

**PLEITAANTEKENINGEN**  
**BIJ DE BEHANDELING VAN HET BEROEP VAN**  
**Louise van Luijk (AWB 10/3576)**  
**RECHTBANK 'S-GRAVENHAGE**  
**15 februari 2011**



*Ad Astra Advocaten*

Mr. H.M.L. Brands  
Mr. J. Hemelaar  
Mr. J.M. Stevers

Korte Mare 14  
Postbus 304  
2300 AH Leiden

Tel.: 071 – 528 00 25  
Fax: 071 – 528 45 00

Ter toelichting op het beroepschrift zij het volgende opgemerkt:

1. Mijn cliënte heeft een paspoort aangevraagd vorig jaar, omdat zij zich moest kunnen legitimeren. Haar aanvraag werd niet in behandeling genomen, omdat zij haar vingerafdrukken weigerde te geven.
2. De Burgemeester van Den Haag beweerde, dat hij niets kon met het recht op privacy, dat is neergelegd in artikel 8 EVRM, in de Grondwet, in het Europees Handvest van Grondrechten, het IVBPR en nog een aantal andere belangrijke verdragen. Hij moest zich volgens eigen zeggen aan de nationale wet houden en daarmee basta. Mijn cliënte kreeg geen paspoort en daarmee was voor de Burgemeester de kous af.
3. Intussen is wel duidelijk, dat het standpunt van de Burgemeester niet houdbaar is. Er kan wel iets in een of andere wet staan, maar dat is geen reden om dat dan maar klakkeloos uit te voeren. Als er inbreuken worden gemaakt op mensenrechten, dan is er alle reden om te kijken of dat wel toelaatbaar is.
4. En in dit geval is daar temeer reden toe, omdat het wetsvoorstel dat tot de paspoortwet heeft geleid eigenlijk ertussendoor is geglipt, zoals ook wel uit de Handelingen van de Tweede Kamer blijkt. Het wetsvoorstel is aangenomen zonder stemming en in afwezigheid van een aantal partijen die op de agendering niet gerekend hadden en daardoor ook niet in de gelegenheid waren aantekening te vragen<sup>1</sup>. Op dit moment tekent zich een Kamermeerderheid af, die eigenlijk de opzet van de wet weer wil aanpassen, weg van het oorspronkelijk ontwerp dat teveel een doorgeschoten “Big Brother”-gehalte heeft, terwijl er ook vanuit Europa vragen worden gesteld over de toelaatbaarheid van wat er in de paspoortwet is geregeld.
5. Dat is terecht. De mensenrechten zijn inderdaad een serieus te nemen verworvenheid. Daarop mag niet zomaar een inbreuk worden gemaakt.
6. Volgens vaste rechtspraak van het Europees Hof voor de rechten van de mens moeten belemmeringen op een grondrecht voorzien worden bij wet. Maar niet iedere wet kan de grondrechten opzij zetten. Beperkingen zijn alleen toelaatbaar als zij noodzakelijk moeten worden geacht in een democratische samenleving en een rechtmatig doel na te streven. Dat kan alleen het geval zijn als de maatregel beantwoordt aan een "dwingende maatschappelijke behoefte", voorts evenredig is aan het nagestreefde rechtmatig doel én mits de door de nationale autoriteiten aangevoerde rechtvaardig



digingsgronden "relevant en toereikend zijn" <sup>ii</sup>. De nationale autoriteiten beschikken over een beoordelingsruimte "waarvan de omvang niet alleen afhangt van de legitieme doelstelling, maar ook van de aard van de inmenging" <sup>iii</sup>. Deze beoordelingsruimte wordt kleiner indien het recht dat op het spel staat, cruciaal is wil de betrokkene effectief zijn meest persoonlijke of fundamentele rechten kunnen genieten<sup>iv</sup>.

7. Ik wil bij mijn toelichting op het beroepschrift deze verschillende punten langslopen. Dus:

- Voorzien bij wet
- Noodzakelijk wegens een dwingende behoefte maatschappij
- Met inachtneming van:
  - Proportionaliteitsbeginsel
  - Flankerende maatregelen en waarborgen waarin voorzien wordt
  - Subsidiariteitsbeginsel

Ik noemde als onderdeel van de proportionaliteit de flankerende maatregelen. Deels zien die doorgaans op compensatie of inperking van de inbreuk, waardoor het niet ál te disproportioneel hoeft te zijn. Maar bij de beoordeling in deze zaak komt tevens om de hoek kijken, dat de verdragen waaraan Nederland gebonden is ook nog specifieke voorwaarden voor inachtneming van waarborgen. Op het gebied van privacybescherming gaat het dan vooral om informatieplicht, een individuele belangenafweging en de mogelijkheid bezwaar te maken. Mijn conclusie zal luiden dat er in géén enkel van deze opzichten aan de voorwaarden is voldaan bij het besluit van de Burgemeester om aan Louise een paspoort te weigeren.

#### VOORZIENBAAR BIJ WET

8. Beperkingen op grondrechten moeten voorzienbaar bij wet zijn. Artikel 10 van de Grondwet scherpt dat nog aan door te vereisen dat in een geval als dit het moet gaan om een wet in formele zin. Nu is natuurlijk duidelijk dat de paspoortwet inderdaad een wet is, maar wat daarbij geregeld is, is helemaal niet "*foreseeable*". Heel veel is namelijk nog ongeregeld. Op dit moment weten we niet eens of er een landelijke centrale opslag komt, of dat er gewerkt gaat worden met een hele serie lokale databases. Hoe die databases gebruikt gaan worden, dat is iets wat veel burgers helemaal niet weten en waarop ze ook helemaal niet worden geïnformeerd. Wat de risico's zijn dat iemand in de problemen komt omdat de techniek de controlerend ambtenaar in de steek laat, en die ambtenaar vervolgens geen idee heeft wat hij moet met een mismatch, daar wordt de burger volledig over in het ongewisse gelaten. Dat de overheid het zich zelf wél is gaan realiseren blijkt uit het feit dat het baliepersoneel in de gemeentehuizen verboden wordt om zelf de check uit te voeren tenzij er duidelijk iets aan de hand lijkt<sup>v</sup>. Intussen wordt de burger een soort schijnveiligheid voorgespiegeld. Er wordt zoiets gezegd als "*Het moet van Europa en het is veiliger*", terwijl daar helemaal niets van waar is. Dat burgers kunnen weten hoe en wanneer zij inbreuken op hun rechten kunnen verwachten is echter een voorwaarde om te kunnen spreken van "voorzien bij wet". Het gaat immers om de rechtszekerheid. Bij een belangrijk onderwerp als de opslag van biometrisch materiaal, en dan nog nota bene het biometrisch materiaal waarmee de gangen van iemand kunnen worden nagegaan, en waarmee iemand kan worden geïdentificeerd, ligt de lat hoog. Ik wijs op onder andere de uitspraak van het EHRM in *Gilian & Quinton vs VK*<sup>vi</sup>. Als we kijken naar de maatsta-



ven die het EHRM op dit punt aanlegt, dan blijkt zonneklaar, dat de paspoortwet geen genade kan vinden.

9. Daar komt bij, dat voor een wettelijke beperking van het voornoemde grondrecht ook materiële eisen gelden. Het voorschrift zal voldoende nauwkeurig moeten zijn en adequate en effectieve waarborgen moeten bevatten tegen ongeoorloofde inbreuken. Die waarborgen kom ik niet tegen in de paspoortwet. Wie erop toeziet dat er niet gezocht wordt buiten de wijzen die de Staatssecretaris wil toestaan, en hóé dat wordt gecontroleerd, is niet geregeld. De wet zakt ook op dit punt van rechtsbescherming door het ijs.

NOODZAKELIJK: *PRESSING SOCIAL NEED*

10. Dan het belangrijkste onderdeel: de noodzakelijkheid van de inbreuk in een democratische samenleving.
11. Het College voor de Bescherming van de Persoonsgegevens zei het al in 2007: er is helemaal geen *pressing need* om de vingerafdrukken op te slaan.

