grond van de bestaande wetgeving bezitten. Dat is zinloos. Een en andermaal is gebleken dat met name geheimhoudingsbepalingen aan informatie-uitwisseling in de weg kunnen staan. Gebleken is ook dat wettelijke maatregelen noodzakelijk zijn om die geheimhoudingsplicht te doorbreken en dat deze noodzakelijk zijn om een samenwerkingsverband effectief te laten functioneren. Ik wijs in dit verband nogmaals op het eerdergenoemde rapport van de werkgroep Herijking toezichtregelgeving, waarin voorstellen zijn opgenomen voor de structurering van dergelijke wetgeving.
Aan dit rapport heb ik twee conclusies verbonden (Kamerstukken II 2008/09, 31 700 VI, nr. 70). De eerste is dat wanneer een samenwerkingsverband bestaat dat een voldoende bestendig karakter heeft, in de desbetreffende bijzondere wetgeving een op dat samenwerkingsverband betrekking hebbende regeling over de onderlinge gegevensoverdracht kan worden geregeld. Zulke regelingen bestaan reeds in de sociale zekerheidswetgeving en in de vreemdelingenwetgeving. Het opzetten van een dergelijke regeling doet op geen enkele manier afbreuk aan de waarborgen die gelden krachtens de Wbp, of, voor zover van toepassing, de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens. Die waarborgen blijven gewoon gelden. Laatstbedoelde wetten bevatten overigens al op samenwerkingsverbanden waarin politie en OM participeren toegesneden bepalingen.
De tweede conclusie is dat het zinvol is verder na te denken over de mogelijkheid om de Algemene wet bestuursrecht (Awb) – waarin reeds een uitgebreide regeling van het toezicht op de naleving is opgenomen – aan te vullen met een bepaling die de informatiebetrekkingen van toezichthouders onderling regelt, ook in hun relatie tot politie en OM. Juist omdat hieraan nogal wat consequenties zijn verbonden is nader onderzoek nodig naar deze mogelijkheid, voordat kan worden besloten tot de opstelling van een wetsvoorstel. De beslissing om daartoe over te gaan is nog niet genomen. Er kan daarom niet worden vooruitgelopen op de vormgeving van een dergelijke regeling. Daarvoor is nader onderzoek nodig. In het kabinetsstandpunt zijn als aandachtspunten reeds genoemd dat bijzondere geheimhoudingsplichten is de sfeer van de belastingheffing en het financieel toezicht afzonderlijke aandacht vragen. Hetzelfde geldt voor de omvang en de reciprociteit van de gegevensverstrekking tussen bestuursorganen en toezichthouders enerzijds en politie en OM anderzijds. Ook de internationale aspecten vragen aandacht. Een opdracht tot onderzoek is thans nog niet verstrekt.
Wat de waarborgen betreft, geldt wat mij betreft dat de Wbp en de overige gegevensbeschermingswetten onveranderd blijven gelden.

Daarbij moet wel worden opgemerkt dat een regeling in de Awb niet noodzakelijkerwijs beperkt blijft tot een regeling over de overdracht van persoonsgegevens. Een regeling in de Awb zou primair gericht zijn op toezichtinformatie. Dat valt niet noodzakelijkerwijs samen met persoonsgegevens en is ook niet noodzakelijkerwijs in alle opzichten grondrechtgerelateerd.

De leden van de fractie van de VVD geven aan dat het uitwisselen van informatie niet vanzelfsprekend verbetert als dit in wetgeving wordt vastgelegd.

Het kabinet onderschrijft in het algemeen deze stelling. Immers, problemen met betrekking tot informatie-uitwisseling zitten veeleer in de toepassing van vigerende wet- en regelgeving dan in de regels zelf. In dit verband breng ik de reactie van 30 augustus 2007 van de toenmalige Minister van Binnenlandse Zaken en Koninkrijksrelaties in herinnering op het rapport van de Adviescommissie Informatiestromen Veiligheid (TK 2006–2007, 30 800 VI en VII, nr. 65). Daarin is nogmaals benadrukt dat de inlichtingen- en opsporingsdiensten, naar gelang het proces waarin zij werkzaam zijn (inlichtingen, opsporing, calamiteitenbestrijding, ordehandhaving etc.) onderscheiden taken en bevoegdheden hebben en elk vanuit hun eigen verantwoordelijkheid informatie inwinnen en uitwisselen. Dit stelsel is bewust niet gecentraliseerd maar gesegmenteerd zodat verschillende informatiesoorten zorgvuldig worden behandeld en er recht wordt gedaan aan de verschillende taken en verantwoordelijkheden van de betrokken partijen.

3.7. Organiseren van facilitering, voorlichting en educatie

De leden van de fracties van de VVD en de PvdA hebben een aantal vragen gesteld over de inrichting van de helpdesk. De leden van de fractie van de VVD vragen of het kabinet bereid is de Eerste Kamer inzage te geven in het plan van aanpak.

De verschillende vragen die de leden van de fracties van de VVD en de PvdA hebben gesteld over de voorgenomen opzet en inrichting van een helpdesk zullen in het plan van aanpak worden geadresseerd. Ik zal de Eerste Kamer inzage geven in dit plan van aanpak, waarvan de vaststelling in juni 2010 is voorzien.

4. Bescherming van persoonsgegevens op andere terreinen dan veiligheid

4.1. Normering en toekomstbestendigheid van de Wbp

De leden van de PvdA-fractie vragen, onder verwijzing naar de passages in het kabinetsstandpunt met betrekking tot RFID, biometrie en internettoepassingen wat het kabinet voornemens is vanuit een integrale aanpak te ondernemen tegen de risico's van voortschrijdende technologische ontwikkelingen, mede binnen Europees kader.

