BEROEPSCHRIFT

De heer J.Dingler
Jr
Voorburg
Nederland

****

DE NIEUWE PASPOORTWET

Een dossier van wat zich voordeed in de situatie van de heer J.Dingler vanwege de aanvraag van een ID-kaart volgens de "Nieuwe" Paspoortwet.

Voorburg
09 mei 2011

****

VOORWOORD

Voor U ligt mijn beroepschrift d.d. 09-05-11. Het beschrijft de situatie waarin ik afgelopen jaar terecht kwam. Een aanvraag feitelijk voor een identiteitskaart. Een situatie die mij verbaasde over de manier waarop de Overheid optreedt. De gang van zaken wordt vanaf het begin geschetst en waar nodig zal commentaar volgen. De lezer treft ook producties aan. Dit om de juistheid van het verhaal na te gaan. Teneinde de lezer in de gelegenheid te stellen deze situatie correct in te kunnen schatten. Om daarna een oordeel te vellen.

Het beroepschrift is opgebouwd uit twee gedeelten. Deel 1 beschrijft de situatie. In het 2e deel van het beroepschrift dien ik de gemeente van repliek..

Voornamelijk met als doel om de bestuursrechter in deze kwestie te overtuigen

Note: - Waar in dit beroepschrift "de gemeente" staat geschreven kan ook "de Overheid" gelezen worden of andersom. Zij zijn allebei verantwoordelijk.

****

INLEIDING

In deze kwestie verzoek ik hierbij om de vernietiging van de beschikking d.d. 31 maart 2011 van de gemeente Voorburg. Het kenmerk is BJZ / 527082 Die beschikking is gewezen in het kader van de nieuwe Paspoortwet die de burger sinds 21 september 2009 verplicht om vingerafdrukken af te geven

Ik kan mij niet verenigen met de beschikking van de gemeente Voorburg. Temeer omdat Nederland verder gaat dan de Europese regelgeving dat eist.

Reden waarom ik mij wend tot Uw Rechtbank en hiertegen ook in beroep ga. En vraag om in deze zaak een voor mij gunstig oordeel te willen uitspreken.

Kortheidshalve volsta ik met te verwijzen naar dit beroepschrift en producties.

****

INHOUDSOPGAVE

****

DEEL 1

HET DOSSIER

1. Achtergrond en recente ontwikkelingen

Hieronder volgt een schets van de geschiedenis die aan het besluit van de gemeente Voorburg vooraf ging om mijn verzoek te zullen afwijzen.

1. Een aanvraag voor een ID- kaart deed ik op 22 november 2010 bij het Meld- en Informatiecentrum in de gemeente Voorburg. Dat even daargelaten. Ik ging weer onverrichter zake naar huis. Een ID- kaart is mij geweigerd. Vooral omdat ik geen vingerafdrukken wilde afstaan.

2. De gemeente mag mijn vingerafdrukken wel in mijn Paspoort zetten. Maar ik wil niet dat ze in een databank opgeslagen zullen worden.

3. Op 06 december 2010 is de Burgemeester hierover een brief toegezonden. Aan de Burgemeester is de vraag gesteld om een verklaring te ondertekenen dat er veilig zou worden omgesprongen met mijn vingerafdrukken. Alleen dan laat ik mijn vingerafdrukken afnemen. De Burgemeester wilde niet aan dit verzoek voldoen. Niet eens ten aanzien van zijn eigen reisdocumentenadministratie in de gemeente.

4. De genoemde brief diende tevens als bezwaarschrift. Mijn brief is door de gemeente aan een commissie voor bezwaarschriften ter advies voorgelegd. Een hoorzitting is in dit geval gepland. Ik zag de noodzaak niet in om erbij aanwezig te zijn. Het betrof hier wettelijke regelgeving.

5. Het advies van deze commissie was om mijn verzoek niet ontvankelijk te verklaren. De gemeente Voorburg nam dit advies mee in haar besluit. Bij brief van 31 maart heeft de gemeente mij daarvan in kennis gebracht. Tegen dit besluit teken ik beroep aan bij de bestuursrechter.

6. Een burger komt door het toedoen van de gemeente tijdelijk zonder geldig Paspoort te zitten. Alternatieven worden evenwel niet geboden.

2. **De inhoud van mijn beroepschrift betreft:**

1. De aanvraag Identiteitskaart is niet in behandeling genomen.
2. Mijn vingerafdrukken niet in een landelijke database mogen worden opgenomen. Dat is een inbreuk op mijn privacy.
3. Ik ook bezwaar maak tegen het versterkingsregiem.
4. De maatregelen verder gaan dan bet doel dat de nieuwe paspoortwet nastreeft.
5. De centrale opslag van vingerafdrukken fraudegevoelig is.
6. De maatregelen in strijd zijn met artikel 8 (EVRM), de Europese privacyrichtlijn 95/46 en artikel 16 betreffende het Functioneren van de Europese Unie.
7. Alle handelingen die door de gemeente ten aanzien van mijn vingerafdrukken worden verricht moeten voldoen aan de Wet bescherming persoonsgegevens (Wbp).
8. De gemeente aansprakelijk is voor de schade indien mijn vingerafdrukken in strijd met de (Wbp) of anderszins onrechtmatig worden verwerkt.

Kortom: de inperking van mijn persoonlijke levenssfeer, de afbreuk van mijn fundamentele grondrechten op persoonlijke vrijheid, lichamelijke integriteit en recht op bescherming van mijn privé-sfeer en algehele veiligheid zoals deze zijn vastgelegd in het Europees Verdrag van de Rechten van de Mens. Dat Nederland mede heeft geratificeerd.

