Pleitnota zitting Hof van justitie van de Europese unie 06-11-2014.
Gevoegde zaken C-446/12 – C449/12 Willems e.a.

Geacht Hof;

Als gevolg van het intrekken van vraag 1 door de RvS zou de verkeerde conclusie getrokken kunnen worden, dat het Hof in haar oordeel Schwarz / Stad Bochum zich op het punt van de erkende rechten van de artikelen 7 en 8 van het Handvest en 8 EVRM, ten gunste van de verordening heeft uitgesproken, terwijl zij dat feitelijk in het midden heeft gelaten. In rechtsoverweging 39 wordt door het Hof beschreven dat de waarborgen ten opzichte van de mensenrechten in die behandeling maar zijdelings aan bod zijn gekomen, ze zijn door Schwarz niet eens aangevoerd. Het Hof wordt daarmee door de RvS een stelling aan gewreven die zij helemaal niet heeft betrokken. Ik vindt dat zeer kwalijk.

U heeft ons verzocht om, in verband met de intrekking door de RvS van vraag 1, ons te beperken tot het gebruik van de opgeslagen gegevens, zoals dat geregeld is in artikel 4 lid 3 van de verordening en artikel 1 lid 2 niet langer te behandelen.
De aanhef van vraag 2 stelt echter voorop en gaat ervan uit, dat de geldigheid van de verordening onbetwist is. Gezien het voorgaande en nu er onvoldoende garanties tegen een onrechtmatig gebruik van de biometrische gegevens in de verordening zijn voorzien, moet de verordening zelf ter discussie blijven.
Als gevolg van het uitgangspunt van vraag 2 maar ook uit het oogpunt van een effectieve rechtspraak kan naar mijn mening art. 1 lid 2 niet geheel buiten beschouwing blijven.

Terug naar artikel 4 en de vraag of er ook ander gebruik van de gegevens mag worden gemaakt, een vraag waar natuurlijk ook mee samenhangt of gegarandeerd is dat derden en niet geautoriseerde personen deze gegevens niet kunnen benaderen en misbruiken.
Volgens de verordening moeten de technische middelen welke voor de opslag van de gegevens in het paspoort worden gebruikt, aan de hoogste eisen voldoen. Algemeen wordt beseft dat een aantal biometrische gegevens gevoelig zijn voor misbruik.

Ook uw Hof steunt dat en heeft dat benadrukt onder rechtsoverweging 55. De wetgever dient zich ervan te vergewissen dat er specifieke garanties bestaan voor een doeltreffende bescherming van deze gegevens tegen oneigenlijke verwerking en onrechtmatig gebruik.
Ook uit Marper versus Verenig Koninkrijk blijkt dat een overheid gevoelige biometrische gegevens niet toegankelijk mag maken voor onrechtmatige verwerking zowel niet door haarzelf alsook niet door derden. Dat blijkt verder uit de verschillende rechtsoverwegingen van uw Hof van 54 tot 62 waarbij vooral rechtsoverwegingen 56 en 60, vraag 2 van de RvS al redelijk beantwoorden.
De RvS had beter vraag 2 ingetrokken in plaats van vraag 1.

Neen; een ander gebruik dan waarvoor de gegevens zijn afgestaan, dus exclusief voor de doeleinden van het paspoort, een reisdocument, is niet geoorloofd.
Het Hof heeft daarbij de vingerafdrukken benoemd en de digitale foto een beetje buiten de boot laten vallen terwijl daar wel dezelfde argumenten voor gelden. Rechtsoverweging 56 en 60 wijzen erop dat uitdrukkelijk gepreciseerd is dat vingerafdrukken alleen mogen worden gebruikt voor het verifiëren van de authenticiteit van het paspoort en de identiteit van de houder en alleen mogen worden bewaard op het paspoort zelf en dus exclusief in het bezit en onder controle van de paspoorthouder blijven.

De conclusie moet dus zijn dat de erkende rechten van het Handvest en EVRM vereisen dat de paspoorthouder en bezitter van deze biometrische gegevens, zelf de regie over zijn gegevens heeft en houdt.
De vraagstelling van vraag 2 was dus door uw Hof al min of meer beantwoord en behoeft alleen nog een aanvulling met betrekking tot het gebruik van de opgeslagen digitale foto, dus niet van de fysieke afdruk. De digitale foto, welke in dit kader dezelfde status dient te hebben als de vingerafdrukken, waarover later meer.

Het Hof beschikte in haar oordeel Schwarz / Stad Bochum nog niet over de uitgebreide schriftelijke gegevens en bewijsstukken die door ons zijn ingebracht en die onomstotelijk aantonen dat de gekozen praktische c.q.

technische invulling van deze eis van de verordening van een minderwaardige niveau is gebleken.
Er is daardoor een sterke behoefte aan een verdere toelichting door het Hof met betrekking tot de geldigheid van de verordening.