Ten aanzien van de ontwikkelingen waarop de leden van de PvdA-fractie doelen is thans wel zoveel duidelijk dat deze op de langere termijn de begrippen en de uitgangspunten van richtlijn nr. 95/46/EG zullen gaan beïnvloeden. Op dit moment is echter nog onvoldoende duidelijk in welke richting die ontwikkelingen zullen gaan en welke consequenties voor de bescherming van persoonsgegevens daaraan verbonden zijn. Gegeven deze situatie ben ik niet in staat om op dit moment al een afgeronde visie op deze uitdagingen te geven. Gebleken is dat ook bij de Europese Unie een dergelijk eindbeeld nog niet bestaat. Het Europese niveau is echter

wel het niveau waarop het antwoord op deze uitdagingen zal moeten worden geformuleerd. Gegeven het wereldomvattende niveau van deze uitdagingen zal de Europese Unie er niet aan kunnen ontkomen oplossingen te formuleren die rekening houden met de manier waarop in de Verenigde Staten en Azië tegen deze ontwikkelingen wordt aangekeken.

4.2. Het belang van een privacybewuste burger

De leden van de fractie van de PvdA vragen welke maatregelen het kabinet voor ogen staan om het privacybewustzijn van de burger te vergroten.

De Postbus 51-campagne «Veilig internetten heb jezelf in de hand» waaraan de leden van de PvdA-fractie refereren is buitengewoon succesvol gebleken en zal om die reden dit jaar worden herhaald. Daarnaast wordt het publiek met enige regelmaat gewezen op het belang om veilig met reisdocumenten om te gaan en met DigiD.
Naast voorlichting wil het kabinet het privacybewustzijn van de burger vergroten door in samenwerking met onze maatschappelijke partners voorwaarden te scheppen voor het inrichten van eenvoudig toegankelijke klachtprocedures.

4.3. Transparantie

4.3.1. Inzage- en correctierecht

De leden van de fractie van de VVD vragen het kabinet om een toelichting te geven over wat persoonsinformatiebeleid inhoudt.

Het persoonsinformatiebeleid behelst het beleid ten aanzien de opslag en verwerking van persoonsgegevens in de publieke sector. Dit beleid richt zich op het gebruik van persoonsgegevens bij dienstverlening en de uitvoering van taken in de publieke sector waarbij het doel is zorgvuldig om te gaan met persoonsgegevens van de burger en te komen tot een efficiënte inrichting van overheidsorganisaties waarbij de burger zo optimaal mogelijk wordt bediend.

De leden van de PvdA-fractie wijzen erop dat het kabinet voorstander is van het ondersteunen van het inzagerecht door een klachtrecht. Het kabinet, aldus deze leden, geeft echter aan geen wettelijke regeling voor de private sector te willen voorschrijven, omdat het georganiseerd bedrijfsleven en consumentenorganisaties dit beter onderling kunnen regelen. Deze leden vragen of het kabinet verwacht dat dit voldoende is, nu gebleken is dat de resultaten van zelfregulering teleurstellend zijn geweest.

Wat de inrichting van een klachtrecht door bedrijven betreft, geef ik inderdaad de voorkeur aan een vrijwillig georganiseerde inbedding van dat recht. Daarvoor bestaan verschillende argumenten. Een wettelijke verplichting om een dergelijk klachtrecht in te richten leidt onvermijdelijk tot een bepaalde bemoeienis van de wetgever met interne organisatie en werkwijze van ondernemingen. Een dergelijke verplichting is belastend van aard voor het bedrijfsleven. Daarmee moet zeer terughoudend worden omgegaan. Dat geldt nog sterker wanneer er, zoals thans, sprake is van economische omstandigheden die het bedrijfsleven toch al onder druk zetten. Voor een dergelijke bemoeienis is bovendien alleen ruimte als dat gerechtvaardigd is uit hoofde van een zeer zwaarwegend maatschappelijk belang, of als dat zou voortvloeien uit dwingende eisen van internationaal of Europees recht. Hoe belangrijk de bescherming van

gegevens ook is en hoe belangrijk de rol van een klachtenregeling ook kan zijn, aan deze criteria wordt niet voldaan.
Verder moet worden bedacht dat een wettelijke vormgeving van het klachtrecht een vrij gecompliceerde aangelegenheid kan zijn. Het is onvermijdelijk dat daarbij rekening wordt gehouden met de schaalgrootte van ondernemingen.
Een multinationale onderneming met duizenden personeelsleden en een goed ingerichte concernstaf is doorgaans beter geëquipeerd dan een kleine onderneming met weinig personeelsleden om een klachtrecht daadwerkelijk inhoud te kunnen geven. Kleine ondernemingen zouden zich dan weer verplicht moeten aansluiten bij een door een collectiviteit in stand gehouden klachtrecht.
Waar ik mij op wil richten is dat zoveel mogelijk ondernemingen gaan beseffen dat gegevensbescherming voor hun eigen functioneren van belang kan zijn en dat het inrichten van een klachtprocedure juist gericht is op het voorkomen van rechtsgeschillen die de verhoudingen met personeelsleden of klanten onder druk zetten.
Juist omdat het in het verleden inderdaad aan weerklank heeft ontbroken bij de inrichting van vrijwillig georganiseerd privacyrecht, wil ik ondernemingen via positieve prikkels stimuleren over te gaan tot het instellen van een klachtregeling. Het ontheffen of vrijstellen van administratieve lasten als de meldplicht is daartoe een mogelijk middel.

De leden van de fracties van SGP en ChristenUnie vragen of burgers naar de opvatting van het kabinet over voldoende adequate en toegankelijke bezwaar- en beroepsmogelijkheden beschikken indien zij fouten in registraties of foutieve interpretatie van gegevens constateren, ook wanneer een geschil niet tot een rechtszaak leidt.

Op grond van de huidige wetgeving kunnen burgers de rechten van inzage en van correctie inroepen wanneer zij een beeld willen verkrijgen van de gegevens die in een concrete verwerking zijn opgenomen, respectievelijk wanneer zij menen dat hen betreffende gegevens onjuist worden verwerkt. Daarnaast hebben burgers de mogelijkheid om een geschil over de verwerking van persoonsgegevens via relatief eenvoudige procedures aan de rechter voor te leggen. Die laatste weg leidt niet altijd tot een bevredigend resultaat. Er zijn bovendien kosten mee gemoeid, vooral wanneer de weg van de civiele procedure moet worden gevolgd. De uitkomst van een dergelijke procedure zal, gegeven de aard van een geschil over de bescherming van persoonsgegevens, niet altijd bevredigend zijn. Schade die is geleden is bij de foutieve verwerking van persoonsgegevens is niet altijd goed in geld waardeerbaar. Ik ben daarom van oordeel dat inrichting van een laagdrempelige klachtprocedure of andere buitengerechtelijke geschillenregeling hier meer kan oplossen dan een gang naar de rechter. Jegens de overheid heeft de burger natuurlijk al het klachtrecht volgens de Algemene wet bestuursrecht. Dat klachtrecht kan worden ingeroepen bij klachten over verwerking van persoonsgegevens door de overheid.