3. Bespreking van het beroepschrift

3.1 Aanvraag Identiteitskaart

3.1.1 Uit het voorgaande is gebleken dat de burger een geldig legitimatiebewijs niet wordt verstrekt. Vooral wanneer iemand weigert een vingerafdruk te laten opnemen in een digitaal overheidsregister. Hierdoor komt iemand in een oneigenlijke situatie terecht. Een identiteitsbewijs is nodig om aan alle nationale verplichtingen te kunnen voldoen. Nu helaas tevergeefs.

3.1.2 Verontrustend ook. Wie niet over zo'n geldig document beschikt is uitgesloten van het maatschappelijk verkeer. Aangezien men geen arbeidsovereenkomst kan afsluiten, geen uitkering kan ontvangen. Geen huis kan kopen en geen (verplichte) zorgverzekering kan afsluiten. Enkele voorbeelden zijn dit slechts.

3.1.3 Aan de andere kant loopt iemand het risico door de politie te worden gearresteerd vanwege het niet kunnen tonen van een geldig legitimatiebewijs. Zonder dat men zich schuldig maakt aan enig strafbaar feit. Slechts handelt om te voorkomen dat paspoortgegevens voor opsporingsdoeleinden beschikbaar komen.

3.1.4 De politie heeft in dat laatst genoemde geval dan ook wel de bevoegdheid iemand te arresteren om foto's en vingerafdrukken van de betrokken persoon op te slaan in een strafketendossier.

3.1.5 Op nationaal niveau staat een burger nu praktisch machteloos.

3.1.6 De overheid, in deze de Burgemeester van de gemeente Voorburg, brengt de burger feitelijk in de problemen. Daar komt het op neer. Een brief ondertekenen om te garanderen dat zij zorgvuldig omgaat met vingerafdrukken blijft uit. Alternatieven ontbreken.

3.1.7 Anders gezegd, "de gemeente wil in deze kwestie geen positie innemen. Notabene niet eens tegenover de eigen reisdocumenten-administratie. Ik leg hiermee wellicht de vinger op de zere plek. Niet alles schijnt in orde te zijn voor wat betreft de beveiliging."

3.1.8 Wie is er verantwoordelijk voor fouten als burgers schade lijden? Dat zou de overheid moeten zijn. Nu dekt men zich in.

3,2 Opname van Vingerafdrukken in Landelijke database

3.2.1 De uitvoering van de nieuwe Paspoortwet leidt tot verbazing. Een geldig identiteitsbewijs waar ik recht op heb wordt mij ontzegd. Tijdens de aanvraag van een identiteitsbewijs komt een burger voor verrassingen te staan. Vingerafdrukken worden afgenomen.

3.2.2 Een verklaring ondertekenen had in de lijn der verwachting gelegen. Vooral omdat deze gegevens in een decentrale database van de gemeente worden opgeslagen. En naderhand in de centrale database terechtkomen. Hetgeen volgens opgave veilig zou zijn.

3.2.3 De staatssecretaris Ank Bijleveld benadrukte dat (**Productie 1**). Het ging om een database van de Nederlandse Overheid die goed beveiligd is waardoor oneigenlijk gebruik van identiteitsgegevens onmogelijk zou zijn gemaakt. Op zich geruststellend om te weten.

3.2.4 Alles gaat er daadwerkelijk anders aan toe. Die zelfde Overheid weigert juist schriftelijk te verklaren dat alles in orde is met de opslag van gegevens. In deze de Burgemeester van Voorburg. Notabene in opdracht van dezelfde staatssecretaris Ank Bijleveld.

3.2.5 Het Ministerie van Binnenlandse Zaken zit (**Productie 2**). in haar maag met een protest tegen de opslag van vingerafdrukken. Zij adviseert de gemeenten de brieven niet in ontvangst te nemen. Laat staan te ondertekenen. Niet alles schijnt goed in orde te zijn.

3.2.6 De vingerafdrukken achterlaten bij de gemeente is onverstandig. Als er fouten ontstaan wil men niet voor de gevolgen opdraaien.

3.2.7 Een slachtoffer van identiteitsfraude staat er alleen voor. De Nederlandse Overheid geeft niet thuis voor de aansprakelijkheid ervan en de schadeloosstelling. In een vonnis van de rechtbank is de Overheid daarover notabene in het gelijk gesteld (**Productie 3**).

De Paspoortgegevens worden nu nog decentraal opgeslagen. Maar niet voor lang. Ooit worden deze gegevens in een landelijk database gezet.

In dat laatste geval raak ik de regie kwijt over mijn eigen gegevens. Vooral omdat ik geen zicht meer kan houden op wie er toegang heeft tot die gegevens. Waar die gegevens terecht komen en wat ermee gebeurt. Dat deze gegevens voor justitiele doeleinden wordt gebruik is vreemd.

Hoe verzint de Nederlandse Overheid het om van een reisdocument van de burger een beveiligingsdocument voor de staat te maken. Ongepast.

Ik wens niet als potentieel verdachte te worden beschouwd en vrees het ergste voor het geval ik ten onrechte als daadwerkelijk verdachte wordt bestempeld. Bijvoorbeeld omdat men meent mijn lichaamskenmerken te hebben gevonden op een plek waar ik nooit ben geweest... Realistisch.

Dat laatste scenario is zeer wel mogelijk. Zeker als er fouten worden gemaakt in databestanden. Als gegevens fout worden geïnterpreteerd.

Of erger: "Indien onbevoegden met gegevens aan de haal zijn gegaan."

Laat de Overheid garanties inbouwen die identiteitsdiefstal voorkomt.

De Overheid heeft namens de burgers immers een mandaat. En dan diezelfde burgers niet in bescherming willen nemen. Eerst voor een goede beveiliging zorgen. Daar hebben we nu niet zoveel vertrouwen in. Een verklaring ondertekenen dat de beveiliging in orde is wil men niet.

