

Vergaderjaar 2008–2009

**31 324 (R1844)**

## **Wijziging van de Paspoortwet in verband met het herinrichten van de reisdocumentenadministratie**

**C**

### **MEMORIE VAN ANTWOORD**

Ontvangen 28 april 2009

#### **1. Inleiding**

Ik dank de leden van de verschillende fracties voor het voorlopig verslag dat zij op 24 maart 2009 hebben vastgesteld. De leden van de fracties van het CDA, de PvdA, de VVD, de SP, de SGP, de CU en D66 hadden met belangstelling kennisgenomen van het voorliggende voorstel van rijkswet. Gaarne ga ik hieronder in op de gestelde vragen.

#### **2. Beveiliging/bescherming van gegevens**

De leden van de fracties van het CDA, de PvdA, de SP, de VVD en D66 stelden diverse vragen over de beveiliging van het centrale register. De leden van de PvdA-fractie vroegen daarbij op welke wijze de centrale opslag van gegevens vorm zal krijgen. De leden van de D66-fractie vroegen welke rechtsbescherming wordt geboden aan getroffen burgers wanneer het systeem gehackt wordt.

Er is in diverse maatregelen voorzien ter beveiliging van de nieuwe reisdocumentenadministratie: Deze zal alleen via besloten netwerken te benaderen zijn, en niet via het publieke internet. Ook is voor bevragingen en mutaties een elektronische handtekening vereist. Klopt de elektronische handtekening onder een vraag of mutatie niet, dan wordt de vraag niet beantwoord dan wel de mutatie niet verwerkt. De gegevens (en ook de back-ups daarvan) zullen uitsluitend versleuteld worden opgeslagen. Zou ongeautoriseerd toegang tot opslagmedia worden verkregen, dan kan geen inzage worden verkregen in de gegevens die op die media zijn opgeslagen. De locaties waar de apparatuur en programmatuur zich zullen bevinden zullen ook fysiek goed beveiligd zijn om te voorkomen dat onbevoegden fysiek toegang krijgen tot delen van de administratie. Dit zijn de preventieve maatregelen die nu minimaal worden voorzien. Er zijn ook correctieve maatregelen voorzien. Van alle mutaties en bevragingen worden de oorspronkelijke verzoeken en de daarop gegeven antwoorden gelogd. Aan de hand daarvan zijn ook de bevragingen en mutaties achteraf te traceren. Voorzien is dat zo nodig de hele administratie aan de hand van de log met wijzigingen kan worden gereconstrueerd.

De beveiliging is altijd een wedloop tussen bedenkers van dreiging en oplosers daarvan. Monitoring van mogelijke (nieuwe) dreigingen is voorzien om waar nodig de beveiliging te kunnen herzien.

De centrale gegevensopslag zal uit oogpunt van continuïteit en beschikbaarheid plaatsvinden op meer dan één goed beveiligde locatie. Dit is niet ongebruikelijk bij belangrijke systemen zoals de centrale reisdocumentenadministratie. Wordt een van de locaties getroffen door een calamiteit dan kan de werking van de administratie op een andere locatie doorlopen. Daarnaast worden de gegevens op elk van de locaties ook nog verdeeld over meerdere databases. Zo is voorzien dat de biometrische gegevens los van de overige aanvraaggegevens worden opgeslagen. Alle berichten en mutaties op de centrale administratie zullen worden opgeslagen in een afzonderlijke database. Deze database zal niet extern bevroegbaar zijn, maar dient enkel om in geval van twijfel over de integriteit van de administratie de gegevens in de administratie te kunnen controleren. Ook kan hieruit indien nodig de reisdocumentenadministratie weer worden gereconstrueerd. Alle gegevensopslag vindt versleuteld plaats.

Het is helaas nooit 100 procent uit te sluiten dat onbevoegden toegang krijgen tot de gegevens. Niet is op voorhand aan te geven welke gevolgen dat zal hebben voor de individuele burger die in de reisdocumentenadministratie is geregistreerd. Indien mocht blijken dat als gevolg van de onrechtmatige toegang de burger schade heeft geleden, dan zal van geval tot geval bekeken moeten worden wie aansprakelijk kan worden gesteld voor deze schade. Voorts is de Wet bescherming persoonsgegevens van toepassing, die onder meer het recht op inzage en correctie van op de betrokken persoon betrekking hebbende gegevens en de daaraan gekoppelde rechtsbescherming regelt.