De leden van de fractie van D66 constateren dat in het rapport van de Commissie Brouwer-Korf wordt opgemerkt dat er geen specifieke verplichtingen bestaan om informatie over de gebruikswijzen van persoonsgegevens te verschaffen. Volgens deze leden doet dat af aan de werking van de transparantieverplichting. Zij vragen of het kabinet voornemens is een dergelijke voorziening in de Wbp op te nemen. Verder vragen deze leden zich af waarom voor een facultatieve variant van het klachtrecht wordt gekozen en niet voor een algemeen klachtrecht. Zij vragen of effectuering van het inzagerecht niet van zodanig gewicht is dat een algemene wettelijke regeling gerechtvaardigd is.

Het is inderdaad zo dat richtlijn nr. 95/46/EG en de Wbp geen specifieke verplichtingen voor verantwoordelijken bevatten om openbaarheid te geven aan alle varianten van het gebruik van verzamelde persoonsgegevens.
Wel bevat artikel 33, derde lid, van de Wbp de verplichting voor de verantwoordelijke om, met inachtneming van de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, zodanige nadere informatie te verschaffen aan de betrokkene dat een behoorlijke en zorgvuldige verwerking ten opzichte van hem gewaarborgd is. Dit is een voorschrift dat, wanneer het goed wordt nageleefd, een redelijke last op de verantwoordelijke legt en waaraan de betrokkene de nodige houvast kan ontlenen.
Wat wel aandacht verdient is het verschijnsel «profiling». Op basis van een analyse van op zichzelf rechtmatig verzamelde persoonsgegevens worden door tal van bedrijven en instellingen indelingen van betrokkenen in categorieën gemaakt. Op grond van die indeling kunnen bepaalde beslissingen door de verantwoordelijke worden voorbereid en genomen, bijvoorbeeld het gericht adverteren. Ik spreek mij niet principieel uit tegen deze vormen van gegevensverwerking, maar ik ben wel van oordeel dat zoveel mogelijk openheid over deze verwerkingen moet worden gegeven. Ik ben dan ook voornemens de Wbp aan te vullen met een uitbreiding van de transparantieverplichting terzake.
Wat de vragen van de leden van de D66-fractie met betrekking tot de inrichting van het klachtrecht betreft, verwijs ik deze leden graag naar de antwoorden die ik hierboven gaf op gelijkluidende vragen van de leden van de PvdA-fractie.

4.4. Bijzondere aandacht voor de beveiliging van persoonsgegevens

De leden van de PvdA-fractie wijzen op een aantal maatregelen die het kabinet in het vooruitzicht stelt. Het betreft de verzwaring van de bestaande verplichting tot dataminimalisatie, beperking van bewaartermijnen en in het instellen van een wettelijke opschoonverplichting; het sanctioneren van de beveiligingverplichting in de Wbp en een meldplicht voor ernstige doorbraken van beveiligingsmaatregelen. Zij vragen of deze maatregelen zullen worden ingevoerd, en zo ja, wanneer dit zal gebeuren.

De twee laatstgenoemde maatregelen, het sanctioneren van overtreding van de beveiligingsplicht in de Wbp met een bestuurlijke boete en het opleggen van een meldplicht voor ernstige doorbraken van beveiligingsmaatregelen zullen worden ingevoerd. Daartoe is wetgeving noodzakelijk. Ik streef ernaar die wetgeving nog dit jaar aan de ministerraad te kunnen voorleggen. De andere genoemde maatregelen verdienen nog een nadere analyse uit oogpunt van uitvoerbaarheid en handhaafbaarheid. Ik heb daarvoor behoefte aan verder overleg met maatschappelijke partners en advies van het Cbp. Het ligt wel in mijn bedoeling om, wanneer de nodige keuzes zijn gemaakt, in hetzelfde wetsvoorstel als hierboven bedoeld de nodige voorzieningen op te nemen.

De leden van de fractie van GroenLinks geven aan dat zij voorstander zijn van invoering van alle door het kabinet voorgestelde maatregelen op het gebied van de beveiliging van persoonsgegevens. Verder bepleiten deze leden een periodieke «hackproof» bij grote systemen, ook voorafgaand aan de invoering, en bepleiten zij het minimaliseren van het aantal centrale databestanden.

Ik verheug mij over de steun die de leden van de fractie van GroenLinks uitspreken over de voorgenomen maatregelen. Wat het voorstel om een periodieke «hackproof» van systemen voor te schrijven betreft, meen ik dat dit voor vele vormen van gegevensverwerking een bijzonder zinvolle

maatregel is. Het belang van een dergelijke maatregel is zo groot dat ik met instemming kan constateren dat vele bedrijven en instellingen dit reeds eigener beweging doen. Een wettelijke verplichting daartoe lijkt mij dan ook niet nodig. Het minimaliseren van centrale databestanden is iets waarover ik alleen in de sfeer van de overheid iets kan zeggen. Ik moet erop wijzen dat het instellen van centrale databestanden ook uit het oogpunt van beveiliging van persoonsgegevens ook positief te waarderen kan zijn. Schaalvergroting schept immers de mogelijkheid om meer te investeren in betere beveiligingsmaatregelen.

4.5. Het College bescherming persoonsgegevens

4.5.1. Cbp als wetgevingsadviseur

De leden van de CDA-fractie constateren met instemming dat het kabinet op goede gronden niet het advies van de Commissie-Brouwer-Korf heeft overgenomen om bij het Cbp de functie van wetgevingsadviseur geheel te scheiden van de functies van toezicht en handhaving, aangezien de richtlijn nr. 95/46/EG een dergelijke functiecombinatie voorschrijft. Zij vragen of er niettemin sprake is van de bereidheid om in de interne organisatie van het Cbp een vorm van scheiding tussen deze functies mogelijk te maken.

