Ministerie van Veiligheid en Justitie

Directie Wetgeving

Contactpersoon
T 070 370 79 11
F 070 370 79 10

Datum
29 april 2011

Ons kenmerk
5688920/11/6

Datum vaststelling
29 april 2011

bijlage

Reactie op schriftelijke vragen Eerste Kamer ter voorbereiding debat digitale dataverwerking 17 mei 2011

Bijlage nummer	2
Horend bij	Brief van de Staatssecretaris van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties

Bij brief van 12 april 2011 (kenmerk 147654.01U) hebben de vaste commissies voor Justitie, BZK/AZ, OCW, VWS en de JBZ-raad van de Eerst Kamer een aantal vragen aan de regering voorgelegd ter voorbereiding van het beleidsdebat digitale dataverwerking op 17 mei 2011. Inbreng is geleverd door de fracties van het CDA, de PvdA, GroenLinks en de SP, waarbij de laatste fractie zich tevens aansluit bij de inbreng van de PvdA-fractie. De leden van de vaste commissies verzoeken de regering de reactie op deze brief op de kortst mogelijke termijn na de verzending van de brief over het privacybeleid - die verwacht wordt op 29 april 2011 – toe te sturen, waarbij verwijzing naar laatstgenoemde brief een optie is.

Hieronder wordt ingegaan op de door de verschillende fracties gestelde vragen. Een aantal vragen van uw Kamer wordt reeds beantwoord in de brief over het privacybeleid en in de notitie over het privacybeleid (bijlage 1 bij de brief). Waar dat het geval is, wordt hiernaar verwezen.

Een aantal vragen van de fracties refereert aan de aanbevelingen als gedaan door de Wetenschappelijke Raad voor het Regeringsbeleid in het recente rapport iOverheid. Dit rapport werd pas recent, op 15 maart 2011, aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties aangeboden. Momenteel is een separate kabinetsreactie op dit rapport in voorbereiding. Ontwikkelingen die in deze kabinetsreactie aan de orde zullen komen zijn onder meer de rol en verantwoordelijkheid van de overheid met betrekking tot de digitalisering van de samenleving, verschillende aspecten rondom het beheer van informatiestromen, goed opdrachtgeverschap en mogelijkheden voor burgers tot inzage in elektronische dossiers. Op de opmerkingen en vragen van uw Kamer naar aanleiding van de door de WRR geconstateerde ontwikkelingen en gedane aanbevelingen zal daarom pas op een later tijdstip uitgebreid kunnen worden ingegaan.

Bij de beantwoording van de overige vragen wordt zoveel mogelijk de volgorde aangehouden van de vraagstelling in de brief van uw Kamer, waarbij omwille van de leesbaarheid de antwoorden op enkele vragen zijn verplaatst of samengevoegd.

Directie Wetgeving
Sector Staats- en bestuursrecht

Datum
26 april 2011

Ons kenmerk
***

1. Visie regering en reactie op rapporten

1.1. Visie regering
De leden van de commissies vragen de regering op welke terreinen er al gebruik gemaakt wordt van datamining of –profiling en op welke terreinen zij van plan is daarvan gebruik te gaan maken. De indruk ontstaat dat via Europese wetsvoorstellen het gebruik van profielen geïntroduceerd wordt, terwijl Nederland hier in het verleden altijd terughoudend in geweest is.

Het verwerken van persoonsgegevens in de vorm van datamining, of profilering neemt als gevolg van de ontwikkeling van de ICT toe. Technische ontwikkelingen maken het mogelijk om tegen relatief geringe kosten grote hoeveelheden beschikbare gegevens, waaronder persoonsgegevens, te bewaren, deze aan de hand van voor de verantwoordelijke relevante criteria toegankelijk te maken en deze vervolgens te vergelijken met andere beschikbare gegevens. De resultaten van de vergelijking kunnen vervolgens worden gebruikt voor nieuwe doeleinden. Die nieuwe doeleinden kunnen worden geformuleerd op basis van vooronderstellingen. Toetsing van de gegevens aan de vooronderstellingen, kan dan tot een bepaald resultaat aanleiding geven dat iets zegt of iets vooronderstelt over het gedrag van een individu.

Deze technieken zijn op zichzelf genomen niet nieuw. Zij worden al geruime tijd gebruikt door het bedrijfsleven. Met behulp van profilering doen bedrijven voorspellingen over consumentengedrag, en op basis van voorondersteld gedrag of vooronderstelde interesses kunnen klanten worden benaderd. Dat kan passief gebeuren, bijvoorbeeld door het aanbod van bepaalde goederen in winkels te verhogen, dat kan collectief gebeuren door advertentiecampagnes, maar dat kan ook individueel gebeuren, door middel van gericht persoonlijk adverteren. Supermarktketens maken van de gegevens van klantenkaarten gebruik om het aanbod te sturen, energieleveranciers doen op basis van de verbruikcijfers van klanten aanbiedingen voor energiebesparing of tariefgaranties.
Wij achten het gebruik van deze techniek niet principieel onaanvaardbaar.

Wel is het zo dat aan deze techniek zekere risico's voor de persoonlijke levenssfeer zijn verbonden. Dit is reeds bij de totstandkoming van de richtlijn richtlijn nr. 95/46/EG (hierna: privacyrichtlijn) onderkend. Artikel 15 van de privacyrichtlijn formuleert het recht dat eenieder heeft om verschoond te blijven van besluiten die geheel geautomatiseerd worden genomen en die bedoeld zijn om bepaalde aspecten van zijn persoonlijkheid, zoals beroepsprestaties, kredietwaardigheid en andere omstandigheden te evalueren. Het komt er dus op neer dat wanneer verantwoordelijken van deze technieken gebruik maken, er altijd menselijke tussenkomst noodzakelijk is wanneer er ten aanzien van betrokkenen meer of minder belangrijke besluiten worden genomen. Deze bepaling is geïmplementeerd in artikel 42 van de Wet bescherming persoonsgegevens (Wbp).
Een ander aandachtspunt is dat de transparantie over de toepassing van deze techniek van gegevensverwerking in de regel niet erg groot is. Dat is wel een punt van zorg. Profileren (van welk proces datamining een onderdeel is) is een veel gecompliceerder proces van gegevensverwerking dan het eenvoudig rechtstreeks verstrekken van persoonsgegevens door een betrokkene aan een verantwoordelijke. De risico's voor de bescherming van de persoonlijke levenssfeer zijn ook groter, onder meer doordat wordt gewerkt met vooronderstellingen die aan een bepaald profiel te grondslag liggen. Dit heeft

geleid tot het aannemen van een resolutie (nr. CM/Rec (2010) 13) door het Comité van Ministers van de Raad van Europa op 13 november 2010 over profileren. De kern van die resolutie is een uitbreiding van de transparantieverplichtingen bij de toepassing van profileringstechnieken.
De resolutie zal in een wetsvoorstel worden geïmplementeerd. De brief over het privacybeleid bevat een voornemen daartoe, dat in de notitie privacybeleid (bijlage 1 bij de brief) verder wordt uitgewerkt. De transparantieverplichtingen in de Wbp (artikelen 33 en 34) zullen worden aangescherpt. Er komt een afzonderlijke expliciete regeling voor verantwoordelijken die persoonsgegevens verwerken in het kader van profilen met betrekking tot het bekendmaken van het doel van de verwerking en de daarbij gehanteerde categoriseringen. De betrokkene kan op die manier inzicht krijgen in de doeleinden van het profileren, in het profiel zelf, en de gegevens waarop het is gebaseerd en de verantwoordelijken aan wie verdere verstrekking plaatsvindt.

Wat het gebruik van profileringstechnieken door de overheid betreft, geldt dat er geen principiële redenen zijn om de overheid het gebruik van deze techniek te ontzeggen, om de enkele reden dat deze inbreuk maakt op het recht op bescherming van de persoonlijke levenssfeer. Wel is het zo dat wanneer de overheid zijn toevlucht neemt tot deze techniek dit alleen kan plaatsvinden wanneer daarvoor een behoorlijke wettelijke grondslag aanwezig is en het desbetreffende wetsvoorstel is voorzien van een adequate toelichting waarin de verplichte afweging tussen het belang van de bescherming van de persoonlijke levenssfeer wordt afgewogen tegen het algemene belang dat vergt dat op het eerstgenoemde belang een inbreuk wordt gemaakt. Wanneer de Wbp of één van de andere belangrijke wetten op het terrein van de gegevensbescherming niet rechtstreeks van toepassing zijn, moeten in de desbetreffende wet waarborgen voor de bescherming van de persoonlijke levenssfeer worden opgenomen, zoals de recht op inzage en correctie, en moet worden gezorgd voor adequaat intern en extern toezicht.

De overheid maakt gebruik van profileringstechniek op twee terreinen. Het eerste terrein betreft de screening van personen. Op grond van de Wet justitiële en strafvorderlijke gegevens wordt bij de beslissing over het afgeven van een verklaring omtrent het gedrag aan de hand van profielen beoordeeld of er redenen zijn om aan te nemen dat er een risico voor de samenleving bestaat dat de betrokkene in een bepaalde werkkring het strafbare feit waarvoor een veroordeling heeft plaatsgevonden herhaalt. Zo wordt daarbij betrokken dat wanneer iemand veroordelingen op zijn naam heeft staan voor, bijvoorbeeld, een of meer ernstige verkeersdelicten niet zonder meer in aanmerking komt voor afgifte van een verklaring wanneer hij solliciteert als chauffeur. Maar afgifte van een verklaring hoeft niet noodzakelijkerwijs vanwege diezelfde feiten te worden geweigerd wanneer de betrokkene solliciteert als accountant.
Een recent voorbeeld van een wettelijke regeling met betrekking tot profilering is de nieuwe Wet controle op rechtspersonen. De Minister van Veiligheid en Justitie verwerkt gegevens met betrekking tot rechtspersonen uit tal van bij en krachtens de wet genoemde bronnen. Aan de hand van risicoprofielen wordt beoordeeld of er aanwijzingen zijn die rechtvaardigen dat bepaalde rechtspersonen - en de daarmee verbonden natuurlijke personen - nadere aandacht verdienen van politie, OM of de Belastingdienst. De Minister van Veiligheid en Justitie kan in die gevallen een risicomelding aan deze diensten zenden.

