PLEITAANTEKENINGEN
BIJ DE BEHANDELING VAN HET BEROEP VAN
J. DINGLER
12/2606 BESLU V86
RECHTBANK DEN HAAG
9 november 2015

Ter toelichting op het beroep zij het volgende opgemerkt:

1. Eiser is verheugd dat zijn zaak vandaag eindelijk wordt behandeld. Hij heeft er lang op gewacht en het valt op, dat de laatste tijd er ook op politiek vlak weinig schot zit in de aanpassing van de praktijk waarbij Burgemeesters inbreuk maken op het recht op privacy, wanneer een burger om een paspoort komt vragen. Hopelijk geeft de uitspraak in deze zaak weer momentum aan de ontwikkelingen.

2. Eiser is vrij uitgebreid geweest in zijn beroepschrift. Tegen de beroepsgronden is geen verweer gevoerd, althans niet binnen de termijn.

3. Eiser heeft als principale grond, dat het hogere recht op eerbiedging van de privacy, zoals vastgelegd in artikel 8 EVRM derogeert aan de lagere nationale wetgeving. Ook de EU-paspoortverordening is hiermee in strijd en zal vanwege het feit dat de EU de mensenrechten die zijn vastgelegd in het EVRM tevens als beginselen van de EU heeft omarmt buiten werking moeten blijven. De verbindendheid aan de EU-Verordening erkent eiser niet. Overigens: adressaat van die Verordening zijn de lidstaten en niet de Burgemeesters, terwijl de Burgemeesters wél gebonden zijn aan de eerbiedigende werking van mensenrechten waartoe het EVRM strekt.

4. Van belang is in dezen voorts, dat de vraag of de Verordening wegens strijd met artikel 8 EVRM onverbindend is nog niet is beantwoord, althans in het licht van de proportionaliteitstoetsing en de eisen van subsidiariteit. Wel is er een oordeel gegeven door het Hof van Justitie te Luxemburg over de wijze waarop de Verordening tot stand is gekomen, maar helaas heeft de Afdeling van de Raad van State de vraag naar de verbindendheid in de bij de Afdeling Bestuursrechtspraak aanhangige paspoortzaken, en op grond van de in de Nederlandse procedures aangevoerde argumenten, die zich hadden toegespitst op p[proportionaliteit en subsidiariteit, laten vallen. We zullen dus nog moeten wachten op een nieuwe zaak om die vraag beantwoord te krijgen.

5. Déze zaak, de zaak van de heer Dingler zou die zaak kunnen zijn. U als Rechtbank zou de vraag aan het EU Hof van Justitie kunnen stellen die de Afdeling heeft laten vallen.

6. Die vraag zou dan moeten luiden:

   Is artikel 1, tweede lid, van verordening (EG) 2252/2004 van de Raad van 13 december 2004 betreffende normen voor veiligheidskenmerken van en biometrische gegevens in door de lidstaten af te geven paspoorten en reisdocumenten (PB L 385, blz. 1), zoals gewijzigd bij Verordening (EG) nr. 444/2009 van het Europees Parlement en de Raad van 28 mei 2009 tot wijziging van Verordening (EG) nr. 2252/2004 (PB L 142, blz. 1), geldig in het licht van de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie en artikel 8 van het Verdrag tot bescherming van de rechten van de mens en fundamentele vrijheden, met name ook gelet op de vraag of de inbreuk die zij op de beschermde rechten maakt wel proportioneel is en wel voldoet aan de eisen van subsidiariteit, en voorts of zij wel met voldoende waarborgen omgeven is?