Het is inderdaad zo dat uit artikel 28 van richtlijn nr. 95/46/EG voortvloeit dat de nationale toezichthoudende instantie ook het recht heeft om op voorgenomen wetgeving die gevolgen heeft voor de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer advies te verlenen. Het spreekt voor zichzelf dat de regeling in de Wbp die uitvoering geeft aan deze verplichting daarom niet wordt gewijzigd. Hoe het Cbp intern de taak van de wetgevingsadvisering organiseert, en hoe het deze scheidt van de uitvoering van de toezichts- en handhavingstaken is een taak voor het Cbp zelf. Het Cbp is een zelfstandig bestuursorgaan en voor de uitoefening van zijn taken geen verantwoording verschuldigd aan de Minister van Justitie. Dat brengt ook met zich dat de inrichting van de organisatie een verantwoordelijkheid is van het Cbp.

4.5.2. Toezichthoudende taak van het Cbp

De leden van de CDA-fractie vragen of het kabinet van plan is het bij de evaluatie van de Wbp geconstateerde nalevingstekort te gaan bestrijden door ook ten aanzien van materiële bepalingen in de Wbp sancties als het toepassen van bestuursdwang, het opleggen van een last onder dwangsom en het opleggen van een bestuurlijke boete mogelijk te maken.

Op grond van de geldende wet is het al mogelijk om overtreding van de materiële bepalingen te sanctioneren met behulp van het opleggen van een last onder bestuursdwang of een last onder dwangsom. Slechts de overtreding van administratieve verplichtingen, zoals bijvoorbeeld het niet naleven van de meldplicht, kan onder de geldende wet worden gesanctioneerd met een bestuurlijke boete. Deze normen kunnen bovendien strafrechtelijk worden gehandhaafd. Ik meen dat, mede gelet op het geconstateerde nalevingstekort, de tijd thans is aangebroken om ook overtreding van de materiële normen van de Wbp te sanctioneren met een bestuurlijke boete.

De leden van de PvdA-fractie spreken gerede twijfel uit over de aanbevolen robuustheid van het toezicht, zolang versterking van het Cbp in kwantitatief en kwalitatief opzicht achterwege blijft. Het Cbp geeft volgens deze leden regelmatig signalen af in die richting. Zij vragen het kabinet waarom geen maatregelen zijn aangekondigd in die richting.

De in het kabinetsstandpunt voorgenomen maatregelen lijken mij, waar het betreft de versterking van de Wbp in algemene zin en de voorgenomen introductie van de punitieve sanctionering van de materiële bepalingen, een belangrijke steun in de rug van het Cbp. Het Cbp mag daarin ook erkenning en waardering zien voor de taken die het uitvoert. Het is dus beslist niet zo dat versterking van het Cbp in het kabinetsstandpunt achterwege blijft. Voor het overige geldt natuurlijk wel dat de financiële en personele middelen voor geen enkele overheidsinstelling in onbeperkte mate voorhanden zijn.

De leden van de fractie van GroenLinks hebben een aantal vragen gesteld op het terrein van het toezicht op de naleving, de handhaving en de rechtsbescherming en de positie van het Cbp.
Zo vragen deze leden waarom de bepleite versterking van de handhaving budgettair neutraal moet verlopen. Deze leden menen dat een versterking van de handhaving om meer middelen vraagt en zij vragen zich in dat verband af hoe het kabinet de gewenste versterking van de handhaving denkt te bereiken als er niet meer middelen ter beschikking worden gesteld. Zij vragen zich ook af hoe het kabinet anders denkt het geconstateerde nalevingstekort terug te dringen.
Deze leden vragen ook naar de oorzaak van het achterblijven van het aantal rechterlijke uitspraken over de Wbp bij de verwachtingen en of het kabinet dit heeft onderzocht. Zij vragen of de gebrekkige informatievoorziening van burgers en de relatief lage organisatiegraad van consumenten belemmerend werkt bij de toegang tot de rechter. Zij vragen of het kabinet bereid is te onderzoeken of de toegang tot de rechter wel afdoende is gewaarborgd en welke maatregelen de toegankelijkheid kunnen vergroten.
Deze leden vragen vervolgens of de regering zicht heeft op de rechtsbescherming ten aanzien van internationale gegevensstromen of de noodzakelijke verbeteringen daarin. De leden van de fractie van GroenLinks vragen verder of het kabinet tevreden is over de rol van het Cbp terzake en of het Cbp hier voldoende prioriteit bij legt. Zij vragen of deze taak wordt uitgebreid en of het ook een rol krijgt bij de Privacy Impact Assessments.

Wat het toezicht op de naleving en de handhaving van de Wbp betreft, heb ik er, mede op aandringen van het Cbp, voor gekozen om het geconstateerde nalevingstekort aan te pakken met versterking van het toezicht langs kwalitatieve weg. Dat houdt onder meer in dat overtreding van de materiële bepalingen van de Wbp gesanctioneerd kan worden met een bestuurlijke boete, op te leggen door het Cbp. Ik ben bovendien bereid om nogmaals een verscherping van strafrechtelijke sanctionering te overwegen. In mijn overtuiging zal de naleving van de Wbp met de oplegging van afschrikwekkende sanctie, gecombineerd met een goede en afgewogen publiciteit rondom deze sanctietoepassing stellig kunnen bijdragen aan terugdringing van het nalevingstekort. Wat betreft de budgettering van het Cbp kan worden vermeld dat deze enige jaren geleden reeds structureel verhoogd is. Financiële en personele middelen zijn niet onbeperkt voorhanden, en ook overigens niet vanzelfsprekend het eerst in aanmerking komende instrument om het toezicht en de handhaving te verbeteren. Terugdringing van het nalevingstekort kan ook bereikt worden met andere middelen dan versterking van het Cbp. Ik wijs erop dat in het kabinetsstandpunt een zwaar accent wordt gelegd op instelling van een helpdesk. Die helpdesk heeft tot taak professionals bij de staan bij de naleving van de Wbp. Dit zal leiden tot een beter normbewust én normconform gedrag.
Het is inderdaad zo dat uit de evaluatie naar voren komt dat het aantal rechterlijke uitspraken over de uitleg van de Wbp wat achterblijft bij de verwachtingen die bij de totstandkoming van de Wbp zijn uitgesproken.