Het tweede terrein waarop de overheid profilering toepast, is op het terrein van toezicht en handhaving. Belastingdienst en Douane gebruiken deze technieken om de zwaartepunten bij het toezicht mee te bepalen. Het is gebruikelijk dat de Belastingdienst jaarlijks aankondigt welk onderdeel van belastingaangiften bijzondere aandacht krijgt en dat de Douane bij de controle van het goederenverkeer op basis van bestaande gegevens bijvoorbeeld risicovluchten selecteert en de passagiers daarvan na aankomst op Schiphol bijzondere aandacht geeft. Belastingdienst en Douane kunnen deze technieken toepassen op grond van de specifieke wetten die hun eigen taken en bevoegdheden regelen.

Ingewikkelder ligt het bij samenwerkingsverbanden van verschillende toezichthouders en handhavers. Het verdient aanbeveling dat daarvoor nieuwe wettelijke grondslagen worden gemaakt, wanneer een samenwerkingsverband een min of meer permanent karakter krijgt en op basis van de bestaande wetgeving, of op basis van geldende geheimhoudingsplichten de conclusie moet worden getrokken dat de gewenste gegevens in dat onderlinge verband niet mogen worden gedeeld of verder mogen verwerkt. Dit probleem verdient aandacht van de wetgever, zoals ook vermeld in de brief en de notitie over het privacybeleid.

Aandacht verdient ook dat in de sfeer van het toezicht en de handhaving niet steeds volledige transparantie kan worden betracht op dezelfde wijze als dat in de private sector zou moeten gebeuren. Transparantie en onderzoeksbelangen kunnen in concreto conflicterende waarden vormen. Die belangen wordt erkend in artikel 13, eerste lid, van de privacyrichtlijn en in artikel 43 van de Wbp. Dat kan er, onder omstandigheden, toe leiden dat een zorgvuldige afweging wordt gemaakt tussen het belang bij transparantie, dat primair het belang van de bescherming van de persoonlijke levenssfeer dient, en het algemene belang van het houden van toezicht op de naleving en de handhaving van wettelijke voorschriften.

De leden van de CDA-fractie vragen de regering of het juist is dat de overheid streeft naar een consolidatie van datacentres, en wat hierbij de concrete voordelen zijn mede gelet op de beheersbaarheid en kwetsbaarheid voor een ongestoorde en verantwoorde informatievoorziening.

Het kabinet kan bevestigen dat er plannen zijn om het aantal datacenters van de rijksdienst terug te brengen van ruim 60 naar een beperkt aantal datacenters, zoals ook beschreven in project 4 van het Uitvoeringsprogramma Compacte Rijksdienst. Gelet op de beheersbaarheid en kwetsbaarheid voor een ongestoorde en verantwoorde informatievoorziening zijn er een aantal concrete voordelen van deze consolidatie. Allereerst zal dit leiden tot standaardisatie (op grotere schaal), wat de beheersbaarheid in algemene zin ten goede komt. Ten tweede zal de consolidatie van datacenters leiden tot vergroting van de mogelijkheden tot het treffen van maatregelen ten behoeve van de continuïteit voor organisaties die thans op een te kleine schaal een en ander moeten regelen. Ten derde, zal het helpen de verbrokkeling van de ICT bij de Rijksdienst terug te dringen. En ten slotte kan consolidatie bijdragen aan borging van de continuïteit, bijvoorbeeld door het goed regelen van uitwijkvoorzieningen.

De leden van de SP-fractie vragen hoeveel overheidsdatabanken er bestaan.

Het is niet doenlijk om binnen de termijn waarop deze vragen moeten worden beantwoord een enigszins betrouwbare schatting te geven van het aantal databanken waarin de overheid gegevens van burgers verwerkt. Een dergelijke inventarisatie is zeer arbeidsintensief en zal, naar het zich thans laat aanzien, ook langdurig zijn. Dat wordt mede veroorzaakt doordat er geen echt duidelijke omschrijving bestaat wat in dit verband onder "overheid" moet worden verstaan. In het veelgeciteerde rapport van het onderzoeksbureau Considerati "Onze digitale schaduw, Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat" (Amsterdam, 2009), kon ook geen betrouwbare schatting worden gegeven van het aantal databases in de sterk met elkaar verknoopte sectoren overheid, sociale zekerheid, zorg en onderwijs.

De leden van de PvdA-fractie vragen, met verwijzing naar diverse constateringen van de Algemene Rekenkamer, naar de mening van de regering over de spreekwoordelijke overheidsmissers, in de vorm van onhaalbare deadlines en kostbare mislukkingen als het gaat om grootschalige ICT projecten.

Sinds 2008 zijn er, mede naar aanleiding van de rapportages van de Algemene Rekenkamer, door de verschillende kabinetten maatregelen genomen om de beheersing van de grote ICT-projecten te verbeteren. Deze maatregelen (Kamerstukken II 26 643, nrs. 135, 143 h1, 160, 172) omvatten onder andere de inrichting van het CIO-stelsel, het introduceren van Gateway reviews op ICT-projecten en de jaarlijkse rapportage aan de Tweede Kamer over de grote en vanaf dit jaar ook de hoogrisico ICT-projecten. In deze rapportage worden naast de kosten en doorlooptijd van de gerapporteerde projecten ook de op dat project uitgevoerde externe kwaliteitstoetsen meegenomen.

De leden van de PvdA-fractie vragen naar de interactie met burgers via web 2.0. Deze leden wensen te vernemen wat het beeld is dat de regering heeft van de wijze waarop burgers actief zijn via het internet. Tevens vragen zij of burgers op meer interactieve wijze kunnen worden betrokken in maatschappelijke processen via de digitale middelen.

Het nieuwe internet - het web 2.0 - biedt verschillende nieuwe mogelijkheden voor interactie. Op dit moment wordt daar door diverse overheidsorganisaties, waaronder veel gemeenten, ervaring mee opgedaan. Uit deze ontwikkelingen volgt onder meer dat een informatiesamenleving vergt dat de overheid op een andere wijze om gaat met informatie. De Minister van Binnenlandse Zaken en Koninkrijksrelaties zal in dat kader voor de zomer een brief sturen aan de Tweede Kamer over hergebruik van openbare overheidsinformatie en de ontwikkeling van een visie op deze zogenaamde 'open data' in Nederland. In deze brief zal bovendien nader worden ingegaan op de aanbevelingen uit een recent onderzoek van TNO over 'Open Overheid'. In dit onderzoek geeft TNO aan dat nieuwe internettechnologieën, zoals mobiel internet en web 2.0, nieuwe mogelijkheden bieden om overheidsinformatie toegankelijk te maken en te hergebruiken.

1.2. Reactie regering rapporten
De leden van de CDA-fractie vragen naar het regeringsstandpunt ten aanzien van het rapport “Data voor daadkracht” (2007), waarin expliciet de spanning tussen veiligheid en privacy wordt behandeld. De Commissie beveelt een systematiek aan waarin inwinning en uitwisseling van informatie worden gecentraliseerd. De

leden van de CDA-fractie vragen de regering in het bijzonder in te gaan op de knelpunten die in het rapport zijn gesignaleerd rond het proces van het inwinnen van gegevens uit verschillende gekoppelde (externe) databases.

Bij brief van 30 augustus 2007 aan de Voorzitter van de Tweede Kamer (Kamerstukken II 2006/07, 30 800 VII en 30 800 VI, nr. 65) heeft de toenmalige Minister van Binnenlandse Zaken en Koninkrijksrelaties, mede namens de ministers van Defensie en Justitie, het rapport, voorzien van een reactie, aan de Tweede Kamer aangeboden. Daarin wordt de hoofdconclusie van de Commissie om tot centrale informatieuitwisseling over te gaan niet in z'n integraliteit overgenomen. Voor een nadere toelichting op dit standpunt wordt verwezen deze reactie.

In voornoemde reactie uit 2007 wordt diverse malen verwezen naar de nieuw vast te stellen kabinetsvisie op veiligheid en privacy. 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 is bij brief van 3 november 2009 aan de Voorzitter van de Tweede Kamer aangeboden (Kamerstukken II 2009/10, 31051, nr. 5). Vervolgens heeft een schriftelijk overleg met uw Kamer heeft plaatsgevonden. Het huidige kabinet volgt de door het vorige kabinet ingeslagen weg als het gaat om de visie op privacy en veiligheid, hetgeen ook blijkt uit de notitie privacybeleid. Verderop in deze reactie zal (onder 2.1. Toetsingskader) nader worden ingegaan op de actuele uitgangspunten en het toetsingskader van het kabinet ten aanzien van maatregelen op het gebied van privacy en veiligheid.

De leden van de PvdA-fractie stellen enkele vragen naar aanleiding van het rapport "Check-in Check-out, De digitalisering van de openbare ruimte" (Rathenau Instituut, 2010) over het gebruik van persoonsgegevens voor de opsporing. Ten eerste wijzen deze leden erop dat in het rapport een beschrijving van de technische realisatie van herroepbare privacy in de sfeer van de opsporing wordt gegeven door middel van het opbouwen van een digitale identiteit en het gebruik van versleuteling. Deze leden vragen om een reactie van de regering op deze invulling van de afweging tussen privacy en veiligheid. Daarnaast wensen deze leden te vernemen of de regering de opvattingen in het rapport deelt dat burgers inzicht dienen hebben in de bevoegdheden van opsporingsinstanties en dat de overheid duidelijk dient te maken in welke situaties en hoe opsporingsinstanties gebruik mogen maken van de informatie.