3.3. Het Verstrekkingsregiem

3,3,1 Tegen deze achtergrond is de wens van de Overheid om een versprekkingsregiem te realiseren opmerkelijk. De burger moet haar vingerdrukken afstaan. Maar de Overheid kan en wil daarentegen niet garanderen dat het verzamelen van privégegevens een burger later niet in de problemen zal brengen.

3.3.2 Een woordvoerder van het Ministerie van Binnenlandse Zaken laat weten dat dit niet relevant is. Een bezwaar kan niet door de beugel. Over de uitvoering van publiekrechtelijke zaken worden geen overeenkomsten met individuele burgers gesloten **(Productie 4)**.

3.3.3 In de praktijk wordt de daad inderdaad bij het woord gevoegd. Het uitleveringsverdrag met Amerika is daarvan een sprekend voorbeeld. De landen krijgen toegang tot elkaars database. Daardoor kunnen ze dus gegevens opvragen van DNA-profielen en vingerafdrukken. Dit heeft Nederland op eigen houtje gedaan.

3.3.4 Volgens het verdrag van Lissabon is dit verboden **(Productie 5)**.

3.3.5 Het gaat echter veel verder. Ik doel op het Ministerie "Obfuscatie en Transparantie", afgekort (OT) wat van plan is de centrale database waar alle DNA-profielen van Nederlandse burgers worden verzameld open te stellen voor alle overheden ter wereld. Inclusief landen als Noord-Korea, China, Pakistan. **(Productie 6)**

3.3.6 Ook de database met de NAW, vingerafdruk- en paspoortgegevens worden beschikbaar voor alle landen. De stap van de regering is geregeld in een supergeheim handelsverdrag, HACTA. (High Anti-Freedom Clueless Terror Agreement). Het verdrag is zonder enige inspraak of goedkeuring van burgers of parlement ingevoerd.

3.3.7 In landen met corrupte regeringen kan de informatie makkelijk doorgespeeld worden aan kwaadwillenden. In feite ligt nu alles al op straat. Het behoeft geen toelichting dat het heimelijk delen van persoonlijke gegevens privacyproblemen met zich meebrengt.

3.3.8 Deze vingerafdrukken en de Nederlandse reisdocumenten worden opgeslagen in een databank bij het bedrijf Sagem Identification in Frankrijk. En dat vormt volgens de AIVD een risicofactor. Vooral omdat deze gegevens in verkeerde handen kunnen komen.

Tegen die achtergrond is sprake van collectie mensenrechtenschending.

Alle landen van de Europese Unie moeten paspoorten en ID-kaarten uitgeven waarin twee vingerafdrukken van de houder opgenomen zijn.

Het doel ervan is om identiteitsfraude te voorkomen. Met twee vingerafdrukken in je paspoort is te controleren of de identiteit klopt. Opslag van deze gegevens in een database is daarvoor niet nodig. De Nederlandse Overheid blijkt daar wel voorstander van te zijn geweest.

De Nederlandse Overheid ondermijnt kort gezegd haar eigen doelstelling. Het tegenstrijdige van deze extra stap is het risico op het ontstaan van identiteitsfraude. De voorwaarden die worden gesteld aan gebruik van de databank voor opsporingsdoeleinden zijn flinterdun.

In de praktijk is de databank CIOT een voorbeeld. Nog steeds lappen opsporingsdiensten privagyregelgeving aan hun laars. **(Productie 7)**

3.4 De maatregel verder gaat dan het doel van de nieuwe PaspoortWet

Inleiding.

Op 21 september 2009 reikte de staatssecretaris Ank Bijleveld het eerste biometrische paspoort van Nederland uit. **(Productie 1)**

Het was conform de geldende Europese regelgeving. **(Productie 8)**

De Europese Commissie heeft een voorstel ingediend dat de Richtlijn inzake 'standaarden voor veiligheidskenmerken en biometrie in paspoorten en reisdocumenten uitgevaardigd door de lidstaten' wijzigt. De wijziging houdt in dat alle kinderen vanaf zes jaar verplicht worden hun vingerafdrukken te laten afnemen bij het aanvragen van een Europees paspoort én andere reisdocumenten uitgevaardigd door de lidstaten van de Europese Unie De Liga voor Mensenrechten waarschuwt voor onnodige en zeer verregaande inbreuken op de privacy van alle inwoners van de EU. De ondemocratische wijze waarop dit voorstel tot stand kwam, is bijzonder verontrustend.

De Europese Commissie lanceerde op 18 oktober 2007 het voorstel dat iedereen vanaf de leeftijd van zes jaar twee vingerafdrukken moet laten afnemen bij het toekennen van Europese paspoorten en andere reisdocumenten. Men mag aannemen dat de term 'en andere reisdocumenten' ook verwijst naar het gebruik van nationaal uitgevaardigde identiteitskaarten die worden gebruikt om te reizen in het EU-Schengen gebied. Dit heeft voor gevolg dat éénieder die in de Europese Unie woont (en ouder is dan zes jaar) verplicht zijn vingerafdrukken moet laten afnemen en dat deze unieke, persoonlijke gegevens zullen worden opgeslagen op een RFID-chip op het betrokken document én bijgehouden worden in een nationale (en op termijn in een gedeelde Europese) database.

In dit voorstel van de Europese Commissie verwijst men expliciet naar het tegemoet komen aan de ICAO -standaarden ter legitimatie van hun verregaande beslissingen. De ICAO-standaard vereist geen vingerafdrukken, een gedigitaliseerde foto van het aangezicht volstaat. Bovendien waarschuwen vele studies ons voor het feit dat een systeem waarbij de identiteitscontrole wordt gekoppeld aan biometrische data niet onfeilbaar is (cf. het probleem van 'valse' vingerafdrukken).

