DE INHOUDELIJKE

MOTIVERING

INHOUDSOPGAVE

Bladzijde

VOORWOORD

INLEIDING

0. Aanvullende gronden 1
1. De buitenwerking stelling van een Onrechtmatige Wetgeving 2
   1.1. Belang van de zaak 2
   1.2. Toelichting 3
2. Vraagtekens bij de inwerkingstelling van de Nieuwe PaspoortWet 7
   2.1 Onverbindendheid 7
   2.2 Een verder onrechtmatig overheidshandelen 8
   2.3 Oordeel over de onrechtmatigheid 9
   2.4 De geloofwaardigheid 10
   2.5 Concluderend 10
3. Toegang tot de burgerlijke rechter 11
   3.1 Ontvankelijkheid 11
   3.2 Eigen belang 11
4. Grieven 12
   4.1 RFID-chip 13
   4.2 De digitale gezichtsscan 14
   4.3 Veiligheidsdiensten 15
      4.3.1 Veiligheidsdiensten kunnen aan gegevens komen 15
         4.3.1.1 Databanken biometrische gegevens 15
      4.3.2 Het gevaar is dichterbij dan iemand zich realiseert 16
      4.3.3 Inzage bij Nederlandse wetgeving is geregeld 16
      4.3.4 Tussenbalans 16
   4.4 Nadeelcompensatie 17
      4.4,1 Toelichting 17
      4.4,2 Tegenwerking wetgever en Nederlandse overheid 19
         4.4.2.1 Niet-wetgeven 19
      4.4.3 Speciaal en abnormaal nadeel 20
      4.4.4 Aansprakelijkheid overheid 21
      4.4.5 Schuldvordering 21

4 Grieven

Ik heb nog steeds belang bij de onderhavige zaak. Ook nu er geen sprake meer zou zijn van de afgifte van vingerafdrukken voor een ID-Kaart. Een wetswijziging is een feit. Op 17-01-2014 was dit te lezen in het Staatsblad. Het gerechthof verbood verder ook de centrale databank. [70]

In dit geval meen ik nu als eiser ook in mijn recht te staan. Te weten: -

1. Een toekomstig gevaar t.a.v. de op afstand uit te lezen RFID-chip. Waarom niet met het blote oog uitleesbaar? Het roept ongetwijfeld een vraag op. Maar die optie inbouwen gebeurde met een reden. Totaal buiten-proportioneel voor het doel van identiteitsbewijzen. Een gevaar nu. Niet alleen voor paspoorten. Ook nog steeds voor ID-Kaarten. Afgezien van de gewijzigde wet.
2. De digitale gezichtsscan die als onderdeel vormt van de RFID-chip zorgt voor verwarring. Het wordt nu nog decentraal opgeslagen.
3. Veiligheidsdiensten komen nu onterecht aan iemands gegevens. [71]
4. Nadeel-compensatie staat ook centraal als belang. Ik wilde de procedure uitzitten. En dat is op 1 manier alleen mogelijk. Een zaak moet behandeld worden. Nederlands recht biedt die mogelijkheid niet. Het is 3 jaar uitgesteld. Met schade als gevolg.
5. Het "Fair trial" beginsel wordt zo bekeken met voeten getreden. En dat moest volgens art. 8:69 Awb een ander verloop krijgen.[72]

---

[70] Vzr. HR 's-Gravenhage 18 februari 2014, Zaaknummer: 200.087,096//01 (stichting Privacy First.).

[71] de landsadvocaat stelt:"Vingerafdrukken zullen aan de inlichtingendiensten AIVD en MIVD moeten worden verstrekt. Informatieverstrekking aan deze diensten is geregeld in artikel 17 van de Wet op de Inlichtingen- en veiligheidsdiensten. Dat gold vóór inwerkingtreding van delen van de gewijzigde Paspoortwet. Het wordt met de gewijzigde Paspoortwet niet anders. De vermelding in artikel 4b lid 2 sub d Paspoortwet ("staatsveiligheid") is ingegeven door overwegingen van transparantie."
(Bron: Conclusie van Antwoord in de Paspoort zaak van Privacy First d.d. 28 juli 2010, par. 2.17; woordelijk herhaald in o.a. de verweerschriften van de Staat in de Paspoortzaken van Van Luijk d.d.29 okt.2010& 10 juni 2011 respectievelijk par.3.17 & 5.8) en Deutekom d.d. 23 nov. 2010, par. 4.17.)