Daarbij zijn overigens geen kwantitatieve oordelen geveld, maar ging het er meer om dat de rechter nog relatief weinig heeft kunnen bijdragen aan de uitleg van de Wbp in de praktijk. Uit de evaluatierapporten komt eigenlijk niet duidelijk naar voren wat daarvan precies de oorzaken zijn. Het is ook zeer de vraag of de keuzes die van invloed zijn op beslissing om de weg naar de rechter niet te bewandelen wel op een werkbare manier zijn te onderzoeken. Dat geldt te meer nu er in ieder geval in Nederland geen sprake is van een zekere georganiseerde beweging met enige aanspraak op representativiteit van burgers die specifiek opkomen voor de bescherming van hun gegevens. Ik kan mij goed voorstellen dat het ontbreken van dergelijke initiatieven, maar ook de door de leden van de GroenLinks-fractie genoemde tekortkomingen bij het naleven van de transparantieverplichtingen, van invloed kunnen zijn op de beslissing om geen geschil aanhangig te maken bij de rechter. Maar dat is zeker niet hetzelfde als het constateren van een belemmering voor de toegang tot de rechter, zoals deze leden stellen. Integendeel, bij het ontwerpen van de Wbp is nadrukkelijk gekozen voor een, binnen de normen van het Nederlandse rechtsstelsel, laagdrempelig stelsel van voorzieningen. In het publieke domein staan de rechtsmiddelen van de Awb open, in het private domein is gekozen voor een verzoekschriftprocedure in plaats van een dagvaarding.
Dat alles neemt niet weg dat er nog wel het nodige gedaan kan worden om jurisprudentie te genereren. Het opleggen van bestuurlijke boetes, zo leert de ervaring, wordt vrijwel steeds gevolgd door een procedure van bezwaar en beroep. Introductie van punitieve sanctionering van overtreding van de materiële bepalingen van de Wbp zal dan ook zeker jurisprudentie uitlokken. Verder is in het kabinetsstandpunt aangekondigd dat een rapport van bevindingen van het Cbp, uitgebracht naar aanleiding van een door het Cbp ingesteld onderzoek, kan worden onderworpen aan bezwaar en beroep. Daarvoor is wetswijziging noodzakelijk. Ik zal dat in gang zetten.
Verder moet worden bedacht dat geschillen rondom de toepassing van de Wbp niet steeds goed op geld waardeerbaar zijn. Het maken van een rationele afweging tussen baten en lasten van het volgen van een procedure bij de rechter raakt dan naar de achtergrond. Dat is nu eenmaal eigen aan deze materie. Geschillen van niet-financiële aard zullen daarom op andere wijze moeten worden beslecht dan door rechterlijke uitspraken. Ook dat is van invloed op het ontstaan van jurisprudentie.
Wat internationale gegevensstromen betreft, en de rol van het Cbp daarbij, moet ik erop wijzen dat deze stromen een normaal verschijnsel zijn, en dat die, net zo min overigens als nationale gegevensstromen, als zodanig steeds principieel voorwerp van verzet, bezwaar of beroep moeten zijn. Wat de private sector betreft is het zo dat gegevens binnen de Europese Economische Ruimte vrijelijk kunnen circuleren. Dat kan omdat richtlijn nr. 95/46/EG en het Dataprotectieverdrag van de Raad van Europa zorgen voor materiële en procedurele garanties voor gegevensbescherming en voorzien in onafhankelijk toezicht en rechtsbescherming. Voor gegevensstromen in de private sector naar derde landen ligt dat wat anders. Verzekerd moet zijn dat in het land van bestemming een adequaat niveau van gegevensbescherming bestaat. Er zijn verschillende manieren om dat niveau te beoordelen. Dit is doorgaans geen eenvoudige procedure. In het bij de Tweede Kamer aanhangige wetsvoorstel tot *wijziging van de Wet bescherming persoonsgegevens in verband met de vermindering van administratieve lasten en nalevingskosten, wijzigingen teneinde technische gebreken te herstellen en andere wijzigingen van ondergeschikte aard* (Kamerstukken II 2008/09, 31841) heb ik daarvoor vereenvoudigingen voorgesteld. Zo nodig kan de Minister van Justitie een vergunning verlenen voor data-export. Dat gebeurt alleen na advies van het Cbp. Dat komt per jaar gemiddeld 60 tot 80 maal voor. Ik heb geen

problemen met de wijze waarop het Cbp deze taak uitoefent. Deze vergunningen zijn zelden of nooit voorwerp van bezwaar of beroep. Internationale gegevensstromen in de publiekrechtelijke sfeer bestaan hoofdzakelijk op het gebied van politie en justitie. Voor een belangrijk deel zijn die gegevens onttrokken aan de Nederlandse rechtssfeer, omdat zij worden beheerst door regels van Europees recht. Te denken valt aan gegevensverwerking in het kader van Schengen, Europol of Eurojust. Het Cbp speelt daarbij overigens wel een rol. Het Cbp oefent toezicht uit in collectief verband samen met collega-toezichthouders uit andere EU- en Schengenlidstaten. Het is niet aan mij te oordelen of het Cbp bij de uitoefening van deze taken voldoende prioriteiten legt. Wel merk ik op dat het Cbp ten aanzien van deze taken geen vrijheid heeft om te beslissen of het die al dan niet uitvoert. Dit zal moeten gebeuren.
Het Cbp heeft tenslotte zelf (mede) het initiatief genomen om de methodiek van Privacy Impact Assessments uit te werken. Ik stel dat initiatief op prijs. De beslissing of dergelijke instrumenten ook moeten worden gebruikt in concrete gevallen is geen zaak of taak voor het Cbp, maar zal door verantwoordelijken bij overheid en bedrijfsleven zelf ter hand moeten worden genomen.