In welke reële behoefte wordt voorzien nu het aanvragen en verkrijgen van een reisdocument toch altijd enige dagen de tijd zal vergen vanwege het productieproces voordat deze aan betrokkene wordt overhandigd? Is de toepassing van biometrie in het reisdocument zelf al niet een stap voorwaarts in het bestrijden van identiteitsfraude? Het CBP mist een belangenafweging van de gevolgen van dit wetsvoorstel voor de persoonlijke levenssfeer van de burger in vergelijking met de huidige situatie.<sup>vii</sup>

12. In het beroepschrift ben ik redelijk uitvoerig ingegaan op de drie gunstige effecten die de Minister zag voor centrale opslag. Allereerst het plezier dat men de verdwaalde Nederlandse toerist op Curaçao doet, die zijn paspoort daar verliest, en bij opslag ook 's middags een aanvraag om een nieuw paspoort kan doen, en niet tot de volgende ochtend hoeft te wachten. Dat is natuurlijk, afgezet tegen de hele bevolking geen "*pressing social need*". Het moet gaan om het functioneren van een democratische samenleving, die anders spaak loopt. Niet om een individueel relatief ongemak van een enkeling. Dat rechtvaardigt geen inbreuk op de privacy van 16 miljoen anderen.
13. *Look alike* fraude is een ander argument. Ook daarvoor is geen *pressing social need* aangetoond. Het komt maar in zeer geringe mate voor, en de Staatssecretaris heeft er zelfs geen cijfers over. Als je niet eens kunt vertellen hoe vaak iets voor komt, dan kan het niet iets zijn wat urgent is. Bovendien kan je *look alike* fraude misschien wel bestrijden met de opname van de vingerafdruk in het paspoort, maar niet met het opslaan van die vingerafdrukken in een of meerdere databases.
14. Het derde argument dat de Staatssecretaris heeft aangevoerd, was dat het handig was zo'n database te hebben met het oog op de opsporing. Maar dat mocht natuurlijk alleen als er aan bepaalde voorwaarden werd voldaan. In het beroepschrift heb ik al aangegeven, dat *indien* aan die voorwaarden serieus de hand zou worden gehouden, de politie allang genoeg instrumenten heeft om



langs een andere weg haar doel te bereiken, en dat deze maatregel dan niks toevoegt. Ook in het derde doel ligt dus geen *pressing social need*.

15. Ik merk nog op, dat ook niet *iedere* reden kan worden aangevoerd om te betogen dat dit een rechtvaardiging zou vormen om een inbreuk op de grondrechten te maken.
16. In artikel 8 EVRM wordt een beperking op het te eerbiedigen recht onder voorwaarden slechts toegelaten als het gaat om een specifieke gevallen. Het Verdrag van Straatsburg van 1981, het Dataprotectieverdrag, beperkt de mogelijkheden nog verder. Het voorkomen van wanordelijkheden, en de gezondheid of goede zeden, die onder artikel 8 lid 2 EVRM nog eventueel mogelijk waren, worden door het Dataprotectieverdrag niet genoemd. Die vallen dus af.

Over blijven dan:

- nationale veiligheid,
- de openbare veiligheid,
- het economisch welzijn van het land,
- het voorkomen van strafbare feiten,
- de bescherming van de rechten en vrijheden van anderen.

Het doel “gemak” of “efficiency” bij de uitgifte van paspoorten valt daar niet onder. Ook het doel vaststellen van de identiteit van verdachten valt daar niet onder. Ook niet onder de vierde categorie, want bij verdachten is het strafbare feit al gepleegd, en het gaat bij het EVRM om voorkoming daarvan. Het voorkomen van het gebruiken van paspoorten door look-alikes valt er wél onder, maar dat wordt al bestreden met de opname van de vingerafdrukken in het paspoort zelf, en daar heb je opslag niet voor nodig. Kortom, de aanvullende beperkingen in doelen die genoemd wordt in artikel 8 lid 2 EVRM en 9 Europees Dataverdrag staan aan de opslag in de weg.

17. Noodzakelijk in een democratische maatschappij is de opslag dus niet. Formeel kan zo’n noodzaak niet gevonden worden, noch in de realiteit van alledag.
18. Dat had natuurlijk ook heel eenvoudig bewezen kunnen worden door te wijzen op de landen om ons heen. Nergens is men zo ver gegaan als de Nederlandse wetgever. Nergens loopt het vervolgens met de democratische samenleving in het honderd. In Nederland tot voor kort ook niet overigens. Voor een aantal voorbeelden verwijs ik naar de dagvaarding van Privacy First, waarin onder andere gewezen wordt op Duitsland, waar men veel scherper is op de privacy. Daar is de opslag duidelijk verboden. Ik kan ook wijzen op landen zoals Zweden, of dichterbij Luxemburg. Of op België, dat kopschuw lijkt te zijn geworden na het laatste debacle met hun paspoort. Maar het mooiste voorbeeld is toch wel Engeland. Daar is onlangs een wet aangenomen waarin is bepaald dat de databases moeten worden vernietigd. Engeland heeft de risico’s begrepen, en ook de juiste lessen geleerd uit het Marper arrest, dat ik straks nog zal bespreken. Engeland heeft aangetoond dat het beter is ten halve te keren, dan ten hele te dwalen. En gelet op de stemming die er onder de Nederlandse parlementariërs heerst, zowel die van de Tweede kamer als die in het Europees Parlement, zou het heel goed kunnen, dat Nederland dat voorbeeld gaat volgen.



19. Intussen zit mijn cliënte nog wel zonder paspoort, op grond van een weigering waaraan geen *pressing social need* ten grondslag ligt. Daar moet dan wel wat aan gedaan worden, want bij mijn cliënte bestaat wel degelijk een dwingend gevoelde behoefte om zich te kunnen legitimeren. Ik wijs er maar op, dat er binnenkort weer verkiezingen zijn, en dat je tegenwoordig alleen kunt stemmen als je je kunt legitimeren. Anders wordt je weggestuurd. Ik vraag uw Rechtbank dan ook om -- wanneer dat mogelijk is-- tijdig uitspraak te doen in deze zaak.

#### PROPORTIONALITEIT

20. De maatregel van opslag is ook disproportioneel.
21. Ten eerste worden er vier vingers afgenomen en opgeslagen, terwijl er maar twee in het paspoort terecht komen. Tegen dat laatste heeft mijn cliënte niet geprotesteerd, omdat dat bij EU verordening is voorgeschreven, en zij zich wilde concentreren op de rest van het circus dat de wetgever om die verplichting heen heeft opgebouwd. Maar waarom vier vingers?
22. Het antwoord dat verweerder geeft, is dat de techniek niet voldoende goed is om op twee vingers af te gaan. Maar dan is niet begrijpelijk waarom er ‘maar’ twee vingers nodig zijn van de EU. Als de EU dat voldoende vindt, dan moet de Nederlandse regering maar eens uitleggen waarom dat niet zo is. En nota bene: hoewel de vingerafdrukken van iemand slijten door de jaren en vager worden, kan voor 70-plussers toch volstaan worden met één vingerafdruk. Dan is de verplichting tot afgifte van vier vingerafdrukken helemaal niet meer verklaarbaar.
23. Het is overigens zo, dat het probleem van de vier vingerafdrukken door de regering zelf is gecreëerd. Dat probleem hangt namelijk samen met de grootschaligheid, en de verwarrende dubbele doelen die de regering in de paspoortwet heeft geperst. In een overzicht van de problemen van het grootschalig gebruik van biometrische gegevens geven Kindt en Dumortier aan, dat biometrische gegevens nooit 100 % accuraat zijn. Vingers worden bijvoorbeeld de ene keer met meer kracht op een afname-apparaat geplaatst dan een andere keer, waardoor de afdruk anders wordt. Of de richting waarin gedrukt wordt vervormt de lijnen. En dat hoeft helemaal niet bewust te gebeuren: het kan gewoon omdat het apparaatje onder een andere hoek ten opzicht van de persoon aan de balie ligt. Je moet onderscheiden tussen een gewenst FRR (*false rejection rate*) en een FAR (*false acceptances rate*), en daar moet het systeem op ingesteld worden. Bij een kerncentrale, geven de onderzoekers als voorbeeld, heb je liever af en toe dat iemand teveel de toegang wordt geweigerd, dan dat er één keer een verkeerde figuur doorgelaten wordt.<sup>viii</sup> Ook de rapporten van de WRR waarnaar is verwezen komen met die conclusie: biometrische gegevens verwerken voor identificatiedoeleinden is niet goed te matchen met opslag ervan voor falsificatie. In het laatste geval volstaan gewoon de twee vingerafdrukken in de chip van het paspoort. In het eerste geval komen er heel andere eisen kijken bij de processen en wordt de betrouwbaarheid van het systeem onder druk gezet<sup>ix</sup>. Dit paard van Troje nu heeft de wetgever binnen gehaald door de Paspoortverordening aan te grijpen om een opsporingsdatabase op te zetten.



