

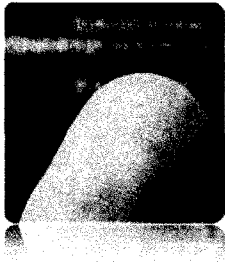
## Platform Bescherming Burgerrechten

HOME ARTIKELEN COLUMNS PLATFORM MAIL

Archief 2011 Archief 2010 Archief 2009

## De rekbare doelen van de vingerafdrukkendatabase

door Ronald Huissen



**Een jaar na de invoering van de nieuwe Paspoortwet geldt nog steeds de vraag: is de vingerafdrukkendatabase een opsporingsregister dat verkocht is als een anti-fraudemaatregel?**

Verantwoordelijke bewindslieden hebben van meet af aan gesteld dat de vingerafdrukkendatabase geen opsporingsregister is, maar een maatregel tegen identiteitsfraude met paspoorten.

Een jaar na de inwerkingtreding van de nieuwe Paspoortwet is er echter reden genoeg om aan te nemen dat dit in de praktijk anders zal uitpakken. De voorwaarden die worden gesteld aan gebruik van de databank voor opsporingsdoeleinden, blijken in de praktijk flinterdun te zijn.

Als hoofdreden voor het aanleggen van een vingerafdrukkenbestand stelde staatssecretaris Bijleveld (CDA) dat dit een maatregel is in de strijd tegen zogeheten lookalike-fraude met identiteitsdocumenten. Dit werkt als volgt: een fraudeur die een tweede paspoort aanvraagt onder de naam van een persoon op wie hij sterk lijkt qua uiterlijk, valt door een 'check' in het vingerafdrukkenbestand door de mand doordat de vingerafdruk van de fraudeur daar al in staat geregistreerd.

Het is echter onbekend hoe groot dit fraudeprobleem is. Cijfers over het aantal personen dat zich met deze praktijk bezighoudt, blijken bij navraag bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties niet te bestaan. Het ECID is het onderzoeksbureau en hulppunt van de Koninklijke Marechaussee dat zich bezighoudt met het controleren van reis- en identiteitsdocumenten voor zowel opsporingsinstanties als particulieren. Het laat via de persvoorlichting van de Marechaussee weten dat het de onderliggende data voor deze cijfers wel in huis heeft, maar deze niet gestructureerd over een bepaalde periode op een presenteerblaadje kan geven. Deze gegevens uitsorteren en ordenen uit de bulk data waarover het ECID beschikt, zou te veel tijd en mankracht kosten, aldus een perswoordvoerder.

*"Er is simpelweg gezegd dat 'dit van Europa moest', maar dat is gewoonweg niet waar"*

Dit leidt tot de conclusie dat er binnen de overheid nauwelijks of geen idee is van de hoeveelheid fraudeurs met een dubbel paspoort. Daarmee is niet alleen het effect van de database ontoetsbaar, maar belangrijker nog: het is niet mogelijk te bepalen of deze maatregel gerechtvaardigd is, wat geen rare vraag is aangezien heel paspoortdragend Nederland voor de aanpak van dit probleem zijn vingerafdrukken moet afstaan.

Vreemd genoeg is dit tijdens het wetgevingstraject niet ter sprake gekomen. SP-Kamerlid Ronald van Raak nam deel aan het Kamerdebat over de nieuwe Paspoortwet in november 2008 en zegt er het volgende over: "Het principiële debat over de rechtvaardiging van deze database is er niet geweest in de Kamer. Ik heb er wel op gehamerd, maar het onderwerp is niet van de grond gekomen.

Er is simpelweg gezegd dat 'dit van Europa moest', maar dat is gewoonweg niet waar. De vingerafdrukkendatabase is een beslissing van onze eigen regering, bovenop de vingerafdruk in het paspoort die Brussel voorschreef."



Ronald van Raak

## Nevenfuncties

Het bestrijden van fraudeurs met dubbele paspoorten is echter niet de enige functie van de database. De Paspoortwet beschrijft nog drie andere toegangswegen tot het vingerafdrukkenbestand. Ten eerste mogen de vingerafdrukken ook gebruikt worden om slachtoffers bij rampen en ongevallen te identificeren.

- december
- november
- oktober
- september
- augustus
- juli
- juni
- mei
- april
- maart
- februari
- januari

Qu



Het 'Platform Bescherming Burgerrechten' is door het Humanistisch Verbond opgezet. Meer hierover vindt u op de pagina 'Platform' boven in het menu.

De Paspoortwet begint echter pas te wringen bij de laatste twee leden van het artikel dat de toegang tot de database reguleert, artikel 4b. Deze twee leden stellen dat vingerafdrucken uit de database verstrekt mogen worden bij respectievelijk 'de opsporing en vervolging van strafbare feiten' en 'onderzoek naar handelingen die een bedreiging vormen voor de veiligheid van de staat en bevriende mogendheden'.