Met de leden van de PvdA-fractie is het kabinet van mening dat burgers inzicht dienen te hebben in het gebruik van informatie door opsporingsinstanties. Naar ons oordeel vloeit een dergelijke opvatting ook voort uit het idee van de rechtsstaat en de daarmee samenhangende 'checks and balances' in de relatie tussen de overheid en de burger. De inzet van strafvorderlijke bevoegdheden die vrijheden of grondrechten van burgers aantasten, vereisen een basis in de wet in formele zin. Ingevolge artikel 8, tweede lid, van het EVRM is beperking van het recht op eerbiediging van de persoonlijke levenssfeer alleen toegestaan voor zover daarin bij de wet is voorzien en dit in een democratische samenleving noodzakelijk is in het belang van enkele met name genoemde doelen, waaronder het voorkomen van strafbare feiten. De regeling moet voor de burger voldoende toegankelijk en voorzienbaar zijn. Deze moet bovendien voldoende precies zijn geformuleerd en waarborgen bieden tegen willekeur en misbruik van bevoegdheid. Dit betekent dat de wet de gevallen en gronden moet omschrijven

waarin en waartoe de bevoegdheid kan worden toegepast en dat de reikwijdte van de bevoegdheid helder is. Ook de aanwijzing van de bevoegde autoriteit en voorzieningen voor transparantie en controleerbaarheid, zoals voorschriften voor motivering, verbalisering en verslaglegging, zijn van belang om duidelijk te maken in welke situaties en hoe opsporingsinstanties gebruik mogen maken van de verkregen informatie.

Het Wetboek van Strafvordering bevat een wettelijke regeling omtrent de bevoegdheden tot het vorderen van gegevens door met opsporing belaste instanties. Het betreft de bevoegdheid tot het vorderen van identificerende gegevens (artikelen 126nc en 126uc), andere dan identificerende gegevens (artikelen 126nd en 126ud), toekomstige gegevens (artikelen 126ne en 126ue,), gevoelige gegevens (artikelen 126nf en 126uf), medewerking aan het ontsleutelen van versleutelde gegevens (artikelen 126nh en 126uh) en de doorzoeking tot ter vastlegging van gegevens (artikel 125i) . Deze regeling voorziet in nauwkeurig omschreven bevoegdheden en legt de verantwoordelijkheid voor de gegevensvergaring bij de met opsporing belaste instanties. Bij de totstandkoming van de regeling zijn het belang van de opsporing, het belang van de derde van wie de gegevens gevorderd worden en het belang van degene op wie de gegevens betrekking hebben zorgvuldig tegen elkaar afgewogen. Naar ons oordeel is hiermee sprake van een evenwichtige regeling met voldoende waarborgen voor de bescherming van de persoonlijke levenssfeer van betrokkenen. Nadere regelingen worden op dit moment niet voorzien.

De leden van de GroenLinks-fractie vragen naar het standpunt van de regering ten aanzien van het rapport en de aanbevelingen van het rapport van de Algemene Rekenkamer over open standaarden en open source software.

Graag verwijzen wij hiervoor naar de reactie van de Minister van Binnenlandse Zaken (Kamerstukken II 2010/11 32 679 nr. 1 en 2) zoals opgenomen in het rapport van de Rekenkamer.

2. Toetsing

2.1. Toetsingskader
De leden van de fracties van CDA en PvdA constateren dat zowel in het rapport 'Gewoon doen' van de commissie Brouwer-Korf als het rapport iOverheid van de WRR een richtinggevend afwegingskader is geformuleerd, dat kan dienen als handvat bij de afweging tussen de bescherming van de persoonlijke levenssfeer en de veiligheid van de burger enerzijds en de digitalisering van de samenleving anderzijds. Deze leden wensen te vernemen hoe de regering voornemens is deze kaders te hanteren en waar sprake is van samenhang tussen beide kaders.
Ook de leden van de GroenLinks-fractie vragen de regering in te gaan op de belangafweging tussen veiligheid, effectiviteit en privacy uit het WRR-rapport. Zij verzoeken hierbij aandacht te besteden aan specifieke thema's als ANPR, de VerwijsIndex Risicojongeren, het SchengenInformatie Systeem en het EPD.

Wij erkennen dat het gebruik van ICT door de overheid gevolgen kan hebben voor de burger. Wij zijn van oordeel dat de wetgever de burger dient te beschermen tegen negatieve aspecten van de informatiesamenleving op de bescherming van zijn persoonlijke levenssfeer. Het regeerakkoord bevat hiertoe initiatieven, zoals een meldplicht datalekken – die zal worden uitgewerkt in de Wbp - en

aanscherping van het toezicht op grootschalige informatiseringsprojecten. Bij de invoering van grootschalige ICT-netwerken in het overheidsdomein dient vooraf een effectiviteitstoets plaats te vinden. Voor zover het gaat daarbij gaat om maatregelen in de sfeer van wetgeving zullen de ministeries van Veiligheid en Justitie en Binnenlandse Zaken en Koninkrijksrelaties, uit een oogpunt van wetgevingskwaliteitsbeleid, meer gaan toezien op de juridische eisen die voortvloeien uit de Wbp en het Europees en internationaal echt. Bij die toetsing komt ook aan de orde of een wetsvoorstel is voorzien van een evaluatiebepaling en of het opnemen van een horizonbepaling aan de orde is.

In de kabinetsreactie op het WRR-rapport zal het kabinet met een visie komen op de conclusies uit in het WRR-rapport, waarbij ook de door de WRR geformuleerde criteria voor de afweging van de bescherming van de persoonlijke levenssfeer en de digitalisering van de samenleving zullen worden betrokken. In afwachting van dit kabinetsstandpunt zullen wij ons hieronder beperken tot een uiteenzetting over hoe wij het toetsingskader bij (wettelijke) maatregelen op het gebied van privacy en de veiligheidszorg voor ons zien. In dat verband wensen wij tevens een antwoord te geven op de vraag van de leden van de SP-fractie die vragen naar het standpunt van de regering met betrekking tot de door Eurocommissaris Reding geconstateerde onbalans tussen het bewaken van de veiligheid en het recht van de burger op bescherming van zijn persoonlijke levenssfeer, een constatering die door de leden van deze fractie overigens wordt gedeeld.

Het kabinet is, evenals het vorige kabinet, van mening dat bescherming van de persoonlijke levenssfeer en de zorg voor veiligheid van samenleving en individu niet noodzakelijkerwijs tegengestelde belangen zijn, maar belangen die zorgvuldig tegen elkaar moeten worden afgewogen. Het kabinet rekent het tot zijn taak om beide belangen te beschermen. Onder omstandigheden kan de afweging neerkomen op het aanvaarden van een beperking van de persoonlijke levenssfeer ten behoeve van de zorg voor veiligheid van de samenleving.
Elke maatregel dient individueel te worden afgewogen. In geval van uitwerking door middel van wettelijke maatregelen dient een transparante toetsing aan de grondrechten plaats te vinden. In het kader van de wetgevingstrajecten rondom de thema's waarnaar de leden van GroenLinks in de vraagstelling verwijzen heeft deze toetsing telkens plaatsgevonden.

In de notitie privacybeleid geeft het kabinet aan niet met een nieuwe beleidsvisie op het gebied van veiligheid en privacy te komen, maar de ingeslagen weg van het vorige kabinet verder te willen volgen. De criteria van de Commissie Brouwer-Korf zijn daarbij richtinggevend, maar verdienen nog wel nadere uitwerking. In de notitie privacybeleid kondigt het kabinet een aantal maatregelen ter uitwerking van het richtinggevend kader aan, variërend van feitelijke maatregelen, zoals de oprichting van een servicecentrum privacy en veiligheid voor professionals, tot wetgevende maatregelen ter aanvulling van de Wbp.

De leden van de PvdA-fractie vragen nog of de regering de ontwerpprincipes uit het rapport Check in/check out van het Rathenau Instituut op onderdelen wellicht in hogere mate hanteerbaar achten dan het richtinggevend kader van de Commissie Brouwer-Korf.

Uit het voorgaande mag blijken dat het kabinet, als het gaat om afwegingen met betrekking tot gegevensverwerking in het veiligheidsdomein, het richtinggevend kader van de Commissie Brouwer – Korf leidend acht. De ontwerpprincipes in het

rapport 'Check In/Check uit', van het Rathenau Instituut zien op identiteitsbeheer in de gedigitaliseerde openbare ruimte, waarmee sprake is van een andere invalshoek. In de kabinetsreactie op het WRR-rapport zal het kabinet met een visie op het gebruik van persoonsgegevens door de overheid in een digitale samenleving komen.

De leden van de SP-fractie vragen naar de stand van zaken omtrent een overkoepelend beoordelingskader in het kader van de Wet algemene bepalingen BSN. In de brief van 25 augustus 2010 (kenmerk: 2010-0000546862) heeft de toenmalige Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties aan de voorzitter van de Eerste Kamer gerapporteerd dat er op dat moment geen basis bestond om te komen tot een overkoepelend beoordelingskader. In deze brief is de huidige stand van zaken weergegeven, namelijk dat er momenteel ter zake geen nieuwe wetgeving of wetswijzigingen zijn ingediend, op basis waarvan een overkoepelend beoordelingskader kan worden opgesteld. In een daaropvolgende brief van 28 september 2010 heeft uw Kamer het verzoek hernieuwd om over twee jaar te rapporteren over de mogelijkheid om te komen tot een overkoepelend beoordelingskader. Hierop heeft de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties op 13 oktober 2010 bevestigend geantwoord.

