

P. Deutekom
[adres]
[postcode/plaats]

Aan:
Rechtbank Amsterdam, sector Bestuursrecht
Postbus 75850
1070 AW Amsterdam

Betreft:
Procedurenummer 10 / 4445 WET 64 G493

Amsterdam, 22 februari 2011

Edelachtbaar college,

Het verweerschrift dat mr. C.M. Bitter namens de Burgemeester van Amsterdam verstuurd heeft, geeft aanleiding tot enige opmerkingen. Daar ik vrees dat de zitting van 9 maart a.s. te kort zal duren om deze allemaal te behandelen, maak ik hierbij alvast enkele schriftelijke opmerkingen.

1. Geldigheid van de verordening

De geldigheid van de EG-verordening 2252/2004 is niet alleen door mijzelf ter discussie gesteld, maar ook door de lidstaten van de EU! Bij het verdrag van Lissabon is een nieuwe bepaling aan het EG-verdrag toegevoegd:

Artikel 77 lid 3

Indien een optreden van de Unie noodzakelijk blijkt om de uitoefening van het in artikel 20, lid 2, onder a), bedoelde recht [het vrije verkeer van burgers van de Unie, PD] te vergemakkelijken, kan de Raad, volgens een bijzondere wetgevingsprocedure, bepalingen inzake paspoorten, identiteitskaarten, verblijfsvergunningen en daarmee gelijkgestelde documenten vaststellen, tenzij de Verdragen in de daartoe vereiste bevoegdheden voorzien. De Raad besluit met eenparigheid van stemmen, na raadpleging van het Europees Parlement.

De lidstaten geven hier een uitdrukkelijke bevoegdheid om te regelen wat nu in de verordening geregeld wordt, voor het geval mocht blijken **dat deze bevoegdheid hiervoor nog niet bestond**. Een bevoegdheidstoekenning kan echter geen terugwerkende kracht hebben. Als de bevoegdheid niet bestond op het moment dat de verordening werd vastgesteld, was - en is - de verordening nietig.

Uit het verdrag zelf blijkt dus dat de verordening allerm minst zonder meer geldig is. Ten einde hierover voor alle EU-burgers rechtszekerheid te verkrijgen zal de vraag naar de geldigheid op enig moment door een rechter aan het Hof van Justitie van de Europese Unie moeten worden voorgelegd.

2. Strijd met de verordening

Als de verordening toch geldig is, moet deze gelezen worden in het licht van de algemene rechtsbeginselen van het verbod op *détournement de pouvoir* en van de eerbiediging van de persoonlijke levenssfeer, die beide deel uitmaken van de gemeenschappelijke constitutionele tradities van de lidstaten.

Als biometrische gegevens, die door burgers verplicht worden afgestaan ten einde te voldoen aan de verordening, vervolgens worden gebruikt voor een ander doel, dan worden bovengenoemde beginselen geschonden. De verordening kan dit rechtens niet bedoeld hebben.

Verwerking van biometrische gegevens voor andere doelen is slechts dan toegestaan, wanneer deze geheel buiten de werkingssfeer van de verdragen ligt. Hierbij valt te denken aan het afnemen van vingerafdrukken van verdachten in het kader van een strafrechtelijk onderzoek.

De aanwijzing van de autoriteiten en organisaties die toegang hebben tot de in het opslagmedium opgeslagen gegevens is een zaak van de nationale wetgeving. Naar mijn mening beoogt deze bepaling slechts de lidstaten de vrijheid te laten om, indien zij dat wensen, hun nationale autoriteiten en organisaties te hernoemen of te reorganiseren. Voorbeelden hiervan zijn de Bundesgrenzschutz / Bundespolizei in Duitsland en de Rijkswacht / Federale Politie in België. Dit alles onder voorbehoud van het communautaire recht, waaronder ook het Handvest van de Grondrechten van de Europese Unie en de richtlijn 95/46/EG begrepen worden.

Verweerder beroept zich verder nog op overweging 5 van de wijzigingsverordening 444/2009. Deze wijzigingsverordening heeft dezelfde rechtsbasis 2252/2004 en lijdt mogelijk aan hetzelfde gebrek aan bevoegdheid als de eerdere verordening.

Voor zover de wijzigingsverordening de bedoeling heeft om de lidstaten de mogelijkheid te geven om de onder verordening 2252/2004 verkregen gegevens voor een ander doel te gebruiken dan waar deze verordening in voorziet, is zij bovendien in strijd met artikel 8 van het Handvest .

Ik verzoek u dan ook om een eventuele prejudiciële vraag aan het Hof van Justitie van de Europese Unie uit te breiden en daar ook de geldigheid van verordening 444/2009 in te betrekken.