24. Als we kijken naar wat er in het WRR rapport van Max Snijder staat over de onverenigbaarheid van de doeleinden identificatie en verificatie, dan moeten we zelfs constateren, dat de uitbreiding van de verplichtingen die bij de paspoortwet zijn gesteld niet slechts een grond ontberen in de Verordening, maar zelfs strijd opleveren met de EU-verordening. Want als het inderdaad zo is, dat de nauwkeurigheid bij identificatie een andere houding tegenover het gebruik en beoordelen van de vingerafdrukken betekent, dan belemmert de wens van de wetgever om de vingerafdrukken ook te gebruiken voor identificatie het doel dat de EU-verordening stelt, namelijk verificatie.
25. Op gelijke wijze komt het nevendoeel dat de wetgever zich stelde, namelijk het plaatsafhankelijk paspoorten kunnen aanvragen in strijd met de Verordening. Dat maakt het hele systeem onbetrouwbaarder, want mensen gaan shoppen, en fraudeurs kunnen zo daar naar toe daar uit waar corruptie bestaat of de controle het minst is.
26. Ook de Europese Toezichthouder heeft keer op keer aangegeven dat het vraagtekens stelt bij de doeltreffendheid van het gebruik van biometrische gegevens op grote schaal:

In dit verband zou de EDPS erop willen wijzen dat hij bij tal van gelegenheden, in uiteenlopende fora en in verschillende adviezen de risico's heeft benadrukt die verbonden kunnen zijn aan de grote gevolgen van het gebruik van biometrische gegevens op de rechten van de burgers. Bij die gelegenheden heeft hij tevens voorgesteld om strenge waarborgen in te voeren voor het gebruik van biometrische gegevens in bepaalde instrumenten en systemen. Bovendien heeft de EDPS de aandacht gevestigd op een probleem met betrekking tot onnauwkeurigheden die inherent zijn aan het verzamelen en vergelijken van biometrische gegevens.<sup>x</sup>
27. Het argument van disproportionaliteit is al eens in een zaak aan de orde geweest voor het EHRM. Ik doel op de zaak *Marper vs VK*. Daarin kwam het EHRM tot de conclusie, dat het categoriaal opslaan van vingerafdrukken een schending is van artikel 8 EVRM.
28. Allereerst stelde het EHRM vast, dat het opslaan daarvan een inbreuk vormde op artikel 8 EVRM. Dat wordt door verweerder ook niet ontkend. In de woorden van het EHRM:

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. (...) the retention of fingerprints constitutes an interference with the right to respect for private life.<sup>xi</sup>
29. In de *Marper case* oordeelde het EHRM vervolgens luid en duidelijk, dat hoewel er in dat geval een legitiem doel aanwezig was geweest voor de afname van vingerafdrukken, de ongelimiteerde opslag daarvan in strijd kwam met de rechten onder het EVRM, meer in het bijzonder artikel 8.
30. De Nederlandse staat, en naar ik aanneem in navolging daarvan verweerder, heeft zich op het standpunt gesteld, dat de *Marper case* geen zeggingskracht heeft voor een zaak als de onderhavige, omdat bij de *Marper case* een rol speelde, dat de burgers zich gestigmatiseerd konden voelen,



omdat zij wat betreft hun vingerafdrukken op één lijn werden geplaatst met veroordeelden, in tegenstelling tot vrijwilligers van wie vingerafdrukken waren afgenomen.

31. Dat laatste wordt inderdaad wel aangehaald in de discussie, maar dat is vooral om het verweer van het VK te weerleggen, dat vingerafdrukken die worden afgenomen in strafrechtelijke onderzoeken in Groot-Britannië niet impliceren, dat de desbetreffende persoon ook echt iets heeft gedaan: er is slechts sprake van de status van verdachte, aldus de vertegenwoordiger van het VK, en in de database zitten dus ook vingerafdrukken van onschuldige personen en niet alleen vingerafdrukken van schuldig bevonden personen. In dat opzicht lijkt het argument van Britse Staat verrassend op dat van de Nederlandse Staat. Daar kwamen de Britten niet mee weg, en de Nederlandse regering gaat hen in dat opzicht achterna.
32. Daar komt bij, dat het argument bij het grote publiek helemaal niet aanslaat. Ook hier verbindt de publieke opinie ‘vingerafdrukken’ meteen met ‘criminaliteit’ en met ‘politie’. Het maakt niet uit of er politiek correct door de Staatssecretaris wordt gezegd, dat het een database is met vingerafdrukken van zowel criminelen, als mensen die nergens van verdacht worden. De associatie blijft. En als klap op de vuurpijl heeft de Staatssecretaris zelf de bevestiging gegeven dat die associatie niet zonder grond is: de Staatssecretaris heeft zelf gepropageerd, dat de vingerafdrukken toeganke-lijk moeten zijn voor het OM om van verdachten de identiteit te kunnen vaststellen. Hoezo niet stigmatiserend?!
33. Verweerder zit dus op het verkeerde spoor. Maar daar komt nog bij, dat de stellingname van verweerder een afleidingsmanoeuvre is. Het gaat uiteindelijk bij Marper vs VK niet om de stigmatisering. Doorslaggevend is, dat het Hof na een kort excurs over het stigmatiserend effect terugkeert bij wat het daarvoor al aanhaalde. In r.o. 119 wordt gesproken van “*the blanket and indiscriminate nature of the power of retention in England and Wales*”. De opslag trof iedereen in Groot-Brittannië wiens vingerafdrukken binnen de grenzen van de wet konden worden verlangd, en duurde zonder einde. **Dat** is met name hetgeen het Hof onacceptabel acht, en dát is ook wat bij de conclusie in r.o. 125 terug komt:

In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society.<sup>xii</sup>

34. Dat dit de kernoverweging is, blijkt ook uit de latere jurisprudentie van het Hof. Ik wijs op de zaak W. tegen Nederland. Daarin verwees het EHRM naar de *Marper case* en gaf het Hof zelf aan waar het in deze kwestie om draait. Het Hof overwoog:  
The Court has further had regard to its findings in *S. and Marper v. the United Kingdom* (cited above, § 119), which concerned the retention of DNA records of two applicants who had not been convicted of a criminal offence. In that case the Court was struck by the blanket and in-



discriminate nature of the power of retention of DNA records in England and Wales whereby the material could be retained without time-limits and irrespective of the nature or gravity of the offence or the personal circumstances of the individual involved. The Court notes however that, contrary to the *S. and Marper* case, the present case deals with the issue of storing and retaining DNA records of persons who have been convicted of a criminal offence. Furthermore the Court considers that, pursuant to the provisions of the DNA Testing (Convicted Persons) Act, DNA material can only be taken from persons convicted of an offence of a certain gravity, and that the DNA records can only be retained for a prescribed period of time that is dependent on the length of the statutory maximum sentence that can be imposed for the offence that has been committed. The Court is therefore satisfied that the provisions of the Act contain appropriate safeguards against blanket and indiscriminate retention of DNA records.”<sup>xiii</sup>

We hoeven dus niet meer te gissen naar wat in de *Marper* case de doorslag heeft gegeven. Het Hof heeft dat zelf in de zaak van 20 januari 2009 duidelijk gemaakt. De stigmatisering wordt in dit arrest helemaal niet genoemd. Het arrest geeft de bevestiging, dat het standpunt van verweerder, als zou de *Marper* case niet toepasselijk zou zijn en genegeerd kan worden bij toetsing van de paspoortwet, onjuist is. Het EHRM vindt duidelijk, dat ongelimiteerde opslag uit den boze is, en evenzo de categoriale, ongedifferentieerde opslag van biometrisch materiaal van onschuldige personen.