De leden van de GroenLinks-fractie vragen welke criteria zijn te destilleren uit het Marper-arrest van het EHRM voor het gebruik en de opslag van persoonsgegevens.

Uit het arrest van het EHRM van 4 december 2008 (app.nr. 30562/04 en 30566/04), S. en Marper tegen Verenigd Koninkrijk kan in elk geval worden afgeleid dat bij de vaststelling van wetgeving met betrekking tot het gebruik van persoonsgegevens als DNA en ander lichaamsmateriaal een strenge toets moet worden aangelegd om de relatief vergaande inmenging in het privé-leven van de betrokkenen die het aangaan te rechtvaardigen. Deze persoonsgegevens kunnen leiden tot de openbaring van gegevens betreffende etniciteit en hebben, door hun aard ook betekenis voor andere betrokkenen die met de betrokkene een familierelatie hebben. In dit verband verwijzen wij graag naar de memorie van toelichting bij het voorstel van wet tot wijziging van het Wetboek van Strafvordering en de Wet DNA-onderzoek bij veroordeelden in verband met de introductie van DNA-verwantschapsonderzoek en DNA-onderzoek naar uiterlijk waarneembare persoonskenmerken van het onbekende slachtoffer en de regeling van enige andere onderwerpen (Kamerstukken II 2009/10, 32 168, nr. 3) waarin uitgebreid wordt ingegaan op deze materie. Wat het gebruik van vingerafdrukken betreft, wijzen wij erop dat met ingang van 1 oktober 2010 een nieuwe regeling in het Wetboek van Strafvordering in werking is getreden die het gebruik van deze persoonsgegevens aan meer voorwaarden met betrekking tot de persoonlijke levenssfeer bindt dan voorheen het geval was. Wij zijn ervan overtuigd dat deze regeling een toets aan de eisen, voortvloeiend uit het EVRM kan doorstaan.

2.2. Leidraad voor de wetgever
De leden van de CDA-fractie vragen hoe ver het ministerie van Veiligheid en Justitie is gevorderd met het opstellen van de Leidraad afstemmen van de wetgeving op de Wet bescherming persoonsgegevens en of de volgende criteria daarbij zijn gebruikt: noodzaak (en effectiviteit), proportionaliteit, privacy impact

assessment, controle en toezicht en horizonbepaling. Deze leden wensen tevens te vernemen of de criteria uit deze leidraad al rijksbreed worden gehanteerd.

De Leidraad afstemmen van de wetgeving op de Wet bescherming persoonsgegevens is in juli 2010 gepubliceerd en is een uitgave van het ministerie van Veiligheid en Justitie. Een fysiek exemplaar van de leidraad is als bijlage bij deze bijlage gevoegd. De leidraad is opgesteld door een werkgroep bestaande uit wetgevingsjuristen van diverse ministeries en van de Raad van State. De leidraad heeft het als doel om de wetgevingspraktijk zo goed mogelijk te ondersteunen bij de ontwikkeling van regelingen waarbij informatieverwerking als beleidsinstrument wordt ingezet. Dit gebeurt door de Wbp en de wijze waarop wetgeving op de Wbp moet worden afgestemd in de leidraad onder de aandacht van de wetgevingspraktijk te brengen. De leidraad bevat hiertoe onder meer een aantal concrete adviezen, waarbij de bovengenoemde criteria elk aan bod komen. De leidraad is bedoeld voor en wordt gebruikt door wetgevingsjuristen die werkzaam zijn op de wetgevingsafdelingen van de ministeries en de Raad van State. Verder kan de leidraad van nut zijn voor beleidsambtenaren en diegenen die werkzaam zijn bij instanties die door middel van adviserende of toezichthoudende taken invloed uitoefenen op de keuze die aan nieuwe regelgeving ten grondslag liggen. De leidraad is elektronisch beschikbaar voor deze doelgroep op de website van het Kenniscentrum Wetgeving.

Met betrekking tot het vijfde criterium, de horizonbepaling, wensen wij graag nog het volgende op te merken. In het regeerakkoord heeft het kabinet verschillende maatregelen in het vooruitzicht gesteld om de bescherming van persoonsgegevens te verbeteren, waaronder het gebruik van een horizonbepaling in wetgeving. In de notitie privacybeleid stelt het kabinet zich op het standpunt dat een horizonbepaling een optie is voor die gevallen waarin dat gelet op de mate en de aard van de inmenging in de grondrechten en de te plegen investeringen in ICT gerechtvaardigd is. Enige terughoudendheid is daarbij geboden.

De ontwikkeling van de Leidraad is ook aanleiding geweest om in de Aanwijzingen voor de regelgeving (Ar) enkele aanwijzingen op te nemen die betrekking hebben op de positie van de Wbp en het verwerken van persoonsgegevens als beleidsinstrument. Een omvangrijke wijziging van de Ar, waarin deze regels zijn opgenomen, is inmiddels vastgesteld en zal op zeer korte termijn in werking treden.

2.3. Privacy Impact Assessment
De leden van de CDA-fractie vragen of het door het ministerie van Veiligheid en Justitie in overleg met het College bescherming persoonsgegevens (Cbp) en VNO/NCW geïnitieerde kader Privacy Impact Assessments (PIA's) al wordt gehanteerd. In dit verband wijzen deze leden nog op een recent verschenen proefschrift over het nut van Privacy Enhancing Technologies. Dergelijke technische toepassingen kunnen de belastende gevolgen van privacybeperkende maatregelen sterk reduceren. Ook de leden van de PvdA-fractie vragen naar de stand van zaken ten aanzien van de ontwikkeling van PIA's. De leden van de SP-fractie wijzen op het pleidooi vanuit het Cbp voor Privacy by design in de architectuur van nieuwe ICT producten. PIA's voor, tijdens en na de ontwikkeling van een groot ICT project zijn nodig om steeds het effect op de privacy te kunnen blijven bewaken, aldus deze leden. Zij wensen te vernemen of de regering overweegt deze vorm van toezicht wettelijk verplicht te stellen.

Met het Cbp is het kabinet van mening dat privacy by design een goede manier is om privacybescherming concreet vorm te geven in informatiesystemen waarin persoonsgegevens worden verwerkt. Door toepassing van privacy by design wordt gegevensbescherming vanaf het begin meegenomen in het systeemontwerp. Het kabinet wil de toepassing van privacy by design stimuleren. Daarvoor is kennis van de kansen en de belemmeringen voor de toepassing noodzakelijk. Het ministerie van Economische Zaken, Landbouw en Innovatie heeft TNO gevraagd hiernaar onderzoek te doen.
Het kabinet ondersteunt de initiatieven vanuit het bedrijfsleven voor het ontwikkelen van PIA´s, maar is geen voorstander van het verplicht voorschrijven van het gebruik van PIA´s in wetgeving. Naar het oordeel van het kabinet zou een dergelijke verplichting leiden tot een onevenredig zware (financiële) belasting voor het bedrijfsleven. In de notitie privacybeleid wordt nog uitgebreider ingegaan op de visie van het kabinet op het beginsel van privacy by design en de ontwikkeling van PIA's.

3. Toezicht

De leden van de CDA vragen of de regering wil ingaan op de gemaakte opmerkingen in de brief van het Cbp van 6 december 2010 aan de Tweede Kamer der Staten-Generaal over de verantwoordelijkheid van de functionaris voor de gegevensbescherming.

Het kabinet beschouwt de brief van het Cbp als een belangrijke ondersteuning van de inzet ten aanzien van de herziening van de richtlijn en voelt zich gesteund door het Cbp waar het de uitwerking van het beginsel van accountability betreft. De notitie privacybeleid bevat een integrale reactie op de brief van het Cbp. Kortheidshalve wordt hiernaar verwezen.

De leden van de SP-fractie wensen te vernemen welke instantie toezicht houdt op grensoverschrijdend gegevensverkeer.

Op grensoverschrijdend verkeer van persoonsgegevens is de privacyrichtlijn van toepassing. Het aangrijpingspunt bij grensoverschrijdend gegevensverkeer binnen de EU is de plaats waar de verantwoordelijke is gevestigd. Als een verantwoordelijke meerdere vestigingen heeft binnen de EU, dan dient hij in alle lidstaten waarin hij een vestiging heeft te voldoen aan de regels. Als de verantwoordelijke geen vestiging heeft binnen de EU, maar wel met behulp van zich binnen een of meerdere lidstaten van de EU persoonsgegevens verwerkt, zijn de regels van de locatie van de voor gegevensverwerking gebruikte fysieke middelen van toepassing. Wat betreft het grensoverschrijdend gegevensverkeer met landen buiten de EU geldt dat, voor zover de gegevens worden verwerking in een lidstaat binnen de EU, de wetgeving van de desbetreffende lidstaat van toepassing is. De richtlijn eist dat een verantwoordelijke een vertegenwoordiger aanwijst op het grondgebied van de lidstaat. De nationale toezichthouders zien toe op naleving van de desbetreffende privacyregels.

De leden van de PvdA-fractie wensen te vernemen hoe de regering zou staan tegenover een verzoek om adequate voorzieningen voor het parlement met betrekking tot informatievoorziening over technische aspecten met grote beleidsmatige gevolgen waarvoor specifieke deskundigheid noodzakelijk is. Ter illustratie wijzen deze leden naar de drie expertmeetings die nodig waren voor de

informatievoorziening over het EPD en uiteindelijk ook voor het onderhavige beleidsdebat.