7. In de zaak Schwarz zijn niet dezelfde argumenten gevoerd als in de Nederlandse zaken waarom er strijd zou zijn met van de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie en artikel 8 van het Verdrag tot bescherming van de rechten van de mens en fundamentele vrijheden. Het Hof geeft in de uitspraak uitdrukkelijk aan, dat de in die zaak gevoerde argumenten geen aanleiding geven om te komen tot het oordeel dat er strijd bestaat. Het Hof laat daarbij bewust de mogelijkheid open, dat andere argumenten tot een andere uitkomst zouden kunnen leiden. Vandaar dat de uitspraak in de zaak Schwarz niet in de weg staat aan een andersluidend antwoord op de eerste vraag dan het antwoord dat het Hof in de zaak Schwarz gegeven heeft. Oftewel: uit het arrest Schwarz kan niet zonder meer het antwoord op deze vraag afgeleid worden.

8. De inbreuk die de Burgemeester toelaat en zelfs voorschrijft voordat hij bereid is aan eiser een paspoort uit te reiken is een ernstige. Vingerafdrukken zijn heel persoonlijk, en er is een groot belang bij het als enige kunnen beschikken over de eigen biometrische gegevens.

9. De eigenaar van die dactyloscopische kenmerken geeft daarmee immers een toegang tot zijn identiteit. Wanneer ergens dactyloscopische kenmerken van een persoon worden gevonden, wordt daarmee ook aangenomen, dat die persoon op die plaats is geweest. Het bezit van de kennis over de kenmerken geeft toegang tot het private verleden van de desbetreffende persoon. Het geeft tevens toegang tot andere gegevens van die persoon, omdat in Europa door diverse instanties (en kennelijk ook door de Europese Commissie en het parlement) ervan wordt uitgegaan, dat je je met vingerafdrukken kunt legitimeren, oftewel: dat daarmee de identiteit kan worden vastgesteld van een persoon. Diefstal van de gegevens opent derhalve de poort naar diefstal van de identiteit, met alle ingrijpende gevolgen van dien.

10. Met het verkrijgen van de dactyloscopische gegevens kan zelfs een verleden worden gecreëerd dat niet bestond: anderen kunnen de vingerafdruk nabootsen en ergens achterlaten waar de eigenaar helemaal niet geweest is, waardoor die eigenaar ernstig gecompromitteerd kan worden of in verlegenheid gebracht. Het verkrijgen van kennis over de vingerafdrukken is derhalve een gebeurtenis met ingrijpende gevolgen.

11. Niet vergeten moet worden, dat het een vergissing zou zijn te menen, dat het paspoort exclusief in het bezit blijft van de houder ervan. Paspoorten moeten worden afgegeven aan consulaten waar men een visum aanvraagt (waar men het meestal pas een paar dagen later kan ophalen), zij moeten uit handen gegeven worden aan de buitengrens van het Schengengebied, maar ook aan controlerende instanties binnen het Schengengebied, er wordt om gevraagd door bankemployees die ergens achter in hun bankgebouw geacht worden een kopie te maken van dat paspoort en dat in het dossier te voegen ter voorkoming van witwaspraktijken en andere financiële malversaties (N.B.: dit betreft een wettelijke verplichting!), ze worden gegeven aan de voorzitters van stembureaus, aan beveiligingspersoneel van locaties zoals gevangenissen en Ministeries, aan verzekeringsmaatschappijen en andere dienstverleners die op grond van wetgeving verplicht zijn de identiteit van hun cliënt vast te stellen. Zelfs advocaten die een cliënt bijstaan zijn in Nederland verplicht voor hun dossier een kopie van een identiteitsdocument te maken!

12. Kortom, paspoorten gaan van hand tot hand, en uiteindelijk worden ze zelfs weer ingeleverd bij de balie van het stadhuis als ze verlopen zijn, maar terwijl de chip nog steeds uitleesbaar is. Wat er dan mee gebeurt is de vraag, en wie de ongeldige paspoorten en chips daarna nog in handen krijgt is eiser niet bekend. In ieder geval weet hij dat velen het paspoort onder zich zullen krijgen, en het risico lopen dat bij een van die gelegenheden de in het paspoort opgeslagen biometrische gegevens in verkeerde handen komen, is een risico, dat eiser niet wil lopen, en al helemaal niet als daar geen goede reden voor is.