Uit onderzoek is gebleken dat de opgeslagen biometrische data in de RFID-chip onvoldoende beschermd zijn én bovendien oneigenlijk gebruik toelaten. Deze chip zendt een radiosignaal uit die een identiteitscontrole mogelijk maakt op élk moment en op élke plaats zonder medeweten van de houder van het betrokken document. Het risico bestaat dat ongemachtigde derden de chip kunnen lezen en persoonlijke informatie verkrijgen, wat een schending inhoudt van het recht op privacy en persoonlijke data-bescherming.

Het systeem van elektronische identiteitskaarten met biometrische gegevens vormt een ontoelaatbare inbreuk op fundamentele

mensenrechten en vrijheden. De geplande maatregelen zijn in strijd met artikel 8 van het Europees Verdrag voor de Rechten van de Mens, als ook met de Resolutie inzake biometrie in paspoorten, identiteitskaarten en reisdocumenten aangenomen in Montreux op 16 september 2005 door de Europese toezichthouders van gegevensbescherming.

De strijd tegen terrorisme, illegale immigratie en handel in valse documenten kan niet gevoerd worden ten koste van deze fundamentele rechten. Het voorstel van de Europese Commissie doorstaat de proportionaliteitstoets niet. Het steeds gebruik van biometrische gegevens en de manier waarop deze een onderdeel zijn geworden van ons dagelijkse leven degraderen éénieder tot de status van een verdachte en versterken tegelijkertijd de greep van de staat op zijn burgers.

De Liga is verontrust over het feit dat de Europese Commissie met dit voorstel volledig buiten haar bevoegdheden treedt. Zo stelt artikel 18(3) van het EG verdrag uitdrukkelijk dat de Europese Commissie niet bevoegd is bepalingen in te voeren ten aanzien van paspoorten, identiteitskaarten, verblijfsvergunningen of andere gelijkaardige documenten. Ze kan niet optreden om het beleid daaromtrent in de verschillende lidstaten te harmoniseren. De Europese Commissie doet dit voorstel zonder het Europese Parlement ten gronde te betrekken. Het totale gebrek aan transparantie en de afwezigheid van een democratisch debat vindt de Liga zorgwekkend.

De Liga vraagt dat dit voorstel van de Europese Commissie aan een democratisch debat wordt onderworpen bij het Europese en Belgische Parlement. Het gebruik van biometrie in officiële identiteitsdocumenten wordt niet opgelegd door de ICAO-standaarden en er zijn onvoldoende data-beschermingsmechanismen voorzien. Het voorstel steunt op zeer dubieuze rechtsgronden en schendt tal van fundamentele mensenrechten en internationale conventies.

De Liga vraagt zich af of e en pluralistische, democratische cultuur kan overleven wanneer een staat de vingerafdrukken van zijn hele bevolking kan afnemen en elke beweging van zijn onderdanen onder toezicht kan plaatsen. De Liga vraagt aan de individuele lidstaten dat ze de democratische beginselen en fundamentele mensenrechten en conventies respecteren.

3.4.1 Europese wetgeving schrijft dus voor dat er twee digitale vingerafdrukken worden opgeslagen in een chip op het paspoort. Het feit daargelaten of deze wetgeving de toets der kritiek kan doorstaan. De Europese Commissie treedt buiten haar bevoegdheden zoals dit door de Liga hierboven is uiteengezet.

3.4.2 Op 21 september 2009 trad in Nederland de nieuwe Paspoortwet in werking. Het is feitelijk een maatregel om fraude te voorkomen.

3.4.3 Nederland was destijds "voorlopig" het enige EU-land dat vingerafdrukken ook centraal gaat opslaan. De staatssecretaris Ank Bijleveld stelde dat de veiligheid gegarandeerd zou zijn. Het was strikt omschreven waarvoor de biometrische gegevens gebruikt mogen worden. Alleen voor vaststelling van identiteit.

3.4.4 Het ministerie van Binnenlandse Zaken denkt paspoortfraude hiermee beter tegen te kunnen gaan (**Productie 9**).

3.4.5 Voor de opsporing van criminelen konden deze gegevens niet worden gebruikt. Een wetswijziging was dan nodig, (**Productie 1**). Het wordt problematisch wanneer we de situationele context bekijken waarin biometrische gegevens gebruikt mogen worden.

3.4.6 Bestaande wetsartikelen krijgen een andere bredere strekking door de opname van die gegevens in het paspoort en databanken. Artikel 128nc WvSr biedt als de mogelijkheid om identificerende gegevens aan de officier van Justitie (OvJ) te verstrekken. Vooral omdat de toegang tot die databank voor opsporing in lagere wetgeving is geregeld via de "zogeheten" maatregel van bestuur.

Deze uitspraak staat niet op zich. Het is gedaan door een Kamerlid die zich uitsprak over de nieuwe Paspoortwet (**Productie 10**). Inhoudelijk betrof: het de 2e alinea van onderen van dat artikel.

3.4.7 Met de herindeling van de reisdocumentenadministratie worden er derhalve geheel nieuwe identificerende gegevens beschikbaar gesteld die geraadpleegd kunnen worden op verzoek van de OvJ.

3.4.8 Een centrale databank met foto's en vingerafdrukken van alle Nederlandse burgers is een schoolvoorbeeld van "Function creep". De oorspronkelijke doelstelling wordt langzaam verschoven. Nieuwe functies worden eraan toegevoegd. In dit geval dus ook.

3.4.9 Na een wetswijziging mocht de databank ook voor opsporings-doeleinden gebruik worden. Iets waarvoor men al lang vreesde.

Een opmerkelijke gang van zaken. De centrale databank van de Overheid is als opsporingsdoeleinde aangewend. De invoering van de nieuwe Paspoortwet voldoet niet aan het oorspronkelijke uitgangspunt. Het doet afbreuk aan wat de EU ermee voorstond.

