

DAGVAARDING
ALSMEDE VERZOEK TOT HET STELLEN VAN PREJUDICIËLE VRAGEN

Heden, de zesde mei tweeduizendtien, op verzoek van:

1. De stichting **STICHTING PRIVACY FIRST**, statutair gevestigd te (1013 JH)
Amsterdam aan de Haarlemmerdijk 104 c, (verder ook te noemen: "Privacy First");
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.
- 11.
- 12.
- 13.
14.]
]
15.]
 ;

16.

17.

18.

19.

20.

21.

22.

23.

te dezer domicilie kiezend te (1011 TR) Amsterdam aan de Schippersgracht 1-3 ten kantore van SOLV Advocaten van wie Mrs Chr. A. Alberdingk Thijm en V.A. Zwaan te dezer zake als advocaten zullen optreden alsmede te (2514 JL) Den Haag ten kantore van Udink en De Jong Advocaten van wie Mr W.P. den Hertog te dezer zake door verzoekers tot procesadvocaat wordt gesteld en als zodanig zal optreden;

Heb ik,

GEDAGVAARD:

De **STAAT DER NEDERLANDEN (MINISTERIE VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES)**, zetelende te 's-Gravenhage, aldaar aan het parket van de procureur-generaal bij de Hoge Raad der Nederlanden, (2514 CV) aan de Kazernestraat 52 (verder ook te noemen: de "Staat")

, aldus op dat adres dit exploit gedaan en afschrift van dit exploit:

- ☐ gelaten aan:
- ☐ achtergelaten in een gesloten envelop waarop de door de wet voorgeschreven gegevens zijn vermeld, omdat ik daar niemand aantrof aan wie ik rechtsgeldig een afschrift kon laten,

OM:

Op woensdag, de negentiende mei tweeduizendtien (de "**Roldatum**"), des voormiddags te tien uur, niet in persoon, maar vertegenwoordigd door een (proces)advocaat, te verschijnen in het geding en ten overstaan van de Arrondissementsrechtbank te Den Haag, die alsdan, aldaar zal worden gehouden in een van de zalen van de rechtbank aan de Prins Clauslaan 60.

MET AANZEGGING DAT:

- indien gedaagde niet uiterlijk op de eerste of op een door de rechter nader bepaalde Roldatum in het geding verschijnt dan wel verzuimt een (proces)advocaat te stellen, en de voorgeschreven termijnen en formaliteiten in acht zijn genomen, de rechtbank verstek zal verlenen en de vorderingen zal toewijzen, tenzij deze haar onrechtmatig of ongegrond voorkomt;
- dat eisers de gedaagde peremptoir stellen voor het indienen van de conclusie van antwoord met een termijn van uiterlijk zes weken na het uitbrengen van de dagvaarding tegen de zitting d.d. 19 mei 2010, dus tegen de rol van 30 juni 2010, en eisers nu reeds voor alsdan aanzeggen bij het niet indienen van een conclusie van antwoord daarvan akte te vragen;
- dat gedaagde tegelijkertijd met het indienen van een conclusie van antwoord opgave dient te verstrekken aan de rolrechter van de verhinderdata in verband met de eventuele comparitie van partijen, bij gebreke waarvan eiser de rechtbank zal verzoeken geen rekening te houden met mogelijk verhinderdata van rechthebbenden;

TENEINDE:

Te antwoorden op de volgende vorderingen van eisers:

INHOUDSOPGAVE

▪ Inleiding	6
▪ Plan van behandeling	9
▪ Privacy First	9
▪ De Verordening	10
▪ Wijzigingen Nederlandse Paspoortwet	12
a. Positief register	13
b. Centrale opslag	13
c. Verstrekkingenregime	16
d. Delegatiebepalingen	18
e. Strijdig met proportionaliteit en subsidiariteit	19
f. Doeleinden	22
▪ Juridisch kader	24
- Strijd met het gemeenschapsrecht	25
- Strijd met artikel 8 EVRM	29
- Onrechtmatige wetgeving	33
- Vorderingen	33
▪ Procesverloop	36
▪ Verweer gedaagden	36
▪ Bewijsaandracht	37
▪ Verzoek tot het stellen van prejudiciële vragen	39
▪ Bevoegdheid	41
▪ Petitum	41

INLEIDING

1. Deze zaak betreft een onrechtmatige daad van de Staat jegens Privacy First en/of jegens hen wier belangen door Privacy First worden behartigd. In het bijzonder betreft het een daad van onrechtmatige wetgeving. De wetgeving waar het in deze zaak om gaat betreft de Rijkswet van 11 juni 2009 tot wijziging van de Paspoortwet in verband met het herinrichten van de reisdocumentenadministratie (hierna: "de Nieuwe Paspoortwet") [productie 1].¹ De Nieuwe Paspoortwet is op 28 juni 2009 gedeeltelijk in werking getreden.
2. Uit de parlementaire geschiedenis volgt dat de Nieuwe Paspoortwet voornamelijk tot doel moet hebben het bestrijden van paspoort- en identiteitsfraude. Op grond van de Nieuwe Paspoortwet wordt daartoe een nationale, geautomatiseerde databank gecreëerd met onder meer biometrische gegevens van alle Nederlandse burgers van 12 jaar en ouder met een (nieuw) reisdocument.² Deze gegevens zullen echter niet alleen worden gebruikt om paspoort- en identiteitsfraude te voorkomen; de gegevens kunnen op grond van een uitvoerig "verstrekkingenregime" relatief eenvoudig voor allerlei doeleinden worden gebruikt, in het bijzonder opsporingsdoeleinden..
3. De wijze waarop en de voorwaarden waaronder de (biometrische) gegevens worden bewaard en de wijze waarop de vertrekking plaats zal vinden, moet nog worden uitgewerkt in algemene maatregelen van rijksbestuur. Niettemin is de Nieuwe Paspoortwet al van kracht en wordt ondertussen uitvoering gegeven aan de verplichting (biometrische) gegevens af te nemen bij burgers. Ten aanzien van de wijze waarop dit gebeurt en met name de wijze waarop deze gegevens worden opgeslagen, bestaat op dit moment geen enkel (deugdelijk) beleid. Bij onder meer alle Nederlandse gemeenten worden dus zeer privacygevoelige gegevens verzameld en opgeslagen, zonder dat daarbij de persoonlijke levenssfeer van de betrokkenen voldoende in acht wordt genomen. Het systeem dat aldus is gecreëerd is dermate risicovol dat ernstige ongelukken een kwestie van tijd zijn. Privacy First wil met deze procedure ongelukken voorkomen en in zijn algemeenheid paal en perk stellen aan de ongebreidelde inbreuken op de privacy van Nederlandse burgers voortvloeiend uit de Nieuwe Paspoortwet.
4. Deze zaak staat niet op zichzelf. Diverse organisaties, academici, volksvertegenwoordigers en bezorgde burgers hebben al gewezen op de onnodige

¹ Rijkswet van 11 juni 2009 tot wijziging van de Paspoortwet in verband met het herinrichten van de reisdocumenten administratie, Stb. 2009, 252.

² Met "paspoort" worden ook alle andere soorten reisdocumenten bedoeld.

privacygevaaren die de Nieuwe Paspoortwet met zich meebrengt. Het betreft onder meer:

- Advies van het College Bescherming Persoonsgegevens ("CBP") [productie 2];³
- Advies van de Groep Gegevensbescherming Artikel 29 [productie 3];⁴
- Advies van de Europese Toezichthouder voor gegevensbescherming [productie 4];⁵
- Brief van de Permanente commissie van deskundigen in internationaal vreemdelingen-, vluchtelingen en strafrecht aan de vaste commissie voor Binnenlandse Zaken en Koninkrijksrelaties [productie 5];⁶
- Juryrapport Big Brother Awards 2009. De Nieuwe Paspoortwet is winnaar in de categorie Overheid en tevens winnaar van de publieksprijs [productie 6];
- Verslag Iustrumcongres Nederlands Juristen Comité voor de Mensenrechten ("NJCM"), waar verschillende academici alsmede de nationale ombudsman hun zorgen uitspraken [productie 7];⁷
- Grootschalige actie Het Nieuwe Rijk (de zogenaamde "tatoeagefolder" die breed werd gesteund) [productie 8];
- Procedure Vereniging Vrijbit bij het Europees Hof voor de Rechten van de Mens ("EHRM") [productie 9];
- Open brief van Tilburg Institute for Law, Technology and Society ("TILT") aan Eerste Kamer [productie 10].

5. Naar de overtuiging van Privacy First en vele anderen is het werkelijke doel van de Nieuwe Paspoortwet niet het verbeteren van de inrichting van de reisdocumentenadministratie, maar het bestrijden van vermeende terreur.⁸ Onlangs benadrukte oud-minister Ter Horst nog dat criminaliteitsbestrijding naar haar mening de belangrijkste reden vormt voor de opslag van vingerafdrukken.⁹ Nederland loopt daarmee in Europa voorop. Dat inbreuken op de persoonlijke levenssfeer ten behoeve

³ Advies College Bescherming Persoonsgegevens d.d. 30 maart 2007, z2007-00010 [productie 2].

⁴ Groep Gegevensbescherming Artikel 29, Advies 3/2005 betreffende de uitvoering van Verordening (EG) nr. 2252/2004 van de Raad van 13 december 2004 betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten, *PB* L 385 van 29.12.2004.

⁵ Advies van de Europese Toezichthouder voor gegevensbescherming over het voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EG) nr. 2252/2004 van de Raad betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten, *PbEU* 2008/C 200/01.

⁶ Brief Permanente commissie van deskundigen in internationaal vreemdelingen-, vluchtelingen en strafrecht aan de vaste commissie voor Binnenlandse Zaken en Koninkrijksrelaties van de Tweede kamer der Staten-Generaal betreffende het voorstel van de Minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties voor de inrichting van een centrale administratie van paspoorten en reisdocumenten, met inbegrip van biometrische gegevens d.d. 13 april 2006, kenmerk CM0603.

⁷ 16 Miljoen BN-ers? Bescherming van Persoonsgegevens in het Digitale Tijdperk' (verslag Iustrumcongres), *NJCM-Bulletin*, jrg. 34 (2009), nr. 8.

⁸ *Kamerstukken II* 2007/08, 31 324 (R1844), nr. 3, p. 3; *Kamerstukken II* 2004/05, 25 764, nr. 26.

⁹ Discussie tijdens symposium "De burger in de knel" i.v.m. de presentatie van Frank Kuitenbrouwers *Recht & Vrijheid* d.d. woensdag 28 april 2010 te Amsterdam.

van (pretense) veiligheid de Nederlandse overheid niet al te veel zorgen baart, mag wel blijken uit het rapport van het ministerie van BZK uit 2009 met de veelzeggende titel "Gewoon Doen, beschermen van veiligheid en persoonlijke levenssfeer". De conclusie van dit rapport is dat als het opslaan en uitwisselen van privacygevoelige persoonsgegevens nodig is om de veiligheid van burgers te garanderen, dat "gewoon moet gebeuren".¹⁰ Dat standpunt wordt onderschreven door de ministers van Justitie en van BZK in een brief aan de Tweede Kamer van november 2009.¹¹

6. De totstandkoming van de Nieuwe Paspoortwet is dan ook geen op zichzelf staande ontwikkeling. Zo is Nederland kampioen afluisteren. In 2008 werden 26.425 telefoons afgetapt, terwijl dat in de VS in hetzelfde jaar maar 2208 keer gebeurde.¹² Ook werd een DNA-databank voor kinderen tot stand gebracht, waarin al van 12.000 kinderen een profiel met genetische informatie is opgeslagen.¹³ Door politie en justitie werden via het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) in 2008 ongeveer 3 miljoen keer klantgegevens van telecomgebruikers opgevraagd. In hoog tempo wordt de privacy van de burgers sinds de jaren '90 steeds verder aangetast door het tot stand brengen van verschillende digitale databanken die uiterst gemakkelijk aan elkaar kunnen worden gekoppeld.¹⁴ Dagblad Trouw publiceerde in juni 2009 een open brief van veertien hoogleraren van Nederlandse Universiteiten waarin zij waarschuwen voor deze "opslaghysterie" en het dichterbij komen van een controlestaat als gevolg van maatregelen als de Nieuwe Paspoortwet en de bewaarplicht voor telecom verkeersgegevens **[productie 11]**.¹⁵
7. Met de Nieuwe Paspoortwet is de Nederlandse Staat in haar kennelijke strijd tegen terrorisme en ander kwaad echter veel te ver gegaan en heeft zij de wettelijke grenzen overschreden. De wet en de wijze waarop daaraan uitvoering wordt gegeven zijn evident in strijd met uiteenlopende Europese en verdragsrechtelijke bepalingen die ertoe strekken de persoonlijke levenssfeer van de burger te beschermen. In deze procedure beroept Privacy First zich onder meer op twee Europese verordeningen waarop de Nieuwe Paspoortwet is gebaseerd **[producties 12 & 13]**,¹⁶ de zogenaamde

¹⁰ Rapport 'Gewoon Doen, beschermen van veiligheid en persoonlijke levenssfeer', Commissie Brouwer-Korf, in opdracht van Ministerie van BZK 22 januari 2009.