De leden van de D66-fractie vragen zich in het licht van de door het kabinet geconstateerde nalevingstekort af of er geen behoefte blijft aan advisering door het Cbp. Zij vragen dan ook waarom uitbreiding van middelen geen reële optie wordt genoemd. Verder vragen deze leden waarom het kabinet meent dat de handhaving van de Wbp aan de hand van aansprekende voorbeelden zou moeten plaatsvinden. Zij menen dat niet zozeer sprake moet zijn van het stellen van een daad om aandacht te genereren, maar van een vaste handhavingslijn. Verder constateren deze leden met instemming dat het kabinet overweegt om bezwaar en beroep open te stellen tegen bevindingen van het Cbp.

Bij de beantwoording van de gelijkluidende vragen van de leden van de fractie van GroenLinks heb ik reeds aangegeven dat het mijn voorkeur heeft om het geconstateerde nalevingstekort door middel van versterking van de kwalitatieve positie van het Cbp aan te pakken. Ik verwijs de leden van de D66-fractie graag naar mijn antwoorden terzake.
Wat de toekomstige wijze van handhaven betreft, ben ik het eens met deze leden dat van het Cbp mag worden verwacht dat het waar mogelijk een vaste handhavingslijn formuleert die ook uniform wordt toegepast. Daarbij moet wel worden bedacht dat alle toezichthouders – dus niet alleen het Cbp – hun activiteiten in de regel verrichten met behulp van risicoanalyses en de selectie van bepaalde aandachtsgebieden. Het is immers onwenselijk en overigens ook volstrekt onmogelijk elke verwerking van persoonsgegevens aan een voortdurend toezicht te onderwerpen. Bij een dergelijke benadering sluit aan dat aan de hand van aansprekende voorbeelden de aandacht van het algemene publiek kan worden gevestigd op door het Cbp in een of meer actuele zaken geconstateerde misstanden en op de maatregelen die het Cbp terzake heeft getroffen. Ik ben ervan overtuigd dat een dergelijke werkwijze ook zal bijdragen aan het verkleinen van het nalevingstekort van de wet.
Ik ben de leden van de D66-fractie erkentelijk voor hun steun aan mijn voornemen om tegen een verslag van bevindingen in de zin van artikel 60 van de Wbp bezwaar en beroep open te stellen.

4.6. Ruimhartiger vrijstellingsbeleid t.a.v. de meldplicht

De leden van de VVD-fractie merken op dat zij het voornemen van het kabinet om de vrijstelling van de meldplicht voor bedrijven te verlenen wanneer deze bedrijven een functionaris voor de gegevensbescherming aanstellen ongelukkig achten, aangezien bedrijven die een dergelijke

functionaris kennen hun verwerkingen niet bij het Cbp, maar slechts bij deze functionaris behoeven te melden.

De voornemens ten aanzien van de meldplicht gaan verder dan de bestaande faciliteit om uitvoering van de meldplicht te vergemakkelijken door middel van aanwijzing van een functionaris voor de gegevensbescherming (FG). Mijn beleidsvoornemens zijn erop gericht om in de private sector het bewustzijn van het belang van gegevensbescherming te stimuleren. Bedrijven hebben een eigen commercieel belang bij de zorgvuldige behandeling van de persoonsgegevens van hun klanten en medewerkers. Het is hun eigen verantwoordelijkheid, en niet de verantwoordelijkheid van de overheid om dat ook daadwerkelijk te doen. Dat was overigens ook de bedoeling van de richtlijn. Ik ben van oordeel dat het verder stimuleren van het bedrijfsleven om die verantwoordelijkheid inhoud te geven de beste weg is om dit doel uiteindelijk te bereiken. Aangezien uit de evaluatie wel voldoende naar voren is gekomen dat de door de richtlijn geïntroduceerde instrumenten – de gedragscode en de FG – tot dusverre erg bescheiden resultaten hebben opgeleverd, ligt het in de rede dat de wetgever iets meer moet kunnen bieden. Ik denk daarbij aan het volgende: bedrijven die bereid zijn gebleken een eigen privacybeleid op te zetten dat in ieder geval voldoet aan een aantal eisen, kunnen in aanmerking komen voor een algehele vrijstelling van de meldplicht. Een formele melding aan een FG hoeft dan ook niet meer plaats te vinden. Die eisen waaraan een bedrijf dan moet voldoen zijn: een behoorlijke inhoud geven aan de transparantieverplichtingen op grond van de Wbp en dat ook op een voor klanten, consumenten en werknemers gemakkelijk toegankelijke manier doen. Het duidelijk maken dat betrokkenen hun rechten op inzage, correctie en verzet geldend kunnen maken op een gemakkelijk toegankelijke manier, het zorgdragen voor een klachten- of geschillenregeling die (mede) ziet op geschillen die betrekking hebben op de verwerking van persoonsgegevens en het zorgdragen voor een vorm van intern toezicht op de gegevensverwerking. Het interne toezicht hoeft dan niet noodzakelijkerwijs door middel van de instelling van een FG te geschieden. En aantal grote Nederlandse bedrijven heeft bijvoorbeeld geen FG, maar een Privacy Officer, die min of meer hetzelfde werkpakket heeft. Gelet op de formele inbedding van de FG in de Wbp schrikken bedrijven er soms voor terug een FG aan te stellen. Het geeft de wetgever geen pas om zich zonder dringende maatschappelijke noodzaak te bemoeien met de interne organisatie van bedrijven. In plaats van het dwingend voorschrijven van een functionaris waarvan de aanstelling tot dusverre een vrijwillig initiatief was, geef ik er de voorkeur aan die vrijwilligheid aantrekkelijker te maken door een ruimere keuze te bieden. Dit geheel aan maatregelen moet overigens nog wel op een aantal punten verder worden uitgewerkt in nader contact met Cbp, georganiseerd bedrijfsleven en consumentenorganisaties.

4.7. Bevorderen van zelfregulering

De leden van de VVD-fractie geven aan dat het kabinet meer ziet in het door middel van wetgeving stimuleren van het gebruik van gedragscodes of het aanstellen van FG's. Deze leden vragen of zij het verkeerd zien dat deze middelen reeds in de wet zijn opgenomen, maar desondanks weinig worden toegepast. Zij vragen wat het kabinet gaat doen om deze toepassing te stimuleren.