3.4.10 Nadere opmerking

Deze database is in aanleg een nationaal opsporingsregister. Een ernstige inbreuk op de persoonlijke levenssfeer. Vooral omdat ook de gegevens van "Niet" verdachte burgers zijn opgenomen. De burger raakt zo de controle over haar eigen gegevens kwijt.

Hiermee wordt een belangrijk beginsel van de Rechtstaat geschonden. Namelijk dat er eerst sprake moet zijn van een redelijk vermoeden van schuld voordat iemands privacy geschonden mag worden. Nu gebeurt dat precies andersom.

Tel daarbij op het feit dat deze gegevens ook in het buitenland terechtkomen. Onderdeel vormen van een verstrekkingsregime.

Een uitleveringsverdrag met Amerika is daarvan een sprekend voorbeeld. De landen hebben toegang tot elkaars database. **(Productie 5)**.. Niet te vergeten het geheime verdrag HACTA. (High Anti-Freedom Clueless Terror Agreement) **(Productie 6)**.

Tegen die achtergrond schijnt de inwerkingtreding van de centrale databank van de Nederland Overheid al een feit te zijn

- Verstrekking van gegevens is volgens opgave via een databank. En die is na een half jaar al in gebruik genomen. **(Productie 1)**
- Na een wetswijziging is artikel 4b aan de Paspoortwet toegevoegd voor opsporingsdoeleinden. Zie ook **(Productie 30)**.

Het is de vraag of de doelstelling van de nieuwe Paspoortwet langzaam is verschoven door het toevoegen van een nieuwe gebruikerswens om opsporingsdoeleinden na te streven? Of dat alles bewust is gepland? Zoiets is niet geheel onwaarschijnlijk.

Momenteel blijkt er feitelijk sprake te zijn van ""Function creep".

3.4.11 Tenslotte

De Nederlandse Overheid heeft verder nauwelijks of geen idee hoe een centrale databank deugdelijk beveiligd moet worden. Volgens de staatssecretaris is alles in orde. We kunnen er allerminst gerust op zijn. En historisch gezien is dat ook niet verstandig. Het lukt de Overheid niet eens op lange termijn. Een voorbeeld is de Telecomdatabank (CIOT).

Ophef is ontstaan over de databank van de (CIOT). De aanleiding is het voortdurende gebrek aan controle over wie, wanneer en hoe men in de databank kan grazen. Op 28 juli 2010 werd dat gepubliceerd. Al jaren lang is de controle daartoe beneden de maat **(Productie 11)**.

Afwijkend. Die databank is in 2002 opgericht. Maar de strikte naleving van de voorschriften is nog steeds niet geborgd **(productie 20)** pagina 4. Het uitvoeren van de technische en organisatorische maatregelen voor de beveiliging zorgt voor problemen. Zie pagina 6 van die productie.

3.5 De centrale opslag van vingerafdrukken fraudegevoelig is

De veiligheid van de vingerafdrukken is gegarandeerd. Als we de voormalige Staatssecretaris Ank Bijleveld van Binnenlandse Zaken mogen geloven althans. Maar hoe het allemaal feitelijk werkt? Laten we ons daarvoor tot de praktijk beperken. Daar voltrekt zich immers alles.

Een centrale databank moest vanzelfsprekend goed beveiligd zijn. Vooral vanwege de gevoelige aard van de gegevens Het gaat vaak mis. Als je naar de geschiedenis kijkt moet je vaststellen dat dit niet lukt. Het probleem zit hem in de toegang beheer en bewaking van gegevens.

Het beveiligen van databanken staat ongetwijfeld hoog op de prioriteitenlijst. Op papier klopt het wellicht. Theorie en praktijk wijken vaak af. Ze horen wel bij elkaar "theorie en praktijk". De theorie is het hoofddoel. Hetgeen we proberen te bereiken. Maar dat lukt niet altijd.

In de praktijk heeft de Nederlandse Overheid de beveiliging van databanken niet goed onder controle. Talloze voorbeelden tonen dit aan.

Een voorbeeld waar de controle van databanken misgaat is de (CIOT).

Op bladzijde 9 in de 3e alinea is onder meer door de Liga betoogd dat de RFID-chip voor het opslaan van data onvoldoende bescherming biedt. Het is in Amerika ook gebleken. Een hacker kraakte een PFID-paspoort. Deze RFID-chip zit ook op het Nederlands paspoort. **(Productie 12)**.

Bij de behandeling van de vraag of de opslag van vingerafdrukken in een centrale databank fraudegevoelig is is een korte uitleg gegeven. Daarbij is gesproken over het standpunt van de Nederlandse Overheid. Anders gezegd: de veiligheid van de centrale databank is gegarandeerd.

De Nederlandse Overheid heeft dat steeds gesteld. Maar nooit bewezen. Het tegendeel doet zich overal in de praktijk voor. Nu reeds al is dat gebleken. Websites van de Overheid worden platgelegd. Het systeem van de OV-chipkaart is diverse malen gekraakt. En datzelfde geldt voor de beveiliging van toegangspassen voor de overheidsgebouwen.

Het zogeheten verstrekkingsregime zou volgens opgaven nog niet zijn uitgewerkt. Maar er zijn wel verdragen tussen diverse landen om gegevens uit te wisselen. En de verplichting voor het afgeven van een vingerafdruk bij een paspoortaanvraag is nu ook al van kracht. Terwijl de voorwaarden voor een deugdelijke veilige opslagmethode niet is uitgewerkt. Een omgekeerde werkwijze. Met alle gevolgen van dien.

Een inbraak in de centrale databank voor de opslag van biometrische gegevens zal nog veel ernstiger zijn. Het werkt meer fraude in de hand.

De aanpak van de Overheid is heel tegenstrijdig. Het botst met elkaar.

Voor de beoordeling hiervan neem ik de beschreven situatie in chronologische volgorde op deze plaats in het beroepschrift door.