13. Afgelopen maand is bovendien naar buiten gebracht, dat de politie uitgerust gaat worden met een app op hun telefoon waarmee identiteitsbescheiden kunnen worden uitgelezen en via de app de gevonden gegevens kunnen worden vergeleken met de database in het politiebureau, of bij het OM. Dat werd als een innovatieve matregel in de strijd tegen de criminaliteit beschouwd. Het was te verwachten dat de techniek dit soort methodes in de praktijk worden ingevoerd. Maar dat heeft wél ernstige gevolgen voor degenen die vingerafdrukken hebben laten opslaan in hun paspoort. Want als die uitleesbaar worden, dan kan de politie dus zonder dat daarvoor strafvorderlijke waarborgen zijn voortaan over eenieders vingerafdrukken de beschikking krijgen. Op dit moment is

dat alleen nog zo bij personen die van een ernstig misdrijf worden evrdacht of voor een misdrijf zijn veroordeeld. Maar straks kan dat op basis van artikel 447 e r iedereen zijn waarvan de politie vindt dat zij zich zouden moeten legitimeren. Iedereen die onder de werking van artikel 2 Politiewet wordt gebracht, getuigen, hulpbehoevenden, personen die enige wetenschap dragen van iets wat de politie aanbelangt, zij kunnen allemaal hun vingerafdrukken in handen van de politie zien vallen als deze ontwikkeling zich doorzet.

14. Het gaat bij het kunnen beschikken over en verwerken van vingerafdrukken over zeer gevoelige informatie, heeft het EHRM meermaals uitgemaakt. Eiser verwijst naar de bekende uitspraak van Marper c.s. vs VK (EHRM 4 december 2008). In r.o. 104 overweegt het EHRM:

> The interests of the data subjects and the community as a whole in protecting the personal data, including fingerprint and DNA information, may be outweighed by the legitimate interest in the prevention of crime (see Article 9 of the Data Protection Convention). However, the intrinsically private character of this information calls for the Court to exercise careful scrutiny of any State measure authorising its retention and use by the authorities without the consent of the person concerned.

15. Ook in andere gevallen waar het om iemands hoogst persoonlijke identiteit gaat, meestal gerelateerd aan zaken die het lichaam raken, oordeelt het EHRM dat er bijzonder weinig *margin of appreciation* is. Het Hof verwijst zelf al in de Marper case naar de zaak Z. tegen Finland (EHRM 25 februari 1997). Een andere zaak waar dit eveneens opgaat, is de zaak Dudgeon vs VK (EHRM 22 oktober 1981). Daarin oordeelde het EHRM:

> it is for the national authorities to make the initial assessment of the pressing social need in each case; accordingly, a margin of appreciation is left to them. However, their decision remains subject to review by the Court. However, not only the nature of the aim of the restriction but also the nature of the activities involved will affect the scope of the margin of appreciation. The present case concerns a most intimate aspect of private life. Accordingly, there must exist particularly serious reasons before interferences on the part of the public authorities can be legitimate for the purposes of Article 8.

16. Kijken we naar de beroepsgronden die zijn aangevoerd, dan is eiser ervan overtuigd, dat we hier niet te maken hebben met "*particularly serious reasons*".

17. Ik wijs op de informatie die in Nederland bekend is geworden met betrekking tot de omvang van fraude met *look alikes*, de enige vorm van fraude waartegen de vergelijking met vingerafdrukken wellicht zou kunnen worden ingezet. Dat betreft één geval per jaar. En dáárvoor moeten alle Nederlanders het risico lopen dat informatie over hun vingerafdrukken in andermans handen komt? Daar is iedere verhouding zoek. Dat is ook de hoofdreden dat ik u vraag prejudiciële vragen te

stellen. Verwezen kan dan worden naar de stukken die voorgelegen hebben in de zaken die aanhangig zijn bij de Raad van State en waarin die van Louise van Luijk de best gedocumenteerde en vergelijkbare is (http://www.louisevspaspoortwet.nl/). Daarin zijn niet alleen de rapportages van de KMar opgenomen, maar ook het gegeven, dat de check op vingerafdrukken z'n hark is vergeleken met de stofkam die andere controlemiddelen vormen, dat er met die hark niks uit de bulk van informatie geselecteerd kan worden dat niet al eerder ontdekt zou zijn bij de conventionele vertrouwde middelen (VIS-check, lengte, leeftijd, pasfoto, nummer van het identiteitsbewijs en eventuele registratie in het register van verloren /gestolen documenten).