35. Hier lopen de lijnen van het EHRM en het HvJEU parallel. Het EHRM vindt, dat mensen bezwaar moeten kunnen maken tegen de opslag, en dat naar de individuele omstandigheden moet worden gekeken. De paspoortwet biedt die ruimte niet. Het HvJEU wijst op Ri 95/46/EG, dat dezelfde voorwaarde stelt. Beide, zowel EHRM als HvJEU vallen daarnaast over het ongelimiteerd opgeslagen blijven. Ook dat kan niet, en ook daarin voorziet de paspoortwet niet. Kortom, op twee essentiële aspecten van waarborgen voor opslag wordt niet voldaan.
36. Overigens meent eiseres, dat ook als iederéén zijn vingerafdrukken afgeeft, dit nog steeds niet het stigmatiserend effect wegneemt. Alleen worden dan alle burgers als potentiële criminele beschouwd. Ik wijs er nog maar een keer op, dat de opslag van die vingerafdrukken ook uitdrukkelijk dient voor strafvorderlijke doelen: de Officier van Justitie heeft daar in een aantal gevallen toegang toe, en de AIVD en MIVD kunnen er naar hartelust in grasduinen, zonder dat iemand het in de gaten heeft.
37. Verweerder kan daarover opmerken: “Ja maar dat kan ook al met de huidige opgeslagen gegevens”. Ten eerste is het niet waar, omdat de paspoortwet een ander verstrekkingenregime kent en anders ingerichte databases<sup>xiv</sup>. Maar zelfs afgezien daarvan is het al bestaan van opslag van sommige gegevens geen reden om die opslag nog eens extra uit te breiden met een biometrisch kenmerk. Het maakt wel verschil uit of het gegevens zijn die heel dicht op de huid zitten of wat algemener blijven. En vooral, het maakt flink uit of die gegevens voor iedereen zichtbaar zijn of alleen voor opsporingsdiensten. Mijn gezicht is herkenbaar voor iedereen die hier in de rechtszaal naar mij kijkt. Maar mijn vingerafdrukken zijn dat niet. Bovendien zijn er grotere gevolgen verbonden aan het matchen van vingerafdrukken, dan het tonen van een foto. Mijn vingerafdrukken laat ik in





principe op allerlei plaatsen achter. Mijn pasfoto niet. Dat betekent, dat het opslaan van vingerafdrukken veel ingrijpender is dan het opslaan van een pasfoto. Die laatste kan men alleen vergelijken als ik er zelf bij ben<sup>xv</sup>. Maar vingerafdrukken kan men achter mijn rug om vergelijken met wat zich in de databank bevindt. Ten slotte is het zo, dat aan een match met vingerafdrukken een grotere waarde wordt gehecht: als die match wordt gemaakt, wordt daarmee een zekere identificering aangenomen. Met andere gegevens wordt prudenter en minder kritiekloos omgegaan. Dat maakt de opgeslagen data van vingerafdrukken tegelijk ook zo aantrekkelijk voor misbruik door kwaadwillenden.

38. Zo kom ik bij de risico's. Als mijn vingerafdrukken worden opgeslagen, dan worden ze bij onvoldoende bescherming toegankelijk voor derden. Dan kunnen die vingerafdrukken ook worden nagemaakt en ergens geplaatst. Of iemand kan mijn sporen gaan verzamelen (of de uwe), die tot nu toe onherkenbaar waren, althans onherleidbaar. Dat kan bijzonder nare gevolgen hebben. Hoe dan ook vormt het een ernstige inbreuk op het privéleven. Dat zijn allemaal redenen waarom mijn cliënte niet wenst mee te werken aan afgifte van haar vingerafdrukken zolang die worden opgeslagen in een database.
39. Naar mijn mening behoeft het, gelet op deze risico's, geen nader betoog, dat het verlangen dat 16 miljoen Nederlanders meewerken aan opslag van hun vingerafdrukken in raadpleegbare bestanden alle grenzen van de proportionaliteit overschrijdt, als dat alleen maar is voor de doelen die hiervoor zijn aangegeven.

#### VOORWAARDEN EN WAARBORGEN

40. Dan kom ik bij de waarborgen en andere voorwaarden die gesteld moeten worden in het kader van de proportionaliteit of in het kader van een specifieke regeling. Aan bedroevend weinig van die waarborgen wordt voldaan.
41. De beveiliging van de databases waarin de overheid de vingerafdrukken wil bewaren is niet gewijzigd ten opzicht van de beveiliging die er vóór de invoering van het biometrisch paspoort was. Terwijl de omvang van de databases veel groter is, de gegevens gevoeliger en de aantrekkelijkheid om de database voor eigen gebruik te hacken gemultipliceerd is. In het Dataprotectieverdrag is expliciet opgenomen, dat de bescherming moet voldoen aan de *the state of the art*. Er moeten speciale maatregelen worden getroffen. Maar als je kijkt wat er nu gebeurt, dan zie je dat de databases waarin de vingerafdrukken worden opgeslagen niks beter beschermd zijn dan toen er alleen nog maar een handtekening van de aanvrager van het paspoort in zat.
42. Artikel 9 WPB bepaalt voorts, dat persoonsgegevens niet verder mogen worden verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen. Het is duidelijk dat de enige reden die een burger kan verleiden om zijn vingerafdrukken af te geven bij het aanvragen van een paspoort is, de verkrijging van dat paspoort. Burgers, en in ieder geval mijn cliënte, komen niet naar het stadhuis om hun vingerafdrukken te geven in de strijd tegen terrorisme of het



mogelijk maken van herkenning van hen door de Officier van Justitie, als die ooit eens met een foto en een set vingerafdrukken benieuwd mocht zijn naar hun naam. Nu de gegevens wél ter beschikking worden gesteld voor dit doel, gaat de opslag en verwerking duidelijk verder dan is toegelaten op grond van de wet.

43. Daarnaast geldt, dat Richtlijn 95/46/EG, de richtlijn over gegevensverwerking en privacy, een rol van betekenis speelt. De artikelen 6, 7 en 8 van deze Richtlijn hebben rechtstreekse werking<sup>xvi</sup> Ik heb in het beroepschrift er al op gewezen, dat er een mogelijkheid moet zijn om individuele belangen te laten wegen in een procedure waarin iemand bezwaren kan uiten. In zo'n procedure is niet voorzien in de gewijzigde paspoortwet. De burgemeester heeft miskend, dat de richtlijn rechtstreekse werking heeft, en mijn cliënte ten onrechte het recht onthouden is haar inhoudelijk bezwaren naar voor te laten brengen en te laten wegen. Dit slaat zó'n fors gebrek in de besluitvorming, dat gesproken kan worden van een onvoldragen besluit. In zo'n geval kan er eigenlijk geen andere beslissing meer volgen in beroep dan gegrondverklaring van het beroep van mijn cliënte en de opdracht aan de Burgemeester om zijn huiswerk over te doen.
44. Het recht om zich te verzetten tegen de eis vingerafdrukken af te staan is niet de enige waarborg die kan worden afgeleid uit de Richtlijn, en die genegeerd is.
45. In een van de adviezen van de Europese Toezichthouder geeft deze aan, dat het beschermingsniveau niet lager mag liggen dan de Richtlijn 95/46/EG<sup>xvii</sup>. In de punten 11 en 12 van dat advies geeft de Toezichthouder aan, dat als de uitwerking van het gebruik van de gegevens nog niet rond is, de eis om die gegevens af te geven nog niet mag worden gesteld. Dan is immers de rechtszekerheid voor de burger niet te garanderen<sup>xviii</sup>.
46. Wat voorts niet is geregeld --en waardoor het opslaan van vingerafdrukken in strijd komt met Richtlijn 95/46/E--, is de informatieverschaffing aan degene van wie de vingerafdrukken zijn, als de opgeslagen informatie wordt geraadpleegd. De Europese Toezichthouder is daar duidelijk over. De informatieverstrekking mag in gevallen als deze niet afhangen van het al dan niet aanwezig zijn van een verzoek van de eigenaar van de vingerafdrukken<sup>xix</sup>.
47. Nog weer een ander aspect betreft de duur van het bewaren van de gegevens. Volgens verweerder zou *look alike* fraude kunnen worden bestreden met het opslaan van de vingerafdrukken. Hiervoor heb ik al aangegeven, dat dit een onzinnig argument is. *Look alike*s halen niet zelf hun paspoort op, maar stelen of kopen dat. Ik heb als advocaat inmiddels een aantal *look-alike* zaken gezien -- dat hangt ook samen met de rechtsgebieden waarop ik als advocaat actief ben--, en ik ben het nog nooit tegengekomen, dat een *look-alike* zelf naar het loket bij de gemeente ging om een paspoort op naam van een ander te halen. Dan zou die *look-alike* overigens ook de exacte data (voornaam, geboortedatum, etc) moeten kennen, en weten wanneer het paspoort ongeveer dreigt te verlopen. Bovendien wordt er aan de balie ook altijd naar het oude paspoort gevraagd, dus het kan dan ook nog alleen ten aanzien van iemand die daarvoor nog geen paspoort bezat. Komt iemand zónder paspoort, dan wordt verlangd, dat de persoon in kwestie eerst aangifte gaat doen van verlies of