¹¹ Kamerstukken II 2009/10, 31 051, nr. 5.

¹² S. Derix, 'Nederland is kampioen afluisteren', NRCNext 10 september 2009 (<http://www.nrcnext.nl/blog/2009/09/10/nederland-is-kampioen-afluisteren/>).

¹³ 'Minderjarigen in de DNA-databank', nieuwsbericht Nederlands Forensisch Instituut 8 december 2009 <<
[>>](http://www.forensischinstituut.nl/nieuws/minderjarigen_in_de_dna_databank.aspx).

¹⁴ 16 Miljoen BN-ers? Bescherming van Persoonsgegevens in het Digitale Tijdperk' (verslag lustrumcongres), NJCM-Bulletin jrg. 34 (2009), nr. 8, p. 936 en 937.

¹⁵ 'We vallen ten prooi aan Europese opslaghysterie', Trouw 26 juni 2009.

¹⁶ Verordening (EG) Nr. 2252/2004 van de Raad van 13 december 2004 betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten en Verordening (EG) Nr. 444/2009 van het Europees Parlement en de Raad van 6 mei 2009 tot wijziging van

Privacyrichtlijn¹⁷ [productie 14], artikel 8 van het Europees Verdrag voor de Rechten van de Mens ("EVRM"), en het Verdrag betreffende de werking van de Europese Unie. Als gevolg van het feit dat de Nieuwe Paspoortwet in strijd is met voornoemde wetgeving, is deze onrechtmatig. Privacy First zal de rechtbank ter fine van deze dagvaarding dan ook onder meer verzoeken voor recht te verklaren dat de aangegeven bepalingen van de Nieuwe Paspoortwet onrechtmatig zijn en dat deze buiten werking worden gesteld danwel niet in werking zullen treden.

PLAN VAN BEHANDELING

8. In het onderstaande zal eerst kort iets worden opgemerkt over Privacy First en de 22 eisers, natuurlijke personen. Vervolgens zal worden ingegaan op de Europese Verordening die aanleiding is geweest voor de totstandkoming van de Nieuwe Paspoortwet, waarna zal worden aangegeven welke aspecten van de Nieuwe Paspoortwet Privacy First met name onrechtmatig acht.
9. In het juridische kader wordt behandeld waarom deze aspecten onrechtmatig zijn, dat sprake is van onrechtmatige wetgeving en worden enkele aspecten van de vorderingen nader toegelicht. Daarna zal kort aandacht worden besteed aan het procesverloop, het verweer van gedaagde en de bewijsaandracht. Ten slotte wordt de rechtbank, mocht er enige aarzeling bestaan over de juistheid van de standpunten van Privacy First, in overweging gegeven om prejudiciële vragen te stellen aan het Europese Hof van Justitie, waarna het petitum wordt geformuleerd.

PRIVACY FIRST

10. Privacy First, opgericht op 26 maart 2008, is een stichting die zich blijkens haar statuten ten doel stelt het bevorderen en behouden van het recht op privacy, alsmede de persoonlijke vrijheid van leefomgeving, op welke wijze dan ook, en voorts al hetgeen met een en ander rechtsreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin van het woord [productie 15].

Verordening Nr. 2252/2004 van de Raad van 13 december 2004 betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten.

¹⁷ Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

11. Privacy First is actief om wetgeving op het gebied van privacy rechten, alsmede de uitvoering daarvan, te verbeteren en is dan ook op grond van artikel 3:305a lid 1 BW bevoegd de onderhavige rechtsvorderingen in te stellen. De vorderingen deze strekken immers tot bescherming van gelijksoortige belangen van andere personen en Privacy First behartigt deze belangen blijkens haar statuten.
12. Naast Privacy First treden in deze zaak 22 natuurlijke personen op als eisers. Het betreft allemaal burgers met de Nederlandse nationaliteit die bezwaar maken tegen de Nieuwe Paspoortwet, in het bijzonder de opslag van hun biometrische gegevens en de mogelijke gevolgen daarvan. Voorzover zij biometrische gegevens hebben verstrekt bij de aanvraag van een nieuw paspoort hebben zij dat gedaan onder protest daartoe gehouden te zijn. Deze 22 mede-eisers hebben recht en belang bij een paspoort, zonder dat daarbij biometrische gegevens worden opgeslagen. Met Privacy First zijn zij van mening dat de Nieuwe Paspoortwet (op onderdelen) onrechtmatig is. Waar in het navolgende over "Privacy First" wordt gesproken, wordt daarmee tevens deze 22 natuurlijke personen bedoeld.

DE VERORDENING

13. De Nieuwe Paspoortwet strekt er in de eerste plaats toe de Paspoortwet in lijn te brengen met een Europese Verordening uit 2004 betreffende de normen voor veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten (hierna: de "Verordening") **[productie 12]**.¹⁸ De Verordening is in 2009 op bepaalde punten gewijzigd (de "Wijzigingsverordening") **[productie 13]**.¹⁹ Het betreft hier met name de eis dat door lidstaten afgegeven paspoorten een opslagmedium bevatten dat een gezichtsopname bevat en dat twee vingerafdrukken in een interoperabel formaat worden opgenomen.
14. Fundamentele doelstelling voor de Verordening is volgens overweging 9 van de Verordening het invoeren van gemeenschappelijke veiligheidsnormen en interoperabele biometrische identificatiemiddelen.
15. In artikel 4 lid 3 is limitatief bepaald voor welke doeleinden de biometrische gegevens in paspoorten mogen worden gebruikt. Dat is alleen voor a) de authenticiteit van het

¹⁸ Verordening (EG) Nr. 2252/2004 van de Raad van 13 december 2004 betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten.

¹⁹ Verordening (EG) Nr. 444/2009 van het Europees Parlement en de Raad van 6 mei 2009 tot wijziging van Verordening Nr. 2252/2004 van de Raad van 13 december 2004 betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten.

paspoort; of b) de identiteit van de houder door middel van direct beschikbare vergelijkbare kenmerken wanneer het overleggen van een paspoort of reisdocument wettelijk vereist is. Er bestaat dus ingevolge de Verordening geen ruimte voor de lidstaten om verdergaande mogelijkheden in nationale wetgeving op te nemen.

"Biometrische gegevens worden verzameld en opgeslagen in het opslagmedium voor paspoorten en reisdocumenten, met het oog op de afgifte van zulke documenten. Voor de toepassing van deze verordening mogen de biometrische kenmerken in paspoorten en reisdocumenten alleen worden gebruikt voor het verifiëren van:

- a) de authenticiteit van het paspoort of reisdocument;*
- b) de identiteit van de houder door middel van direct beschikbare vergelijkbare kenmerken wanneer het overleggen van een paspoort of reisdocument wettelijk vereist is."* [onderstreping, adv.]

16. Het is van belang te constateren dat deze bepaling door het Europees Parlement in een amendement aan de Verordening toegevoegd. Daarbij gaf het Parlement aan dat de reden voor toevoeging van de bepaling was gelegen in het feit dat de opname van biometrische gegevens in paspoorten expliciet, passend, proportioneel en duidelijk moet zijn en dat daarom in de Verordening moet worden opgenomen waarvoor de gegevens mogen worden gebruikt. Volgens het Parlement moet het absoluut duidelijk zijn dat biometrische gegevens in paspoorten van Europese burgers alleen zullen worden gebruikt voor het verifiëren van de authenticiteit van het paspoort en de identiteit van de houder.

"Since the reason for incorporating biometric features into passport documents has to be explicit, appropriate, proportionate and clear, it needs to be incorporated into the legal text. It has to be absolutely clear that biometrics in EU citizens' passports are going to be used only for verifying the authenticity of the document and the identity of the holder."²⁰

17. In overweging 8 bij de Verordening is bepaald dat de Privacyrichtlijn op de Verordening van toepassing is en op grond van artikel 1bis lid 2 van de Verordening moeten de biometrische gegevens van de aanvrager van een paspoort worden verzameld in overeenstemming met onder meer het EVRM.

²⁰ Report on the Commission proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports (COM(2004)0116 – C5 – 0101/2004 – 2004/0039(CNS)), FINAL A6-0028/2004, 28 October 2004, amendment 12.

18. In overweging 5 van de Wijzigingsverordening wordt benadrukt dat de Verordening *niet* voorziet in een rechtsgrondslag voor het opzetten of bijhouden van gegevensdatabanken voor de opslag van deze gegevens in de lidstaten.
19. Opgemerkt zij dat in het voorstel voor de Verordening een centrale database door de Europese Commissie tot doel werd gesteld. Het Europees Parlement was echter van mening dat het tot stand brengen van een centrale databank niet proportioneel is en het risico op misbruik van de gegevens zou vergroten, alsook de kans op zogenaamde *function creep*. Daarnaast zou volgens het parlement het risico worden vergroot dat biometrische kenmerken worden gebruikt als toegangssleutels tot verschillende databanken en dat op die manier gegevens worden gecombineerd.
- "The setting up of a centralised database would violate the purpose and the principle of proportionality. It would also increase the risk of abuse and function creep. Finally, it would increase the risk of using biometric identifiers as 'access keys' to various databases, thereby interconnecting data sets."*²¹
20. Dat Nederland veel verder gaat dan de Verordening voorschrijft, zal in het navolgende aan de orde komen.

WIJZIGINGEN NEDERLANDSE PASPOORTWET

21. Privacy First maakt in deze procedure bezwaar tegen de gehele Nieuwe Paspoortwet, behoudens voorzover daarin verplichtingen zijn opgenomen die voortvloeien uit de Verordening. Naar de overtuiging van Privacy First kan de wet wegens strijd met de in het volgende hoofdstuk te behandelen (internationale) wet- en regelgeving in haar huidige vorm niet in werking blijven en/of in werking treden. Privacy First zal in het navolgende een aantal aspecten van de Nieuwe Paspoortwet beschrijven die zij in het bijzonder onrechtmatig acht.
- De creatie van een zogenaamd "positief" register;
 - De al dan niet centrale opslag van gegevens;
 - Het verstrekkingenregime ten aanzien van de opgeslagen gegevens;
 - Het feit dat al uitvoering wordt gegeven aan de wet, terwijl een groot deel van de regels nog in delegatiebepalingen vastgesteld moet worden;

²¹ Report on the Commission proposal for a Council regulation on standards for security features and biometrics in EU citizens' passports (COM(2004)0116 – C5 – 0101/2004 – 2004/0039(CNS)), FINAL A6-0028/2004, 28 October 2004, amendment 5.