3. Strijd met artikel 8 EVRM

Verweerder ontkent niet dat het afnemen en opslaan van vingerafdrukken een inbreuk op artikel 8 EVRM oplevert. De vraag is of deze inbreuk gerechtvaardigd is. Om gerechtvaardigd te worden moet zo'n inbreuk bij de wet voorzien zijn, en noodzakelijk zijn in een democratische samenleving ter bescherming van een beperkt aantal belangen.

3.1. Bij de wet voorzien?

Verweerder stelt dat aan het criterium 'bij de wet voorzien' voldaan is, doordat de regering bij algemene maatregel van bestuur beperkingen kan stellen aan het gebruik van de gegevens.

Het probleem is echter dat ik op dit moment een inbreuk op mijn persoonlijk levenssfeer moet dulden, terwijl er eveneens op dit moment noch in een wet in formele zin, noch in enige lagere regeling minimumwaarborgen zijn tegen misbruik, met name door inlichtingendiensten. Dit is in strijd met de jurisprudentie van het Europees Hof voor de Rechten van de Mens.

3.2. Legitimiteit van het doel

Verweerder stelt dat er een afweging moet worden gemaakt tussen het recht op bescherming van de persoonlijke levenssfeer en het belang van een accurate en effectieve reisdocumentenadministratie.

De beperkingsgronden van artikel 8 EVRM zijn echter limitatief opgesomd. Het voorkomen van fraude met, en misbruik van reisdocumenten kan geschaard worden onder de begrippen nationale veiligheid, openbare veiligheid en het voorkomen van wanordelijkheden en strafbare feiten.

Het opzetten van een databank die met het oog op snelle dienstverlening aan de burger 7 dagen per week, 24 uur per dag toegankelijk is, kan echter niet geschaard worden onder een van de legitieme belangen uit artikel 8 EVRM en kan dus niet gebruikt worden om een inbreuk te rechtvaardigen.

3.3. Marge

De jurisprudentie laat aan de verschillende staten die partij zijn bij het EVRM een zekere marge bij het beoordelen welke maatregelen noodzakelijk zijn in een democratische samenleving. De grootte van deze marge is onder meer afhankelijk van de mate van consensus over de waarde van de te beschermen belangen.

De staten die partij zijn bij het EVRM zijn ook allemaal partij bij het Verdrag van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens. Artikel 5 van dit laatste verdrag bepaalt:

Persoonsgegevens die langs geautomatiseerde weg worden verwerkt, dienen:

- a. op eerlijke en rechtmatige wijze te worden verkregen en verwerkt;*
- b. te worden opgeslagen voor bepaalde en legitieme doeleinden en niet te worden gebruikt op een wijze die onverenigbaar is met die doeleinden;*
- c. toereikend, ter zake dienend en niet overmatig te zijn, uitgaande van de doeleinden waarvoor zij worden opgeslagen;*
- d. nauwkeurig te zijn en, zo nodig, te worden bijgewerkt;*
- e. te worden bewaard in een zodanige vorm dat de betrokkene hierdoor niet langer te identificeren is dan strikt noodzakelijk is voor het doel waarvoor de gegevens zijn opgeslagen.*

Artikel 6 van het verdrag kent nog een verdergaande bescherming toe aan bepaalde categorieën van 'gevoelige' gegevens, waaronder gegevens die het ras of de gezondheid betreffen. Tenslotte voorziet artikel 9 van het verdrag in een uitputtende regeling van uitzonderingen en beperkingen.

Hieruit volgt dat er voor wat betreft persoonsgegevens slechts een kleine beoordelingsmarge is.

3.4. Proportionaliteit

Een inbreuk moet, om gerechtvaardigd te kunnen worden, evenredig zijn met het belang dat de staat met die inbreuk beoogt te beschermen.

Vingerafdrukken en foto's bevatten unieke informatie over de betreffende persoon waardoor hij of zij in een breed scala aan omstandigheden geïdentificeerd kan worden (S. en Marper, par. 84).

Uit een foto kan rechtstreeks iemands ras worden afgeleid.

Uit vingerafdrukken kan in sommige situaties rechtstreeks informatie over iemands gezondheid worden afgeleid. Mocht dit feit betwist worden, dan ben ik bereid om, zo de rechtbank dit nodig vindt, dit feit te bewijzen door middel van aanvullende literatuur en/of een deskundige.

Een biometrisch reisdocument kan door middel van speciale apparatuur op (korte) afstand worden uitgelezen, ook zonder dat de houder van het document hieraan meewerkt, of zich er zelfs maar van bewust is. Als politieagenten in burger met zulke apparatuur langs of door een demonstratie lopen, kunnen de deelnemers aan die demonstratie hun anonimiteit verliezen.