Voor de beantwoording van de vraag van de leden van de SP-fractie of onderzocht is in hoeverre de techniek in staat is om te functioneren zonder grote onvolkomenheden die ernstige gevolgen kunnen hebben voor burgers, verwijs ik naar het gestelde aan het slot van de derde paragraaf van deze memorie.

De leden van de PvdA-fractie vroegen in welke mate en op welke wijze misbruik werd gemaakt van de mogelijke zwakheden van het huidige paspoort, en waarom, en in welke mate, deze problemen met de introductie van het nieuwe paspoort kunnen worden ondervangen.

Doordat Nederlandse reisdocumenten sinds 2001 centraal worden vervaardigd en gepersonaliseerd, en de beveiliging sindsdien sterk is verbeterd, is het aantal vervalsingen met gegevens in reisdocumenten verminderd. Een andere vorm van fraude met reisdocumenten bestaat uit personen die zich uitgeven voor een ander dan de houder van het reisdocument (de zgn. «look-alikes»).

De fraude bestaat in dit geval niet uit vervalsing van gegevens in het document zelf, maar in het op grond van valse of vervalste gegevens aanvragen van een reisdocument, dan wel in het gebruik maken van een reisdocument van een ander als ware het aan de desbetreffende persoon zelf verstrekt.

De uitgevende en controlerende instanties konden slechts op basis van een pasfoto ter grootte van enkele vierkante centimeters verifiëren of degene die het reisdocument aanbiedt, dezelfde persoon is als de rechtmatige houder van het document. Om de mogelijkheden voor een deugdelijke gezichtsherkenning te vergroten, bevatten reisdocumenten, uitgegeven vanaf eind augustus 2006, een elektronische chip waarin de

kleurenfoto van de houder digitaal is opgenomen. Deze chip kan met behulp van lezers worden uitgelezen. Dit maakt het mogelijk dat de afbeelding van de houder vergroot en in kleur kan worden opgeroepen op een scherm. Daarnaast bevat de chip ten behoeve van een unieke identificatie binnenkort ook de vingerafdrukken van de houder. Door de vingerafdrukken in de chip te vergelijken met de vingerafdrukken van de houder van het document ontstaan meer mogelijkheden om vast te stellen of houder en document bij elkaar horen. Met voornoemde maatregelen kan «look-alike»-fraude met het document beter worden bestreden dan voorheen.

De leden van de fracties van de VVD en de SP vroegen om een nadere motivering waarom gekozen is voor een centraal register en niet voor decentrale registers met een verwijzindex.

De keuze voor een centrale online raadpleegbare reisdocumenten-administratie is primair ingegeven vanuit de noodzaak om het aanvraag- en uitgifteproces van de Nederlandse reisdocumenten betrouwbaarder te maken. Secundair heeft meegewogen het streven om, in het kader van de vermindering van administratieve lasten voor burgers, het aanvragen van een reisdocument plaatsafhankelijk te maken. De keuze voor een decentrale opzet zou een aantal nadelen met zich meebrengen, zoals ook aangegeven in de memorie van toelichting en de nota naar aanleiding van het verslag. Graag grijp ik deze gelegenheid aan om dit nogmaals te illustreren.

Bij een decentrale opzet moeten niet 1 maar ongeveer 700 administraties online raadpleegbaar worden gemaakt. De decentrale reisdocumenten-administraties zijn thans niet online raadpleegbaar. Het online beschikbaar maken van de reisdocumentenadministratie leidt bij een decentrale opzet tot een aantal complicaties.

Ten eerste zijn bij een decentrale opzet (ook) centrale componenten nodig. Een van de benodigde centrale componenten is, zoals de leden van de VVD-fractie aangaven, een centrale verwijzindex. De verwijzindex heeft de functie om na te gaan welke aanvragen voor reisdocumenten de aanvrager (in het verleden) heeft gedaan en waar (bij welke uitgevende instantie) die zijn gedaan. Daartoe zal de centrale verwijzindex permanent een substantieel aantal gegevens moeten gaan bevatten die ook in de decentrale administraties opgeslagen moeten zijn.

Ten tweede moeten bij een decentrale opzet de circa 700 administraties beschikken over programmatuur om na te kunnen gaan of onder verschillende identiteiten een reisdocument is aangevraagd (de zogenaamde biometrische zoekfunctie). Elke aanvraag die wordt gedaan (er worden per dag gemiddeld ongeveer 15 000 aanvragen voor reisdocumenten ingediend) moet naar alle decentrale administraties worden gezonden zodat in de decentrale administratie op basis van geslacht, gezichtsopname en vingerafdrukken kan worden nagegaan of de betreffende aanvrager onder een andere identiteit reeds over een reisdocument beschikt. De resultaten van die zoekactie – de mogelijke indicaties van fraude – dienen te worden onderzocht.