- e. Strijd met de beginselen van proportionaliteit en subsidiariteit;
- f. De veelheid van doeleinden waarvoor de gegevens worden opgeslagen en kunnen worden gebruikt.

a) Positief register

22. De oude Paspoortwet voorzag in een zogenoemd *negatief* basisregister. Hierin werden alleen bepaalde gegevens opgenomen ten aanzien van reisdocumenten die zijn onvreemd of anderszins als vermist zijn opgegeven of van rechtswege zijn vervallen.
23. Op grond van het, nog in werking te treden, nieuwe artikel 4a van de Nieuwe Paspoortwet wordt nu een *positief* register tot stand gebracht. Volgens het nieuwe artikel 4a lid 1 van de Paspoortwet wordt door de minister een reisdocumentenadministratie gevoerd waarin gegevens worden bijgehouden met betrekking tot *alle* reisdocumenten, in plaats van met betrekking tot reisdocumenten die zijn vermist of vervallen. Bovendien zullen ook de vingerafdrukken in deze administratie worden opgeslagen.
24. Feitelijk komt de totstandbrenging van het positieve register er dus op neer dat van *alle* Nederlandse burgers die een paspoort aanvragen een groot aantal gegevens worden opgeslagen. Waar in het verleden alleen gegevens ten aanzien van een verwaarloosbaar aantal vermiste paspoorten werden opgeslagen, zullen nu dus de gegevens ten aanzien van miljoenen paspoorten worden opgeslagen.

b) Centrale opslag

25. De administratie van reisdocumenten is op grond van artikel 3 lid 8 Paspoortwet op dit moment nog grotendeels decentraal opgezet. De gegevens die bij de aanvraag van een reisdocument zijn verzameld en het feit dat een reisdocument is uitgereikt worden decentraal opgeslagen door de uitgevende instanties (onder andere de burgemeesters van de Nederlandse gemeenten).²²
26. Slechts twee administraties zijn op dit moment centraal vormgegeven: het eerder genoemde negatieve Basisregister Reisdocumenten (artikel 4a Paspoortwet) en het Register paspoortsignaleringen (artikel 25 lid 3 Paspoortwet).²³ Het Register paspoortsignaleringen bevat informatie over personen aan wie op bepaalde gronden een reisdocument kan worden geweigerd of vervallen kan worden verklaard danwel vervallen verklaard is.

²² Kamerstukken II 2007/08, 31 324 (R1844), nr. 3, p. 6.

²³ Kamerstukken II 2007/08, 31 324 (R1844), nr. 3, p. 6.

27. Volgens de Memorie van Toelichting bij de Nieuwe Paspoortwet voldoet het huidige systeem van administraties niet meer, onder meer omdat de decentrale administraties onderling niet met elkaar zijn verbonden waardoor verificatievragen tussen de verschillende paspoortverstrekende autoriteiten op papier zouden moeten worden uitgewisseld.²⁴
28. Op grond van de Nieuwe Paspoortwet zullen er niet langer drie verschillende administraties bestaan. In het nieuwe Basisregister Reisdocumenten - ook wel Online Raadpleegbare Reisdocumentatie Administratie ("ORRA") genoemd - zullen *alle* gegevens uit de decentrale administraties en het oude Basisregister Reisdocumenten plus de vingerafdrukken aan elkaar worden gekoppeld en gezamenlijk *centraal* worden opgeslagen.
29. Artikel 65 lid 3 van de Nieuwe Paspoortwet bepaalt dat de gegevens die op grond van artikel 4a, artikel 65 en de gewijzigde Paspoortuitvoeringsregeling Nederland & Buitenland 2001 op dit moment decentraal worden opgeslagen, bij inwerkingtreding van de nieuwe artikelen 4a en 4b zullen worden overgebracht naar de centrale reisdocumentenadministratie.
30. Voor de al dan niet centrale opslag van gegevens biedt de Verordening nadrukkelijk geen grond. Overweging 5 van de Wijzigingsverordening benadrukt immers dat de Verordening géén rechtsgrondslag biedt voor het opzetten of bijhouden van gegevensdatabanken voor de opslag van de gegevens uit paspoorten.
31. Een groot aantal lidstaten heeft er dan ook voor gekozen de paspoortgegevens alleen in het paspoort zelf of anderszins decentraal op te slaan (productie 16 biedt een overzicht van bepaalde aspecten van de implementatie van de Verordening in de verschillende lidstaten). Het betreft hier onder meer landen als Denemarken, Zweden, Italië, Liechtenstein en België. In de Zweedse wet (§6a en §6b Passlag) is bijvoorbeeld expliciet bepaald dat vingerafdrukken niet ergens anders worden opgeslagen dan in de chip op het paspoort. Daarnaast mogen de foto, vingerafdrukken en biometrische gegevens die uit beide kunnen worden afgeleid, niet worden gebruikt voor geautomatiseerde verwerking.
32. In Duitsland mogen Paspoortgegevens, waaronder biometrie, alleen bij paspoortagentschappen worden opgeslagen. Vingerafdrukken moeten worden gewist

²⁴ Kamerstukken II 2007/08, 31 324 (R1844), nr. 3, p. 8.

nadat het paspoort is afgegeven (§16, lid 2 PaßGesetz). De instantie die de paspoorten drukt, mag hiervoor biometrische gegevens slechts tijdelijk opslaan.

“Beantragung, Ausstellung und Ausgabe von Pässen dürfen nicht zum Anlaß genommen werden, die dafür erforderlichen Angaben und die biometrischen Merkmale außer bei den zuständigen Paßbehörden zu speichern. Entsprechendes gilt für die zur Ausstellung des Passes erforderlichen Antragsunterlagen sowie für personenbezogene fotografische Datenträger (Mikrofilme). Die bei der Passbehörde gespeicherten Fingerabdrücke sind spätestens nach Aushändigung des Passes an den Passbewerber zu löschen.”

33. Duitsland heeft de inrichting van een centrale reisdocumentenadministratie zelfs expliciet verboden (§4, lid 3 PaßGesetz).

“Auf Grund der Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten (ABl. EU Nr. L 385 S. 1) sind der Reisepass, der Dienstpass und der Diplomatenpass mit einem elektronischen Speichermedium zu versehen, auf dem das Lichtbild, Fingerabdrücke, die Bezeichnung der erfassten Finger, die Angaben zur Qualität der Abdrücke und die in Absatz 2 Satz 2 genannten Angaben gespeichert werden. Die gespeicherten Daten sind gegen unbefugtes Auslesen, Verändern und Löschen zu sichern. Eine bundesweite Datenbank der biometrischen Daten nach Satz 1 wird nicht errichtet.”

34. Daarnaast geldt dat van de lidstaten die wel centraal gegevens opslaan, het grootste deel slechts *bepaalde* gegevens opslaat en niet *alle* beschikbare (biometrische) gegevens, zoals in Nederland het geval is. In Denemarken, Luxemburg, Hongarije, Oostenrijk en Ierland wordt bijvoorbeeld alleen de pasfoto centraal opgeslagen.
35. Andere landen het de doeleinden waarvoor de gegevens mogen worden gebruikt beperkt. In Tsjechië bijvoorbeeld dienen de opgeslagen gegevens niet tot identificatie van personen.
36. Uit het voorgaande, beknopte overzicht volgt dat Nederland met de centrale opslag van gegevens niet alleen veel verder dan de Verordening voorschrijft, maar ook dan de meeste andere lidstaten.

c) Verstrekkingenregime

Huidig verstrekkingenregime

37. De drie voornoemde bestaande administraties kennen elk een eigen verstrekkingenregime. In artikel 73 van de Paspoortuitvoeringsregeling Nederland 2001 (hierna de "Paspoortuitvoeringsregeling") is het verstrekkingenregime ten aanzien van de decentrale administraties geregeld. Daarin zijn de voorwaarden opgenomen waaronder gegevens aan bepaalde limitatief opgesomde instellingen en personen kunnen worden verstrekt.
38. Het verstrekkingenregime ten aanzien van het negatieve Basisregister reisdocumenten is geregeld in artikel 4a. Op grond van lid 6 kunnen gegevens worden verstrekt aan instellingen en personen belast met een publiekrechtelijke taak voor zover de gegevens noodzakelijk zijn voor de vervulling van hun taak. De gegevens kunnen worden ingezien door de ambtenaren van politie en de inlichtingendiensten.
39. Deze inzage vindt plaats door een online en *realtime* verbinding tussen de diensten en het register. Toegang is voorbehouden aan personen binnen de diensten die daartoe ten behoeve van de aan hen opgedragen taak zijn geautoriseerd. Op grond van artikel 4a lid 7 kan de minister besluiten ook andere instellingen en personen aan te wijzen die belang hebben bij verstrekking van gegevens uit het Basisregister. Het is dat geval alleen om de mededeling van een "hit/no-hit", met andere woorden, de vraag *of* er gegevens in het register zijn opgenomen ten aanzien van een bepaald reisdocument en niet *welke* gegevens. Dit gebeurt vanuit het zogenaamde verificatieregister waarin alleen documentnummers zijn opgenomen.²⁵
40. Ten aanzien van het voornoemde Register paspoortsignaleringen geldt een heel beperkt verstrekkingenregime. Alleen de autoriteiten die bevoegd zijn een aanvraag voor een reisdocument in behandeling te nemen, een reisdocument te weigeren of vervallen te verklaren of in te houden ontvangen een mededeling aan welke personen een reisdocument kan worden geweigerd of van wie het kan worden ingehouden. Het betreft een papieren administratie waaruit de bevoegde instanties iedere maand een uitdraai ontvangen met een beperkt aantal gegevens.²⁶

Nieuw verstrekkingenregime

²⁵ Kamerstukken II 2007/08, 31 324 (R1844), nr. 3, p. 7-8.

²⁶ Kamerstukken II 2007/08, 31 324 (R1844), nr. 3, p. 8.

41. De nieuwe (centrale) reisdocumentenadministratie zal 7 dagen per week, 24 uur per dag online toegankelijk zijn. Volgens het voorgestelde artikel 4b lid 1 kunnen gegevens worden verstrekt aan bepaalde instanties voor zover zij die gegevens nodig hebben voor de uitvoering van de Paspoortwet. Op grond van leden 2, 3 en 4 van het voorgestelde artikel 4b kunnen echter ook andere instanties, instellingen en personen (zoals politie en justitie, maar ook niet-overheidsinstellingen zoals banken) gegevens opvragen voor geheel andere doeleinden. Het betreft hier doeleinden als de opsporing en vervolging van strafbare feiten en het verrichten van onderzoek naar handelingen die een bedreiging vormen voor de veiligheid van de Staat en "andere gewichtige belangen" van een of meerdere landen van het Koninkrijk dan wel de veiligheid van met het Koninkrijk "bevriende mogendheden".
42. Artikel 4b van de Nieuwe Paspoortwet noemt, kortweg, de volgende doeleinden voor verstrekking:
- het aanvragen en uitgeven van reisdocumenten (lid 1);
 - het voorkomen en bestrijden van fraude met en misbruik van reisdocumenten (lid 2 sub a);
 - de identificatie van slachtoffers van rampen en ongevallen (lid 2 sub b);
 - de opsporing en vervolging van strafbare feiten (lid 2 sub c);
 - het verrichten van onderzoek in het kader van de staatsveiligheid en andere gewichtige belangen .²⁷
43. De reisdocumentenadministratie wordt dus in belangrijke mate gebruikt als een opsporingsregister, waaruit naar hartenlust informatie kan worden geput. Door wie deze informatie kan worden geraadpleegd, is bovendien nog niet eens (geheel) duidelijk. Een groot deel van de instellingen en personen die aanspraak zullen hebben op verstrekking van de gegevens moet nog bij AMvB worden vastgesteld.
44. Naast het verstrekkingenregime dat op grond van artikel 4b en de 23 nog tot stand te brengen AMvBs zal gaan gelden, zal tevens een geheel nieuwe zoekfunctie worden geïmplementeerd die op de centrale administratie kan worden toegepast. Deze zoekfunctie moet nog worden ontworpen, zoals ook blijkt uit de verslagen van het gesprek tussen Privacy First en het ministerie van BZK (waarop later nog zal worden teruggekomen) **[producties 17 & 18]**.
45. In de Memorie van Toelichting wordt aangegeven dat van de zoekmogelijkheid gebruik zal kunnen worden gemaakt op verzoek van de officier van justitie ten behoeve van de

²⁷ Zie ook *Kamerstukken II* 2007/08, 31 324 (R1844), nr. 3, p. 37-41.

identiteitsvaststelling van verdachten en veroordeelden. Daarnaast kunnen "verifiërende autoriteiten" nagaan of een paspoort in het maatschappelijk verkeer mag voorkomen.²⁸

46. De gevallen waarin op grond van de Nieuwe Paspoortwet gegevens kunnen worden verstrekt, gaat evident aanzienlijk verder dan wat is toegestaan op grond van artikel 4 lid 3 van de Verordening. Het is dan ook niet verrassend dat andere lidstaten die een bepaalde vorm van centrale opslag kennen, niet een dergelijk ruim verstrekkingenregime hanteren [**productie 16**]. Zo is in de Duitse wet is bepaald dat alleen de politie, douane en paspoortagentschappen de gegevens die zijn opgeslagen op de chip in het paspoort mogen lezen en gebruiken ter verificatie van de echtheid van het paspoort en de identiteit van de houder. Hierna moeten de verzamelde gegevens worden gewist (§16a PaßGesetz).

d) Delegatiebepalingen

47. De Paspoortwet bevat een groot aantal delegatiebepalingen, 23 om precies te zijn. **Productie 19** bevat een brief van de minister aan de Tweede Kamer van 2 december 2008 met als bijlage een schema waarin alle delegatiebepalingen zijn opgenomen en waar bij elke delegatiebepaling is aangegeven wat het onderwerp is, wat voor soort delegatiebepaling in het wetsvoorstel voor de Nieuwe Paspoortwet wordt voorgesteld, wat de huidige situatie is en wat nieuw is aan de betreffende delegatiebepaling.²⁹
48. In dit schema is duidelijk te zien dat de inhoud van een zeer groot deel van de nieuwe paspoortwetgeving nog niet bekend is, omdat deze nog bij lagere wetgeving moet worden vastgesteld. Het betreft hier belangrijke regelgeving, bijvoorbeeld ten aanzien van de doeleinden waarvoor (biometrische) paspoortgegevens kunnen worden verstrekt, de categorieën instanties die voor verstrekking van de gegevens in aanmerking kunnen komen en de vaststelling van de gegevens die verstrekt kunnen worden (artikel 4b, derde en zesde lid in het schema). Ook de beveiliging van de in de (centrale) databank opgenomen gegevens moet nog bij AMvB worden geregeld. Dat zal pas gebeuren als de nieuwe reisdocumentenadministratie tot stand is gebracht.³⁰
49. Dit resulteert in de situatie dat alle gegevens, dus ook de vingerafdrukken, ten behoeve van het nieuwe register wel al worden afgenomen en opgeslagen, maar dat geen enkele waarborg wordt geboden ten aanzien van het gebruik dat van de gegevens wordt en zal worden gemaakt.