diefstal, en daarbij wordt reeds op een andere manier en door een andere instantie de identiteit gecheckt. Maar goed, gesteld, dat verweerder een situatie kan bedenken, waarin *look-alike* fraude bestreden kan worden bij de uitgifte van een eerste paspoort, dan heeft het opslaan van de vingerafdruk alleen zin tot het moment van de daadwerkelijke uitgifte. Dat zou betekenen, dat de gegevens daarna alsnog vernietigd moeten worden. In de zaak Rijkeboer tegen B&W Rotterdam overwoog het HvJEU immers in r.o. 33:

Artikel 6 van de richtlijn (*Ri 95/46/RG, JH*) ziet op de kwaliteit van de gegevens. Ingevolge lid 1, sub e, daarvan moeten de lidstaten bepalen dat persoonsgegevens niet langer worden bewaard dan voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, noodzakelijk is. De gegevens moeten dus worden uitgewist wanneer deze doeleinden zijn bereikt.<sup>xx</sup>

48. Ook het EHRM hecht sterk aan de duur van de opslag, en het vernietigen van de data wanneer zij niet meer strikt noodzakelijk zijn. Dat bleek al uit het zo-even besproken Marper arrest<sup>xxi</sup>.
49. In de huidige regeling wordt niet voorzien in onmiddellijke vernietiging na het bereiken van het doel. Voor bestrijding van *look-alike* fraude ná uitgifte van het paspoort hebben de gegevens geen serieus doel meer, want dan volstaat de vingerafdruk in het paspoort zelf.
50. Daarnaast wordt op alle niveaus, van de Europese toezichthouder<sup>xxii</sup> tot ons Nederlandse CBP, van wetenschappers tot journalisten, van individuele burgers met gezond verstand tot parlementariërs gewezen op het gevaar van *function creep*. Alle deskundigen, en ook de politici van diverse pluimage onderschrijven dat *function creep* opgesloten ligt in de aanwezigheid van de mogelijkheden die opslag van biometrische data biedt. Opmerkelijk helder is de uitlating van Europarlementariër Hennis Plasschaert, die in het WRR rapport wordt geciteerd:

In feite zijn 16 miljoen Nederlanders hiermee op voorhand verdachte (...). Ik vind het ongelooflijk dat een meerderheid in de Tweede Kamer hiermee akkoord is gegaan. Er wordt wel gezegd dat het geen database is om lekker in rond te shoppen, maar die waarborgen zijn nog niet in de wet vastgelegd. Demissionair staatssecretaris Bijleveld van Binnenlandse Zaken zegt in feite: vertrouw me op mijn blauwe ogen dat we niets verkeerd doen met die gegevens.

Nu wil ik daar in het geval van het CDA nog best vanuit gaan, maar straks zit er misschien een andere partij in de regering die daar heel anders over denkt. (...) Al die sprookjesverhalen dat het van Brussel moest komen mijn neus uit. Het biometrisch paspoort is er gekomen om identiteitsfraude te bestrijden. Als je de vingerafdrukken vervolgens ook centraal gaat opslaan en gaat gebruiken voor het bestrijden van criminaliteit laat je dat doel helemaal los.<sup>xxiii</sup>

51. Ook op dit punt zijn dus geen waarborgen opgenomen. Wellicht dat zulke waarborgen ook niet te geven zijn. Maar dat betekent dan dat de vereiste afgifte van vingerafdrukken voor opslag niet mogelijk is zonder schending van de mensenrechten, in het bijzonder artikel 8 EVRM, zonder schending van de Europeesrechtelijke beginselen, zoals vastgelegd in het Handvest van de Grondrechten van de Europese Unie (artikel 8) en zonder schending van Verdragen die zien op verwer-



king van persoonsgegevens. Kortom, dan is de wet met hogere regelgeving in strijd en moet buiten werking blijven.

52. Nog drie andere voorwaarden waaraan niet is voldaan wil ik kort noemen.
53. Allereerst de passende bescherming van de gegevens, die is voorgeschreven op grond van het Europees Dataprotectieverdrag uit 1981 bij gegevens die iets kunnen zeggen over de medische situatie van een persoon. Artikel 6 legt de lat wat dit betreft nog een streepje hoger dan artikel 7 al doet. In de wetgeving zien we daarvan echter niets terug.
54. Verder zien we niets terug van de verplichting die de Staat heeft om de burger te compenseren voor het verlies van de exclusieve eigendom van informatie omtrent zijn biometrische gegevens, dat artikel 17 Handvest van de Gondrechten van de Europese Unie voorschrijft.
55. Ten slotte, voor wat betreft de waarborgen en voorwaarden, geldt dat de inbreuk ook niet in strijd mag komen met het discriminatieverbod. Maar dat doet deze wet wél. Immers, straks zou de overheid kunnen beschikken over een database met vingerafdrukken van alle ingezetenen, die de Nederlandse nationaliteit hebben, maar niet van andere ingezetenen, waaronder EU-onderdanen van een andere nationaliteit, en derdelanders, asielzoekers en ga zo maar door. Ik wijs er in het laatste geval op, dat de asielzoekers wél hun vingerafdrukken moeten afstaan, maar niet voor opslag die toegankelijk is voor justitie. Nederlanders worden onder de paspoortwet slechter behandeld. Zij moeten hun vingerafdrukken afstaan voor opslag in een of meerdere databases die wél door Justitie mogen worden bekeken. Dat is discriminatie op grond van de nationaliteit.
56. In de zaak *Huber vs Duitsland*<sup>xxiv</sup> bepaalde de Grote Kamer van het Hof van Justitie, dat onder bepaalde voorwaarden wel was toegestaan om een centraal register op te zetten voor buitenlanders, mits allereerst aan het vereiste van noodzakelijkheid was voldaan, en daarnaast nog die buitenlanders daar voordeel van zouden genieten. Maar, voegde het Hof daaraan toe, artikel 12 lid 1 van het EG verdrag staat eraan in de weg, dat een dergelijk systeem wordt gebruikt voor bestrijding van criminaliteit. Dat zou immers ongeoorloofde discriminatie op grond van nationaliteit opleveren. Nu de database waarin de Burgemeester van Den Haag de vingerafdrukken laat opslaan óók dient ter bestrijding van criminaliteit, geldt de redenering van het Hof evenzeer in deze zaak met betrekking tot de paspoortwet. Dat het deze keer de eigen burgers zijn, die gediscrimineerd worden ten opzichte van andere op het grondgebied van de lidstaat verblijvende burgers, maakt niet uit. In dit opzicht doet eiseres overigens niet alleen een beroep op de jurisprudentie van het HvJEU, maar tevens op het EVRM en IVBPR.