De verstrekking gebeurt aan de officier van justitie, in twee mogelijke gevallen. Het eerste is de identificatie van een verdachte wiens vingerafdrucken al eens eerder zijn afgenomen in een strafproces. Het andere is een onderzoek naar een misdrijf waarbij een voorlopige hechtenis van de verdachte is toegelaten.



De twee laatstgenoemde 'nevenfuncties' werpen een aantal principiële vragen op over de aard van het vingerafdruckenregister. Is dit in wezen nu een anti-fraudemaatregel of een opsporingsdatabank? En kun je zomaar de vingerafdrucken van miljoenen onschuldige burgers voor een reisdocumentenadministratie verzamelen om ze later te kunnen gebruiken voor strafrechtelijke doeleinden?

Dat laatste moet de vaste Tweede-Kamercommissie voor Binnenlandse Zaken en Koninkrijksrelaties zich ook afgevraagd hebben toen ze in december 2008 staatssecretaris Bijleveld een uitspraak van het EHRM (Europees Hof voor de Rechten van de Mens, zetelend in Straatsburg) voorlegde over een rechtszaak die opvallende raakvlakken heeft met de Nederlandse praktijk van vingerafdruckenopslag.

Deze zaak draaide om twee Britse burgers die hun vingerafdrucken hadden moeten afgeven als verdachten in een strafzaak. Deze vingerafdrucken werden opgeslagen in een justitiële databank. Toen de ene persoon werd vrijgesproken en de zaak tegen de andere werd geseponneerd, eisten beiden dat hun vingerafdrucken uit de databank werden verwijderd. Dit werd hun geweigerd en ze spanden vervolgens een rechtszaak aan tegen de Britse staat.

In deze zaak besliste het EHRM dat de opslag van vingerafdrucken gold als een inbreuk op iemands privéleven die slechts onder bepaalde omstandigheden, te weten een dringend maatschappelijk belang, gerechtvaardigd is. Het Hof stelde dat de Britse staat in dit geval geen onafhankelijke beoordeling had uitgevoerd waarmee de opslag van de vingerafdrucken van deze twee onschuldige personen gerechtvaardigd kon worden.

Met andere woorden: de staat had geen geldige reden aangevoerd om vingerafdrucken van onschuldige burgers op te slaan in de opsporingsdatabank. Dit leidde ertoe dat de twee personen door het Hof in het gelijk werden gesteld en hun vingerafdrucken uit de databank moesten worden verwijderd.

## Houdbaarheid

De Tweede-Kamercommissie vroeg of de nieuwe Nederlandse Paspoortwet door deze uitspraak niet in het geding kwam. De vingerafdrucken in de Nederlandse databank konden immers ook gebruikt worden voor justitiële doeleinden. De staatssecretaris verdedigde de houdbaarheid van de wet door te zeggen dat de insteek van de Nederlandse vingerafdrukkendatabase wezenlijk anders was.

Het ging volgens haar niet om een strafrechtelijk register, maar om een reisdocumentenadministratie. Dit neemt echter niet weg dat de database ook gebruikt kan worden voor strafrechtelijke doeleinden.

- Echter, stelde de staatssecretaris, een officier van justitie kan slechts in een beperkt aantal gevallen het vingerafdruckenbestand raadplegen. Deze toegang was volgens de staatssecretaris aan strenge regels gebonden, iets wat ze ook had aangegeven in het Kamerdebat over de Paspoortwet.

Over die regels verscheen begin dit jaar een interessante publicatie vanuit onverwachte hoek. De Arnhemse officier van justitie Hermans schetste in het juridische vakblad NJCM-Bulletin van januari 2010 een fictief praktijkvoorbeeld van een situatie waarin een officier van justitie de database kan raadplegen. De strenge regels die de staatssecretaris beschreef in haar commentaar op de uitspraak van het EHRM, vormen volgens Hermans in de praktijk nauwelijks een drempel. De voorwaarden voor een officier van justitie om toegang te krijgen tot de database bestaan uit de volgende eisen; er moet een gezichtsopname van de verdachte beschikbaar zijn, het geslacht van de verdachte moet bekend zijn en er moeten vingerafdrucken zijn gevonden.

### *'Het moet nog blijken hoe gretig officieren van justitie vingerafdrucken opvragen'*

Hermans stelt dat het opsporen van de dader van een 'doorsnee' winkeldiefstal in een kruidenierszaak in het centrum van Amsterdam al aan alle eisen voldoet om een officier van justitie toegang te geven tot het vingerafdruckenregister; er zijn hoogstwaarschijnlijk beelden van bewakingscameras beschikbaar waarop legio gezichten van winkelbezoekers voorkomen, naar aanleiding hiervan heeft de politie een redelijk idee van het geslacht van de dader en ook vingerafdrucken (of die nu van de dader zijn of van klanten) zullen ongetwijfeld op de plaats delict aanwezig zijn.