3.5.1 Tussenconclusie

Op grond van bovenstaande argumenten kunnen we van oordeel zijn dat er gegronde redenen zijn om te veronderstellen, dat getwijfeld kan worden aan de juistheid van het beleid van de Overheid. Het gevoerde beleid draagt elementen in zich die voor problemen zorgen.

3.5.2 De Feiten

Zonder pretentie van volledigheid noem ik hierna een aantal feiten die van belang zijn voor de beoordeling welke zaken met elkaar botsen..

Omwille van een duidelijk beeld wordt de totale situatie kort belicht. En daarmee ben ik terug bij het moment waarop ik een aanvraag deed voor een ID-kaart. Een aanvraag is geweigerd. De gemeente zond mij daarna "wel"een brief dat alles goed wordt verwerkt. **(Productie 13)**.

1. Maatregelen treffen om de privacy van een burger te beschermen

In eerste plaats gebeurt dit door in de Paspoortwet en in regelgeving die hieruit voortvloeit juridisch vast te leggen. Te weten:

- waarvoor gegevens mogen worden gebruikt
- wie ze mag opvragen
- op welke manier ze geraadpleegd mogen worden

Het feit dat Binnenlandse Zaken altijd nog uitdrukkelijk toestemming moet geven voor raadpleging daargelaten. Niet altijd verloopt het goed. In dit verband is de telecomdatabank (CIOT) sprekend. **(Productie 14)**. Daarmee gaat het al jarenlang fout. En nu moet het ineens bij een databank voor vingerafdrukken wel goed gaan? Heel erg speculatief.

In het geval van de telecomdatabank (CIOT) zijn nog steeds problemen. Een keer de fout in gaan kan gebeuren. Maar dan dient er een beleidsverandering te komen. Drie achtereenvolgende jaren niets doen wekt de indruk dat men er lak aan heeft. Niet zo erg professioneel dus

Tegen deze achtergrond is een databank voor vingerafdrukken niet geruststellend. Bovendien wil de gemeente niet tekenen voor veiligheid.

De gemeente wilde de veiligheid van vingerafdrukken in haar databank uiteindelijk niet garanderen. Er een verklaring voor ondertekenen. Opvallend. Een brief ontvangen waarin staat dat er regels zijn. Maar niet voor de gevolgen willen opdraaien als er zich problemen voordoen.

Het dilemma is te doorzien natuurlijk. De gemeentelijke databank steunt op het internet.. En dat vereist vanzelfsprekend ook aparte beveiliging.

Er ontstaan twijfels of alles wel goed geregeld is voor de bewuste opslag.

2. De informatieverstrekking vanuit de Overheid is onvolledig

Over de veiligheid van databanken doet de staatssecretaris slechts vage uitspraken.: "Maakt U zich maar geen zorgen, de databank is veilig. Want hij is beveiligd. Maar geen woord over wat die veiligheid precies inhoudt. Er is niemand die kan controleren of die bewering ook klopt.

De staatssecretaris negeerde daarmee voor de zoveelste keer de kritiek van esperts. Experts die vanuit een onafhankelijke positie alles nagaan.

Een verslaggever is een onderzoek in maart 2010 gestart om technische aspecten opgehelderd te krijgen. Hij begon een juridische procedure.

3. Het onvolledig informeren van Kamerleden over de Paspoortwet

Een regeringsadviseur hekelt Nederland om de gang van zaken rond de wetgeving van de vingerafdrukken. De Overheid doet geheimzinnig naar het parlement. De Tweede Kamer is slecht geïnformeerd. En het schort ook aan voldoende informatie voor de politici. **(Productie 15)**.

De slechte informatievoorziening typeert hij als een democratisch tekort.

3.5.3 Inwerkingstelling van de Nieuwe PaspoortWet

Kortom: De Paspoortwet verloopt anders dan verwacht. De dingen zijn tegenstrijdig. Botsen met elkaar. Veel is gaandeweg duidelijk geworden. De staatssecretaris wenst haar verantwoording alleen niet te nemen. Terwijl dat laatste vanuit haar openbare functie wel moest gebeuren.

De staatssecretaris heeft de gemeente een mandaat gegeven om bij de aanvraag van een identiteitsbewijs vingerafdrukken af te laten afnemen.

In het kader van de Paspoortwet wordt de burger in het nauw gedreven. Deze wet is veel te snel inwerking getreden en is niet goed doordacht. Een protest tegen opslag van vingerafdrukken leidt tot problemen. In die situatie kan een burger zich niet legitimeren. Zie pagina 4, punt 3.1.2.

Een weigering van de burger om vingerafdrukken af te staan is gerechtvaardigd. Zeker nu de veiligheid niet volledig is aangetoond.

Het beleid van de Overheid hield geen rekening met een weigeraar. Dat de burger geen vingerafdrukken wilde afstaan. Hieraan ging de Overheid totaal voorbij. En zij werkt achteraf niet mee. Adviseert een gemeente om een protestbrief van de burger niet in ontvangst te nemen.

3.5.4 Het beleid van de Overheid

Zoals hierboven al uiteengezet mankeert het aan de inwerkingstelling van de PaspoortWet. Bij de besluitvorming van deze wet is veel mis gegaan. Zo was er weinig oog voor privacy. En was het gehele proces ondoorzichtig. De Overheid wilde verder niet instaan voor de veiligheid.

De Nieuwe PaspoortWet iis zonder medeweten van de burger doorgezet.

Tegelijkertijd ontbreken de bijbehorende veiligheidsmaatregelen.. Niet zonder gevolgen overigens. In de praktijk ontstonden al snel problemen. Een half jaar na inwerkingstelling van de PaspoortWet bleek dat.. De staatssecretaris ziet geen reden om procedures te herzien. (Productie 16).