Ook bij een decentrale opzet is een centrale voorziening nodig om de uitkomsten van de biometrische zoekfunctie te onderzoeken. Het is niet realistisch om te veronderstellen dat de circa 700 uitgevende instanties over de specialisten kunnen gaan beschikken om dit onderzoek uit te voeren. Dat betekent dat het onderzoek centraal zal moeten plaatsvinden. Hiervoor zullen de decentraal verkregen resultaten van de zoekactie op dubbele identiteiten weer centraal moeten worden verzameld.

Met een decentrale opzet is voorts de beschikbaarheid van de online raadpleegbare reisdocumentenadministratie kwetsbaarder. De mate van beschikbaarheid is een belangrijk punt waarbij de voordelen van de centrale opzet groter zijn. In een decentrale opzet moeten meer dan 700 reisdocumentenadministraties beschikbaar zijn. Dat is een dermate lastige opgave dat voorzien wordt dat bij een decentrale opzet aanvragen van reisdocumenten vaker aangehouden zullen moeten worden. Een decentrale opzet vereist namelijk bij het raadplegen van eerdere aanvragen dat zowel de centrale verwijfsindex als één of meerdere decentrale administraties beschikbaar zijn, waardoor het risico dat een of meer decentrale componenten tijdelijk niet beschikbaar zijn veel groter is. Bij een centrale opzet is er maar één centrale component die meervoudig gebruikt kan worden. Bij een decentrale opzet zal het verwerken van een aanvraag en een uitgifte bovendien meer tijd in beslag nemen, omdat eerst de centrale verwijfsindex en vervolgens één of meerdere decentrale administraties moeten worden geraadpleegd. Dat vergt, doordat meerdere systemen in de beantwoording zijn betrokken, per definitie meer tijd dan bij één systeem.

Bij een decentrale opzet van de administratie kan elke afzonderlijke administratie bovendien met een piekbelasting te maken krijgen, die de beschikbaarheid van de administratie in gevaar kan brengen. Om een acceptabele respons te krijgen zou elke decentrale administratie daarom moeten zijn toegerust op piekbelastingen. De vragen die gaan over de gegevens uit één specifieke decentrale administratie kunnen namelijk niet worden beantwoord door een andere decentrale administratie. De verwerkingscapaciteit van een decentrale administratie die op dat moment minder vragen te verwerken heeft, kan dus niet worden aangewend door een decentrale administratie die een piek aan vragen te verwerken krijgt. Alle 700 afzonderlijke systemen moeten in dat geval op piekbelastingen worden gedimensioneerd. Bij een centrale opzet kan een piekbelasting efficiënter worden afgehandeld, omdat de verwerkingcapaciteit is geconcentreerd. Bevragingen worden door meerdere databases waarop de administratie draait, afgehandeld. Het vergroten van de verwerkingcapaciteit betekent bij een centrale administratie een investering op één plek, bij een decentrale opzet op 700 plekken.

In het geval van onderhoud en aanpassingen in de administraties moeten deze bij een decentrale opzet op 700 plekken doorgevoerd worden. Die aanpassingen moeten bovendien gecoördineerd en op hetzelfde moment worden doorgevoerd. Daarbij moet natuurlijk tijdens de «verbouwing» de on-line bevraging gewoon doorgaan. Dat is bij een decentrale opzet van administraties die over de hele wereld zijn verspreid en te maken hebben met andere tijdzone's een eveneens lastige opgave.

Ten slotte kan in een centrale opzet voorzien worden in een optimalere beveiliging van de reisdocumentenadministratie. Bij een decentrale opzet moeten alle administraties niet alleen on-line bevragebaar worden voor de andere uitgevende instanties maar ook voor andere geautoriseerde gebruikers. De beveiliging van de reisdocumentenadministraties is daar thans niet op berekend en zeker niet geschikt voor. Om de decentrale administraties online bevragebaar te maken moet de beveiliging van alle ca 700 naar een veel hoger niveau worden gebracht met in achtneming van het feit dat elke uitgevende instantie een eigen beveiligingsbeleid heeft. De beveiligingsrisico's zijn bij een decentrale opzet overigens zeker niet minder dan bij een centrale opzet. Inbreken op één decentrale administratie betekent dat de integriteit van alle administraties in het geding is. Het is in een dergelijke situatie immers ongewis waar en hoeveel inbreken hebben plaatsgevonden of nog zullen plaatsvinden en welke gegevens mogelijk gecorrumped zijn.