#### SUBSIDIARITEIT

57. Wanneer iemand deze aspecten goed tot zich door laat dringen, dan doemt de vraag op: Waarom is het eigenlijk zo ver gekomen? Want het kan toch eigenlijk niet? Wordt er dan niet nagedacht?



De Europese Toezichthouder signaleert een algemene trend om rechtshandavingsinstanties toegang te verlenen tot verschillende grootschalige informatie- en identificatiesystemen, maar ook een nieuwe stap in de tendens om rechtshandavingsinstanties toegang te verlenen tot gegevens van normale, oppassende burgers. Het gaat bovendien om gegevens die zijn verzameld voor doeleinden die niet gerelateerd zijn aan criminaliteitsbestrijding. De Europese Toezichthouder geeft een aantal voorbeelden in Europees verband<sup>xxv</sup>, maar we kennen dezelfde tendens in ons nationale recht.

58. “In zijn adviezen over deze initiatieven heeft de EDPS zich kritisch uitgelaten over het verlenen van toegang aan rechtshandavingsinstanties tot voor andere doeleinden verzamelde gegevens van personen die niet van het plegen van strafbare feiten worden verdacht. De EDPS heeft benadrukt dat dit een degelijke rechtvaardiging behoeft, en dat de noodzakelijkheid en de evenredigheid ervan moeten worden getoetst. In zijn advies over het gebruik van PNR-gegevens heeft hij zelfs gewaarschuwd voor een evolutie naar een volledig gecontroleerde samenleving.”

Dat is niet *mijn* conclusie, maar ik citeer hier letterlijk de tekst van de EDPS zelf<sup>xxvi</sup>.

59. Mijn cliënte is geboren in 1984. Dat was toevallig het jaar waarover George Orwell zijn visionaire boek schreef. Het jaar van Big-brother-is watching-you. In Nederland zijn er mensen die op t-v naar mensen kijken die zich vrijwillig in een Big Brother huis willen laten filmen. Maar het wordt heel anders als het dagelijkse praktijk wordt voor eenieder, onvrijwillig, en dan nog zónder de roem en glorie of het prijzengeld die de bewoners van het Big Brother-huis ten deel vallen. Mijn cliënte wil niet in een “1984” leven. En met haar vele anderen niet. Het is essentieel dat wordt nagegaan of wetgeving op dit gebied de rechtmatigheidstoets op grond van artikel 8 van het Europees Mensenrechtenverdrag kan doorstaan. Wetgeving en daarop gebaseerde besluiten moeten voldoen aan de beginselen van noodzakelijkheid en evenredigheid, *rekening houdend met reeds beschikbare instrumenten*<sup>xxvii</sup>. Dat laatste lijkt ten enenmale te ontbreken als het om de paspoortwet gaat.

60. De Europese Toezichthouder vervolgt en stelt:

Er is thans meer dan ooit behoefte aan een grondige bezinning over hoe de informatie-uitwisseling van de EU en grootschalige informatiesystemen er zouden moeten uitzien. Tijdens die bezinning moet door middel van periodieke evaluaties adequate aandacht worden besteed aan de gevolgen voor de persoonlijke levenssfeer en aan de doeltreffendheid van de wetshandhaving; in eerste instantie wanneer nieuwe instrumenten worden voorgesteld en besproken, maar ook nadat die instrumenten zijn ingevoerd. Er moeten in dit verband ook op maat gesneden garanties en een sterkere focus op het doelbindingsbeginsel komen.<sup>xxviii</sup>

Ook die waarschuwing is hier zonder meer van toepassing. Verwezen zij naar het wetgevingsadvies van het CBP van maart 2007 waarin exact dezelfde waarschuwing werd gegeven en naar de eindconclusies van het WRR rapport “Happy Landings?”

61. Daarnaast stelt de Europese Toezichthouder, dat  
“het evenredigheidsbeginsel respecteren niet alleen inhoudt dat de voorgestelde maatregel doeltreffend is, maar ook dat het met het voorstel beoogde doel niet kan worden bereikt met bestaande instrumenten. Deze instrumenten moeten zorgvuldig worden geëvalueerd



alvorens aanvullende/nieuwe maatregelen worden vastgesteld voor het verwerken van persoonsgegevens.”

Ook dit is een letterlijk citaat, en de Toezichthouder sluit het betoog af met:

“Volgens de EDPS heeft deze alomvattende evaluatie niet plaatsgevonden.”<sup>xxxix</sup>

62. Het CBP merkte op in 2007, dus al vóór de behandeling van de wetgeving in de Kamer op over de Nederlandse situatie:

Nog daargelaten de vraag of een centrale reisdocumentenadministratie hieraan een wezenlijke bijdrage kan leveren, wijst het CBP erop dat dit wetsvoorstel voor deze doeleinden weer één extra is bovenop alle andere maatregelen die al zijn genomen in de afgelopen periode. Het CBP denkt hier bijvoorbeeld aan de verplichting tot het bewaren van verkeersgegevens en uitbreidingen van bevoegdheden in het Wetboek van Strafvordering. Nu de officier van justitie de biometrische gegevens kan ontvangen bij bepaalde misdrijven, krijgt deze administratie in feite ook de functie van een opsporingsregister. Deze consequentie vormt een ernstige inbreuk op de persoonlijke levenssfeer omdat ook de gegevens van niet verdachte burgers zijn opgenomen in het register.<sup>xxx</sup>

63. De conclusie moet luiden, dat ook aan het subsidiariteitsbeginsel niet is voldaan.

64. Ik heb ‘*forseeable by law*’ behandeld, ik heb de *pressing social need* gehad, de proportionaliteit en daaraan gelieerd de voorwaarden en waarborgen, en ik heb het gehad over de subsidiariteit. Ten slotte kom ik nog toe een paar slotopmerkingen.



65. Ik heb in het beroepschrift aangegeven, dat op dit moment de politiek oren heeft voor wat de Rechtbank zou kunnen beslissen omtrent de onrechtmatigheid van de gestelde eis om vingerafdrukken af te staan voor opslag.

66. Ik kwam nadien nog een zeer lezenswaardig artikel tegen van de hand van voormalig Minister Ernst Hirsch Ballin getiteld “De rechtsstaat: wachten op een nieuwe dageraad?” De voormalig Minister van Justitie pleit daarin voor een krachtdadige aanpak door de rechterlijke macht, waar de politiek eigenlijk blij mee zou moeten zijn, omdat de legitimatie van een democratische volksvertegenwoordiging altijd alléén bestaat binnen het kader van een constitutionele democratie in de vorm van een rechtsstaat waarin mensenrechten als waarborgen gelden.

Democratische macht is altijd beperkte macht, “*limited government*”, regeren met eerbiediging van duurzame fundamentele rechten van de burger, vrijheden die niemand mogen worden ontnomen.

Wie fundamentele rechten van individuen wil opofferen aan het belang van de gemeenschap, overschrijdt de Rubicon, aldus Hirsch Ballin.<sup>xxxi</sup>

Nu het bestreden besluit niet in stand kan blijven verzoekt eiseres om het beroep gegrond te verklaren.

Ik dank u voor uw aandacht.