De staatssecretaris stelt dat alles veilig is. Ofschoon vingerafdrukken vanwege technische fouten niet meer kloppen in de centrale databank. Maar ook sprake is van verwisseling van vingerafdrukken. Het is onduidelijk waar de staatssecretaris zich op baseert. Zij blijft verbazen.

Het is de vraag waar de staatssecretaris zich op baseert? Ondanks dat alles misging. Wie zegt haar dat alles goed gaat.. Haar collega's zeker?

De risico's van de opslag daarvan moest tot het minimale beperkt blijven. Passende technische en organisatorisch maatregelen dus. Een verantwoordelijkheid van de Overheid. Maar hoe groot is de ervaring met ICT bij de Overheid. Beslissingen moet je nemen vanuit de inhoud.

3.5.4.1 Regeringsadviseurs

Laten we objectief zijn. ICT is heel complex en voor veel mensen te complex. En politici zijn ook maar mensen. Het zijn experts die de ingewikkelde keten van de informatie- en communicatietechnologie goed kunnen volgen. Zij zijn ook allang in deelgebieden gespecialiseerd.

Deze ICT-experts die het wel goed begrijpen hebben daar bovendien een dagtaak aan. En zij hebben weer weinig kaas gegeten van andere zaken, zoals bijvoorbeeld politiek en recht . Andersom geldt dat voor politici ook: thuis in politiek en recht. Maar niet zo erg in techniek.

Zo bekeken kan men een advies dus als vanzelfsprekend beschouwen.

Een advies van een regeringsadviseur is dus van relevante betekenis voor de deugdelijke uitvoering van beleid. Op diverse terreinen ook..

Op basis van zo'n advies ontwikkelt de Overheid een richtinggevend kader. Dit kader beoogt bij te dragen aan rationaliteit bij beslissingen.

De Overheid diende een advies tot inzicht te brengen. Maar de vanzelfsprekendheid ervan moet niet als logisch worden verondersteld. Niet in het geval van de Overheid althans.. Zij geeft er geen blijk van. Keer op keer worden adviezen van regeringsadviseurs ter zijde gelegd.

Laat het bovenstaande op zich al een brevet van onvermogen zijn. Dat is een taxatiefout. Alles gaat nog een stapje verder. Adviezen van Nederlandse en Europese toezichthouders worden gebagatelliseerd of zelfs geheel genegeerd. Zie het rapport "Happy Landings" bladzijde 151.

Het rapport "Happy Landing." is bekend bij de rechtbank. Maar zij verbindt er geen conclusie aan. De aanpak van de Overheid daargelaten.

Wat de toegevoegde waarde daarvan is blijft onduidelijk. De Nederlandse Overheid neemt beslissingen terwijl de kennis ontbreekt. Daarmee blijkt dat de Overheid haar verantwoordelijkheid niet neemt. Een deugdelijke beveiliging is zo onmogelijk. De aanpak is te vrijblijvend.

De Overheid trad gewoon op zonder het besef van de uitvoering ervan.

Een weinig positieve conclusie is onontkoombaar. De beveiliging van de centrale databank voor vingerafdrukken staat zo op losse schroeven. Niet verwonderlijk. Zeker nu de werkwijze van de Overheid duidelijk is. De Overheid wijkt categorisch af wat logischerwijs moest gebeuren.

Anders gezegd: "De Overheid heeft een standpunt waarin politieke opportuniteit zwaarder weegt dan de wetenschappelijke rationaliteit."

3.5.4.2 De beveiliging van databanken

In de vorige paragraaf werd de werkwijze van de Overheid besproken. We zagen op welke wijze dat gestalte kreeg. Er is geen inhoudelijke reden om voor de werkwijze van de Overheid te zijn. Anders dan een politieke gedachtegang. Politiek scoren in plaats van goed je werk doen.

De glans gaat "meer en meer" af van de geloofwaardigheid van de Overheid. Haar optreden is staatsrechtelijk verwerpelijk te noemen.

Aan een deugdelijke beveiliging voor vingerafdrukken wordt geen aandacht besteed. De inzet van de Overheid daargelaten. Onderzoeken plannen en maatregelen slaan de plank mis. Hoe dat komt weten we nu. Het ontbreekt de Overheid aan kennis en zij volgt geen adviezen op.

Een beveiliging komt daardoor in gevaar. Op termijn leidt dit juist tot identiteitsfraude. Hetzij van binnenuit door inherente technische onvolkomenheden en foutmarges, menselijke corruptie of datalekken. Hetzij van buitenaf door hacking. De deskundigen gaven dit ook aan.

3.5.4.3 Fraudegevoeligheid

In dit verband dient ook te worden gewezen op een praktijkvoorbeeld.

Een gelijksoortig probleem speelt bij de telecomdatabank CIOT. Het is fraudegevoelig gebleken. De rechtmatigheid van de verzoeken tot informatie wordt niet gecontroleerd. Concreet komt het er op neer dat een agent 3 jaar ongemerkt kan checken of zijn vrouw 2 mobieltjes heeft.

Verder konden journalisten een bevriende agent vragen om het emailadres van een celebrity of van een politicus. **(Productie 17)**

Deze databank is in 2002 opgezet. Maar jaren later blijken zich vanwege onterechte toegang nog steeds problemen voor te doen.

Op 22 maart 2011stelt de minister van Justitie de opsporingsdiensten een ultimatum voor strikte naleving. De minister neemt deze maatregel naar aanleiding van de aanhoudende problemen met procedures zoals autorisatie en verslaglegging rondom het opvragen van de gegevens. Hiervoor worden de producties **(Productie 18, 19 en 20)** toegevoegd.