De leden van de VVD-fractie vroegen in dit verband nog of er ervaringen bekend zijn van andere landen met decentrale registers, en of deze ervaringen zijn betrokken in de afweging om tot een centraal register te komen.

De regering beschikt niet over een overzicht van de wijze waarop andere landen centraal dan wel decentraal registers hebben ingericht voor de administratie van hun reisdocumenten. In EU-verband heeft overleg dan wel uitwisseling van informatie hierover niet plaatsgevonden. De oorzaak hiervoor is dat de EU-verordening geen betrekking heeft op de opslag van de gegevens in het kader van het aanvragen en uitgeven van de reisdocumenten. Verder speelt een rol dat de wet- en regelgeving in de lidstaten van de Unie (en overigens ook daarbuiten) sterk van elkaar verschilt wat een zinvolle vergelijking in de weg staat. Welke keuzes de landen hebben gemaakt en wat de achtergronden daarbij zijn geweest is dus niet geïnventariseerd en heeft derhalve ook geen rol gespeeld in afweging die de regering heeft gemaakt.

Voor de beantwoording van de vraag van de leden van de fracties van SGP en CU hoe wordt voorkomen dat de wettelijke verankerde doelbinding in gevaar komt, verwijs ik naar § 8 van deze memorie.

### **3. Biometrie**

De leden van de fracties van de CU en de SGP vroegen naar een reactie op de conclusies van het onderzoek «The use of privacy enhancing aspects of biometrics» van de universiteit van Tilburg.

Het onderzoek waarnaar genoemde leden verwezen heeft betrekking op de vraag in hoeverre biometrische gegevens worden gebruikt als privacy versterkende technologie. Dergelijke technologieën beschermen de privacy door het verzamelen van identificerende gegevens tot een minimum te beperken of uit te sluiten. Met name is de rol en het gebruik van dergelijke technologieën onderzocht in de semi-publieke en private sector. Het gebruik van biometrische gegevens in reisdocumenten valt dan ook – strikt genomen – buiten de reikwijdte van het onderzoek. Niettemin wordt in het onderzoek gerefereerd aan het onderhavige voorstel van rijkswet, en wordt de keuze om de vingerafdrukken niet alleen op te slaan in reisdocumenten, maar deze ook te registreren in de reisdocumentenadministratie, ondersteund.<sup>1</sup> Het onderzoek wijst erop dat wanneer het reisdocument en de biometrische gegevens in verkeerde handen vallen, er zonder registratie niets is om op terug te vallen. Belangrijkste conclusie is dat het onderzoek een sterkere rol van en meer bevoegdheden en instrumenten voor het College bescherming persoonsgegevens bepleit. Over versterking van het toezicht op de privacy heeft ook de commissie Brouwer een aantal aanbevelingen gedaan in haar advies over het beschermen van veiligheid en persoonlijke levenssfeer. Het kabinetsstandpunt op dit advies is op dit moment in voorbereiding. Voor een reactie op deze aanbeveling verwijs ik dan ook naar het nog uit te brengen kabinetsstandpunt, dat naar verwachting voor de zomer gereed zal zijn.

Voorts vroegen genoemde leden of biometrische gegevens uitsluitend gebruikt mogen worden ter verificatie van de echtheid van documenten en het vaststellen van de identiteit van paspoorthouders.

Op grond van artikel 4, derde lid, van de Verordening betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgeven paspoorten en reisdocumenten, mogen *voor de toepassing van de verordening* biometrische kenmerken alleen worden gebruikt

---

<sup>1</sup> Zie § 1.6 op pagina 13 van het onderzoek.

voor de verificatie van de authenticiteit van het document en voor de verificatie van de identiteit van de houder door middel van direct beschikbare vergelijkbare kenmerken wanneer het overleggen van een paspoort of andere reisdocumenten wettelijk vereist is. De verordening staat er derhalve niet aan in de weg dat in de reisdocumenten opgenomen biometrische gegevens ook worden opgeslagen in een reisdocumentenadministratie en daaruit kunnen worden verstrekt met inachtneming van de regels ter bescherming van persoonlijke levenssfeer.