Voor zover uw Kamer van mening is dat een adequate informatievoorziening ontbreekt om haar taken goed te kunnen uitoefenen op specialistische terreinen als het onderhavige, staat het uw Kamer naar ons oordeel volkomen vrij hiervoor de nodige voorzieningen te treffen, zoals het inwinnen van externe deskundigheid. Aan het voorstel van de WRR voor een Commissie iOverheid die jaarlijks rapporteert aan het parlement zal in de kabinetsreactie op het WRR-rapport aandacht worden besteed.

3.1. Bevoegdheden Cbp
De leden van de CDA-fractie vragen om een uiteenzetting over de wijze waarop aan de aanbeveling van de commissie Brouwer- Korf om het extern toezicht robuuster te maken gevolg wordt gegeven. Ook de leden van de PvdA-fractie wensen de huidige stand van zaken op dit punt te vernemen, mede naar aanleiding vanuit signalen van het Cbp. Deze leden wijzen erop dat het Cbp de effectiviteit van haar eigen mogelijkheden tot handhaving niet sterk vindt en vragen naar het standpunt van de regering ten aanzien hiervan.

Met deze leden zijn wij van mening dat het sanctieinstrumentarium van het Cbp versterking verdient. In voornoemde brief over het privacybeleid en de notitie privacybeleid wordt versterking van het sanctieinstrumentarium aangekondigd, waaronder de invoering van de bestuurlijke boete voor het Cbp en het opnieuw bezien van het strafrechtelijk instrumentarium.

De leden van het CDA wensen te vernemen of het aanbeveling verdient om het College bescherming persoonsgegevens zelf de bevoegdheid te geven om in ernstige gevallen een overtreding bij de rechter aan te brengen.

Een dergelijke aanbrengmogelijkheid voor het Cbp wordt thans niet overwogen en past ook niet bij de rol die het Cbp inneemt als zelfstandig bestuursorgaan dat verantwoordelijk is voor het toezicht op de naleving van de Wbp. In geval van overtreding van de Wbp is het Cbp zelf bevoegd om een sanctie op te leggen. Tegen besluiten van het Cbp kan desgewenst beroep worden ingesteld bij de bestuursrechter. In een beperkt aantal gevallen zijn strafrechtelijke sancties mogelijk.

Het is niet uitgesloten dat in de wetgevingsvoorstellen van de Commissie wel een rol, vergelijkbaar met die waarop de leden van de CDA-fractie doelen, wordt opgenomen voor de nationale toezichthouders. Dat doet enigszins denken aan de positie van de Consumentenautoriteit in de Wet handhaving consumentenbescherming. Wij zijn daar niet op voorhand tegen gekant en wachten de voorstellen van de Commissie graag af.

Het Cbp combineert taken die volgens de idee van de trias politica niet bij elkaar horen, zo stellen de leden van de SP-fractie. Het Cbp is toezichthouder en handhaver, is betrokken bij beleidsvorming en adviseert de regering over wetgeving. Deze leden wensen te vernemen wie het onderscheid tussen deze taken bewaakt.

Het Cbp is gepositioneerd als zelfstandig bestuursorgaan en functioneert onafhankelijk van de overheid. De privacyrichtlijn verplicht hier overigens ook

toe. De taakomschrijving van het Cbp is neergelegd in de hoofdstukken 9 en 10 van de Wbp. Binnen de kaders van de wet is het Cbp zelf verantwoordelijk voor de verdere invulling van zijn taken. Op grond van de Kaderwet ZBO's heeft de Staatssecretaris van Veiligheid en Justitie enkele bevoegdheden om de ministeriële verantwoordelijkheid ten aanzien van het Cbp als zelfstandig bestuursorgaan waar te kunnen maken. Deze bevoegdheden zien nadrukkelijk niet op de inhoudelijke taakuitoefening van het Cbp. Zo is het Cbp volledig vrij in zijn prioriteitstelling.

De leden van de SP-fractie wensen te vernemen hoe de regering denkt over de positie van het Cbp na verwerping van het wetsvoorstel 31 466 L-EPD. Het Cbp heeft twee jaar een onwettige situatie gedoogd, namelijk dat zorgaanbieders zonder wettelijk grondslag patiëntgegevens aanmeldden en uitwisselden, zonder voorafgaande toestemming van de patiënt zelf.

In de bijlage van de brief van 11 april 2011 heeft de Minister van Volksgezondheid, Welzijn en Sport aan uw Kamer gemeld dat er geen sprake is geweest van een onwettige situatie bij het L-EPD. De wettelijke grondslag van het L-EPD voor inwerkingtreding van het wetsvoorstel EPD is beschreven in de brief aan uw Kamer van 14 juni 2010. Hierin is aangegeven dat voor inwerkingtreding nog geen verplichting geldt tot aansluiting van de zorgaanbieder op het LSP. De uitwisseling dient wel te voldoen aan de eisen van de Wbp en de Wet op de geneeskundige behandelovereenkomst. Zorgverleners moeten volgens de huidige wetgeving een dossier over de patiënt bijhouden. Gegevens die uitgewisseld kunnen worden via de landelijke infrastructuur maken onderdeel uit van dit dossier. Als een huisarts op een huisartsenpost, een apotheker of een medisch specialist gegevens wil inzien via het LSP moet hij daarvoor eerst toestemming vragen van de patiënt. Ook voor het uitwisselen van de gegevens tussen zorgverleners geldt dat dit alleen mogelijk is met toestemming van de patiënt. Op het moment dat een andere zorgverlener dan de eigen zorgverlener gegevens wil opvragen over een patiënt, zal expliciet om toestemming moeten worden gevraagd. Zonder deze toestemming mag de zorgverlener geen gegevens raadplegen. Daarnaast is iedere patiënt de mogelijkheid geboden om voorafgaand aan de uitwisseling van de medische gegevens tussen de zorgverleners aan te geven niet te willen deelnemen aan het EPD.
Wanneer het Cbp van mening is dat er sprake is van een onwettige situatie is het aan het Cbp om te beoordelen welke acties noodzakelijk zijn.

3.2. Voorstellen voor 'iPlatform en iAutoriteit'
Zoals hiervoor aangegeven, zal het kabinet in een later stadium een kabinetsreactie uitbrengen naar aanleiding van het iOverheid-rapport van de WRR. Hierin zal ook worden ingegaan op de aanbevelingen die betrekking hebben op de wenselijkheid van instelling of oprichting van een zogenaamd iPlatform en een iAutoriteit.

4. Doelbinding

De leden van de CDA-fractie, wijzen, mede naar aanleiding van de op 21 februari 2011 gehouden expertmeeting in de Eerste Kamer op het ontstaan van een vernetwerkte wereld. Al deze koppelingen en netwerken veroorzaken dat aan de doelbinding van de individuele systemen niet meer of niet voldoende de hand wordt of kan worden gehouden. Deze leden stellen de vraag hoe de noodzakelijke

afwegingen (kunnen) worden gemaakt om de doelbinding van de systemen toch te realiseren.

Wij brengen de leden van de CDA-fractie graag in herinnering dat op het vlak van wetgeving al het nodige wordt gedaan aan effecten van wat tijdens de expertmeeting als de vernetwerkte samenleving werd aangeduid. Vele wetten bevatten regels over een verplichte gegevensverstrekking. Er is meer aandacht voor de regelgeving van samenwerkingsverbanden in de Wet politiegegevens en op grond van de Wet justitiële en strafvorderlijke gegevens. In 2008 is door het vorige kabinet een rapport naar de Tweede Kamer gestuurd van de ambtelijke werkgroep "Herijking toezichtsregelgeving" waarin zeer nadrukkelijk aandacht wordt gegeven aan het formuleren van wettelijke voorschriften die de - overigens noodzakelijke en ook onvermijdelijke - gegevensverstrekkingen regelen in het domein van het toezicht en de handhaving. Dat gebeurt juist met het oog op de doelbinding. Dat gebeurt ook met het oog op de noodzaak deze gegevensoverdrachten met een maximum aan transparantie en democratisch gehalte te kunnen vaststellen. Het is dus bepaald niet zo dat het kabinet hier geen initiatieven heeft genomen.

De leden van de fractie van het CDA wensen te vernemen of het juist is dat gegevens van de OV-chipkaart kunnen worden gebruikt als opsporingsmiddel en wat de bewaartermijn van de gegevens is.

Hiervoor is al uiteengezet dat het Wetboek van Strafvordering een regeling biedt voor het vorderen van gegevens in het kader van de opsporing van strafbare feiten. In geval van verdenking van een misdrijf kunnen opsporingsinstanties in het belang van het onderzoek onder meer identificerende en opgeslagen gegevens vorderen. Voor zover sprake is van gevoelige gegevens is een voorafgaande machtiging van de rechter-commissaris vereist. In voorkomende gevallen kan het OM voornoemde gegevens opvragen bij de kaartuitgever en de deelnemende bedrijven aan de OV-chipkaart.

Het Cbp is in 2010 een onderzoek gestart naar de bewaartermijn van gegevens door verschillende vervoersbedrijven. In reactie op vragen van het Tweede Kamerlid Bashir (Aanhangsel Handelingen II 2010/11 1354) over het te lang bewaren van persoonsgegevens door vervoersbedrijven en Trans Link heeft de Minister van Infrastructuur en Milieu te kennen gegeven dat er sprake is van een lopende procedure bij een onafhankelijke toezichthouder waarvan de uitkomst wordt afgewacht.

De leden van de PvdA-fractie wijzen erop dat het richtinggevend kader in het rapport van de commissie Brouwer-Korf geen nadere criteria voor de afweging tussen privacy en veiligheid bevat, hetgeen door emeritus hoogleraar informatierecht prof. Dommering (UvA) als de bijl aan het beginsel van de doelbinding werd gekarakteriseerd.