De plicht om vingerafdrukken af te staan is ook stigmatiserend. Tot voor kort gold deze namelijk alleen voor verdachten die in verzekering werden gesteld wegens een ernstig misdrijf of die weigerden zich te identificeren. Nu worden alle burgers als verdachten behandeld.

Als een biometrische databank gekoppeld wordt aan bewakingscamera's in openbare ruimten, kan iemand wiens gezicht zich binnen het bereik van een van die camera's bevindt automatisch worden herkend en gevolgd.

Een databank zou bovendien een ideaal doelwit worden voor identiteitsdieven. Er zullen weliswaar beveiligingsmaatregelen genomen worden, maar deze zullen niet waterdicht zijn.

Tenslotte zou de databank voor nog meer doelen gebruikt kunnen worden. Daarvoor is een wetswijziging nodig, maar tegen zo'n wijziging kan een belanghebbende niet in beroep gaan.

Het afzien van een paspoort of identiteitskaart is geen alternatief. Er zijn steeds meer situaties waarin een burger zich moet identificeren om van een dienst gebruik te kunnen maken. Wie geen identiteitsbewijs heeft, wordt volledig uitgesloten van het economische en maatschappelijke verkeer. Het niet kunnen tonen van een identiteitsbewijs aan een opsporingsambtenaar is bovendien strafbaar.

Het belang dat hier tegenover staat is veel kleiner. Fraude met identiteitsbewijzen komt niet vaak voor en kan, als het gebeurt, in de meeste gevallen achteraf ontdekt worden. Voor enkele mensen die slachtoffer zouden kunnen worden van identiteitsfraude wordt nu een inbreuk gemaakt op de rechten van miljoenen mensen.

De inbreuk is daardoor niet evenredig met het belang dat daarmee gediend wordt.

3.5. Subsidiariteit

Wil een inbreuk gerechtvaardigd zijn, dan moet deze ook werkelijk geschikt en noodzakelijk zijn om een legitiem belang te beschermen. Dit is slechts het geval als dat belang niet met minder vergaande middelen beschermd kan worden.

Het aanvragen van een reisdocument op naam van iemand anders kan, ook zonder biometrische databank, voorkomen worden door:

- een nieuw reisdocument voor een minderjarige alleen uit te geven met medewerking van een van de wettelijk vertegenwoordigers,
- een reisdocument voor een volwassene alleen uit te geven indien de aanvrager een eerder uitgegeven maar nog steeds geldig reisdocument kan overleggen, en
- indien de aanvrager beweert zijn reisdocument te hebben verloren, nader onderzoek te doen.

Dubbele aanvragen kunnen worden voorkomen door alle aanvragen - maar niet de biometrische gegevens - centraal te registreren en een nieuwe aanvraag niet in behandeling te nemen, zolang er nog een andere aanvraag op dezelfde naam in behandeling is.

Gebruik van reisdocumenten door anderen kan worden voorkomen door - zoals al heel lang gebeurt - het gezicht van de gebruiker te vergelijken met de pasfoto op het reisdocument zelf.

Eventuele *look alike*-fraude kan in sommige gevallen voorkomen worden door de vingerafdrukken van de gebruiker van het document te vergelijken met de vingerafdrukken die op het reisdocument zelf zijn opgeslagen. Daar is geen databank voor nodig.

Toch werkt deze methode alleen maar als een getrainde beambte zich ervan verzekert dat de vingerafdrukken echt zijn, en bij voorbeeld geen rubberen kopieën van de vingerafdrukken van iemand anders. Een databank brengt daar geen verandering in.

Bovendien beschikken degenen die het meeste belang hebben bij een betrouwbare vaststelling van iemands identiteit, zoals notarissen en bankbedienden, niet over de apparatuur om een reisdocument uit te lezen en iemands vingerafdrukken te controleren. Vingerafdrukken in een reisdocument maken *look alike*-fraude in de praktijk dus niet moeilijker.

Het afnemen, verwerken en opslaan van vingerafdrukken is dus slechts in zeer beperkte mate geschikt en zeker niet noodzakelijk om fraude met en misbruik van reisdocumenten te voorkomen. Het opnemen van biometrische gegevens in een centrale databank is zelfs in het geheel niet geschikt en dus ook niet noodzakelijk om fraude met en misbruik van reisdocumenten te voorkomen.

Mijn conclusie is dat zowel het afnemen van vingerafdrukken als het opslaan van biometrische gegevens in een databank elk afzonderlijk ongerechtvaardigde inbreuken op artikel 8 EVRM zijn.

Hoogachtend,

[ondertekening]

P. Deutekom