De doelen waarvoor biometrische gegevens in de reisdocumentenadministratie op grond van het voorstel van rijkswet gebruikt mogen worden, zijn omschreven in artikel 4b, eerste en tweede lid, van het voorstel. Deze doelen verschillen niet van de doelen waarvoor de overige gegevens in de reisdocumentenadministratie gebruikt mogen worden. Wel gelden er extra beperkingen indien gegevens betreffende de vingerafdrukken worden verstrekt ten behoeve van de opsporing en vervolging van strafbare feiten en ten behoeve van het voorkomen en bestrijden van fraude met en misbruik van reisdocumenten.

De leden van de CU-fractie en de SGP-fractie vroegen voorts hoe de mogelijkheden ter verificatie van het biometrische paspoort zich verhouden tot andere wettelijk aanvaarde identiteitsbewijzen. Zij vroegen ook wat bij grootschalige toepassing en gebruik van biometrie de gevolgen kunnen zijn van intrinsieke fouten in de biometrie. De leden van de D66-fractie vroegen hierover wie aansprakelijk gesteld kan worden wanneer door de foutmarge bij gebruik van biometrie extra kosten ontstaan door vertraging.

In artikel 1 van de Wet op de identificatieplicht zijn de documenten aangewezen waarmee in bij de wet aangewezen gevallen iemands identiteit kan worden vastgesteld. Daarbij is verder geen onderscheid gemaakt tussen identiteitsbewijzen waarin wel in een chip de biometrische kenmerken van de houder van dat document zijn opgeslagen en identiteitsbewijzen waarin dit niet het geval is. Dat betekent dat een paspoort met biometrische kenmerken dezelfde juridische waarde heeft als een ander document dat in artikel 1 van de Wet op de identificatieplicht als identiteitsbewijs is erkend.

Elke techniek, ook biometrie, heeft onvolkomenheden. Bekend is dat een verificatie van de burger aan de hand van vingerafdrukken niet altijd mogelijk is. Dat is niets nieuws want met gezichtsopnamen die nu al in het reisdocument en de administratie zijn opgenomen is het niet anders. De combinatie van gezichtsopname en vingerafdrukken maakt het echter wel mogelijk meer zekerheid te krijgen bij de identiteitsverificatie. Maar ook dan zal er nooit voor de volle 100 procent op kunnen worden vertrouwd. Bij het aanvragen en uitreiken van reisdocumenten zijn de vingerafdrukken dan ook slechts één van de hulpmiddelen om de identiteit van de aanvrager te verifiëren.

Wat de gevolgen zullen zijn van intrinsieke fouten in de biometrie is niet eenduidig aan te geven. Dit zal afhankelijk zijn van de situatie waarin dit gegeven wordt geraadpleegd. In het geval de biometrische verificatie aan de hand van de gegevens in de chip van het reisdocument het laat afweten, zal kunnen worden teruggevallen op de fysiek zichtbare gegevens in het document zelf of op de gegevens in de reisdocumentenadministratie.

Evenals in het geval van onrechtmatige toegang tot gegevens als gevolg van «hacken», geldt ook hier dat, indien mocht blijken dat de burger

schade heeft geleden, van geval tot geval zal moeten worden bekeken wie daarvoor aansprakelijk kan worden gesteld.

#### **4. Belangenafweging/Cbp**

De leden van de fracties van D66 en de SP vroegen in te gaan op de relatie met artikel 8 van het EVRM en op de proportionaliteit, subsidiariteit en functionaliteit van het voorstel.

Om de gevolgen van het voorstel van rijkswet voor de privacy in kaart te brengen, is van belang de situatie zoals deze voorafgaand aan het wetsvoorstel is, in ogenschouw te nemen. De doelen en mogelijkheden om gegevens te verstrekken uit de nieuwe reisdocumentenadministratie ingevolge het wetsvoorstel verschillen niet wezenlijk van die van de bestaande reisdocumentenadministraties. Het primaire doel blijft immers om gegevens vast te leggen met betrekking tot alle Nederlandse reisdocumenten en deze gegevens beschikbaar stellen aan de autoriteiten die belast zijn met de uitvoering van de Paspoortwet voor zover deze gegevens noodzakelijk zijn voor de vervulling van hun taken. Dit is vastgelegd in artikel 4b, eerste lid, van het wetsvoorstel. Ook de overige mogelijkheden om gegevens te verstrekken, genoemd in artikel 4b, tweede lid (bestrijding en voorkoming van fraude met reisdocumenten, slachtofferidentificatie, strafrechttoepassing en staatsveiligheid), komen in hoge mate overeen met de mogelijkheden die in de huidige Paspoortwet en de daarop gebaseerde uitvoeringsregelingen zijn opgenomen. Er is overigens zowel in de huidige als in de toekomstige situatie geen sprake van «toegang» van de officier van justitie tot de reisdocumentenadministratie, zoals de leden van de D66-fractie suggereren, maar uitsluitend van verstrekking van gegevens op aanvraag, voor zover deze verstrekking past binnen de wettelijke kaders.