Het kabinet is op de hoogte van de - zeer boeiende - beschouwing van prof. Dommering "Recht op persoonsgegevens als zelfbeschikkingsrecht" die hij schreef in de bundel "16 miljoen BN'ers, Bescherming van Persoonsgegevens in het Digitale Tijdperk" (Leiden, 2010). Prof. Dommering wijst er terecht op dat de Adviescommissie veiligheid en de persoonlijke levenssfeer nalaat inhoudelijke criteria te beschrijven waaronder het recht op bescherming van persoonsgegevens in concreto moet wijken voor het belang van de veiligheid.

Nadere uitwerking is dan ook noodzakelijk, zoals het kabinet ook erkent in de notitie privacybeleid. Dit gebeurt deels in de vorm van feitelijke maatregelen en deels in de vorm van wetgeving.

In de brief aan de Voorzitter van de Eerste Kamer (Kamerstukken I 2009/10, 31 051, A) is, in reactie op een vergelijkbare vraag van de leden van de PvdA, eerder uiteengezet dat een aanvulling van de Wbp met een grondslag voor de verdere verwerking van persoonsgegevens ten behoeve van de veiligheid van het individu als een verduidelijking en nadere concretisering van een reeds bestaande regeling moet worden gezien. In de notitie privacybeleid wordt hieraan toegevoegd dat de EU-privacyrichtlijn voldoende ruimte biedt om een regeling te treffen voor het delen van gegevens wanneer het vitaal belang (daaronder wordt verstaan een onmiddellijke of dreigende aantasting van leven of gezondheid) van de betrokkene of een derde dat vergt. Wij zijn van oordeel dat daarmee een verantwoorde afweging van belangen van de betrokkene en die van anderen in concreto kan worden uitgevoerd.

De leden van de SP-fractie vragen naar het belang dat wordt gehecht aan externe onafhankelijke audits door teams die ook een hoge mate van ICT deskundigheid in zich moeten bergen. Zij vragen voorts of de overheid zelf over voldoende kennis en inzicht in ICT systemen beschikt om de resultaten te kunnen beoordelen.

Het kabinet is van mening dat externe onafhankelijke audits belangrijk zijn. Externe kwaliteitstoetsen zijn een integraal onderdeel in beheersing van grote en hoogriscio ICT-projecten evenals in de verantwoording in de vorm van de rapportage grote en hoogriscio ICT-projecten. Externe kwaliteitstoetsen worden uitgevoerd door voldoende onafhankelijke en professionele partijen en hebben betrekking op: de meest kritische aspecten van de projectbeheersing (kosten, baten, risico's, mijlpalen en planning). Daarbij wordt gebruik gemaakt van breed geaccepteerde beheersingsmodellen als MSP en Prince2, waarbij het niet alleen gaat om procedurele correctheid (formele toets), maar vooral ook of sprake is van een adequate projectbeheersing voor het realiseren van de gestelde projectdoelen en de (beheersing van de) kwaliteit van de door het project opgeleverde (deel-)producten. De uitvoering van externe kwaliteitstoetsen wordt bij voorkeur gerelateerd aan beslismomenten, waarbij de projectstart als een belangrijk beslismoment wordt gezien. Bij belangrijke wijzigingen in het projectplan gedurende de projectduur, wordt deze paragraaf met externe kwaliteitstoetsen herbeoordeeld en zonodig herzien. Externe kwaliteitstoetsen kunnen zowel Gateway reviews zijn, als audits door interne of externe partijen of adviezen van experts. In de eerder genoemde rapportage grote en hoogrisico ICT-projecten worden per project de uitgevoerde externe kwaliteitstoetsen vermeld.

5. Ondersteuning en rechten van burgers

5.1. Ondersteuning van burgers

De leden van de PvdA-fractie refereren aan uitlatingen van diverse experts tijdens de expertmeeting op 21 februari 2011 in de Eerste Kamer over de digitalisering van de samenleving. De verdergaande digitalisering, deze leden wijzen op het verschijnsel van een vernetwerkte wereld, noodzaakt tot goede advisering en voorlichting van de burger. De leden van de PvdA-fractie wensen te vernemen of het klopt dat voor de advisering van professionals in het kader van het rapport

Brouwer- Korf, per 1 maart 2011 slechts 3 fte's zijn vrijgemaakt, hetgeen als teleurstellend ervaren wordt. Tevens vragen deze leden hoe een en ander zich verhoudt tot de risico's van de gedigitaliseerde samenleving voor burgers en wat de regering voornemens is hiertegen te ondernemen ter bescherming van haar burgers. Daarnaast vragen deze leden met verwijzing naar schriftelijk overleg over de kabinetsreactie op het rapport van de commissie Brouwer- Korf waarin zij hun zorgen hebben geuit over de uitholling van privacywaarborgen door onder meer achterblijvende bewustwording bij professionals en burgers, naar de recente stand van zaken op dit punt. Tot slot vragen de leden, met verwijzing naar het eerdergenoemde rapport 'Check in/Check uit', of de regering voornemens is initiatieven te stimuleren die gebruikers helpen bij de onderhandeling met de aanbieder over het gebruik van persoonsgegevens en de beperking tot het overeengekomen gebruik.

Het kabinet is voornemens de professional in het veiligheidsdomein beter te ondersteunen door de oprichting van een servicecentrum privacy en veiligheid. Op 1 januari 2011 is gestart met de inrichting van dit servicecentrum binnen het ministerie van Veiligheid en Justitie. Het servicecentrum richt zich op ondersteuning van professionals in de sector veiligheid en justitiële jeugdzorg. Het servicecentrum zal op 1 januari 2012 operationeel zijn en zal op vraaggedreven wijze ondersteuning gaan geven aan de professionele praktijk. Voor de bezetting van het servicecentrum zijn 3 fte's beschikbaar gesteld. Verwacht wordt dat op deze wijze voldoende ondersteuning geboden kan worden aan professionals in het veiligheidsdomein.

Wat betreft de ondersteuning van burgers merken wij op dat het Cbp recent initiatieven genomen heeft om de voorlichting aan burgers uit te breiden. Zo is het telefonisch spreekuur voor burgers onlangs uitgebreid naar vijf dagen per week. Daarnaast biedt de website www.mijnprivacy.nl algemene informatie over de rechten van burgers op het gebied van privacy. Via een signaalformulier kunnen burgers het CBP informeren over mogelijke overtredingen op het gebied van privacy. Ook bevat de site tal van modelbrieven. Het kabinet is op dit moment niet voornemens nog op nadere wijzen het contact van gebruikers met aanbieders over gebruik van hun persoonsgegevens te stimuleren.

5.2. Rechten van burgers
De leden van de CDA-fractie wijzen op het WRR-rapport waarin de WRR spreekt over het belang van het recht om vergeten te worden. Deze leden vragen hoe de regering tegen een cultuuromslag aankijkt waarin de vrijheid van informatievergaring wordt beperkt. Als voorbeeld van een dergelijke omslag noemen deze leden een plicht van de overheid om gegevens uit databestanden na een bepaalde tijd te verwijderen en een regeling in het privaatrecht (het arbeidsrecht) dat het verstrekken van bepaalde informatie geweigerd kan worden. Ook de leden van de PvdA-fractie vragen naar het standpunt van de regering ten aanzien van het recht om vergeten te worden, zoals eveneens bepleit tijdens de expertmeeting in de Eerste Kamer op 21 februari 2011. De leden van de SP-fractie wensen graag specifiek te vernemen wat onder het recht van vergeten dient te worden verstaan en of dit een verantwoordelijkheid van de overheid is.

Graag brengen wij in herinnering dat de Wbp (artikel 10) al voorschrijft dat persoonsgegevens niet langer worden bewaard dan noodzakelijk. De bepaling richt zich tot de verantwoordelijke. Deze dient te bepalen welke gegevens om welke redenen voor welke termijn bewaard mogen worden. Soms wordt de

bewaartermijn ook specifiek vastgelegd in bijzondere wetgeving. Het kabinet ziet het gebruik van bewaartermijnen als een goede invulling van het beginsel van de transparantiebeginsel en wil de handhaving hiervan versterken, Daarom kondigt het kabinet in de brief over het privacybeleid een aanvulling van de Wbp aan met een verplichting voor de verantwoordelijke om de door hem vastgestelde bewaartermijn bekend te maken.

In Europees verband wordt momenteel gesproken over het recht om vergeten te worden. In de Mededeling van 4 november 2010 van de Europese Commissie van 4 november 2010, COM (2010) 609 def., "Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie" besteedt de Europese Commissie aandacht aan de grotere zeggenschap van de burger over de eigen gegevens. De Commissie kondigt aan het beginsel van gegevensminimalisatie te willen versterken. Eén van de maatregelen waar de Commissie in dat verband aan denkt is het expliciteren van het recht om te worden vergeten (het verplicht wissen van persoonsgegevens na afloop van een bewaartermijn of na het intrekken van de toestemming voor die verwerking door de betrokkene). Over het recht op vergeten heeft het kabinet in de BNC-fiche over de mededeling opgemerkt dat dit vragen oproept. Dit recht bestaat in zekere zin al, omdat uit het intrekken van een gegeven toestemming of het verstrijken van een bewaartermijn toch al voortvloeit dat persoonsgegevens niet langer mogen worden verwerkt. Het kabinet meent dan ook dat primair moet worden ingezet op ondersteuning van die mogelijkheden, bijvoorbeeld door middel van verplichte bekendmaking van de bewaartermijn, zoals hierboven uiteengezet. Daarnaast roept het de vraag op hoe het recht om te worden vergeten moet worden geëffectueerd ten opzichte van derden die persoonsgegevens eerder rechtmatig hebben verwerkt, zeker als daar nog een grensoverschrijdend effect aan is verbonden.