[72] Art. 8:69 Awb. is zeer kort samengevat bepalend. Deze bepaling luidt als volgt: '1 De rechtbank doet uitspraak op de grondslag van het beroepschrift, de overgelegde stukken, het verhandelde tijdens het vooronderzoek en het onderzoek ter zitting. 2 De rechtbank vult ambtshalve de rechtsgronden aan. 3 De rechtbank kan ambtshalve de feiten aanvullen. 'De actieve instelling van de rechter betekent dat zij de verplichting heeft om zich actief met het proces bezig te houden om een aanvaardbaar resultaat te bereiken. Een taak van de Rechter feitelijk. {Momenteel lopen zaken nu toch anders. Een beoordeling in 1e aanleg van een gerechtelijke procedure bleef uit. Nota bene ten aanzien van 2 beroepschriften.}

4.1. RFID-chip

De op-afstand-uitleesbare RFID-chip is ronduit een gevaarlijke overheidsdaad. Vooral vanwege de risico's van identiteitsdiefstal. Nota bene op afstand en zonder dat de betrokken burger het merkt. Het zich überhaupt ooit op dat moment bewust zal zijn. [73]

Gebruik van de RFID-chip is derhalve disproportioneel te noemen.

Een functie van een ID-kaart of een paspoort heeft uitsluitend tot doel om het gemeenschappelijke identiteitsbeleid te verbeteren. Routinematige toegang tot Reisdocumenten door onbevoegden is niet in overeenstemming met dit doel. Het is feitelijk verboden.[74]

Artikel 13 van Richtlijn 95/46/EC geeft in deze situatie ondubbelzinnig duidelijkheid. Toegang kan niet stelselmatig worden verleend. Maar uitsluitend op ad-hoc basis, in specifieke omstandigheden en mits ook passende garanties worden geboden.

Toegang tot reisdocumenten kan alleen worden verleend voor acties die met de doelstelling van identiteitsfraude te verenigen is.

Op het moment kan elke idioot met ICT-kennis gegevens uitlezen.

Het plaatsen van een RFID-chip heeft nu negatieve consequenties. Voor gedetailleerde achtergrond informatie verwijs ik verder.[75]

Kortom: " Een papieren paspoort had meer opgeleverd. Zeker tegen deze achtergrond." Sprake is van gevaar op een gerichte beroving. En erger. [76]

---

[73] Totdat de burger in de problemen komt en aan zijn lot wordt overgelaten. Zie voetnoot 10 op blad 2.

[74] Het publicatieblad van "de Europese Unie"d.d. 23-07-2005 aangaande de Europese toezichthouder Peter Hustinx voor de gegevensbescherming gelet op doelbinding, bladzijde C181/17, kopje 3.2.

[75] Ik verwijs onder andere naar de bevindingen van de Liga.(zie bladzijde 39 van mijn beroepschrift ingediend op 09 mei 2011 (deel 2 van dit beroepschrift repliek: omtrent de juridische kant van de zaak). Alsmede gelet op deel 1 van datzelfde beroep dossier: omtrent de ontstane situatie, de bladen 9 en 22).

[76] Zie pagina 24 van mijn beroepschrift ingediend op 09 mei 2011.(deel 1 van dit beroepschrift dossier: omtrent ontstane situatie). En deel 2 van datzelfde beroepschrift repliek: "pagina 39, punt 40 en verder.

4.2. De digitale gezichtsscan

De Nieuwe Paspoortwet bevat nog steeds bepalingen waartegen ik als burger met de onderhavige procedure opkom. Ik word geconfronteerd met de afname en opslag van mijn biometrische gegevens: "Nu feitelijk dus ook nog van een digitale gezichtsscan."

Het doel van de uitleesbare chip is vaag? Dat is voorlopig gissen. In elk geval niet verenigbaar met de aanvankelijke doelstelling.

Mogelijke intelligence-doeleinden van biometrie liggen op de loer.

In dit verband constateer ik dat van "function creep" sprake is.

Voor handhaving van gebiedsverboden wil de VVD in Amsterdam camera's gaan inzetten. Dit laat de partij op haar website weten. [77] Het doel is om te onderzoeken of "gezichtsherkenning" via intelligente camera's bruikbaar is om overtreders aan te houden.

Een gezichtsscan wordt dus gebruikt voor opsporingsdoeleinden.

Op zich een voorbeeld van toekomstig gebruik van gezichtsscans. Voor het misbruik van vingerafdrukken gold dat immers net zo. [78]

Feitelijk is de RFID-chip daarvoor op reisdocumenten neergezet.

Ik verzet mij derhalve tegen de opname van een digitale gezichtsscan in een ID-kaart. Zeker nu sprake is van misbruik.

Het eerste doel (identificatie) voldoet beter met een gewone foto.