In die zin kan er dan ook geen sprake zijn van een inbreuk op de privacy ten gevolge van het onderhavige voorstel van rijkswet.

Wat wel verandert is het volgende. Ten eerste worden er straks naast de bestaande gegevens ook de vingerafdrukken van de houder in reisdocumenten opgenomen en geregistreerd in de reisdocumentenadministratie. Het opnemen van vingerafdrukken in reisdocumenten vloeit voort uit Verordening (EG) nr. 2252/2004. Het opnemen van vingerafdrukken in reisdocumenten en het opslaan daarvan is inderdaad een inbreuk op de bescherming van de persoonlijke levenssfeer. Die inbreuk is naar mijn mening gerechtvaardigd, met name omdat deze leidt tot een meer betrouwbaar en effectief aanvragen uitgifteproces van reisdocumenten. Fraude met reisdocumenten, zoals look-alike-fraude, kan daarmee beter worden bestreden. In de memorie van toelichting ben ik uitgebreid ingegaan op die afweging. Van belang is dat de registratie van vingerafdrukken met voldoende waarborgen is omkleed. Dat is in het onderhavige wetsvoorstel het geval, onder meer doordat zeer nauwkeurig is beschreven voor welke doeleinden de gegevens mogen worden gebruikt.

Ten tweede worden alle decentrale reisdocumentenadministraties samengevoegd tot één centrale administratie, die – in tegenstelling tot de huidige administraties – online bevroegbaar is. De vervanging van de decentrale administraties door een centrale digitale administratie heeft echter geen negatieve gevolgen voor het niveau van privacybescherming. Uitvoeringsinstanties krijgen door de invoering van de nieuwe reisdocumentenadministratie bij voorbeeld niet meer rechten dan voorheen om gegevens op te vragen. Wel gaat de gegevensverstrekking sneller en efficiënter, en kan de beveiliging bij een centrale administratie beter worden geregeld. Ook kan de opslag van de gegevens en de gegevens-

verstrekking – anders dan bij de decentrale administraties – op een uniforme wijze worden geregeld. De huidige, decentrale administraties voldoen niet aan de noodzakelijke eisen van toegankelijkheid en kenbaarheid, onder meer doordat de gegevensuitwisseling veelal op papier geschiedt, en deze administraties niet 7 X 24 uur per week bevragebaar zijn.<sup>1</sup>

De belangenafweging ten aanzien van de gevolgen van dit wetsvoorstel voor de persoonlijke levenssfeer van de burger in vergelijking met de huidige situatie is beschreven in paragraaf 3.5 van de memorie van toelichting. Naar aanleiding van het advies van het Cbp is de memorie van toelichting aangevuld. Onder meer in paragraaf 3.2 zijn naar aanleiding van het Cbp-advies de voor- en nadelen van een centrale reisdocumentenadministratie uitvoerig tegen elkaar afgewogen en wordt geconcludeerd dat de invoering van een decentraal systeem met een centrale verwijzingsindex als een onwerkbaar optie moet worden beschouwd.

## **5. Officier van justitie**

De leden van de D66-fractie vroegen naar aanleiding van de zaak Marper-UK of de toegang van de officier van justitie tot de reisdocumentenadministratie geen strafrechtelijke context creëert, en vroegen zich af of die zaak gelet op die toegang geen gevolgen heeft voor het voorstel. De leden van de fracties van CU en SGP vroegen in dit verband of de centrale reisdocumentenadministratie, nu de officier van justitie in bepaalde gevallen biometrische gegevens kan ontvangen in feite niet de functie van opsporingsregister verkrijgt, en daarmee een ernstige inbreuk is op de persoonlijke levenssfeer nu daarin ook gegevens van niet verdachte burgers zijn opgenomen.