Leiden, 15 februari 2011

Gemachtigde



- 
- <sup>i</sup> V. Böhre, *Happy landings? Het biometrisch paspoort als zwarte doos* (WWR webpublicatie 46), p. 83-84
- <sup>ii</sup> Zie onder andere punt 55 van het arrest van 24 november 1986 in de zaak Gillow tegen het Verenigd Koninkrijk, *A-serie, nr. 109*.
- <sup>iii</sup> Zie punt 59 van het arrest van 26 maart 1987 in de zaak Leander tegen Zweden, *A-serie, nr. 116*. Zie ook punt 83 van het arrest van het HvJ van 20 mei 2003 in de gevoegde zaken C-465/2000, C-138/01 en C-139/01, *Österreichischer Rundfunk et al., Jurisprudentie 2003-I, blz. 4989*.
- <sup>iv</sup> Zie punt 82 van het arrest van 27 mei 2004 in de zaak Connors tegen het Verenigd Koninkrijk, nr. 66746/01.
- <sup>v</sup> Intern nieuwsbericht BiZa 17 september 2009 [http://www.bprbzk.nl/Reisdocumenten/Nieuws/Retourdocumenten\\_in\\_verband\\_met\\_mislukte\\_verificatie\\_vingerafdruk](http://www.bprbzk.nl/Reisdocumenten/Nieuws/Retourdocumenten_in_verband_met_mislukte_verificatie_vingerafdruk) Zie ook M. Snijder, *Biometrisch paspoort in Nederland: crash of zachte landing* (WRR-webpublicatie 51) p. 95,96, 102 en vooral 124-126.
- <sup>vi</sup> Europees Hof voor de Rechten van de Mens 12 januari 2010, nr4158/05 RvdW 201,739, met name r.o. 77:  
For domestic law to meet these requirements it must afford a measure of legal protection against arbitrary interferences by public authorities with the rights safeguarded by the Convention. In matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate with sufficient clarity the scope of any such discretion conferred on the competent authorities and the manner of its exercise (Rotaru v. Romania [GC], no. 28341/95, § 55, ECHR 2000-V; Hasan and Chaush v. Bulgaria [GC], no. 30985/96, § 4, ECHR 2000-XI; Maestri v. Italy [GC], no. 39748/98, § 30, ECHR 2004-I; see also, amongst other examples, Silver and Others v. the United Kingdom, 25 March 1983, §§ 88–90, Series A no. 61; Funke v. France, §§ 56–57, judgment of 25 February 1993, Series A no. 256-A; Al-Nashif v. Bulgaria, no. 50963/99, § 119, 20 June 2002; Ramazanov and Others v. Azerbaijan, no. 44363/02, § 62, 1 February 2007; Glas Nadezhda EOOD and Anatoliy Elenkov v. Bulgaria, no. 14134/02, § 46, ECHR 2007-XI (extracts); Vlasov v. Russia, no. 78146/01, § 125, 12 June 2008; Meltex Ltd and Movsesyan v. Armenia, no. 32283/04, § 81, 17 June 2008). The level of precision required of domestic legislation — which cannot in any case provide for every eventuality — depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed (see, for example, Hashman and Harrup v. the United Kingdom [GC], no. 25594/94, § 31, ECHR 1999-VIII; S. and Marper, cited above, § 96)
- <sup>vii</sup> Wetgevingsadvies van het College voor de Bescherming van Persoonsgegevens, 31 mei 2007, p. 5, [http://www.cbppweb.nl/downloads\\_adv/z2007-00010.pdf](http://www.cbppweb.nl/downloads_adv/z2007-00010.pdf)
- <sup>viii</sup> E. Kindt en J. Dumortier, "Biometrie als herkenning- of identificatiemiddel? Enkele juridische beschouwingen" in *Computerrecht 2008/132*, p. 185-198 (uitgeverij Kluwer BV, ISSN 0771-7784) met name par 1.3.1 - 3.2 <http://highlight.legalintelligence.com/default.aspx?URL=http%3a%2f%2fwww.legalintelligence.com%2fProtectedContent%2fKluwer%2fjournals%2fCOMP%2f2008%2f08013200.htm>
- <sup>ix</sup> V. Böhre, *Happy landings? Het biometrisch paspoort als zwarte doos* (WWR webpublicatie 46) en M. Snijder, *Biometrisch paspoort in Nederland: crash of zachte landing* (WRR-webpublicatie 51), met name het laatste rapport legt stap voor stap uit op een voor leken uitstekend te begrijpen manier waarom identificatie- en verificatie-doelen elkaar bijten en het resultaat van een combinatie daarvan om technische redenen per definitie problemen oplevert.
- <sup>x</sup> *Advies van de Europese Toezichthouder voor gegevensbescherming over de mededeling van de Commissie aan het Europees Parlement en de Raad getiteld — "Overzicht van het informatiebeheer op het gebied van vrijheid, veiligheid en recht" [52010XX1229(03)] punt 45*
- <sup>xi</sup> Marper vs UK EHRM 4 december 2008 R.o. 85 en 86, <http://www.bailii.org/eu/cases/ECHR/2008/1581.html>





- 
- xii Marper vs UK EHRM 4 december 2008 R.o. 119 en 125, <http://www.bailii.org/eu/cases/ECHR/2008/1581.html>
- xiii Europees Hof voor de Rechten van de Mens 20 januari 2009, nr20689/08, RvdW 2009,992 In het citaat wordt alleen gesproken over DNA-afname en opslag, omdat daar in deze zaak over geklaagd was, maar uit Marper vs VK blijkt al, dat dat niet essentieel anders is ten aanzien van vingerafdrukken.
- xiv Zie hierover uitgebreider de dagvaarding van Privacy First waarnaar is verwezen in het beroepschrift, met name de punten 21-29 en 41- 53. <http://www.privacyfirst.nl/weblinks/undisclosed.html>
- xv Tenzij inbreuk wordt gemaakt op het portretrecht en men foto's van mij schiet. Maar het spreekt vanzelf, dat dan al een schending van artikel 8 EVRM zich voordoet, dus die situatie kan ik verder buiten beschouwing laten.
- xvi De artikelen 6, lid 1, sub c, en 7, sub c en e, van richtlijn 95/46 hebben rechtstreekse werking in die zin, dat een particulier er zich voor de nationale rechterlijke instanties op kan beroepen om de toepassing van met deze artikelen strijdige bepalingen van nationaal recht te verhinderen.  
*Hof van Justitie van de Europese Gemeenschappen, 20 mei 2003, nrC-138/01,C-139/01,C-465/00, LJN:AO8036, NJ 2005/15*
- xvii De EDPS acht het een goede zaak dat de Raad ruimschoots aandacht besteedt aan dit belangrijke voorstel. Hij is evenwel bezorgd over de evolutie van dit dossier. In de teksten die thans bij de Raad worden besproken, zijn noch de amendementen van het Europees Parlement noch de adviezen van de EDPS en van de Conferentie van Europese gegevensbeschermingsautoriteiten verwerkt. Daarentegen, zijn in heel wat gevallen de bepalingen in het Commissievoorstel die waarborgen voor de burgers bevatten, geschrapt of aanzienlijk afgezwakt. Dientengevolge is er nu een geringe kans dat het beschermingsniveau lager zal zijn dan het geval was met Richtlijn 95/46/EG, of zelfs lager dan krachtens het meer algemeen geformuleerde Verdrag nr. 108 van de Raad van Europa, dat bindend is voor de lidstaten. Hoewel ook de EDPS erkent dat het belangrijk is dat de Raad het kaderbesluit zo snel mogelijk aanneemt, waarschuwt hij dat een snelle besluitvorming niet mag resulteren in lagere beschermingsnormen. De teksten die thans bij de Raad in behandeling zijn, doen eraan twifelen of het resultaat voldoende stevig zal zijn om de burger een adequaat niveau van bescherming te garanderen. In de huidige situatie lijkt de nagestreefde snelheid ertoe te leiden dat controversiële bepalingen worden geschrapt of afgezwakt. Indien men te weinig tijd neemt om overeenstemming te bereiken over mogelijk omstreden bepalingen kan dit afbreuk doen aan de kwaliteit van het kaderbesluit. Gezien dit alles beveelt de EDPS de Raad aan om voor de onderhandelingen meer tijd uit te trekken, met het oog op een resultaat dat voldoende bescherming biedt.  
*Tweede advies van de Europese Toezichthouder voor gegevensbescherming betreffende het voorstel voor een kaderbesluit van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politieke en justitiële samenwerking in strafzaken [EurLex 52007XX0426(02)] punten 4, 8 en 9.*
- xviii In zijn advies van december 2005 heeft de EDPS opgemerkt dat beperking tot met andere lidstaten uitgewisselde gegevens het toepassingsgebied van het kaderbesluit buitengewoon ongewis en onduidelijk zou maken, hetgeen zou indruisen tegen de voornaamste doelstelling van dit besluit. Wanneer persoonsgegevens worden verzameld of verwerkt, is immers nog niet bekend of deze gegevens later in aanmerking komen voor uitwisseling met bevoegde autoriteiten uit andere lidstaten. Derhalve is een beperkter toepassingsgebied onwerkbaar; dit zou binnen de databestanden van de wetshandhavingsautoriteiten een moeizaam en nauwkeurig onderscheid vergen tussen verschillende gegevenscategorieën, hetgeen slechts kan leiden tot extra complicaties en kosten voor deze autoriteiten, terwijl de rechtszekerheid van de betrokkenen wordt geschaad.  
*Tweede advies van de Europese Toezichthouder voor gegevensbescherming betreffende het voorstel voor een kaderbesluit van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politieke en justitiële samenwerking in strafzaken [EurLex 52007XX0426(02)] punten 11 en 12.*
- xix Iedere betrokkene heeft het recht om ingelicht te worden over de verwerking van gegevens die op hem betrekking hebben. Dit recht houdt verband met het beginsel van een eerlijke en rechtmatige verwerking van persoonsgegevens, dat op zichzelf in het kaderbesluit wel in acht wordt genomen en dat voorts beschermd is krachtens Verdrag nr. 108 van de Raad van Europa, en met name de artikelen 5, onder a) en 8. Een wezenlijk onderdeel van dit recht is dat de verantwoordelijke voor de verwerking van de gegevens deze inlichtingen ambtshalve moet verstrekken. Aangezien de betrokkene