De leden van de PvdA-fractie stellen een vraag over het cameratoezicht. Zij menen dat de wettelijke regeling de mogelijkheid bevat voor de burger om de digitale identiteit te wissen. Tegelijkertijd constateren deze leden dat deze optie niet altijd wordt geboden en dat niet iedere burger zich van de optie bewust is. Zij wensen te vernemen of de regering bereid is proactiever op te treden in deze.

Op grond van de Wbp (in geval van privaat cameratoezicht) en de Wet bescherming politiegegevens (in geval van publiek cameratoezicht) heeft een betrokkene recht op informatie over, inzage in, aanvulling, verbetering, verwijdering en afscherming van zijn persoonsgegevens. Het Cbp heeft een infoblad uitgebracht getiteld “Als u gefilmd wordt met een videocamera” www.mijnprivacy.nl waarin de rechten van de betrokkene worden beschreven. Tevens worden op deze site voorbeeldbrieven beschikbaar gesteld voor een verzoek om verwijdering of afscherming van gegevens. Daarmee wordt naar ons oordeel op goede wijze voorzien in ondersteuning van de burger. Nadere initiatieven worden op dit moment niet voorzien.

De leden van de PvdA-fractie wijzen op het rapport van de Staatscommissie-Thomassen, in het bijzonder op de aanbevelingen over aanpassing van informatie(grond)rechten naar aanleiding van ontwikkelingen in het digitale tijdperk.

Op dit moment heeft het kabinet een standpunt in voorbereiding over het rapport van de Staatscommissie.

De leden van de SP-fractie constateren dat met de inwerkingtreding van het Verdrag van Lissabon en het Handvest van de grondrechten van de EU het recht op bescherming van persoonsgegevens in EU-verband uitdrukkelijk erkend is. Graag vernemen deze leden op welke wijze dit grondrecht in de Nederlandse wetgeving wordt geïmplementeerd.

Met het Verdrag van Lissabon is er een einde gekomen aan de pijler-structuur van de Europese Unie en zijn er nieuwe algemene rechtsgrondslagen in het leven geroepen voor het grondrecht op bescherming van persoonsgegevens binnen de Unie, voor alle onderdelen van het Unierecht, behalve het gemeenschappelijk buitenlands en veiligheidsbeleid. De inwerkingtreding van de nieuwe grondslagen heeft geen gevolgen voor de bestaande (EU)wetgeving. De privacyrichtlijn, die de basis vormt voor de Nederlandse Wbp, blijft onverkort van kracht. Implementatie van de nieuwe algemene grondslagen in de Nederlandse wetgeving is niet nodig.

6. Internationale aspecten

De leden van de CDA-fractie vragen of het bewaren van de gegeven, waartoe het Verdrag van Prüm de bevoegdheid geeft, in een centrale database gebeurt en of dit al plaatsvindt of een serieus streven is. Deze leden wensen tevens te vernemen wat de overwegingen zijn om tot een dergelijke opslag te komen.

Het Verdrag van Prüm uit 2005 - dat grotendeels is opgenomen in een EU-raadsbesluit 2008/615/JBZ uit 2008 - bestaat uit afspraken voor de uitwisseling van informatie tussen EU-lidstaten. Een belangrijk onderdeel van het verdrag en het raadsbesluit is de uitwisseling van gegevens over DNA-profielen, vingerafdrukken en voertuighouders (kentekenregister) door bevoegde autoriteiten van een EU-lidstaat toegang te verlenen tot de nationale databanken van andere EU-lidstaten. Zo kunnen de bevoegde autoriteiten in lidstaten door deze verbinding vaststellen of een DNA-profiel of vingerafdruk bekend is in een ander land (hit-no hit-bevraging). Bij een treffer dienen de bevoegde autoriteiten de naamsgegevens die bij het profiel of afdruk horen, op te vragen via een regulier justitieel en politieel rechtshulpverzoek. Er is hierbij geen sprake van een centrale (op Europees niveau) opslag van gegevens.

De leden van de CDA-fractie refereren aan diverse berichten in de media waaruit blijkt dat de VS op grote schaal bankgegevens van Europese burgers hebben ingezien en waarschijnlijk nog steeds inzien. Het is bekend dat de door de SWIFT-organisatie hiertegen maatregelen zijn genomen. Graag vernemen deze leden hoe de regering deze gang van zaken beoordeelt en hoe gelet op de bestaande rechtshulpverdragen met de VS-regering de stand van zaken thans is.

Graag verwijzen wij u in antwoord op de eerste vraag graag naar de geannoteerde agenda voor de JBZ-Raad van 11 en 12 april 2011 (Kamerstukken I 2010/2011, 32 317, AF), waarin onder meer wordt ingegaan op de recente evaluatie van de zgn. TFTP-overeenkomst tussen de EU en de Verenigde Staten. Voor het antwoord op de tweede vraag brengen wij u graag de brief van op 6 april 2011 in herinnering (Kamerstukken I 2010/2011, 32 317, AH), waarin wordt aangegeven dat de bewering in NRC Handelsblad van 19 maart 2011 dat het rechtshulpverdrag tussen Nederland en de Verenigde Staten gebruikt wordt om banktransactiegegevens van SWIFT aan de Amerikaanse autoriteiten beschikbaar te stellen niet klopt. In deze brief wordt tevens uitgelegd onder welke

voorwaarden de Amerikaanse autoriteiten om bankgegevens in Nederland kunnen verzoeken op basis van de bilaterale rechtshulpovereenkomst.

De leden van de CDA-fractie vragen of de regering kan bevestigen dat er met betrekking tot het binnen de EU gebruikte Schengen Informatie Systeem grote verschillen bestaan tussen de signaleringen van de lidstaten en tussen de nationale interpretaties van wat wordt beschouwd als een 'bijzonder ernstig misdrijf'. Zij vragen of het juist is dat in de diverse Schengenlanden verschillende procedures bestaan voor een 'artikel 99 signalering' en wat de consequenties zijn wanneer deze vragen bevestigend worden beantwoord.

Op grond van artikel 99 van de Schengen Uitvoeringsovereenkomst (SUO) is signalering toegestaan met het oog op het beletten van strafbare feiten en ter voorkoming van gevaar voor de openbare veiligheid indien er concrete aanwijzing zijn dat de betrokken persoon in aanzienlijke mate bijzonder ernstige misdrijven beraamt of pleegt, dan wel dat de algemene beoordeling van de betrokken persoon doet verwachten dat deze bijzonder ernstige misdrijven zal blijven plegen. Uit de artikelsgewijze toelichting in de memorie van toelichting bij de goedkeuringswet (Kamerstukken II 1990/1991, 22 140, nr. 3) blijkt dat onder "bijzonder ernstige misdrijven" in ieder geval "CIE-delicten" kunnen worden verstaan. De toelichting sluit evenwel niet uit dat artikel 99 signaleringen ook gebruikt kunnen worden in geval van andere misdrijven. In andere lidstaten is dit tevens de praktijk.
Het SUO wordt in de toekomst vervangen door Besluit 2007/533/JBZ van de Raad van 12 juni 2007 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem van de tweede generatie (SIS II). Ingevolge dit raadsbesluit is signalering toegestaan indien sprake is van duidelijke aanwijzingen of verwachtingen van "ernstige misdrijven" zoals de in artikel 2, lid 2, van Kaderbesluit van de Raad van 13 juni 2002 betreffende het Europees aanhoudingsbevel en de procedures van overlevering tussen de lidstaten (2002/584/JBZ) vermelde strafbare feiten.
Het OM bereidt momenteel een nieuwe aanwijzing voor over, onder meer, artikel 99 signaleringen. Hierin zal aandacht besteed worden aan de nadere invulling van de definitie “bijzonder ernstige misdrijven”, waarbij het voornemen bestaat om zoveel mogelijk aansluiting te zoeken bij het nieuwe raadsbesluit SIS II.

De leden van de SP-fractie vragen naar de inzet van de regering voor de herziening van de privacyrichtlijn. Deze leden worden graag op de hoogte gesteld van de inhoud van de reactie op de brief van het Cbp van 6 december 2010 over de herziening van de richtlijn. De leden van de CDA-fractie wensen te vernemen of op Europees niveau harmonisatie van compliance rules serieus nagestreefd en of hiertoe ook stappen worden gezet in het rechtspersonenrecht. Ook vragen deze leden of de regering een visie heeft op een verbetering van handhavingsinstrumentarium in het geval van een internationale casus. Als voorbeeld wordt genoemd kwesties waarbij hoofd- en bijkantoren in verschillende (EU)landen een rol spelen.

In voornoemde mededeling van 4 november 2010 heeft de Commissie geconstateerd dat de richtlijn de lidstaten op bepaalde gebieden een manoeuvreerruimte toestaat, hetgeen heeft geleid tot verschillen tussen de nationale wettelijke regelingen. De Commissie acht dit in strijd met de hoofddoelstelling van de richtlijn, namelijk het verzekeren van het vrije verkeer van persoonsgegevens binnen de interne markt. Onderkend wordt het ontbreken

van harmonisatie een aandachtspunt is en extra kosten meebrengt. Dit geldt met name voor verantwoordelijken voor gegevensverwerking die in verscheidene lidstaten vestigingen hebben en verplicht zijn zich in elk van die landen aan de voorschriften en gangbare praktijken te conformeren. Voorts is voor de gegevensverwerkingverantwoordelijken en voor de gegevensbeschermingsautoriteiten niet altijd duidelijk welke lidstaat verantwoordelijk is en welk recht moet worden toegepast wanneer er meerdere lidstaten betrokken zijn. Dit is met name het geval wanneer een voor de verwerking verantwoordelijke aan verschillende eisen van verschillende lidstaten moet voldoen, wanneer een multinationale onderneming vestigingen heeft in meerdere lidstaten of wanneer de voor de verwerking verantwoordelijke niet in de EU gevestigd is maar wel diensten verleent aan EU-inwoners. De Commissie kondigt aan in de mededeling te onderzoeken hoe een verdere harmonisatie van de regels inzake gegevensbescherming op EU-niveau kan worden bereikt. Tevens zal de Commissie onderzoeken hoe te komen tot een herziening en verduidelijking van de bestaande regels betreffende het toepasselijke recht, inclusief de aanknopingspunten, om zo de rechtszekerheid te vergroten en uiteindelijk EU-betrokkenen eenzelfde beschermingsniveau te bieden, ongeacht waar de voor de gegevensverwerking verantwoordelijke zich bevindt.