²⁸ Kamerstukken II 2007/08, 31 324 (R1844), nr. 3, p. 17.

²⁹ Kamerstukken II 2008-09, 31 324, nr. 10 met bijlage [**productie 19**].

³⁰ Kamerstukken II 2007-08, 31 324 (R1844), nr. 3, p. 18.

50. Zo is geen sprake van passende technische en organisatorische maatregelen ter beveiliging van de gegevens die worden afgenomen en opgeslagen. Er is geen enkele nieuwe beveiligingsmaatregel genomen ter bescherming van de (digitaal) opgeslagen vingerafdrukken. De beveiliging is precies hetzelfde als toen alleen nog de "oude" gegevens zoals naam en handtekening werden opgeslagen. Die maatregelen zijn vanzelfsprekend niet geschikt om de uitermate gevoelige biometrische gegevens te beveiligen. Blijkens de Paspoortuitvoeringsregeling 2001 gaat het hier om sterk verouderde maatregelen als de fysieke opslag van materialen in kluizen, het maken van back-ups en de plaatsing van apparatuur. Geen enkele adequate beveiliging voor biometrische persoonsgegevens. Dat heeft tot gevolg dat burgers die op dit moment al gedwongen hun vingerafdrukken afgeven bij de gemeente, omdat zij een nieuw paspoort nodig hebben, geen enkele garantie hebben dat hun vingerafdrukken niet kunnen worden gebruikt voor oneigenlijke doeleinden.
51. Ook volgens het CBP is door de regering onvoldoende stilgestaan bij de vraag wat de gevolgen zijn als wordt ingebroken in het systeem, zelfs met de voorgenomen op termijn te nemen maatregelen.³¹
52. Verder is ten aanzien van een groot aantal onderwerpen in het delegatieschema aangegeven dat "in beginsel" dezelfde regels zullen gelden als in bestaande ministeriële regelingen zijn vastgelegd. Er wordt echter geen enkele garantie gegeven dat dit daadwerkelijk het geval zal zijn. Bovendien wordt met betrekking tot een groot aantal van deze regels in het schema tevens nieuwe regelgeving opgenomen.
53. Ondanks het feit dat de burger dus voor een groot deel niet kan overzien wat er met zijn gegevens zal gebeuren, is hij op grond van de Nieuwe Paspoortwet wel al verplicht de biometrische gegevens aan de overheid te verstrekken. Ook Tweede Kamerleden hebben aangegeven de indruk te hebben dat een onvoldragen wetsvoorstel aan de Kamer is voorgelegd.³²

e) Strijdig met proportionaliteit en subsidiariteit

54. De maatregelen die in de Nieuwe Paspoortwet worden getroffen zijn niet noodzakelijk, nu de maatregelen niet voldoen aan de fundamentele beginselen van proportionaliteit en subsidiariteit. De inbreuk op de belangen van de betrokkenen is onevenredig aan het doel van de maatregelen en de Staat heeft geenszins aangetoond dat het doel niet

³¹ Advies College Bescherming Persoonsgegevens d.d. 30 maart 2007, z2007-00010, p. 6-7 [productie 2].

³² Kamerstukken II 2007/08, 31 324, nr. 4, p. 2.

in redelijkheid ook op een andere, voor de betrokkenen minder nadelige wijze kan worden bereikt.

55. In de Memorie van Toelichting wordt eenvoudigweg gesteld dat de voorgestelde inrichting van de reisdocumentenadministratie gerechtvaardigd is, *omdat* deze leidt tot een meer effectief en betrouwbaar aanvraag- en uitgifteproces van reisdocumenten en het gebruik van de gegevens daarnaast voor enkele andere doeleinden gerechtvaardigd wordt geacht. Van een concrete belangenafweging ten aanzien van de opslag van, onder meer, biometrische gegevens van alle Nederlanders boven de 12 jaar aan de hand van de uitgangspunten van proportionaliteits- en subsidiariteitsbeginsel is echter geen enkele sprake.
56. De Europese wetgever heeft ten aanzien van de afname van vingerafdrukken een leeftijdsgrens gesteld, namelijk bij 12 jaar. Uit onderzoek was gebleken dat de vingerafdrukken van jongere kinderen niet van voldoende kwaliteit zijn, met name bij kinderen jonger dan zes jaar. Een dergelijke afweging had de Nederlandse wetgever ook moeten maken ten aanzien van de opname van de vingerafdrukken in reisdocumentenadministratie. Onderzoek, dat niet is verricht, had in dat verband kunnen uitwijzen dat identiteitsfraude zich met name voordoet bij personen van 12 jaar en ouder. Inmiddels blijkt overigens dat de opname van vingerafdrukken bij personen van 70 jaar en ouder ook lastig is. De kwaliteit van de vingerafdrukken neemt immers met het ouder worden af. In een brief van 17 maart 2010 aan de Tweede Kamer geeft de staatssecretaris aan met een oplossing hiervoor te komen. Vragen naar nut en noodzaak van afname en opname in de reisdocumentenadministratie hadden echter in een veel eerder stadium door de staatssecretaris moeten worden gesteld.
57. Evenmin wordt een oplossing gegeven voor de enorme risico's van misbruik en onjuist gebruik en kan de regering aangeven waarom de voordelen van het door haar gewenste systeem opwegen tegen deze risico's. Het door het CBP voorgestelde alternatief voor een decentraal stelsel met centrale verwijzindex wordt in de Memorie van Toelichting eenvoudig afgedaan met de stelling dat dit praktisch niet uitvoerbaar zou zijn.³³ Van enig onderzoek naar andere alternatieven is kennelijk ook geen sprake. De regering heeft hierdoor onvoldoende blijk gegeven van een gedegen belangenafweging.
58. Dat de beginselen van proportionaliteit en subsidiariteit onvoldoende aan bod zijn gekomen in de totstandkoming van de Nieuwe Paspoortwet is een zorg die door

³³ Kamerstukken II 2007-08, 31 324 (R1844), nr. 3, p. 12.

meerdere instanties wordt gedeeld. Zo oordeelde het CBP dat het wetsvoorstel een ernstige inbreuk op de persoonlijke levenssfeer oplevert die niet wordt gerechtvaardigd door de door het wetsvoorstel te realiseren doeleinden en dat sprake is van een ernstige inbreuk op de privacy van burgers, met geen of minieme positieve effecten voor het algemeen belang.³⁴

59. Ook de Permanente Commissie van deskundigen in internationaal vreemdelingen-, vluchtelingen- en strafrecht heeft zich uitgesproken tegen de centrale administratie van biometrische gegevens. Volgens de commissie houdt een dergelijke centrale administratie onmiskenbaar risico's van misbruik en onjuist gebruik in. De commissie wijst erop dat de minister geen doorslaggevend argument geeft voor oprichting van een centrale administratie en vraagt zij zich af de voordelen wel opwegen tegen de risico's en of deze voordelen door andere technische maatregelen kunnen worden verkregen **[productie 5]**.³⁵
60. De toenmalig minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties is niet inhoudelijk ingegaan op de kritiek en vragen van de Permanente Commissie. Hij zegde slechts toe dat waar nodig in de Memorie van Toelichting bij het wetsvoorstel verder zou worden ingegaan op expliciete punten die door de Permanente Commissie werden genoemd.³⁶ Dat is echter niet gebeurd.
61. De Groep Gegevensbescherming Artikel 29 (de onafhankelijke Europese werkgroep die kwesties op het gebied van de bescherming van persoonsgegevens en privacy behandelt) heeft tevens haar zorgen geuit over het opzetten van een centrale administratie, omdat het risico bestaat dat hierdoor inbreuk wordt gemaakt op het fundamentele beginsel van proportionaliteit **[productie 3]**.³⁷
62. In het S. and Marper-arrest heeft het EHRM geoordeeld dat het feit dat vingerafdrukken van verdachten door de Engelse justitie niet uit een databank werden verwijderd op het moment dat niet langer sprake was van een verdenking, disproportioneel was. Voor de opname van vingerafdrukken in de Nederlandse centrale databank hoeft niet eens sprake te zijn van een verdenking. De vingerafdrukken van *alle* burgers met een paspoort worden immers opgeslagen. Dat sprake is van een ernstige inbreuk op de persoonlijke levenssfeer, omdat ook de gegevens van niet-

³⁴ Advies College Bescherming Persoonsgegevens d.d. 30 maart 2007, z2007-00010, p. 4-5 **[productie 2]**.

³⁶ Kamerstukken II 2005/06, 25 764, nr. 30, p. 4-5.

³⁷ Groep Gegevensbescherming Artikel 29, Advies 3/2005 betreffende de uitvoering van Verordening (EG) nr. 2252/2004 van de Raad van 13 december 2004 betreffende normen voor de veiligheidskenmerken van en

verdachte burgers in het register zijn opgenomen wordt ook door het CBP benadrukt.³⁸

f) Doeleinden

63. De doeleinden waarvoor de (biometrische) persoonsgegevens in het kader van de Nieuwe Paspoortwet worden verzameld en verwerkt zijn te talrijk en te breed geformuleerd.
64. In de inleiding van de Memorie van Toelichting is aangegeven dat het voornaamste doel van de nieuwe reisdocumentenadministratie is *"het creëren van een betrouwbaar aanvraag- en uitgifteproces van reisdocumenten met het oog op het voorkomen van identiteitsfraude, hetzij bij het aanvragen van een nieuw reisdocument, hetzij bij het gebruik van het reisdocument."*³⁹
65. Op een later moment in de Memorie van Toelichting blijkt echter dat de nieuwe reisdocumentenadministratie ook een veelheid aan andere doeleinden kan dienen, namelijk
 - Het voorkomen en bestrijden van fraude met en misbruik van reisdocumenten;
 - De identificatie van slachtoffers van rampen en ongevallen;
 - De opsporing en vervolging van strafbare feiten;
 - Het verrichten van onderzoek naar handelingen die een bedreiging kunnen vormen voor de veiligheid van de staat en andere gewichtige belangen van een of meer landen van het Koninkrijk dan wel de veiligheid van met het Koninkrijk bevriende mogendheden;
 - Het bevragen van het systeem in het kader van de in de verschillende landen van het Koninkrijk geldende wettelijke regelingen betreffende de identificatieplicht en het beheer en het gebruik van het burgerservicenummer teneinde vast te stellen of een document in het maatschappelijk verkeer mag voorkomen.⁴⁰
66. De centrale administratie dreigt door deze open geformuleerde en veelzijdige doelstellingen misbruikt te kunnen worden voor allerlei doeleinden. Dit terwijl gevoelige gegevens zoals biometrische gegevens nu juist onderworpen zouden moeten zijn aan strikt doelgebonden gebruik. Daarnaast geldt dat nog niet alle doeleinden voor de verschillende verwerkingen in het kader van de Nieuwe Paspoortwet vastgesteld. Zo moeten de doeleinden voor verstrekking van de gegevens

biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten, PB L 385 van 29.12.2004, p. 1.