De erkende rechten van de artikelen 7 en 8 van het Handvest en 8 EVRM kunnen eenvoudigweg door de gekozen methode niet gewaarborgd worden. De verordening wordt daardoor ongeldig en artikel 1 lid 2 komt toch weer om de hoek kijken.
De toegang tot de gevoelige biometrische gegevens, zonder goedkeur van de drager, is met de op afstand uitleesbare chip ingebakken in de gekozen opslagmethode. Daardoor en omdat samen met de verificatieplicht, waarbij de gegevens onversleuteld ter beschikking van de controleur moeten worden gesteld, staat vast dat een deugdelijke vorm van, integriteit, authenticiteit en de vertrouwelijkheid van de gegevens, zoals die door de verordening verlangd worden, niet kan worden gerealiseerd.

De bescherming die de verordening zegt te bieden en waar het Hof in haar eerdere uitspraak van uitgaat is daarmee illusoir.

De bankenwereld kent aanzienlijk veiligere methodes. Die mogen misschien duurder en gecompliceerder zijn, maar dat mag geen argument zijn om deze waarborgen te ondergraven en de risico's op zijn beloop te laten. Om de verordening in overeenstemming met de erkende rechten van de artikelen 7 en 8 van het Handvest en 8 EVRM te brengen en een veilige opslag te garanderen, moeten in de verordening aanzienlijk meer concrete en daadwerkelijke waarborgbiedende eisen aan de veiligheid van het opslagmedium worden gesteld.
Om te beginnen zou de vraag moeten worden gesteld wat moet worden verstaan onder de "hoogste veiligheidseisen" als bedoeld in artikel 1 lid 2 ? Daarnaast; wat zijn de consequenties voor de plicht onder de verordening om vingerafdrukken op het paspoort op te nemen wanneer niet de hoogste veiligheidseisen kunnen worden gegarandeerd ? Welke zijn de "specifieke garanties" "voor een doeltreffende bescherming van gegevens tegen oneigenlijke en onrechtmatige verwerkingen" ?

Hoe moet de wetgever zich ervan te vergewissen dat daaraan wordt voldaan en welke gevolgen de constatering dat daaraan niet wordt voldaan kan hebben voor de plicht vingerafdrukken op te nemen ?

Terug naar vraag 2. Nu ik met enige regelmaat mij actief in afpersingsgevaarlijke omstandigheden bevindt klemt dit voor mij extra met het oog op art 4 lid 3 van de verordening, waarbij onder b de identiteit van de houder door middel van direct beschikbare vergelijkbare kenmerken moet kunnen worden vastgesteld als het over leggen van een paspoort of andere reisdocumenten wettelijk vereist is. Dat heeft niet alleen gevolgen voor het Schengen-gebied, maar op veel meer dan dat. Een paspoort wordt wereldwijd gebruikt.

Biometrie is niet nieuw. Lengte, gewicht, kleur van haren en ogen van een persoon en een foto worden al langer in het paspoort toegepast.
In Nederland is dat altijd meer dan voldoende gebleken. Look alike is een miniem marginaal randverschijnsel. Het Nederlandse paspoort stond wereldwijd als zeer betrouwbaar en degelijk bekend.
Nieuw zijn de toevoeging van een Radio Frequency Identification chip (RFID), een extra digitale foto en vingerafdrukken.

Chip en digitale foto hebben als probleem dat deze eenvoudig zijn te gebruiken in software welke is ontwikkeld voor het automatisch herkennen en lokaliseren van personen.
Een alles omvattend controlesysteem wordt daarmee mogelijk gemaakt en wordt thans, als we niet opletten, steeds verder uitgerold. Daarbij is voor het identiteitsbewijs en het paspoort een sleutelrol weggelegd.
Een persoon die uiteindelijk continu in de gaten gehouden en gecontroleerd wordt, gaat zijn gedrag daarop aanpassen en is niet langer een vrij mens.
De beste term waar dit onder valt is “Orwelliaans” en het is vergelijkbaar met de gele oorlabels die door het vee in de wei worden gedragen.

In één woord “Mensonwaardig”.

De opname van vingerafdrukken is daarbij bovendien ronduit gevaarlijk nu deze over de gehele wereld als wettig en overtuigend bewijs in juridische procedures kunnen worden gebruikt.
Door de eenvoudige toegang voor derden, ook een ongeoorloofde en kwaadaardige toegang, wordt de regie over de eigen persoonlijke gegevens van de persoon ontnomen en geforceerd in handen gelegd van een Staat en van andere al dan niet betrouwbare mensen en organisaties. Corruptie en afpersing zijn in sommige landen een serieus probleem dat door deze algemeen geldende verordening niet genegeerd mag worden.

Het is mij niet duidelijk of de versleutelingcodes nu al met enkele "bevriende Staten" worden gedeeld. Voor een werkend systeem zal dat uiteindelijk wel moeten gebeuren. Dat betekent in de praktijk dat deze landen de gegevens, waarvan wij besloten hebben om ze niet op te slaan, juist wél kunnen opslaan. De heer Snowden heeft aangetoond dat alle argumenten tegen enige vorm van digitale opslag alleen nog maar krachtiger zijn geworden en nog steeds gelden.
Daarnaast onze regering staat gegevens c.q. bevoegdheden af aan andere Staten. Elke gegevensuitwisseling moet daarom gepaard gaan met een optimale kwaliteit van zowel ons openbaar bestuur, als ook van het openbaar bestuur van deze vreemde mogendheden en heel belangrijk, het moet worden gecombineerd met het afleggen van verantwoording aan de samenleving.
Om het met hoogleraar Ankersmit te zeggen: *Dit betekent dat we altijd de absolute zekerheid moeten hebben dat publieke bevoegdheden corresponderen met de verplichting tot het publiekelijk afleggen van verantwoording. Geen bevoegdheden zonder verantwoordelijkheden, en geen verantwoordelijkheden zonder bevoegdheden.*
Dat is de alfa en omega voor alle goed bestuur.