In de notitie privacybeleid geeft het kabinet aan dat het zich in grote lijnen kan vinden in de uitgangspunten van de mededeling. Het kabinet herkent de belangrijkste knelpunten die de Commissie constateert, waaronder de noodzaak tot uitwerking van de internemarktdimensie en de verbetering van de mogelijkheden voor internationale gegevensdoorgifte, alsmede versterking van de handhaving. Voor de Nederlandse positie wordt verwezen naar de notitie privacybeleid en het BNC-fiche (brief van 21 december 2010 van de Staatssecretaris van Buitenlandse Zaken aan de Voorzitter van de Tweede Kamer). Laatstgenoemde brief bevat een puntsgewijs standpunt ten aanzien van de voorstellen in de mededeling.

Naar aanleiding van de mededeling heeft in januari en februari 2011 in verband van de JBZ-Raad nog intensief beraad plaatsgevonden over Raadsconclusies die terzake kunnen worden vastgesteld. Wat de positie van "compliance" betreft is door Nederland sterk ingezet op de verdere ontwikkeling van het accountability-beginsel. Dat houdt in dat ondernemingen die een sterke mate van zelfbinding op het gebied van de bescherming van persoonsgegevens aan de dag leggen en die op een geloofwaardige en openbare wijze uitdragen en zelf handhaven, beloond zouden moeten worden met meer vrijheid en minder administratieve lasten. Juist de verzoening van die belangen is belangrijk. Geconstateerd moet echter worden dat die gedachte allesbehalve algemeen wordt gedeeld door de andere EU-lidstaten.
Een andere reëel probleem waar door het georganiseerd bedrijfsleven aandacht voor wordt gevraagd is het omgaan met de bescherming van persoonsgegevens in concernverband. Wij menen dat het een gerechtvaardigde wens is van het bedrijfsleven om aan de meldplicht van verwerkingen bij het Cbp te kunnen voldoen op een wijze die een concern zo min mogelijk belast. Het zou mogelijk moeten om een houdstermaatschappij of een deelneming verantwoordelijk te maken voor alle meldingen namens het gehele concern. Het is niet eenvoudig dit binnen het kader van de Wbp op nationaal niveau volledig te realiseren. Dat komt doordat het begrip "verantwoordelijke" uit de richtlijn aan beperkingen onderhevig is. Dat kan dus alleen principieel op EU-niveau echt worden opgelost. Gebleken is dat ook voor dit vraagstuk maar beperkt begrip bestaat in andere

lidstaten. Niettemin is in samenwerking met Duitsland een raadsconclusie totstandgekomen die de Commissie oproept over dit probleem na te denken. Tenslotte menen wij dat het gebruik van "Binding Corporate Rules" (een interne regeling voor gegevensbescherming van een concern) sterk zou kunnen toenemen wanneer de procedures voor de goedkeuring van deze regels aanmerkelijk kan worden vereenvoudigd en versneld. Dat kan alleen op EU-niveau echt goed worden geregeld. Het is noodzakelijk dat Binding Corporate Rules een eigen regeling in een nieuwe richtlijn of verordening krijgen. De Commissie onderkent dit.
Voor de volledigheid wijzen wij erop dat deze problemen geen regeling kunnen vinden in het Nederlands rechtspersonenrecht, maar op EU-niveau in een nieuwe richtlijn of verordening een plaats verdienen.

7. Tot slot

De leden van de CDA-fractie vragen of de huidige wetgeving voldoet om de veiligheid van de burger te waarborgen, niet alleen ten aanzien van de beveiliging van de systemen en de overdracht van gegevens, maar ook ten aanzien van het gebruik en beheer door private partijen. Als voorbeeld noemen deze leden het datalekken, waarop individuele burgers bedrijven alleen achteraf kunnen aanspreken, hetgeen vaak buitengewoon belastend is. Tevens vragen deze leden wat de opvatting is van de regering over een meldplicht bij datalekken.

Op grond van artikel 13 van de Wbp is de verantwoordelijke voor een verwerking van persoonsgegevens verplicht om passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. De Wbp regelt niet welke feitelijke gevolgen moeten worden verbonden aan gevallen waarin sprake is van verlies of onrechtmatig gebruik van persoonsgegevens als gevolg van ontoereikend gebleken beveiligingsmaatregelen. In voornoemde brief over het privacybeleid wordt, conform eerdere toezeggingen in het kabinetsstandpunt van 3 november 2009 en de inhoud van het regeerakkoord, een wettelijke regeling voor een meldplicht datalekken in de Wbp aangekondigd. In een wetsvoorstel dat medio 2011 in consultatie zal gaan zal een dergelijke verplichting worden opgenomen. Voor nadere specificaties van de voorgenomen wettelijke regeling wordt verwezen naar de notitie privacybeleid waarin de achtergrond van het voorstel nader beschreven wordt.

De leden van de CDA-fractie vragen of Google zoekopdrachten deel uitmaken van de verkeersgegevens van het desbetreffende informatieverzoek.

Met de term 'verkeersgegevens' wordt doorgaans gedoeld op de gegevens, bedoeld in de artikelen 126n en 126u van het Wetboek van Strafvordering. Deze gegevens worden limitatief aangewezen in het Besluit vorderen gegevens telecommunicatie en hebben betrekking op een gebruiker van een communicatiedienst. Het gaat hier om gegevens over de gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker, zoals de naam, het adres en de woonplaats van de gebruiker, het nummer van de gebruiker, de naam, het adres, de woonplaats en het nummer van de natuurlijke persoon of rechtspersoon met wie de gebruiker verbinding heeft gehad en de datum en het tijdstip en de duur van de verbinding. Deze gegevens hebben geen betrekking op het gebruik van internet als middel om informatie te verzamelen. Wij zijn het dan

ook niet eens met de constatering dat Google zoekopdrachten deel uitmaken van de verkeersgegevens.

De leden van de SP-fractie stellen, met verwijzing naar de eerdergenoemde expertmeeting, vragen over de kwaliteit van informatie, het streven naar de juistheid en volledigheid ervan. De leden vragen in het bijzonder of de regering de mening deelt dat de kans op onjuistheid van informatie toeneemt naarmate het systeem grootschaliger wordt, en dat de bedreiging voor privacy toeneemt naarmate systemen grootschaliger worden.

In deze context moet er allereerst op worden gewezen dat een "een grootschalig systeem" niet als een individuele applicatie of database kan worden beschouwd, maar als een samenhangend geheel van afzonderlijke elementen met een bepaalde werking. Die elementen zijn de organisaties, werkprocessen, functionarissen en vaak meerdere gekoppelde applicaties en databases die dit geheel ondersteunen. Het kabinet onderschrijft de observatie van de leden van de SP-fractie in die zin dat met een toename van het aantal bewerkingsslagen op informatie, het aantal betrokken functionarissen, de betrokken werkprocessen of organisaties, ook het aantal kansen toeneemt dat de juistheid, volledigheid of integriteit van informatie wordt aangetast. Evenwel worden daartoe ook de risico-analyses aangepast en worden vervolgens de daarbij behorende maatregelen getroffen. Indien deze maatregelen effectief worden uitgevoerd is geen sprake van een toename van bedreiging voor de privacy. Er bestaat daarmee volgens de regering geen relatie tussen de omvang van een informatiesysteem en de complexiteit van de informatiebeveiliging.

De leden van de GroenLinks-fractie vragen of de regering zich bewust is van het risico dat bij voor meer instanties toegankelijke databases er geen enkele instantie is die de verantwoordelijkheid neemt voor signaleringen die vragen om actie. Als voorbeeld noemen deze leden het EKD en de VerwijsIndex Risicojongeren.

Het kabinet kondigt in de brief over het privacybeleid en de notitie privacybeleid een verbetering van de effectiviteit van de handhaving aan door het delen van gegevens in samenwerkingsverbanden, zonodig met behulp van wetgeving. Voor de gegevensverstrekking aan en door samenwerkingsverbanden waarbij verschillende partijen betrokken zijn, is het maken van goede afspraken noodzakelijk. Vaak gebeurt dit in de vorm van een samenwerkingsconvenant. Het kabinet is van mening dat de gegevensuitwisseling binnen samenwerkingsverbanden zorgvuldig dient plaats te vinden, overeenkomstig het volgende zesstappenplan: het bepalen van a. de taken en belangen b. het doel van het delen van informatie, c. de desbetreffende gegevens d. de vorm en inhoud van het delen, e. de verantwoordelijke f. afspraken over hoe en wanneer de verantwoordelijke de betrokkene van informatie voorziet.

Voor het EKD-DD JGZ geldt overigens dat geen sprake is van een voor meer instanties toegankelijke database. Het betreft de digitalisering van de dossiers van de jeugdgezondheidszorg. Hierbij zijn geen andere instanties dan de jeugdgezondheidszorg betrokken. Evenmin hebben anderen dan de behandelend zorgverleners toegang tot de dossiers.