³⁸ Advies College Bescherming Persoonsgegevens d.d. 30 maart 2007, z2007-00010, p. 5 [productie 2].

³⁹ Kamerstukken II 2007-08, 31 324 (R1844), nr. 3, p. 2.

⁴⁰ Kamerstukken II 2007-08, 31 324 (R1844), nr. 3, p. 12-13.

in het kader van artikel 4b nog nader worden vastgesteld bij AMvB, zoals ook hierboven aangegeven.

67. De doeleinden zijn bovendien onverenigbaar met het primaire doel van de administratie, het creëren van een betrouwbaar aanvraag- en uitgiftesysteem. Het CBP heeft ook aangegeven een nadere beschouwing van de verenigbaarheid van het opsporingsdoel met het doel van het aanvragen en uitgeven van reisdocumenten te missen.⁴¹
68. Daarenboven bestaat er ten aanzien van de nieuwe reisdocumentenadministratie een aanzienlijk risico op *function creep*, dat wil zeggen dat de gegevens die eens werden opgeslagen voor specifieke doeleinden, de belangstelling krijgen van andere personen en organisaties en worden gebruikt voor andere doeleinden dan waarvoor zij oorspronkelijk zijn bedoeld. Zo blijkt uit onderzoek van de heer Schermer van het platform ECP.nl dat de gegevens van een Nederlandse burger gemiddeld in 250 à 500 databanken zijn opgenomen en dat deze verschillende databanken steeds meer aan elkaar worden gekoppeld. Door deze "decontextualisering" wordt doelbinding steeds moeilijker te realiseren.⁴²
69. Op geen enkele manier wordt uitgesloten dat de gegevens in de centrale administratie voor visexpedities zullen worden gebruikt. De functie van het systeem kan gemakkelijk verschuiven en hiertegen zijn geen maatregelen genomen. In een interview op Radio 1 van 31 maart 2010 heeft de verantwoordelijk staatssecretaris al gewezen op een mogelijke verruiming van het gebruik van de opgeslagen gegevens in de toekomst.
70. Voor het gevaar van *function creep* is door meerdere organisaties gewaarschuwd. De Europese Toezichthouder voor Gegevensbescherming (EDPS) benadrukte dat een centrale opslag van gegevens uit reisdocumenten bijkomende risico's inhoudt voor de bescherming van die gegevens, zoals het ontstaan van verdere, niet in de verordening voorziene doelen, of zelfs visexpedities in de gegevensbank die moeilijk te bestrijden zullen zijn **[productie 4]**.⁴³
71. Ook de Artikel 29-Groep en het CBP waarschuwen dat een centrale database de kans op oneigenlijk gebruik en functieverhuizing (*function creep*) vergroot. Het CBP acht

⁴¹ Advies College Bescherming Persoonsgegevens d.d. 30 maart 2007, z2007-00010, p. 5-6 **[productie 2]**.

⁴² 16 Miljoen BN-ers? Bescherming van Persoonsgegevens in het Digitale Tijdperk' (verslag Iustrumcongres), *NJCM-Bulletin* jrg. 34 (2009), nr. 8, p. 936 en 937.

⁴³ Advies van de Europese Toezichthouder voor gegevensbescherming over het voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EG) nr. 2252/2004 van de Raad betreffende

de kans groot dat ten aanzien van het verstrekkingenregime in de loop van de tijd zal worden verruimd en geeft aan dat het risico op function creep door de Nieuwe Paspoortwet niet wordt uitgesloten.⁴⁴

72. Ten slotte geldt dat de regels in de Nieuwe Paspoortwet niet geschikt zijn om de in de Memorie van Toelichting aangegeven doeleinden te bereiken. De Staat verzamelt en verwerkt vingerafdrukken met het doel de identiteit van burgers vast te kunnen stellen. Biometrische persoonsherkenning is echter gebaseerd op kansberekening en leidt dus altijd tot een aantal onterechte herkenningen en een aantal onterechte afwijzingen. Er wordt door middel van biometrische persoonsherkenning daarom nooit 100% zekerheid verkregen dat iemand de juiste persoon is. Bovendien kan biometrie niets zeggen over de juistheid van documenten of gegevens waaraan een persoon door middel van biometrie wordt gekoppeld noch over de juistheid van de koppeling zelf.
73. Dat wordt ook benadrukt door Prof. dr. mr. Grijpink, raadadviseur op het ministerie van Justitie, hoogleraar informatiekunde en voorzitter van het Nederlands Biometrie Forum. Hij waarschuwt ook voor zogenaamde niveauvergissingen. Inzichten die zijn ontleend aan een bepaald niveau (bijvoorbeeld kleinschalige toepassingen) zijn op andere niveaus vaak namelijk vaak niet geldig. Zo kan het inzicht dat iemand kan worden herkend aan zijn vingerafdruk volgens hem niet zomaar worden doorgetrokken naar de nationale of internationale schaal van grensbewaking[productie 20].⁴⁵

JURIDISCH KADER

74. De Nieuwe Paspoortwet is (op belangrijke onderdelen) onrechtmatig. De wet en de wijze waarop daar uitvoering aan wordt gegeven is namelijk in strijd met het gemeenschapsrecht, te weten de Verordening, de Privacyrichtlijn en het Verdrag betreffende de werking van de Europese Unie alsmede met het EVRM. Bij de behandeling hiervan zal waar nodig worden verwezen naar hetgeen hierboven in het hoofdstuk Wijzigingen Nederlandse Paspoortwet in de paragrafen a t/m f is opgenomen.

normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten, *PbEU* 2008/C 200/01.

⁴⁴ Groep Gegevensbescherming Artikel 29, Advies 3/2005 betreffende de uitvoering van Verordening (EG) nr. 2252/2004 van de Raad van 13 december 2004 betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten, *PB* L 385 van 29.12.2004, p. 1; Brief CBP aan Staatssecr. van BZK, Adviesaanvraag wijziging Paspoortwet i.v.m. de herinrichting van de reisdocumentenadministratie, 30 maart 2007, kenmerk z2007-00010.

⁴⁵ J.H.A.M. Grijpink, 'Zinvol, betrouwbaar en veilig gebruik van biometrie', *Privacy & Informatie* 2009/6, p. 276 [productie 20].

Strijd met het gemeenschapsrecht

Strijd met de Verordening

75. Een Verordening maakt, zodra zij in werking is getreden, deel uit van de nationale rechtsorde net als nationale wetten dat doen.⁴⁶ Zij behoudt echter wel haar karakter van EG-recht, als gevolg waarvan de verordening voorrang heeft boven strijdig nationaal recht. Het is lidstaten dan ook niet toegestaan maatregelen te nemen als gevolg waarvan de strekking van een verordening wordt gewijzigd of bepalingen worden toegevoegd.⁴⁷
76. Dat de Nieuwe Paspoortwet in strijd is met de Verordening is in het voorgaande reeds uitgebreid aangegeven. De Verordening biedt immers onder meer geen grond voor de centrale opslag van gegevens. Bovendien is het in de Nieuwe Paspoortwet vastgelegde verstrekkingenregime in strijd met artikel 4 lid 3 van de Verordening.

Strijd met de Privacyrichtlijn

77. Overweging 8 van de Verordening bepaalt dat de Privacyrichtlijn van toepassing is op de persoonsgegevens die in verband met paspoorten en reisdocumenten worden verwerkt. Nu de Privacyrichtlijn van een hogere rangorde is dan de Nederlandse Wet bescherming persoonsgegevens ("Wbp"), zal de Nieuwe Paspoortwet in het onderstaande aan de richtlijn worden getoetst. Van belang is dat de richtlijn in de Wbp is geïmplementeerd en dat de Wbp derhalve tevens van toepassing is. De Nieuwe Paspoortwet is in strijd met meerdere bepalingen van de Privacyrichtlijn.

Strijd met artikel 6

78. In de eerste plaats is de wet in strijd met de volgende bepalingen van artikel 6:
- Lid 1 sub a:
De verwerking van persoonsgegevens in het kader van de Nieuwe Paspoortwet is niet eerlijk en rechtmatig, zoals artikel 6 lid 1 sub a vereist. 'Rechtmatig' ('lawful', in de Engelse versie van de richtlijn) betekent dat de verwerking van persoonsgegevens alléén mag plaatsvinden in overeenstemming met de wet. Bovendien houdt een eerlijke en rechtmatige verwerking de noodzaak in de betrokken belangen af te wegen. Bij deze afweging spelen het subsidiariteitsbeginsel en het proportionaliteitsbeginsel een belangrijke rol. De Nieuwe Paspoortwet voldoet noch aan het vereiste van proportionaliteit, noch aan het vereiste van subsidiariteit (zie hierboven paragraaf e).

⁴⁶ HvJEG 13 december 1967, zaak 17-67 (*Firma Max Neumann / Hauptzollamt Hof*).

⁴⁷ HvJEG 18 februari 1970, zaak 40-69 (*Hauptzollamt Hamburg-Oberelle / Firma Paul B. Bollmann*); HvJEG 2 februari 1977, zaak 50-76 (*Amsterdam Bulb BV / Produktschap voor Siergewassen*).

- Lid 1 sub b:

De persoonsgegevens zijn niet verkregen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en mogen en worden verwerkt op een wijze die onverenigbaar is met die doeleinden (zie hierboven paragraaf f).

- Lid 1 sub c en d:

De persoonsgegevens zijn niet toereikend, terzake dienend en wel degelijk bovenmatig in het kader van de doeleinden waarvoor zij worden verzameld en verwerkt. Evenmin zijn de vingerafdrukken die in het kader van de Nieuwe Paspoortwet worden verwerkt, voldoende nauwkeurig. Hierboven is aangegeven dat vingerafdrukken niet geschikt zijn voor het beoogde doel (zie hierboven paragraaf f).

- Lid 1 sub e:

De Nieuwe Paspoortwet is tevens in strijd met artikel 6 lid 1 sub e. De gegevens worden namelijk voor onbepaalde tijd opgeslagen, althans er is geen bewaartermijn in de wet opgenomen. De Memorie van Toelichting geeft aan dat deze bewaartermijn nader zal worden vastgesteld bij AMvB.⁴⁸

Strijd met artikel 7

79. Artikel 7 van de Privacyrichtlijn bevat een limitatieve opsomming van de gronden die een verwerking van persoonsgegevens kunnen rechtvaardigen. Evident is dat de gronden genoemd sub a, b, c en d van artikel 7 niet van toepassing zijn op de verwerking van persoonsgegevens in het kader van de Nieuwe Paspoortwet. Er is immers geen sprake van ondubbelzinnige toestemming van burgers (sub a), noch van de uitvoering van een overeenkomst waarbij de burgers partij zijn (sub b), noch van een wettelijke verplichting waaraan de Staat is onderworpen (sub c, eerder werd al aangegeven dat de Verordening geen verplichting inhoudt tot opslag van vier vingerafdrukken en/of het tot stand brengen van een centrale databank), noch van een vitaal belang van de betrokken burgers (sub d, daarvan is bijvoorbeeld sprake in geval van een situatie waarin medische hulp dringend geboden is).
80. Artikel 7 sub e biedt evenmin een grond voor de Nieuwe Paspoortwet. Daarvan is alleen sprake wanneer de verwerking van persoonsgegevens noodzakelijk is voor de vervulling van een taak van algemeen belang of die deel uitmaakt van de uitoefening van het openbaar gezag die aan de voor de verwerking verantwoordelijke of de derde aan wie de gegevens worden verstrekt, drager is opgedragen. Hiervoor is ten minste vereist dat een verwerking voldoet aan de vereisten van proportionaliteit en subsidiariteit.

⁴⁸ *Kamerstukken II 2007/08, 31 324 (R1884), nr. 3, p. 35-36.*

81. Artikel 7 sub f, ten slotte, biedt ook geen grondslag voor de verwerking van persoonsgegevens in het kader van de Nieuwe Paspoortwet. De verwerking is niet noodzakelijk voor de behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke of van de derde(n) aan wie de gegevens worden verstrekt en het belang en de fundamentele rechten en vrijheden van de burgers dient te prevaleren, zoals als uit paragraaf e hierboven wel mag blijken.
82. Artikel 7 sub f van de Privacyrichtlijn is geïmplementeerd in artikel 8 sub f van de Wbp. Over dit artikel merkte de Minister van Justitie in de Nota naar aanleiding van het Verslag bij de Wbp het volgende op.