Bij de beantwoording van de vragen van de leden van de VVD-fractie in paragraaf 4.6 ben ik reeds ingegaan op hetgeen de leden van deze fractie in hun vragen aan de orde stellen. Ik verwijs deze leden dan ook graag naar die antwoorden.

De leden van de PvdA-fractie vragen zich af of de beleidswens van het kabinet dat versterking van het extern toezicht niet mag leiden tot een verzwakking van het bestaande interne toezicht wel kan worden gerealiseerd. Deze leden wijzen erop dat tot dusverre maar weinig FG's zijn aangesteld. Zij vragen daarom of de druk op de private sector niet juist moet worden verhoogd. Zij vragen zich af of robuust extern toezicht de positie van de FG niet juist versterkt.

Het is inderdaad zo dat uit de evaluatie van de Wbp naar voren komt dat er tot dusverre relatief weinig FG's zijn aangesteld in de private sector. Maar waar deze wel is aangesteld, zo blijkt uit het tweede evaluatierapport, heeft de enkele aanstelling van de FG tot gevolg dat in de desbetreffende organisatie meer aandacht is voor vraagstukken van gegevensbescherming. Het ligt dan ook voor de hand dat dit gegeven een rol gaat spelen bij de inrichting van het beleid van toezicht en handhaving door het Cbp. Waar een FG is aangesteld, is het risico dat zich ernstige misstanden bij de verwerking van persoonsgegevens voordoen gemiddeld genomen kleiner, zodat de handhavingsinspanningen kunnen worden gericht op bedrijven of sectoren die blootstaan aan grotere risico's. Ik sluit daarom niet uit dat een effectief handhavingsbeleid per saldo inderdaad leidt tot een sterkere positie van interne toezichthouders. Mogelijk is dit op zijn beurt weer een stimulans voor bedrijven om meer van deze toezichthouders aan te stellen. Ik ben niet voornemens om de druk op het bedrijfsleven te vergroten. Ik verwijs de leden van de PvdA-fractie in dit verband graag naar de beantwoording van de vragen van de VVD-fractie in paragraaf 4.6. waar ik inga op de redenen daarvoor.

De leden van de fractie van GroenLinks hebben een aantal vragen gesteld over het interne toezicht op de verwerking van persoonsgegevens. Zo vragen zij zich af of de aanstelling van een privacyfunctionaris niet leidt tot een vermindering van het verantwoordelijkheidsgevoel van andere werknemers. Zij veronderstellen dat bij de voorgenomen privatisering van de privacybewaking effectiviteit voorop moet staan en dat externe druk nodig is om de interne alertheid in leven te houden. Zij vragen dan ook of het kabinet de oplegging van rapportageverplichtingen overweegt, zodat het Cbp kan volgen hoe het beleid wordt toegepast. Zij vragen ook of de vrijstelling kan vervallen wanneer dat beleid niet wordt gevolgd.

Ik wil hier nadrukkelijk onderstrepen dat mijn beleidsvoornemens ten aanzien van intern toezicht op de gegevensverwerking binnen bedrijven of instellingen geen kwestie is van het vervangen van extern toezicht door intern toezicht of van het privatiseren van toezichtrelaties. Ik overweeg niet om de reikwijdte van het extern toezicht door het Cbp te verminderen. Ik zal dan ook niet de totstandkoming van wetgeving bevorderen die extern toezicht vervangt door intern toezicht of die het extern toezicht anderszins privatiseert op terreinen waar dit tot dusverre publiek was georganiseerd. Integendeel, het is het mijn voornemen beide bestaande toezichtsvormen, extern en intern te versterken. Ik ben voornemens het extern toezicht te versterken door uitbreiding van de sanctiebevoegdheden van het Cbp. Ik ben ook voornemens bedrijven de stimuleren om vaker gebruik te maken van bestaande en nieuwe vormen van intern toezicht. Of aanstelling van een interne toezichthouder een negatief effect heeft op het privacybewustzijn van andere werknemers, betwijfel ik. Uit het tweede evaluatierapport van de Wbp volgt nu juist dat aanstelling van een FG een positief effect heeft op dat bewustzijn.
Ik betwijfel of het inrichten van nieuwe rapportageverplichtingen, aanvullend ten opzichte van de reeds bestaande verplichting van de FG een jaarverslag op te stellen over zijn werkzaamheden, veel soelaas biedt. Om te beginnen zou dit leiden tot een toename van administratieve lasten en nalevingskosten. Ik probeer ook op het terrein van de Wbp deze

verplichtingen terug te dringen. Daarnaast lijken de leden van de fractie van GroenLinks in hun vraagstelling terzake uit te gaan van een rol van het Cbp die niet reëel is. Het Cbp kan niet optreden als een instantie die voortdurend nauwlettend jaarverslagen van FG's of het privacybeleid van bedrijven monitort om te bezien of zij nog altijd voldoen aan de voorwaarden voor vrijstelling van de meldplicht. Het Cbp heeft net zo min als elke andere toezichthouder noch de behoefte, noch de mogelijkheden om alle verwerkingen van persoonsgegevens meer of minder intensief te volgen. Het Cbp zal zich net als enigszins vergelijkbare toezichthouders als de NMa, de OPTA, of de AFM moeten verlaten op risicoanalyses.
Over de consequenties van het niet volgen van de voorwaarden die verbonden zijn aan een vrijstelling moet nog nadere besluitvorming plaatsvinden. De leden van de fractie van GroenLinks veronderstellen blijkens hun vraagstelling wellicht dat vrijstellingverlening steeds berust op een afzonderlijk besluit voor een afzonderlijke onderneming. Of dat zo zal zijn moet nog nader worden besproken met Cbp en maatschappelijke partners. Ik geef hierbij wel aan dat het vervallen van administratieve verplichtingen natuurlijk niet moet leiden tot het in het in leven roepen van nieuwe vergunningstelsels die per saldo hetzelfde effect hebben: dan zouden we het paard achter de wagen spannen. In beginsel geef ik de voorkeur aan algemene regels boven een vergunningstelsel, maar ik ben het met de leden van de GroenLinks-fractie eens dat de handhaafbaarheid een aandachtspunt moet zijn.