18. Ik wijs er ook op, dat het Gerechtshof alhier al heeft geoordeeld, dat de klacht dat er vingerafdrukken werden afgenomen en opgeslagen in strijd is met artikel 8 EVRM (Gerechtshof Den Haag18 februari 2014; ECLI:NL:GHDHA:2014:412,) De Hoge Raad heeft het arrest op de ontvankelijkheid van de procederende partij --een belangenvereniging-- vernietigd, maar niets afgedaan aan de inhoud van het arrest. De Hoge Raad heeft zelfs expliciet overwogen, dat burgers zelf als het hen overkomt dat de Burgemeester de inbreuk wil maken op hun privacy zich kunnen ebroepen in d ebestuursrechtelijke procedure daartegen op de argumenten die privacy First hanteerde en die leidden tot de uitspraak van het gerechtshof. Eiser heeft dus het rechterlijk oordeel in deze procedure mee.

19. Intussen heeft eiser wel een paspoort gekregen, maar dat was pas nadat hij zeer met pijn in het hart zijn vingerafdrukken heeft afgestaan, omdat hij geen geld meer had om te overleven. Hij heeft, toen hij werkloos raakte, eerst nog even op zijn gespaarde centen geteerd, maar toen heeft hij onder de druk van honger en dreigend verlies van zijn huis eieren voor zijn geld gekozen. Het College weigerde namelijk hem een bijstandsuitkering toe te kennen, ook al wisten ze drommels goed wie hij was, omdat er oude identiteitsdocumenten waren geweest en het College eiser ook nog persoonlijk uit deze procedure kende. Maar het College van B&W speelde het hard en hield zich strak aan de wet WWB, en toen heeft eiser zich gedwongen gezien zijn gewetensbezwaren opzij te zetten en zichzelf geweld aan te doen.

20. Overigens betekent, dat niet, dat eiser geen belang meer heeft bij de zaak. Hij heeft proceskosten gemaakt, zowel in bezwaar als in beroep. Dat zijn de kosten van zijn advocaat geweest en het griffierecht. In bezwaar is hem geen tegemoetkoming ex artikel 7:15 Awb toegekend. In beroep is geen proceskostenvergoeding aangeboden. Bovendien heeft eiser frustratie ondervonden door het lange wachten. Deze procedure is al ruim over de redelijke termijn heen, en eiser wenst ook op dat punt schadeloos te worden gesteld. Maar voor hem is het belangrijkste, dat wordt aangetoond,

dat het besluit jegens hem onrechtmatig was. In dat geval kan hij immers alsnog een paspoort zonder vingerafdrukken aanvragen, waarmee hij naar het buitenland kan reizen zonder bevreesd te hoeven zijn, dat zijn gegevens van zeer persoonlijke en intieme aard misbruikt zullen worden. De Burgemeester roept, dat dat niet zo'n vaart zal lopen. Er is immers nog niet gebleken, dat de versleuteling gekraakt is. Maar niemand had ook gedacht dat zoals afgelopen zomer de database van de Amerikaanse overheid gekraakt zou worden, zodat alle salarisgegevens adressen en andere persoonlijke informatie van overheidsdienaren, daaronder mensen begrepen die met bekend worden van hun betrokkenheid bij de overheid gevaar zouden lopen –zoals bijvoorbeeld informanten, geheim agenten en inspecteurs—bij onbekende partijen bekend is geworden. Eiser wil niet blootgesteld worden aan gevaren waar hij niet op bedacht hoeft te zijn. En zeker niet, als er geen enkele goede reden is om daaraan blootgesteld te worden.