"Meer in het algemeen kan worden opgemerkt dat het verzamelen van gegevens over willekeurige burgers voor een doel dat mogelijk in de toekomst relevant zal zijn, in beginsel niet is toegestaan. Het vergaren van persoonsgegevens uitsluitend «omdat dat misschien in de toekomst handig kan zijn», of voor «je weet maar nooit» kan dus niet. Dat betekent dat in de regel een rechtvaardiging voor gegevensverwerking aanwijsbaar moet zijn in de individuele persoon over wie gegevens worden vergaard." [onderstreping adv.]⁴⁹

83. Duidelijk is dat de verwerking van persoonsgegevens in het kader van de Nieuwe Paspoortwet niet gebaseerd kan worden op deze grondslag.

Strijd met artikel 17

84. Artikel 17 lid 1 bepaalt dat door de verantwoordelijke passende technische en organisatorische maatregelen moeten worden genomen om persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang.
85. Het EHRM heeft herhaaldelijk onderstreept hoe belangrijk het is dat persoonsgegevens worden beschermd in het kader van artikel 8 EVRM.⁵⁰ Van passende technische en organisatorische maatregelen is in casu geen sprake (zie paragraaf d).

Strijd met artikel 8

86. Tot slot vallen biometrische gegevens onder de categorie gevoelige gegevens (artikel 8 van de Privacyrichtlijn). Biometrische gegevens als vingerafdrukken bevatten immers

⁴⁹ Kamerstukken II 1998/99, 25 892, nr. 6, blz. 34.

⁵⁰ EHRM 17 juli 2008, I v. Finland (verzoekschrift nr. 20511/03); EHRM 25 november 2008, Armonas v. Litouwen (verzoekschrift nr. 36919/02).

ook bijzondere informatie als rasgegevens.⁵¹ De Permanente Commissie van deskundigen in internationaal vreemdelingen-, vluchtelingen- en strafrecht, die zich heeft uitgesproken tegen de centrale administratie van biometrische gegevens, schreef in dit verband het volgende.

*"Bij biometrische gegevens gaat het om bijzondere informatie, zoals gezichtskenmerken die rasgegevens bevatten. De opslag van deze gegevens moet op basis van het geldende recht daarom met strengere en niet met minder strenge eisen worden omkleed. De noodzaak van de opslag van deze gegevens moet expliciet worden afgewogen tegen de risico's van deze opslag voor de rechten en vrijheden van het individu."*⁵²

Strijd met Verdrag betreffende de werking van de Europese Unie

87. De naam van het voormalig EG-Verdrag is op grond van het Verdrag van Lissabon⁵³ gewijzigd in het Verdrag betreffende de werking van de Europese Unie ("VwEU").⁵⁴ In het VwEU zijn de bevoegdheden van de Europese Unie vastgelegd alsmede de manier waarop deze bevoegdheden kunnen worden uitgeoefend. Het VwEU vormt samen met het Verdrag betreffende de Europese Unie de basis van de Europese Unie.
88. Artikel 16 VwEU bepaalt dat een ieder recht heeft op bescherming van zijn persoonsgegevens.

1. Een ieder heeft recht op bescherming van zijn persoonsgegevens.
2. Het Europees Parlement en de Raad stellen volgens de gewone wetgevingsprocedure de voorschriften vast betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie, alsook door de lidstaten, bij de uitoefening van activiteiten die binnen het toepassingsgebied van het recht van de Unie vallen, alsmede de voorschriften betreffende het vrij verkeer van die

⁵¹ Brief Permanente commissie van deskundigen in internationaal vreemdelingen-, vluchtelingen- en strafrecht aan de vaste commissie voor Binnenlandse Zaken en Koninkrijksrelaties van de Tweede kamer der Staten-Generaal betreffende het voorstel van de Minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties voor de inrichting van een centrale administratie van paspoorten en reisdocumenten, met inbegrip van biometrische gegevens d.d. 13 april 2006, kenmerk CM0603, p. 1-2.

⁵² Brief Permanente commissie van deskundigen in internationaal vreemdelingen-, vluchtelingen- en strafrecht aan de vaste commissie voor Binnenlandse Zaken en Koninkrijksrelaties van de Tweede kamer der Staten-Generaal betreffende het voorstel van de Minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties voor de inrichting van een centrale administratie van paspoorten en reisdocumenten, met inbegrip van biometrische gegevens d.d. 13 april 2006, kenmerk CM0603, p. 1-2.

⁵³ Verdrag van Lissabon tot wijziging van het Verdrag betreffende de Europese Unie en het Verdrag tot oprichting van de Europese Gemeenschap, Lissabon 13 december 2007, *PbEU* 2007, C 306/01.

⁵⁴ Geconsolideerde versies van het Verdrag betreffende de Europese Unie en van het Verdrag tot oprichting van de Europese Gemeenschap, *PbEU* 2006, C 321E/01.

gegevens. Op de naleving van deze voorschriften wordt toezicht uitgeoefend door onafhankelijke autoriteiten.

De op basis van dit artikel vastgestelde voorschriften doen geen afbreuk aan de in artikel 39 van het Verdrag betreffende de Europese Unie bedoelde specifieke voorschriften.

89. Artikel 16 heeft rechtstreekse werking.⁵⁵ De inhoud artikel 16 lid 1 VwEU is identiek aan de inhoud van artikel 8 lid 1 van het Handvest van de grondrechten van de Europese Unie ("het Handvest").⁵⁶ Op grond van het Verdrag van Lissabon heeft het Handvest een bindende status verkregen en daarmee rechtstreekse werking.
90. In het voorgaande is al gebleken dat persoonsgegevens als gevolg van de Nieuwe Paspoortwet geenszins worden beschermd. De Nieuwe Paspoortwet is daarmee in strijd met artikel 16 VwEU. Dat geldt ook nu artikel 8 lid 2 van het Handvest bepaalt dat persoonsgegevens eerlijk moeten worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Daarnaast dient een ieder toegang te hebben tot de over hem verzamelde gegevens en op rectificatie daarvan. Een dergelijk recht komt de betrokkenen op grond van de Nieuwe Paspoortwet niet toe.
91. Bovendien geldt op grond van artikel 52 van het Handvest dat beperkingen op de uitoefening van de in het Handvest erkende rechten en vrijheden de wezenlijke inhoud van die rechten en vrijheden moeten eerbiedigen. Op grond van artikel 52 kunnen met inachtneming van het evenredigheidsbeginsel alleen beperkingen worden gesteld indien zij noodzakelijk zijn en daadwerkelijk aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen beantwoorden. Uit het bovenstaande, met name gezien hetgeen sub e en f is besproken, mag blijken dat de Nieuwe Paspoortwet niet aan de vereisten voor deze beperking voldoet.

Strijd met artikel 8 EVRM

92. Artikel 8 EVRM luidt als volgt:

1. Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische

⁵⁵ HvJEG 17 september 2002, zaak C-413/99 (*Baumbast*).

⁵⁶ Handvest van de Grondrechten van de Europese Unie 7 december 2000, *PbEG* C 364.

samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

93. De (centrale) opslag en verwerking van biometrische kenmerken zoals vingerafdrukken en andere persoonsgegevens door de overheid in het kader van de Nieuwe Paspoortwet moet voldoen aan de regels van artikel 8 EVRM, zoals ook in de Memorie van Toelichting wordt aangegeven.⁵⁷

Beperking

94. De plicht om vier vingerafdrukken, een gezichtsopname en andere persoonsgegevens aan de overheid te verstrekken, de (centrale) opslag van al deze gegevens en het feit dat de gegevens aan verschillende partijen kunnen worden verstrekt, resulteert in een beperking van het recht op privacy, zoals ook door de minister wordt bevestigd in de Memorie van Toelichting.⁵⁸

“Daarmee werd en wordt een inbreuk gemaakt op het in de landen van het Koninkrijk geldende recht op bescherming van de persoonlijke levenssfeer. In het bijzonder wordt in verband daarmee gewezen op het nieuwe artikel 4a van het onderhavige voorstel van rijkswet, op basis waarvan de gegevens die bij de aanvraag van een reisdocument worden verstrekt in de on line bevraagbare reisdocumentenadministratie, worden opgeslagen.(...)”

Om te beoordelen of deze inbreuk gerechtvaardigd is, dient een afweging te worden gemaakt tussen enerzijds het recht op de bescherming van de persoonlijke levenssfeer en anderzijds het belang van een accurate en effectieve reisdocumentenadministratie. Onder voorwaarden zoals die zijn neergelegd in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM), artikel 17 van het Internationaal Verdrag voor Burgerlijke en Politieke Rechten (hierna: IVBPR) en – voor Nederland – richtlijn nr. 95/4/EG van het Europees Parlement en de Raad van de Europese Unie van 23 november 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, 1 artikel 10 Grondwet en de Wet bescherming persoonsgegevens die is vastgesteld ter uitvoering van de genoemde EG-richtlijn, kan een inbreuk op het grondrecht tot eerbiediging van de persoonlijke levenssfeer in sommige

⁵⁷ Kamerstukken II 2007/08, 31 324 (R1844), nr. 3, p. 20.

⁵⁸ Kamerstukken II 2007/08, 31 324 (R1844), nr. 3, p. 20.

gevallen worden gerechtvaardigd.”⁵⁹ [onderstreping adv.]

95. Ook in het arrest *S. and Marper* wordt door het EHRM benadrukt dat de opslag van vingerafdrukken een beperking op de privacy oplevert [**productie 21**].

*“The Court accordingly considers that the retention of fingerprints on the authorities’ records in connection with an identified or identifiable individual may in itself give rise, notwithstanding their objective and irrefutable character, to important private-life concerns.”*⁶⁰

96. Op grond van artikel 8 EVRM is een beperking op de privacy alleen toegestaan indien deze voldoet aan drie cumulatieve vereisten:

- De beperking is voorzien bij wet;
- De beperking dient één van de belangen aangegeven in artikel 8 lid 2 EVRM;
- De beperking is noodzakelijk in een democratische samenleving.

97. Er dient op bovenstaande volgorde aan deze eisen worden getoetst. Wanneer aan één der eisen niet is voldaan, komt men aan toetsing van de volgende voorwaarde niet meer toe. In het onderstaande zal worden aangegeven dat de Nieuwe Paspoortwet deze test niet kan doorstaan.

Voorzien bij wet

98. Onder “wet” wordt verstaan zowel wetgeving in materiële en formele zin, ongeschreven recht en bevoegd gegeven bevelen. Van belang is met name dat een beperking toegankelijk en voorzienbaar dient te zijn. Dat blijkt ook uit het *Kruslin* en *Huvig*-arrest, waarin het begrip voorzienbaar is gespecificeerd.

*“The law must be sufficient clear in its terms to give citizen an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.”*⁶¹

99. Zoals in paragraaf d hierboven is aangegeven, moet een groot deel van de regels ten aanzien van de opslag van de biometrische gegevens en het verstrekkingenregime ten aanzien van deze gegevens nog nader worden vastgesteld bij AMvB. Als gevolg

⁵⁹ *Kamerstukken II* 2007/08, 31 324 (R1844), nr. 3, p. 20-21.

⁶⁰ EHRM 4 december 2008, Applications nos. 30562/04 and 30566/04 (*S. and Marper / The United Kingdom*).

⁶¹ EHRM 24 april 1990, *NJ* 1991, 523, r.o. 29.

daarvan is niet het vereiste van voldoende voorzienbaarheid voldaan.

Belangen

100. Een beperking op het recht op privacy is toegestaan indien de beperking één van de volgende doelen genoemd in lid 2 van artikel 8 EVRM dient. Er kan geen misverstand over bestaan dat de Nieuwe Paspoortwet niet noodzakelijk is in het belang van het economisch welzijn van Nederland, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.
101. Of alle in de Memorie van Toelichting opgesomde doeleinden vallen onder belangen geformuleerd in artikel 8 EVRM, is nog maar de vraag. In ieder geval is niet voldaan aan het vereiste van doelbinding, zoals in paragraaf f hierboven is aangegeven.