De verordening mist dit "publiekelijk afleggen van verantwoording" en kan die ook niet realiseren. De drager van het paspoort mist de kracht en de bevoegdheid om, zeker bij Staten buiten het Schengen gebied, bij misbruik van zijn gegevens deze Staten ter verantwoording te kunnen roepen.

Laat mij daar een voorbeeld van geven. In mijn schriftelijke reactie haal ik, voor mij persoonlijk belangrijke derde wereldlanden als gevaarlijk aan. Maar zelfs als we als voorbeeld de verenigde staten van Amerika nemen, waar we nu al alle gegevens, dus ook de digitale foto en vinger afdrukken, uit het paspoort mee delen, blijkt dat dit niet risicoloos is.

Uit de geschiedenis weten we dat sterke Staten soms verschrikkelijk ontsporen. Wie had, voor de vaststelling van de verordening kunnen voorzien dat deze hoog ontwikkelde Natie zich heden ten dage steeds verder verwijderd van de ons bekende internationale en erkende rechtssystemen. Ze weigeren dat ook hen de maat genomen wordt.

De drager van een misbruikt paspoort staat tegen hen volkomen machteloos. Onder het mom van "Terrorisme " worden daar zonder enige vorm van proces, mensen onbeperkt opgesloten of zelf vermoord. Je zult maar Mohamed heten en jouw vingerafdrukken en foto vertonen toevallig enige gelijkenis met de, bij het CIA bekende, afdrukken van een gezochte terrorist. Met een vastgestelde foutmarge van rond de 20/30 % geen echt onwaarschijnlijk scenario.
Better safe than sorrow, Guantanamo Bay maakt alle verschrikkingen duidelijk die vervolgens over deze onschuldige Mohamed kunnen worden uitgestort en dat zonder dat het locale rechtssysteem corrigerend kan ingrijpen.

Hoe hebben wij mensen zo ver kunnen afdalen op de ladder van de beschaving dat wij het nu accepteren dat zonder enige vorm van proces een of andere laffe snotneus ergens in een container in Amerika met een kopje koffie in de hand op een knopje drukt, waardoor een einde aan een of meerdere mensenlevens wordt gemaakt en waarbij onschuldigen als "collateral damage"worden betiteld.

Dit voorbeeld uit Amerika maakt duidelijk dat het zaak is dat een ongebreidelde toegang tot de opgeslagen gegevens coute que coute moet worden voorkomen. Het moet onmogelijk zijn om tegen de wil van de paspoorthouder in, deze gegevens te lezen en te ontvreemden.
Als dat niet kan dan moeten we niet aan deze biometrie beginnen.

Rechtsoverweging 55 van uw Hof geeft klip en klaar aan dat de wetgever zich ervan dient te vergewissen dat er specifieke garanties moeten zijn voor een doeltreffende bescherming van de gegevens tegen oneigenlijke en onrechtmatige verwerkingen.
Het is gebleken dat met deze verordening in de hand; de verschillende regeringen dat uitdrukkelijk niet hebben gedaan.
Voor het gemak van controlerende instanties negeert men het probleem en deze uiterst noodzakelijke bescherming kan dus niet aan hen worden toevertrouwd en overgelaten.
Het zal in de verordening zelf geregeld moeten zijn.

Afsluitend:
In antwoord op vraag 2 van de RvS.
Klip en klaar, een ander gebruik dan waarvoor de gegevens zijn afgestaan, dus exclusief voor de doeleinden van het paspoort, een reisdocument, is niet geoorloofd.
Verder zal de gelijkschakeling van de digitaal, in het paspoort, opgenomen foto met de vingerafdrukken tot uitdrukking moeten komen om zo de geschetste Big Brother ontwikkeling, in ieder geval niet langs deze weg mogelijk te maken.
Laat de politiek dat maar rechtstreeks met haar kiezers uitmaken en niet via deze achterdeur.

Daarnaast; weliswaar zou het een antwoord zijn op de ingetrokken vraag 1 maar het bewijsmateriaal is onomstotelijk en een vaststelling door uw Hof, dat de mensenrechten in deze niet voldoende worden gerespecteerd, ligt in uw lijn en zou voor de hand liggen.
Het zou uit het oogpunt van een efficiënte rechtspraak, een gang naar het EVRM kunnen besparen. Ik heb al vier en een half jaar geen paspoort meer.

De politiek en de ambtenarij hebben slecht werk geleverd en moeten opnieuw aan het werk.

Dank voor uw aandacht,
W.P. Willems