5. Uitgeleide

De leden van de PvdA-fractie uiten hun zorg dat bestaande wettelijke privacywaarborgen worden uitgehold en dat in het verlengde daarvan de compensatie voor de burger in toezicht en handhaving twijfelachtig blijft zolang de robuustheid van het toezicht niet beter wordt gewaarborgd en de bewustwording van professionals en burgers niet meer aandacht krijgt. Deze leden vragen een reactie van het kabinet op hun zorg.

De voornaamste conclusie die het kabinet trekt is dat de Wet bescherming persoonsgegevens niet alleen in het domein van de veiligheid en de daarmee verbonden maatschappelijke hulpverlening onvoldoende bekend is, maar dat er ook in andere sectoren van het maatschappelijk leven onvoldoende bekend is over de doelstellingen van die wet, de wijze waarop de instrumenten van de wet moeten worden toegepast en de wijze waarop de wet gestalte geeft aan een aantal rechten van de burger. Dat betekent dat er op dit moment ten aanzien van deze wet sprake is van een nalevingstekort. Het kabinet doet in zijn brief een aantal voorstellen die een bijdrage moeten leveren aan het terugdringen van het nalevingstekort. Ik wijs in dit verband onder andere op de maatregelen die moeten leiden tot een hoger kennisniveau bij professionals, de introductie van een Privacy Impact Assessment als middel om te bevorderen dat het privacybelang in een vroegtijdig stadium wordt meegewogen bij de ontwikkeling van systemen, de uitbreiding van de sanctiemogelijkheden voor het Cbp en het met meer eigentijdse middelen inhoud geven aan transparantieverplichtingen rond gegevensverwerkingen.

De leden van de PvdA-fractie vragen of het kabinet kan aangeven of en in hoeverre nieuwe technologische toepassingen worden meegenomen in de beleidsontwikkeling ter zake, niet alleen langs de in het kabinetsstandpunt genoemde lijnen, maar ook via meer vanuit de individuele burger opgezette toepassingen met Web 2.0. Bovendien vragen deze leden of het kabinet de indruk deelt dat er gebrek is aan expertise in de technologische mogelijkheden en risico's in alle lagen en sectoren van de samenleving.

Het kabinet ziet veel in de ontwikkeling van Web 2.0 en tracht de mogelijkheden van deze technologie mee te nemen in de beleidsontwikkeling, om zo de interactie met de maatschappij te verbeteren. Omdat deze ontwikkelingen nog relatief nieuw zijn, zijn de kansen en bedreigingen van Web 2.0 echter nog niet duidelijk. Het kabinet is daarom op dit moment op verschillende terreinen actief om meer ervaring en expertise op te doen en uit te wisselen op het gebruik van Web 2.0 door de overheid. Zo wordt bijvoorbeeld geëxperimenteerd met een eigen Web 2.0 platform (www.overheid20.nl) voor de overheid in den brede, en wordt de opgedane kennis actief gedeeld in een netwerk met medeoverheden. Wat betreft de vraag of hierbij niet uitgegaan moet worden van de regie van de regering om kennis te bundelen, en van daaruit te communiceren meent het kabinet dat het van belang is te onderstrepen dat Web 2.0 vooral een maatschappelijke ontwikkeling is, die slechts ten dele door de overheid te beheersen is.

De leden van de fractie van de SP vragen in hoeverre het richtinggevend kader van de commissie Brouwer-Korf is toegepast op een bij de Eerste Kamer aanhangig wetsvoorstel dat zich richt op de bestrijding van terroristische activiteiten. De leden van de fracties van SGP en ChristenUnie wijzen daarenboven op het cumulatief effect van maatregelen gericht op opsporing en bestrijding van terrorisme, ook in EU-verband.

Het kabinet heeft in een brief van 29 januari 2010 toegelicht op welke wijze uitvoering wordt gegeven aan de aanbevelingen zoals die in het rapport van de commissie Evaluatie antiterrorismebeleid (commissie-Suyver) zijn geformuleerd. Daarbij wordt terdege gekeken naar het juridisch kader, de rechtsbescherming en het cumulatief effect van deze maatregelen op de persoonlijke levenssfeer van burgers.

De leden van de fracties van SGP en ChristenUnie vragen of er in kader van de informatie-uitwisseling binnen de EU naar de opvatting van het kabinet toereikende waarborgen bestaan dat registraties op een juiste grondslag berusten en of er gesproken kan worden van een evenwaardig, uniform stelsel van gegevensbescherming.

Voor het antwoord op deze vragen verwijs ik de leden van de fracties van SGP en ChristenUnie graag naar de in paragraaf 3.6.1 gegeven toelichting op de ontwikkeling van een Informatie Management Strategie in antwoord op vragen van de PvdA-fractie.

De leden van de fractie van D66 wijzen erop dat het voorkomt dat persoonsgegevens na een executoriale verkoop van bedrijfscomputers in handen van onbevoegde derden vallen. Zij zijn van oordeel dat de bescherming van privacy steeds onder de aandacht moet blijven, ook wanneer een bedrijf onder leiding staat van een curator. Zij vragen of de regering voornemens is dit punt extra onder de aandacht van de beroepsgroep te brengen.

Het is duidelijk dat wanneer een bedrijf in staat van faillissement is verklaard de curator in veel gevallen zal moeten worden aangemerkt als verantwoordelijke in de zin van de Wbp. Indien dit in een concreet geval inderdaad zo is, dan geldt voor de curator de in de Wbp opgenomen verplichting zorg te dragen voor beveiliging van in de boedel verwerkte persoonsgegevens tegen verlies of onrechtmatige verwerking.

Ik heb deze problematiek aan de orde laten stellen in het periodieke overleg van maart 2010 tussen mijn departement en de Nederlandse Orde van Advocaten. Het is overigens een onderwerp dat binnen de beroeps-

groep leeft, getuige het recente proefschrift van de heer Van Apeldoorn, getiteld «Insolvatieprocedures en grondrechten». Deze advocaat, die vaak als curator heeft opgetreden, vraagt in zijn dissertatie bijzondere aandacht voor de rechtspositie van de gefailleerde schuldenaar.

De minister van Justitie,
minister van Binnenlandse Zaken en Koninkrijksrelaties,
E. M. H. Hirsch Ballin