kene normaliter niet weet noch kan weten dat verwerking van hem betreffende informatie plaatsvindt, zou het tegen het wezen van dit recht indruisen om te eisen dat de betrokkene een verzoek om informatie indient. Uiteraard bestaan er uitzonderingen op het recht om ingelicht te worden en is het duidelijk dat deze uitzonderingen juist op het gebied van de wetshandhaving van belang kunnen zijn, aangezien het verstrekken van inlichtingen over een strafrechtelijk onderzoek dit onderzoek kan schaden. Iedere oplossing waarbij het recht om ingelicht te worden afhangt van een verzoek van de betrokkene is echter onaanvaardbaar en is onverenigbaar met Verdrag nr. 108 van de Raad van Europa.

*Tweede advies van de Europese Toezichthouder voor gegevensbescherming betreffende het voorstel voor een kaderbesluit van de Raad over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politie en justitiële samenwerking in strafzaken [EurLex 52007XX0426(02)] punt 24.*

<sup>xx</sup> HvJEU 7 mei 2009, C 553/07

<sup>xxi</sup> Marper vs UK EHRM 4 december 2008 r.o. 41-44 en 107, <http://www.bailii.org/eu/cases/ECHR/2008/1581.html>

<sup>xxii</sup> Bij een eerdere gelegenheid heeft de EDPS reeds een aantal punten van zorg geformuleerd met betrekking tot het concept van interoperabiliteit. Onder meer kan de interoperabiliteit van systemen prikkels bieden om nieuwe doeleinden voor te stellen voor de toepassing van grootschalige IT-systemen die verder gaan dan het oorspronkelijk beoogde doeleinde en/of voor het gebruik van biometrische gegevens als primaire sleutel op dit gebied. Voor verschillende soorten interoperabiliteit zijn telkens specifieke waarborgen en voorwaarden vereist. De EDPS heeft in dit verband tevens benadrukt dat de gegevensbeschermingsbeginselen, en met name het beginsel van doelbinding, volledig in acht moeten worden genomen wanneer systemen interoperabel worden gemaakt.

*Advies van de Europese Toezichthouder voor gegevensbescherming over de mededeling van de Commissie aan het Europees Parlement en de Raad getiteld — "Overzicht van het informatiebeheer op het gebied van vrijheid, veiligheid en recht" [52010XX1229(03)] punt 47*

Op gelijke wijze ook al: Wetgevingsadvies van het College voor de Bescherming van Persoonsgegevens, 31 mei 2007, p. 6 [http://www.cbppweb.nl/downloads\\_adv/z2007-00010.pdf](http://www.cbppweb.nl/downloads_adv/z2007-00010.pdf)

<sup>xxiii</sup> V. Böhre, *Happy landings? Het biometrisch paspoort als zwarte doos* (WWR webpublicatie 46), p. 120

<sup>xxiv</sup> HvJEU 16 december 2008, C-524/06

<sup>xxv</sup> Te weten:

- Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG;
- Besluit 2008/633/JBZ van de Raad van 23 juni 2008 over de toegang tot het Visuminformatiesysteem (VIS) voor raadpleging door aangewezen autoriteiten van de lidstaten en door Europol, met het oog op het voorkomen, opsporen en onderzoeken van terroristische misdrijven en andere ernstige strafbare feiten;
- het voorstel voor een kaderbesluit van de Raad over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor wetshandavingsdoeleinden .

*Advies van het Europees Parlement en de Raad betreffende de instelling van "Eurodac" voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van Verordening (EG) nr. (.../...) (tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend), alsmede over het voorstel voor een besluit van de Raad over rechtshandavingsinstanties van de lidstaten en Europol die voor rechtshandavingsdoeleinden verzoeken om vergelijking met Eurodac-gegevens [EurLex 2010/C 92/01 52010XX0410(01)] Punt 18*

<sup>xxvi</sup> *Advies van het Europees Parlement en de Raad betreffende de instelling van "Eurodac" voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van Verordening (EG) nr. (.../...) (tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend), alsmede over het voorstel voor een besluit van de Raad over rechtshandavingsinstanties van de lidstaten en Europol die*



---

voor rechtshandhavingsdoeleinden verzoeken om vergelijking met Eurodac-gegevens [EurLex 2010/C 92/01 52010XX0410(01)] Punt 19

<sup>xxvii</sup> Zo ook letterlijk EDPS in *Advies van het Europees Parlement en de Raad betreffende de instelling van "Eurodac" voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van Verordening (EG) nr. (.../...) (tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend)*, alsmede over het voorstel voor een besluit van de Raad over rechtshandhavingsinstanties van de lidstaten en Europol die voor rechtshandhavingsdoeleinden verzoeken om vergelijking met Eurodac-gegevens [EurLex 2010/C 92/01 52010XX0410(01)] Punt 22

<sup>xxviii</sup> *Advies van het Europees Parlement en de Raad betreffende de instelling van "Eurodac" voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van Verordening (EG) nr. (.../...) (tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend)*, alsmede over het voorstel voor een besluit van de Raad over rechtshandhavingsinstanties van de lidstaten en Europol die voor rechtshandhavingsdoeleinden verzoeken om vergelijking met Eurodac-gegevens [EurLex 2010/C 92/01 52010XX0410(01)] Punt 22

<sup>xxix</sup> *Advies van het Europees Parlement en de Raad betreffende de instelling van "Eurodac" voor de vergelijking van vingerafdrukken ten behoeve van een doeltreffende toepassing van Verordening (EG) nr. (.../...) (tot vaststelling van de criteria en instrumenten om te bepalen welke lidstaat verantwoordelijk is voor de behandeling van een verzoek om internationale bescherming dat door een onderdaan van een derde land of een staatloze bij een van de lidstaten wordt ingediend)*, alsmede over het voorstel voor een besluit van de Raad over rechtshandhavingsinstanties van de lidstaten en Europol die voor rechtshandhavingsdoeleinden verzoeken om vergelijking met Eurodac-gegevens [EurLex 2010/C 92/01 52010XX0410(01)] Punt 27

<sup>xxx</sup> Wetgevingsadvies van het College voor de Bescherming van Persoonsgegevens, 31 mei 2007, p. 5  
[http://www.cbpweb.nl/downloads\\_adv/z2007-00010.pdf](http://www.cbpweb.nl/downloads_adv/z2007-00010.pdf)

<sup>xxxi</sup> E. Hirsch Ballin, "De rechtsstaat: wachten op een nieuwe dageraad?" in *Nederlands Juristenblad* 2011, afl 2 dd 14 januari 2011 p. 71- 73.