Voor wat betreft de mogelijkheden voor verstrekking ten behoeve van strafrechtelijke doeleinden van de bestaande gegevens verandert er weinig. Ook op dit moment worden gegevens verstrekt voor strafrechtelijke doeleinden uit de decentrale reisdocumentenadministraties en de verstrekking voor dit doel is dan ook niet een nieuw gevolg van het wetsvoorstel. Wel nieuw is de mogelijkheid om gegevens betreffende de vingerafdrukken te verstrekken. De mogelijkheden daartoe zijn in het wetsvoorstel aan strenge voorwaarden onderworpen. De centrale reisdocumentenadministratie krijgt in verband met de verstrekking in bepaalde gevallen van vingerafdrukken aan de officier van justitie niet het karakter van een opsporingsregister of een register met een strafrechtelijke context. Anders dan in het geval van registers met een strafrechtelijke context is het criterium om persoonsgegevens te registreren niet de vraag of de betrokkene een strafrechtelijk verleden heeft, maar de vraag of de betrokkene in het bezit is van een reisdocument. Dat is dan ook een belangrijk verschil met de registratie, waarop de zaak Marper-UK betrekking had. De registratie van vingerafdrukken in de reisdocumentenadministratie geldt in beginsel voor iedere aanvrager van een reisdocument en heeft derhalve als zodanig geen enkel stigmatiserend effect. Het EHRM achtte het ongelimiteerd opslaan en bewaren van (onder meer) vingerafdrukken van personen die verdacht waren, maar niet zijn veroordeeld, in een database met vingerafdrukken van verdachten, in strijd met artikel 8 van het EVRM. Er waren bovendien geen grenzen gesteld aan de ernst van het strafbare feit en de duur van het opslaan. Verder was er bij de opzet van de betreffende registratie niet of in onvoldoende mate een afweging gemaakt tussen het private en het publieke belang. Die afweging is bij de reisdocumentenadministratie wel gemaakt. De toelichting bij het voorstel tot wijziging van de Paspoortwet gaat uitvoerig in op de vraag waarom het belang van een accurate en effectieve reisdocumentenadministratie het opslaan van vingerafdrukken rechtvaardigt. Gelet op de verschillen van de registratie waarop de uitspraak betrekking had en de

<sup>1</sup> Voor de bezwaren van de huidige decentrale administraties zij verwezen naar 3.1.3 van de memorie van toelichting.

reisdocumentenadministratie heeft genoemde uitspraak geen gevolgen voor de nieuwe reisdocumentenadministratie.

## **6. Bezwaar en beroep**

De leden van de CDA-fractie vroegen of en op welke wijze erin wordt voorzien dat informatie wordt gegeven aan aanvragers van reisdocumenten, waarin wordt gewezen op de mogelijkheden die de Wet bescherming persoonsgegevens biedt (recht op inzage, correctie etc., en de mogelijkheden van bezwaar en beroep).

Gemeenten geven bij de uitreiking van reisdocumenten aan de burgers de folder «Belangrijke informatie over uw elektronische paspoort of Nederlandse identiteitskaart» mee. Hier staat onder meer in dat het document zorgvuldig gebruikt moet worden en wordt aangegeven wat de burger moet doen bij diefstal of vermissing van zijn document. De folder wordt door het ministerie van BZK beschikbaar gesteld. Vanzelfsprekend zal op het moment dat de centrale reisdocumentenadministratie wordt ingevoerd de tekst in de folder worden uitgebreid met een korte uiteenzetting over het opnemen en het gebruik van de gegevens in deze administratie alsmede de rechten van de burger ten aanzien van zijn opgeslagen gegevens.

## **7. Vreemdelingen en vluchtelingen**

De leden van de vaste commissie vroegen naar een oplossing voor het probleem dat zich voordoet bij vreemdelingen en vluchtelingen die hun exacte geboortedatum niet kennen. Zij vroegen te bezien of deze personen een administratieve geboortedatum kunnen krijgen.

De persoonsgegevens in de Gemeentelijke basisadministratie persoonsgegevens (GBA) worden ontleend aan brondocumenten. In het geval van een geboortedatum worden de gegevens ontleend aan een daartoe aangewezen brondocument, of bij het ontbreken daarvan aan de verklaring van de betrokkene. De GBA registreert de (op deze wijze ontleende) feiten. Als de geboortedatum onbekend is wordt dát feit geregistreerd in de GBA. In technische zin geschiedt dat door het opnemen van het cijfer nul op de onbekende posities. Ik heb geen signalen ontvangen dat een (deels) onbekende geboortedatum op een volstrekt geldig reisdocument voor de burger in het dagelijks leven meer dan eens tot problemen leidt. Daarbij wijs ik u erop dat het opnemen van een (deels) onbekende geboortedatum ook conform internationale voorschriften geschiedt. Wel ben ik bereid het gesprek hierover het gesprek aan te gaan met de Nederlandse Vereniging voor Burgerzaken en VluchtelingenWerk Nederland. Mocht dit gesprek leiden tot een ander inzicht van mijn kant, dan zal ik daarover rapporteren.