Noodzakelijk in een democratische samenleving

102. Een beperking op artikel 8 EVRM moet, wil deze gerechtvaardigd zijn, noodzakelijk zijn in een democratische samenleving. Deze noodzakelijkheid moet volgens het Barthold-arrest van het EHRM overtuigend worden gesteld.⁶² Dit betekent dat niet moet worden bekeken of er voor het verbod een klemmende reden van publiek belang is, maar of er voor de beperking op het recht op privacy een *dringende noodzaak* bestaat.⁶³ Om aan dit vereiste te voldoen moet de beperking voorzien in een "pressing social need" en proportioneel zijn. De vraag of de beperking necessary in a democratic society is, levert dus een dubbele toets op:
 - (i) Is er een *pressing social need* voor de beperking?
 - (ii) Is de beperking proportioneel aan het nagestreefde doel?
103. Het feit dat een beperking onmisbaar, toegestaan, gebruikelijk, redelijk of wenselijk is, is dus niet voldoende om bij te dragen aan de noodzakelijkheid in een democratische samenleving die artikel 8 EVRM lid 2 vereist. Dat kan enkel het geval zijn als er een *pressing social need* bestaat.⁶⁴
104. Daarnaast moet de beperking proportioneel zijn ten opzichte van het te bereiken doel. Dat betekent dat de ernst van de beperking moet opwegen tegen het met de beperking gediende belang. Des te ingrijpender de beperking, des te zwaarder de proportionaliteitstoets. Daarbij is ook de subsidiariteit van groot belang. In paragraaf e hierboven is al aangegeven dat voornoemde maatregelen in de Nieuwe Paspoortwet

⁶² EHRM 25 maart 1985, NJ 1987, 900 (*Barthold*), overweging 58.

⁶³ G.A.I. Schuijt, 'Hoge Raad niet meer bang voor de uitingsvrijheid?', *Informatierecht/AMI* 1990-5, p. 83-88.

⁶⁴ EHRM 26 april 1979, NJ 1980, 146, m.nt. E.A. Alkema (*Sunday Times*).

niet noodzakelijk zijn en niet voldoen aan de vereisten van proportionaliteit en subsidiariteit.

Onrechtmatige wetgeving

105. In het bovenstaande is aangegeven dat de Nieuwe Paspoortwet op belangrijke punten in strijd is met verschillende bepalingen van het gemeenschapsrecht en met artikel 8 EVRM. Als gevolg hiervan is de wet (gedeeltelijk) onrechtmatig op grond van artikel 6:162 BW. Door het uitvaardigen van de wet heeft de wetgever een onrechtmatige daad begaan.⁶⁵
106. Het is vaste jurisprudentie dat materiële wetgeving onrechtmatig kan zijn op grond van artikel 6:162 BW. Dat volgt bijvoorbeeld uit het arrest *Pocketbooks II*.⁶⁶ In dit arrest oordeelde de Hoge Raad dat geen rechtsregel eraan in de weg staat dat artikel 1401 BW (het huidige artikel 6:162 BW) van toepassing kan zijn op wetgeving.
107. Het vaststellen van de Nieuwe Paspoortwet door de minister en het bekendmaken, uitvoeren en doen uitvoeren daarvan, resulteert dan ook in een onrechtmatige daad van de Staat jegens Privacy First en de degenen wier belangen zij behartigt.

Vorderingen

108. Uit het voorgaande mag genoegzaam blijken dat Privacy First en de 22 mede-eisers, natuurlijke personen recht op en belang bij toewijzing van de vorderingen hebben. Daar kan nog het volgende aan worden toegevoegd.

Buiten werking stellen wetgeving

Wegens strijd met gemeenschapsrecht

109. Nationale regelgeving mag niet in strijd zijn met normen van gemeenschapsrecht, zoals verordeningen en richtlijnen. Dat is onlangs nog bevestigd in een verklaring bij het Verdrag van Lissabon, waarin de Intergouvernementele Conferentie stelt dat in overeenstemming met de vaste rechtspraak van het Hof van Justitie van de Europese Unie, de verdragen en het recht dat de Unie op grond van de verdragen vaststelt, voorrang hebben boven het recht van de lidstaten.⁶⁷
110. Ook het Hof van Justitie van de Europese Gemeenschappen ("HvJEG") heeft in meerdere arresten benadrukt dat de rechtsorde van de EG is opgenomen in de

⁶⁵ R.J.B. Schutgens, *Onrechtmatige wetgeving*, Deventer: Kluwer 2009, p. 38-39.

⁶⁶ HR 24 januari 1969, NJ 1969, 316.

rechtsorde van de lidstaten en dat aan het gemeenschapsrecht voorrang toekomt boven nationale voorschriften, bijvoorbeeld in het arrest *Costa / Enel*.⁶⁸ Dat geldt niet alleen voor bepalingen van primair gemeenschapsrecht, maar ook voor afgeleid gemeenschapsrecht.⁶⁹

111. Indien nationaal recht strijdig is met gemeenschapsrecht, moet de nationale rechter het buiten toepassing laten.⁷⁰ Op lidstaten rust dus de verplichting te vermijden dat een met het gemeenschapsrecht strijdige bepaling wordt aangenomen en om elke bestaande strijdige bepaling zodanig te wijzigen dat de strijdigheid wordt opgeheven.⁷¹ Sterker nog, onder omstandigheden is de nationale rechter zelfs verplicht om de uitvoering van nationale wetgeving op te schorten als er nog twijfel bestaat over de verenigbaarheid van de wetgeving met het gemeenschapsrecht.⁷²
112. De Nieuwe Paspoortwet is in ieder geval op drie verschillende grondslagen in strijd met het gemeenschapsrecht, te weten
 - i) de Verordening;
 - ii) de Privacyrichtlijn
 - iii) het VwEU.
113. Wetgeving die in strijd is met gemeenschapsrecht, moet buiten werking worden gesteld. Dat geldt ook voor wetten in formele zin.⁷³ Van belang daarbij is dat de onderhavige vorderingen niet zien op het *intrekken* van (formele) wetgeving, maar louter op *buiten werking te stellen* daarvan. Voor het intrekken van de Nieuwe Paspoortwet is gerechtelijk bevel voor het tot stand brengen van wetgeving in formele zin nodig, hetgeen volgens de Hoge Raad niet is toegestaan.⁷⁴
114. De vordering tot buiten werking stelling van wetgeving vereist echter geen intrekking, maar ziet louter op het buiten toepassing laten van bepaalde wetgeving, met andere woorden: een toepassingsverbod.⁷⁵ De Hoge Raad heeft deze rechtsfiguur in het arrest

⁶⁷ Verklaringen gehecht aan de slotakte van de intergouvernementele conferentie die het verdrag van Lissabon heeft aangenomen ondertekend op 13 december 2007, *PbEU* C 115/335.

⁶⁸ HvJEG 15 juli 1964, *Jur.* 1964, p. 585 (*Costa / Enel*). Zie in gelijke zin Rb. Utrecht 20 februari 2009, *LJN* BH9177 (r.o. 5.3).

⁶⁹ HvJEG 9 maart 1978, nr. 106/77, *Jur.* 1978, p. 629 (Simmenthal);

⁷⁰ HvJEG 9 maart 1978, nr. 106/77 (*Administratie van de staatsfinanciën / Naamloze Vennootschap Simmenthal*); HvJEG, 23 april 2009, nr. C-261/07 (*VTB-VAB / Total Belgium*); HvJEG 23 april 2009, C- 299/07 (*Galatea BVBA/Sanoma Magazines Belgium N.V.*).

⁷¹ K. Lenaerts & P. van Nuffel, *Europees recht in hoofdlijnen*, Antwerpen; Maklu 2008, p. 402.

⁷² HvJEG 19 juni 1990, C-231/89 (*The Queen t. Secretary of State for Transport, ex parte Factortame Ltd. e.a.*).

⁷³ V.zr.Rb. Den Haag 19 maart 2008, *NJ* 2008, 304.

⁷⁴ HR 1 oktober 2004, *NJ* 2004, 679 (*Faunabescherming / Provincie Fryslan*).

⁷⁵ R.J.B. Schutgens, *Onrechtmatige wetgeving*, Deventer: Kluwer 2009, p. 93.

LSV zo uitgelegd, dat deze in de dogmatiek past. Dat wordt ook bevestigd in de literatuur.

*"Tegen de term 'buitenwerkingstelling' is het bezwaar ingebracht, dat deze ten onrechte de suggestie wekt, dat de burgerlijke rechter een rechtshandeling verricht die de regeling haar rechtskracht ontnemt. De Hoge Raad heeft deze rechtsfiguur in LSV echter zo uitgelegd, dat zij in de dogmatiek past. De term is ingeburgerd. Ik zie daarom weinig reden om ervan af te stappen. Een rechter die de term dogmatisch onzuiver vindt, kan overigens in plaats daarvan een algemeen toepassingsverbod uitspreken. Dat verschilt inhoudelijk niet van een buitenwerkingstelling."*⁷⁶

Wegens strijd met artikel 8 EVRM

115. Op grond van artikel 94 van de Grondwet (Gw) vinden wetten geen toepassing indien die toepassing niet verenigbaar is met een ieder verbindende bepalingen van verdragen en van besluiten van volkenrechtelijke organisaties. Ook formele wetten dienen op grond van artikel 94 Gw buiten toepassing te worden gelaten indien zij in strijd zijn met een ieder verbindende bepalingen van verdragen.⁷⁷
116. Op grond van artikel 94 dient de rechter zowel te toetsen of een nationaal wettelijk voorschrift als zodanig in strijd is met een verdragsbepaling, als of de uitwerking van de wettelijke bepaling op de partij die de niet-toepasselijkheid daarvan inroept. Dat is ook bevestigd door de regering tijdens de totstandkoming van de huidige Gw.

*"wij zijn van oordeel dat juist de gebruikte formulering duidelijk laat uitkomen dat de grondwetgever niet slechts de nationale wetsregel zelf, maar evenzeer de uitwerking ervan op de rechtszoekende getoetst wil zien bij de beoordeling van de vraag of de nationale bepaling moet wijken voor de bepalingen van het internationale recht."*⁷⁸

117. Algemeen bekend is dat artikel 8 EVRM een ieder verbindende bepaling is als bedoeld in artikel 94 Gw. Dat blijkt duidelijk uit literatuur⁷⁹ en jurisprudentie.⁸⁰ Nu de Nieuwe Paspoortwet in strijd is met artikel 8 EVRM, dient deze op grond van artikel 94 Gw buiten toepassing te worden gelaten.

⁷⁶ R.J.B. Schutgens, *Onrechtmatige wetgeving*, Deventer: Kluwer 2009, p. 81.

⁷⁷ HR 19 mei 2000, *NJ* 2001, 407.

⁷⁸ *Kamerstukken II* 1979/80, 15 049 (R 1100), nr. 7, p. 19.

⁷⁹ F.M.C. Vlemminx, 'Een ieder verbindend verdragsrecht en de bevoegdheden van de (bestuurs)rechter', *NJB* 1999/12, p. 950.

⁸⁰ HR 22 februari 1985, *NJ* 1986, 3; Rb. Leeuwarden 14 april 2004, *LJN* OA8248.

PROCESVERLOOP

118. Op 8 december 2009 hebben de advocaten van Privacy First in een brief aan het ministerie van Binnenlandse Zaken en Koninkrijksrelaties ("BZK") aangegeven dat de Nieuwe Paspoortwet in zijn huidige vorm onrechtmatig is en geheel of gedeeltelijk buiten werking dient te worden gesteld danwel niet in werking dient te treden [productie 22]. Gelet op het bepaalde in artikel 3:305a BW is de minister namens Privacy First en de andere partijen wiens belangen Privacy First behartigt, verzocht met Privacy First binnen een bepaalde termijn in overleg te treden teneinde deze onrechtmatigheid op te heffen.
119. Op 18 december 2009 heeft de staatsecretaris van BZK Privacy First per brief geïnformeerd bereid te zijn in overleg te treden. Daarbij werd wel aangegeven dat het ministerie van BZK geen voornemen had om op de door Privacy First aangegeven punten een wijziging in de Paspoortwet te initiëren [productie 23]. Desalniettemin heeft Privacy First het nadere bericht van BZK afgewacht en heeft op 20 januari 2010 overleg tussen partijen plaatsgevonden. Als productie 17 wordt overgelegd het verslag van de bespreking dat op 4 maart 2010 aan de Staat is gezonden. Daarop heeft Privacy First op 6 april 2010 een reactie ontvangen van de Staat [productie 18]. In de reactie geeft de Staat aan dat het verslag van 4 maart 2010 in algemene zin een adequate weergave vormt van het overleg, slechts ten aanzien van enkele detailpunten worden een opmerking gemaakt. Ook wordt aangegeven dat de Staat nog nagaat op welke wijze aan de verzoeken tot verstrekking van informatie over de zelfevaluaties en audits met betrekking tot de beveiliging van reisdocumentenadministraties en over de cijfers met betrekking tot vermiste paspoorten tegemoet kan worden gekomen.