Kortom: De gezichtsscans gebruikt men nu al voor opsporing. Het wordt voor burgers onmogelijk te bepalen wie persoonlijke informatie te zien krijgt en hoe die informatie zal worden gebruikt. Heel ongewoon: "een gezichtsscan is alleen verkregen voor een strikt omschreven doel".

---

[77] http://vvdamsterdam.nl/article/4633/Gebiedsverboden-handhaven-door-slimme-cameras-met-gezichtsherkenning/

[78] Zie beroepschrift 22-03-2012: de punten 2.1.2 (blz. 4), 2.1.11 (blz. 23) en punt 5.2.2.1 op pagina 38.

4.3. Veiligheidsdiensten

Een belangrijk onderwerp is tot nu toe onderbelicht gebleven: "Het gebruik van gevoelige persoonsgegevens door geheime diensten."

Het draait om digitale gezichtsscans en vingerafdrukken die via paspoorten en identiteitskaarten in databanken terechtkomen. Momenteel bevinden die databanken zich bij de gemeenten en bij de paspoortfabrikant in Haarlem (Morpho. Voorheen Sagem).

In de toekomst is onduidelijk wat met die gegevens wordt gedaan.

Naar aanleiding hiervan merk ik het volgende op: -

4.3.1 Veiligheidsdiensten kunnen aan gegevens komen

4.3.1.1 Databanken biometrische gegevens

De gegevens op RFID-chips in reisdocumenten kunnen worden gebruikt voor andere doeleinden. Bijvoorbeeld door minder vriendelijke regimes. Een land daarvan is Amerika. In dat land heeft de FBI het plan om in 2015 een volledige gezichtherkenningsdatabase operationeel te hebben.

In die database zitten nu al meer dan 100 miljoen individuele gegevens.

Het is zo ontworpen dat het meerdere vormen van biometrische gegevens kan bevatten. Denk daarbij aan: "palmafdrukken, irisscans, vingerafdrukken en gezichtsscans". Al deze gegevens van een individu worden gekoppeld aan: "naam, adresgegevens, leeftijd en al het andere". Op zich gaat het om –de Next Generation Indentification database–".

Een geheim project zo blijkt uit documenten waar de Amerikaanse burgerrechten "Electronic Frontier Foundation" achter wist te komen. [79]

Toegang tot deze databank is geregeld voor 18.000 opsporingsdiensten.

---

[79] https://www.security.nl/posting/384524/'FBI+wil+52+miljoen+foto's+voor+gezichtsherkenning

4.3.2 Het gevaar is dichterbij dan iemand zich realiseert

Nederlandse burgers kunnen zich zorgen maken. Momenteel bevinden deze databanken zich dus ook nog steeds bij de gemeenten en bij de paspoortfabrikant in Haarlem (Morpho, voorheen Sagem). In de toekomst ongetwijfeld naderhand ook elders. Uiteindelijk wereldwijd.

Op termijn zullen de vingerafdrukken en gezichtsscans wellicht tot in de verste uithoeken van de wereld te vinden zijn. Niet alleen in de databanken van "bondgenoten" Maar ook in de databanken van landen waarmee die bondgenoten op hun beurt weer (al dan niet geheime) uitwisselingsverdragen hebben gesloten.[80] En daar is even geen zicht op.

Nog afgezien daarvan: "Morpho" staat op Amerikaans grondgebied. [81]

De Nederlandse overheid wil nu zelf weer een databank verzorgen. [82]

4.3.3 Inzage bij Nederlandse Wetgeving is geregeld

In een aantal rechtszaken tegen de Nieuwe PaspoortWet sprak de landsadvocaat zich daar helder over uit. Zie voetnoot 71 op pagina 12.

Veiligheidsdiensten zijn gewoon bevoegd om die gegevens op te vragen!

4.3.4 Tussenbalans

Uit deze grief blijkt dat persoonlijke gegevens als gezichtsscans niet noodzakelijk zijn voor identificatie. Er wordt misbruik van gemaakt. Teveel mensen hebben inzage. Bovendien op afstand. Dat is niet veilig. En is ook wettelijk verboden. Het EU-hof sprak zich er eerder over uit. [83]

---

[80] Zie beroepschrift ingediend op 09 mei 2011, Punt 3.3.- "Het verstrekkingsregiem" - pagina 6 t/m 8 .(deel 1 van dit beroepschrift dossier: omtrent ontstane situatie).

[81] Ministers in een Europees land hebben zich te voegen naar Amerikaanse wetgeving. (Voetnoot 6).

[82] http://platformburgerrechten.nl/2014/02/27/gezichtsherkenning-biometrie-voor-dummies/

[83] http://www.elsevier.nl/Europese-Unie/nieuws/2014/4/Opslaan-telecomgegevens-mag-niet-meer-wat-nu-1499262W