21. Wat betreft het laatste deel van de mogelijke prejudiciële vraag, die ik hiervoor geformuleerd heb, namelijk de waarborgen die er (niet) zijn, wil ik wijzen op de uitspraak van het Hof van Justitie EU d.d. 8 april 2014 (Digital Rights Ireland, C-293/12 en C-594/12), waarin het Hof oordeelde, dat de Richtlijn betreffende Gegevensbewaring (2002/58/EG) ongeldig was. Drie argumenten waarop het Hof die uitspraak baseerde spelen ook hier.

22. Het eerste argument is dat de Richtlijn geen enkel objectief criterium bood waarmee kon worden verzekerd dat de nationale overheden slechts gebruik konden maken van de gegevens voor het doel waarvoor de Richtlijn was geschreven, namelijk bestrijding van voldoende ernstige criminaliteit. Dat argument is precies wat hier speelt: het ontbreken van waarborgen tegen verdergaand gebruik dan 'slechts' het gebruik waarvoor de Richtlijn, dan wel de Verordening is geschreven. Als er geen wettelijke regeling is ter voorkoming van ander gebruik van de opgenomen biometrische gegevens dan voor controle aan de buitengrens van het Schengengebied, dan geldt voor de Verordening hetzelfde als voor de genoemde Richtlijn.

23. En inderdaad: in de Verordening staat geen enkele clausule die controle aan de hand van de verwerkte gegevens anders dan aan de buitengrens van het Schengen onmogelijk maakt. Zelfs wordt niet gebruik voorkomen dat helemaal niets met grensoverschrijding waar dan ook ter wereld te maken heeft, maar bijvoorbeeld slechts met legitimatie bij banken, instellingen, particulieren. En al helemaal staat er niks over al dan niet heimelijk gebruik door opsporingsdiensten.

24. Het tweede argument was, dat er in de Richtlijn geen toereikende waarborgen werden geboden om een doeltreffende bescherming van gegevens te verzekeren tegen het gevaar van misbruik en

tegen elke onrechtmatige toegang tot en elk onrechtmatig gebruik van gegevens. Ook dat speelt hier. De verwerkte gegevens zijn door de keuze voor een RFID-chip op afstand uitleesbaar. Het is slechts een kwestie van tijd totdat de versleuteling wordt gekraakt of de codes in handen komen van anderen dan de uitgevende Staat. De Staten weten, dat als dat eenmaal gebeurt de doos van Pandora open is. Niet voor niets worden op dit moment de versleutelingscodes niet gedeeld met anderen, zelfs niet onderling met lidstaten van de Unie! Gevolg is wel, dat controle aan de buitengrenzen van Schengen dus vaak niet eens plaats vindt. De nationale overheden zijn zich terdege bewust dat wat je uit handen geeft onomkeerbaar tot verlies van controle leidt. *Áls* er al eens wordt gecontroleerd of de houder van het paspoort dezelfde is als degene die zijn vingerafdrukken heeft laten afnemen, dan gebeurt dit door de eigen overheid, binnen het eigen land en zelden aan de buitengrens van Schengen. In Nederland bijvoorbeeld op het gemeentehuis. Met deze praktijk blijft niets over van het nuttig effect van de Verordening, want voor controle *binnen* de buitengrenzen is zij uitdrukkelijk niet bedoeld.

25. Het derde argument zag op de kwestie, dat de afgekeurde Richtlijn niet voorschreef, dat de communicatiegegevens op het grondgebied van de Unie moesten worden opgeslagen. Daardoor kon de naleving van de eisen die het Handvest stelt niet volledig worden gewaarborgd.