Aangezien winkeldiefstal onder een wetsartikel valt waarvoor voorlopige hechtenis is toegestaan, ziet de officier van justitie in zijn beschouwing geen reden waarom er geen vingerafdrukken verstrekt zouden worden.

De vraag is waar de database vaker voor gebruikt zal gaan worden. Het moet nog blijken hoe gretig officieren van justitie de vingerafdrukken in het kader van strafrechtelijk onderzoek opvragen. Als daar cijfers van zullen verschijnen, zullen deze echter niet te vergelijken zijn met statistieken over het primaire doel van de database; het bestrijden van fraude met identiteitsdocumenten. Die cijfers zouden er volgens het ministerie van Binnenlandse Zaken en de Marechaussee niet zijn.



Daar komt nog bij dat inlichtingendiensten als de AIVD bij wet niet verplicht zijn openbaar te maken hoe vaak en wanneer zij bijvoorbeeld telefoongesprekken aftappen of persoonlijk e-mailverkeer inzien. Dit zal ook voor het raadplegen van de vingerafdrukkendatabase gelden.

SP-Kamerlid Ronald van Raak stelt dat de praktijk moet uitwijzen hoe intensief de vingerafdrukkendatabase gebruikt zal gaan worden als opsporingsregister. Wel laat hij weten er allerminst gerust op te zijn: "Het hele probleem is dat er überhaupt is gekozen voor deze database. Vroeg of laat zal die gebruikt gaan worden als opsporingsregister, hoe dan ook. De voorwaarden tot toegang voor opsporing zullen steeds ruimer geïnterpreteerd worden onder druk van de samenleving, die eist dat criminelen opgespoord en berecht worden. Aangezien deze database al bestaat, is de stap om hem voor opsporingsdoeleinden te gebruiken een kleine. Op die manier zal dit vingerafdrukkenbestand zijn eigen vraag creëren."

De Paspoortwet zelf is bovendien min of meer hierop ingericht. De toegang tot de database voor opsporing is namelijk in lagere wetgeving geregeld, door middel van een zogeheten algemene maatregel van bestuur.

Quirine Eijkman, onderzoeker en docent terrorisme en contraterroreisme aan de Universiteit Leiden zei daar in september 2009 in het NRC Handelsblad het volgende over: "Voor justitie is dat handig, want om later alsnog de bevoegdheid tot opsporing te krijgen hoeft dan alleen die lagere wetgeving te worden aangepast en niet de Paspoortwet."

Op dit moment is het vingerafdrukkenbestand dus nog officieel een 'reisdocumentenadministratie', met als nevenfunctie opsporingsdoeleinden.

In de praktijk kan dit echter zeer wel andersom zijn. Dat moet de toekomst uitwijzen.

## Reacties

[www.twitter.com/robincaron](http://www.twitter.com/robincaron) - 19-09-2010 11:40

Het gaat hier uiteindelijk om de verhouding tussen het recht op privacy en lichamelijke integriteit van Nederlandse burgers (afweerrecht tegen de overheid om met rust gelaten en niet-geregistreerd te worden) en andere belangen, zoals hierboven genoemd. Je kunt je ernstig afvragen waarom deze afweging niet is en wordt gemaakt.

Je moet biometrische gegevens niet alleen maar opslaan omdat het KAN. Het moet ook MOGEN.

Met name art. 8 Europees Verdrag voor de Rechten van de Mens staat schending van de privacy door databank-opslag van vingerafdrukken alleen toe als voldaan wordt aan strenge voorwaarden. Deze schending moet proportioneel en effectief zijn. Er mag verder geen (minder schendend) alternatief beschikbaar zijn en er moeten strenge veiligheidswaarborgen zijn. Aan deze punten voldoet de Paspoortwet niet.

De Paspoortwet noemt in de memorie van toelichting drie doelen:

- 1) betrouwbaarder en effectiever aanvraag- en uitgifteproces van reis-documenten;
- 2a) fraude met reisdocumenten en 2b) look-alike-fraude, kan beter worden bestreden;
- 3) opsporing en vervolging van strafbare feiten zou worden verbeterd.

O.g.v. deze doelen moet de proportionaliteit van de privacy-schendende opslag negatief worden beoordeeld.

We moeten hierbij goed onderscheid maken tussen opslag van biometrische gegevens op de chip van de pas/ID zélf en databank-opslag.

Ad 1) Nu de databank-opslag nog lokaal plaatsvindt kun je helemaal niet overal paspoorten/ID's aanvragen. En niet is duidelijk hoe eventuele foutieve persoonsgegevens door opslag in databanken plotseling correct zouden worden. Kortom, het is een 'bedachte' oplossing voor een niet-bestaand probleem.

Ad 2a) Deze fraude is al verminderd sinds paspoorten centraal worden vervaardigd. Databank-opslag heeft hier verder weinig mee te maken.