## **8. Uitvoering**

De leden van de PvdA-fractie vroegen uitsluitsel te geven over de kosten die naar verwachting voor het nieuwe paspoort bij de burgers in rekening zullen worden gebracht.

In de prijs van de reisdocumenten zullen de kosten van de ontwikkeling en van het beheer van de nieuwe administratie worden doorberekend. Volgens een voorlopige raming zullen de kosten van de nieuwe administratie tussen de € 3.50 à € 4.00 per document bedragen. De omvang van deze kosten en de gevolgen voor de prijs van de reisdocumenten kan pas nauwkeurig worden aangegeven zodra met de bouw van de administratie

en de aanschaf van de benodigde programmatuur en apparatuur is begonnen. Dit is thans nog niet het geval.

De leden van de SP-fractie vroegen welke uitvoeringsmaatregelen zijn gepland waarvan de Eerste Kamer kennis zou moeten nemen.

In het overzicht bij mijn brief van 2 december 2008<sup>1</sup> heb ik aangegeven welke onderwerpen bij algemene maatregel van rijksbestuur (AMvRB) worden geregeld. In het merendeel van de gevallen betreft het op AMvRB-niveau vastleggen van uitvoeringsmaatregelen die nu op het niveau van een ministeriële regeling zijn vastgelegd. In een klein aantal gevallen moeten bij of krachtens AMvRB nieuwe uitvoeringsmaatregelen worden vastgesteld. Die nieuwe uitvoeringsmaatregelen komen voort uit het feitelijk opnemen van vingerafdrukken. De zaken, waarvan kennisneming door uw Kamer naar mijn mening wenselijk is, zoals de doelen waarvoor gegevensverstrekking mogelijk is uit de nieuwe reisdocumentenadministratie, zijn op het niveau van rijkswet geregeld.

Zowel de leden van de D66-fractie, van de SP-fractie als van de fracties van SGP en CU vroegen welke waarborgen worden voorgesteld om zgn. «function creep» te voorkomen, waarbij de doelbinding in gevaar komt. De leden van de D66-fractie maakten zich daarbij zorgen over nieuwe doeleinden die naar hun mening bij algemene maatregel van rijksbestuur aan de centrale reisdocumentenadministratie kunnen worden verbonden.

Het wetsvoorstel bevat waarborgen en beperkingen om te voorkomen dat de gegevens te ruim worden verstrekt. Gegevensverstrekking mag slechts plaatsvinden ten behoeve van een zeer beperkt aantal doeleneinden. Het wetsvoorstel zelf somt deze doelen limitatief op in artikel 4b, eerste en tweede lid. Dit is een verbetering ten opzichte van de huidige tekst van de Paspoortwet, op grond waarvan de doelen van de gegevensverstrekking worden bepaald in de Paspoortuitvoeringsregelingen. De precieze bepaling van de organen die gegevens verstrekt kunnen krijgen, wordt wat betreft de verstrekking van gegevens voor de uitvoering van de Paspoortwet reeds bepaald in de wet zelf, op grond van artikel 4b, eerste lid. Voor zover het gaat om verstrekking voor de doeleinden, genoemd in artikel 4b, tweede lid, wordt de aanwijzing van de precieze instanties die voor gegevensverstrekking in aanmerking komen, nader bepaald bij algemene maatregel van rijksbestuur. Omdat de taakverdeling over verschillende instanties van tijd tot tijd kan wijzigen, is het noodzakelijk de aanwijzing van de instanties op die wijze te regelen. Het wetsvoorstel geeft daarbij de kaders, de algemene maatregel van rijksbestuur kan zich niet buiten die kaders bewegen. Dit betekent onder meer dat geen instanties kunnen worden aangewezen voor verstrekking van gegevens buiten de in de artikel 4b, tweede lid, genoemde doelen.

Als er behoefte ontstaat aan gegevensverstrekking uit de centrale reisdocumentenadministratie voor andere doelen dan de doelen die nu in het wetsvoorstel staan, zal de wetgeving moeten worden aangepast. De discussie over die ruimere verstrekking zal dan ook op dat moment moeten worden gevoerd. Totdat de wetgeving is gewijzigd dient de gegevensverstrekking te blijven binnen de nu vastgestelde grenzen. Het risico van function creep, voor zover daarbij de wettelijke doelbinding in gevaar komt, is naar mijn mening dan ook niet aanwezig.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties.  
A. Th. B. Bijleveld-Schouten

---

<sup>1</sup> Kamerstukken II 2008–2009, 31 324, nr. 10.