26. In Nederland worden de biometrische gegevens in paspoorten verwerkt en versleuteld door een bedrijf dat onderworpen is aan de Patriot Act. Dat wordt niet verboden door de Verordening. Maar dat zet de deur wagenwijd open naar lekken van de privacygevoelige gegevens naar Amerika. Er zijn daarover diverse malen vragen gesteld aan de verantwoordelijke bewindslieden door ons Parlement. Die bewindslieden hebben verklaard, dat ze aannemen, dat het allemaal zo'n vaart wel niet zal lopen, en dat ze zich niet kunnen indenken, dat de VS van langs die weg biometrische gegevens zouden trachten te verkrijgen van Nederlandse burgers. Helaas, hetzelfde is gedacht met betrekking tot het aftappen van internetverkeer bij Frankfurt door de Amerikanen, of het afluisteren van miljoenen Europeanen tot aan Bondspresident Merkel en haar voorgangers toe, en zoals onlangs bleek, ook de Franse presidenten. Daarnaast hebben we gezien hoe Minister Plassterk zich in bochten heeft moeten wringen naar aanleiding van onthullingen dat de Amerikanen hier doen wat de Nederlanders niet mogen, en hoe de Nederlandse overheid daarbij een oogje toeknijpt, of zelfs heimelijk tevreden is dat de Amerikanen het werk opknappen. De werkelijkheid blijkt dus weerbarstiger dan sommige optimistische politici willen geloven. Wat er ook van zij van de vraag of biometrische gegevens die zijn afgestaan voor verwerking in een paspoort op dit moment of in de naaste toekomst worden doorgespeeld aan de Amerikanen op grond van de Pa-

triot Act, de *mogelijkheid* ervan wordt in ieder geval niet uitgesloten of verboden door de Verordening. De Verordening is daardoor op dit punt even ongeldig als de Richtlijn Gegevensbewaring, volgens de criteria die het Hof van Justitie EU aanlegde in de zaak Digital Rights vs Ierland.

27. Ik kom terug bij de vraag "Waar gaat het allemaal over?"

28. Eiser moet VIER vingerafdrukken geven omdat de Burgemeester er TWEE op een op afstand uitleesbare chip wil opnemen. Zogenaamd omdat er gecontroleerd moet worden. Maar wordt er gecontroleerd? Nee, helemaal niet.

29. De Verordening dateert al van 2004 (en de voorbereiding van nog langer geleden) en er tot op heden is nog geen enkele stap gezet richting het verlenen van autorisaties aan andere mogendheden. De realisatie van controle op vingerafdrukken aan de grens ligt nog even ver in het verschiet als zij al lag vóórdat überhaupt een aanvang werd gemaakt met invoering van een systeem waarbij vingerafdrukken in reisdocumenten zouden worden opgenomen. Inmiddels is het al zes jaar verplicht gesteld om vingerafdrukken af te staan. De paspoorten die in de eerste twee jaren zijn uitgegeven met een chip zijn nimmer gecontroleerd op die vingerafdrukken. De houders hebben dus nodeloos een inbreuk op hun privacy moeten dulden, want die paspoorten met chips zijn al niet meer geldig, en de houders hebben zich opnieuw naar het loket moeten begeven voor opnieuw afname van vingerafdrukken. En het ziet ernaar uit dat dit zinloze carrousel van verwerking van biometrische gegevens nog wel even doorgaat, als het geen halt wordt toegeroepen.

30. Dan kan niet meer worden volgehouden, dat in die (mogelijkheid van) grenscontroles een *pressing social need* ligt, *necessary in a democratic society*. Waaruit immers blijkt het predicaat "*pressing*" dan, en waaruit de term "*need*" of het predicaat "*necessary*"? Als het *necessary* was, en als het *pressing* was, dan was er toch allang wat gedaan om die grenscontroles dichterbij te brengen? Kennelijk kunnen we heel goed toe zónder grenscontroles aan de hand van vingerafdrukken.

31. Ik verzoek u het beroep gegrond te verklaren, met veroordeling van verweerder in de kosten van de procedure, en ook meteen schadevergoeding vast te stellen wegens het overschrijden van de redelijke termijn.

Ik dank u voor uw aandacht.

Leiden, 9 november 2015 Gemachtigde