VERWEER GEDAAGDE

120. Er is Privacy First geen verweer bekend van de Staat met betrekking tot de eisen van Privacy First. Noch in haar reactie op de sommatie van Privacy First van 8 december 2009, noch tijdens het overleg tussen partijen op 20 januari 2010 heeft de Staat aangegeven wat de redenen zijn dat zij geen voornemen heeft om op de door Privacy First aangegeven punten een wijziging in de Paspoortwet te initiëren.
121. In het bovenstaande is uitgebreid ingegaan op de parlementaire geschiedenis van de Nieuwe Paspoortwet en de redenen die daarin worden vermeld voor de totstandkoming

van de regelgeving. Voor zover het verweer van de Staat gegrond zou zijn op stellingen uit deze parlementaire stukken, is in het bovenstaande reeds genoegzaam aangetoond dat deze stellingen onjuist zijn en de Nieuwe Paspoortwet niet kunnen rechtvaardigen.

BEWIJSAANDRACHT

122. Ter staving van de gronden van de eis beschikt Privacy First – naast de reeds in deze dagvaarding genoemde bewijsstukken, die zij op de Roldatum in het geding zal brengen – nog over diverse getuigen en deskundigen die over de volgende aspecten kunnen getuigen en verklaren: de wijze waarop biometrische gegevens worden afgenomen en opgeslagen, de mate waarin is voorzien in waarborgen ten aanzien van de veiligheid van de gegevens, het verstrekkingenregime en de consequenties van een en ander.
123. Privacy First wil met het vorenstaande niet geacht worden onverplicht enige bewijslast op zich te hebben genomen die niet rechtens op haar rust.
124. Voorzover de Staat andere stellingen van de Privacy First betwist en de rechtbank van oordeel mocht zijn dat de bewijslast terzake op Privacy First rust, biedt Privacy First aan ook die stellingen te bewijzen.

SAMENVATTING

125. Hierboven is uitvoerig uiteengezet waarom de vorderingen van Privacy First voor toewijzing gereed liggen. Privacy First heeft daartoe – heel kort samengevat – aangegeven in het bijzonder de volgende aspecten van de Nieuwe Paspoortwet en de uitvoering daarvan onrechtmatig te achten:
- Het opslaan, al dan niet centraal, van (biometrische) gegevens ten aanzien van alle houders van een Nederlands paspoort, ouder dan 12 jaar;
 - Het verstrekkingenregime ten aanzien van de gegevens die worden opgeslagen;
 - Het volledige gebrek aan waarborgen ten aanzien van de verstrekking, de integriteit en de veiligheid van de gegevens, met name nu deze waarborgen grotendeels moeten worden geformuleerd in lagere regelgeving (AMvB's), waarbij nauwelijks tot geen democratische controle is;

- De veronachtzaming van elementaire beginselen van proportionaliteit en subsidiariteit en het gebrek aan enige belangenafweging;
- Het ontbreken van de vereiste doelbinding;
- Het risico van *function creep*, het gebruik van de gegevens voor andere doeleinden dan waarvoor zij oorspronkelijk waren bedoeld.

126. De Nieuwe Paspoortwet is (op onderdelen) strijdig met:

- De Verordening en de Wijzigingsverordening. De verordeningen bieden nadrukkelijk geen grond voor de centrale opslag van gegevens. Bovendien bepaalt artikel 4 lid 3 van de Verordening dat de biometrische gegevens slechts mogen worden gebruikt voor het verifiëren van a) de authenticiteit van het paspoort; of b) de identiteit van de houder door middel van direct beschikbare vergelijkbare kenmerken wanneer het overleggen van een paspoort wettelijk vereist is. Het verstrekkingenregime in de Nieuwe Paspoortwet is hiermee in strijd.
- De Privacyrichtlijn. De wet is in strijd met artikel 6 nu
 - de verwerking van persoonsgegevens niet eerlijk en rechtmatig is;
 - de gegevens niet zijn verkregen voor welbepaalde en uitdrukkelijk omschreven en gerechtvaardigde doeleinden;
 - de gegevens niet toereikend, terzake dienend en wel bovenmatig zijn in het kader van de doeleinden waarvoor zij worden verwerkt;
 - de vingerafdrukken niet voldoende nauwkeurig zijn;
 - de gegevens langer worden bewaard dan noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Er is immers in het geheel geen bewaartermijn vastgesteld.

Daarnaast is sprake van strijd met artikel 7, nu er geen rechtmatige grondslag voor de verwerking van persoonsgegevens in het kader van de nieuwe reisdocumentenadministratie bestaat. Het feit dat er geen passende technische en organisatorische beveiligingsmaatregelen zijn genomen, is in strijd met artikel 17. Ten slotte is niet voldaan aan de vereisten voor het verwerken van bijzondere persoonsgegevens die gelden op grond van artikel 8;

- Het Verdrag betreffende de werking van de Europese Unie, op grond waarvan een ieder recht heeft op bescherming van zijn persoonsgegevens en artikel 8 van het Handvest, op grond waarvan persoonsgegevens eerlijk moeten worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet alsmede dat een ieder toegang te hebben tot de over hem verzamelde gegevens en recht heeft op rectificatie daarvan. Daarnaast is sprake van strijd met artikel 52 van het Handvest op grond waarvan met inachtneming van het evenredigheidsbeginsel alleen beperkingen worden gesteld indien zij noodzakelijk zijn en daadwerkelijk aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen beantwoorden;
- Artikel 8 EVRM, nu de Nieuwe Paspoortwet een beperking vormt op het recht op privacy en deze beperking niet is voorzien bij wet, geen rechtmatig belang dient en niet noodzakelijk is in een democratische samenleving.

VERZOEK TOT HET STELLEN VAN PREJUDICIËLE VRAGEN

127. Hierboven is uitvoerig uiteengezet waarom de vorderingen van Privacy First dienen te worden toegewezen. Privacy First beroept zich hierbij nadrukkelijk op meerdere bepalingen van gemeenschapsrecht en heeft aangegeven dat de Nieuwe Paspoortwet in strijd is met de Verordening, de Privacyrichtlijn en het Verdrag van Lissabon.
128. Voorzover de rechtbank enige aarzeling heeft over de juistheid van de standpunten van Privacy First ten aanzien van de strijdigheid van de Nieuwe Paspoortwet met voornoemd gemeenschapsrecht, geeft Privacy First de rechtbank eerbiedig in overweging al in dit stadium van de procedure vragen van uitleg omtrent het gemeenschapsrecht te stellen aan het HvJEG. Indien de rechtbank overweegt prejudiciële vragen te stellen, verzoekt Privacy First de rechtbank eerbiedig zich te mogen laten uitspreken over de inhoud van de vragen.

129. Volledigheidshalve zij opgemerkt dat de bevoegdheid van het HvJEG om prejudiciële beslissingen te geven is neergelegd in artikel 267 VwEU (voorheen artikel 234 EG-Verdrag).

Het Hof van Justitie is bevoegd, bij wijze van prejudiciële beslissing, een uitspraak te doen:

- a) over de uitlegging van de Verdragen,
- b) over de geldigheid en de uitlegging van de handelingen van de instellingen, de organen of de instanties van de Unie,

Indien een vraag te dien aanzien wordt opgeworpen voor een rechterlijke instantie van een der lidstaten, kan deze instantie, indien zij een beslissing op dit punt noodzakelijk acht voor het wijzen van haar vonnis, het Hof van Justitie verzoeken over deze vraag een uitspraak te doen.

Indien een vraag te dien aanzien wordt opgeworpen in een zaak aanhangig bij een nationale rechterlijke instantie waarvan de beslissingen volgens het nationale recht niet vatbaar zijn voor hoger beroep, is deze instantie gehouden zich tot het Hof te wenden.

(...)

130. Artikel 234 van het voormalig EG-Verdrag stelt in de woorden van het HvJEG een:

"[...] rechterlijke samenwerking [in], waarbij de nationale rechter en het Hof van Justitie – elk volgens hun eigen competentie – geroepen zijn, om rechtstreeks en wederzijds bij te dragen tot het vinden van een beslissing, waardoor de uniforme toepassing van het Gemeenschapsrecht in alle lidstaten wordt gewaarborgd."⁸¹

131. HvJEG en de nationale rechter dienen dus samen te werken om de functie van artikel 267 VwEU te vervullen: uniforme toepassing van het communautaire recht in alle lidstaten, met name ten aanzien van de uitlegging van dit recht door de nationale

rechters. In *Costa / Enel* bepaalde het HvJEG dat het voormalig artikel 234 EG-Verdrag, ongeacht enige nationale wet, steeds toepassing dient te vinden wanneer een vraag rijst met betrekking tot de uitlegging van het Verdrag.⁸² Met de ratio en functie van artikel 267 VwEU hangt samen dat de lagere rechter *de facto* niet veel anders zal kunnen doen dan gebruikmaken van zijn bevoegdheid indien aan een aantal eisen is voldaan.

132. De nationale rechter is bevoegd, en in hoogste instantie verplicht, een beslissing aan het HvJEG te vragen indien een vraag van interpretatie of geldigheid van gemeenschapsrecht voor hem wordt opgeworpen.

BEVOEGDHEID

133. De Rechtbank te 's-Gravenhage is te dezer zake bevoegd op grond van artikel 99 Rv.

MITSDIEN

het de Rechtbank te 's-Gravenhage behage bij vonnis, zoveel mogelijk uitvoerbaar bij voorraad:

- I. Voor recht te verklaren dat het de Nieuwe Paspoortwet jegens eisers, een onrechtmatige daad oplevert, in het bijzonder voor wat betreft de al dan niet centrale opslag van (biometrische) gegevens, de wijze waarop de gegevens zijn en worden opgeslagen, waaronder begrepen de mate waarin voorzien is in waarborgen terzake de veiligheid van de gegevens, alsmede het verstrekkingenregime dat zal gelden ten aanzien van de gegevens;
- II. Primair: de Nieuwe Paspoortwet met onmiddellijke ingang buiten werking te stellen, althans partieel buiten werking te stellen voor wat betreft artikelen 3 lid 8, 4a, 4b en 65 van de Nieuwe Paspoortwet alsmede artikelen 28a lid 1 en 3 van de gewijzigde Paspoortuitvoeringsregeling Nederland en artikel 42a lid 1 en 3 van de gewijzigde Paspoortuitvoeringsregeling Buitenland 2001, althans (al dan niet

⁸¹ HvJEG 1 december 1965, C-16/65 (*Schwarze*).

⁸² HvJEG 15 juli 1964, C-6/64, (*Costa/ENEL*).

partieel) jegens de belanghebbenden buiten werking te stellen, althans de inwerkingtreding daarvan alsmede van de daarop gebaseerde Algemene Maatregelen van (Rijks)Bestuur (al dan niet partieel) met onmiddellijke ingang voor onbepaalde tijd op te schorten, althans de op de Nieuwe Paspoortwet gebaseerde Algemene Maatregelen van Bestuur – te weten de Paspoortuitvoeringsregelingen – buiten werking te stellen;

Subsidiair: artikel 65 van de Nieuwe Paspoortwet met onmiddellijke ingang buiten werking te stellen tot het moment dat passende technische en organisatorische maatregelen zijn genomen ter beveiliging van de gegevens die op grond van artikel 65 worden opgeslagen;

Meer-subsidiair: een dusdanige voorziening te treffen als door de Rechtbank in goede justitie te bepalen

III. De Staat in de kosten van deze procedure te veroordelen.

De kosten dezes van mij deurwaarder bedragen

Procesadvocaat

Deze zaak wordt behandeld door
Mr Chr.A. Alberdingk Thijm en Mr V.A. Zwaan
SOLV Advocaten
Postbus 75538, 1070 AM Amsterdam
T: 020-5300160, F: 020-5300170