Ook het CBP en de Europese Commissie buigt zich erover. **(Productie 21)**

Deze zaak staat niet op zich. Incidenten omtrent een slechte beveiliging zijn meerdere malen geconstateerd. Te weten:

a) De nieuwe OV-chipkaart
b) Toegangspoortjes overheidsgebouwen
c) Identiteitsfraude
d) Het platleggen van de website van het OM en de Politie
e) Miljoenen patiëntendossiers zijn door hackers gestolen

a. De OV-chipkaart is door wetenschappers gekraakt. Het is niet alleen in een laboratorium mogelijk. Hackers kunnen dat ook.. Diverse journalisten kregen de software en konden weken gratis met gemanipuleerde kaarten gratis reizen. **(Productie 22)**
b. Het beveiligingssysteem van de toegangspoorten van overheids-gebouwen is gekraakt door een Universiteit **(Productie 23)**
c. Een rapport van de Nationale Ombudsman beschrijft het schrijnend voorbeeld van iemand die op naam van een ander talloze strafbare feiten gepleegd had. Het rapportnummer is 2008/232. Dit punt zal later nog worden toegelicht. **(Productie 3)** Een krantenartikel geeft er verder een soortgelijk beeld van.
d. De websites van zowel het Openbaar Ministerie als van de Politie worden gehackt. **(Productie 24)**
e. Een Patiëntendossier komt op straat te liggen **(Productie 25)**

Vastgesteld kan worden dat databanken fraudegevoelig zijn. Zeker gelet op wat nu duidelijk is. Een somber beeld ontstaat Het gevaar voor een databank met vingerafdrukken is niet geheel ondenkbeeldig. Kwalijk. Het hoeft maar een keer mis te gaan en de gegevens liggen op straat.

De identificatie via vingerafdrukken is dat meteen voor altijd afgelopen. We zijn dan van het probleem af. Hierover denkt de Overheid niet na.

3.5.4.4 Conclusie

Een centrale databank met vingerafdrukken werkt fraudegevoeligheid in de hand.. De opslag is onbeheersbaar gebleken. We zagen dat in de vorige paragraaf. Het risico in het geval van vingerafdrukken wordt alleen maar groter. Vooral gelet op de gevoelige aard van de gegevens.

Het gaat erom dat de techniek zo ingericht wordt dat die werkt zonder lekken of fouten. Dat is nodig in een wereld die zo steunt op het internet.

De systemen werken nu nog niet zo goed als nodig. Sterker nog: Alles was al ingevoerd zonder tegelijkertijd een bijbehorende beveiliging te ontwikkelen. Het is de vraag of de Overheid het niet snapt. Of gewoon niet wil luistern naar de adviezen van de deskundigen. Vreemd.

Een aantal digibeten voeren Overheidsbeleid met alle gevolgen van dien. De Overheid springt roekeloos om met gevoelige persoonsgegevens.

In de praktijk gaat het ook nog steeds mis met de vingerafdrukken. Onder punt 3.5 is dat uiteengezet. De RFID-chip van het nieuwe paspoort bleek reeds door een hacker gekraakt te zijn. De Liga stelde dat deze chip voor het opslaan van data onvoldoende bescherming biedt.

Het RFID-chip in het paspoort heeft bovendien nog veel meer nadelen.

Aan de beveiliging van het paspoort schort het ook. Een paspoort kan op afstand worden ingelezen. En verraadt ongezien uit welk land de persoon komt. Dieven kunnen snel zien of iemand een paspoort bij zich heeft en waar het precies zit. Of het van de gewenste nationaliteit is dus.

Tegen deze achtergrond wordt een gerichte beroving van een paspoort mogelijk. Een eenvoudige RFID-lezer van een paar tientjes voldoet al.

Het gaat verder. Terroristen kunnen een paspoortbom maken die alleen afgaat als een paspoort uit een bepaald land langskomt. **(Productie 26)**

Deze constatering deden de onderzoekers van de Radboud Universiteit.

Opvallend is dat de Minister in antwoord op vragen over misbruik van de RFID-technologie stelt het gebruik van deze techniek niet te staken. Een mooi voorbeeld hoe het middel erger kan zijn dan de kwaal. En omgekeerd de backdoor straks eigenlijk de voordeur blijkt te zijn voor mensen met een foute persoonlijk / ideologische agenda. **(Productie 27)**

Een "papieren" paspoort had tegen deze achtergrond veel meer opgeleverd. Totaal gevrijwaard zijn van gevaar. Nu verloopt het anders.

3.6 Schending van artikel 8 (EVRM)

In deze paragraaf wordt stilgestaan bij de schending van artikel 8 van het Europese Hof voor de Rechten van de Mens. Nader te noemen: (EVRM). Voor de bespreking wordt gerefereerd aan de "Memorie van Antwoord" d.d. 28 april 2009 van de Staatssecretaris aan de diverse fractieleden.

Op pagina 6 en 7 laat Ank Bijleveld zich uit over de rechten van de mens in combinatie met de doelstelling van de herziende Paspoortwet.

Ik citeer: "Het belang van de persoonlijke levenssfeer behoorde prioriteit te hebben boven het opnemen van vingerafdrukken en de opslag ervan."

De staatssecretaris stelde op pagina 7, 4e alinea dat het opnemen van vingerafdrukken en het opslaan ervan een inbreuk op de bescherming van de persoonlijke levenssfeer betekende.. Die inbreuk was volgens haar gerechtvaardigd. Met name omdat deze leidt tot een meer betrouwbare en effectief aanvragen en uitgifte van reisdocumenten.

Een overweging daarbij om de privacy wel te schenden was om fraude te voorkomen. Te weten: "look-alike fraude". En dat was gewaarborgd.

In de optiek van de staatsecretaris is van belang dat de registratie van vingerafdrukken met voldoende waarborgen is omkleed. Dat is in het onderhavige wetsvoorstel onder meer doordat zeer nauwkeurig is beschreven voor welke doeleinden de gegevens mogen worden gebruikt.

Op grond van die belangenafweging heeft de burger veel te vrezen. Met de herindeling van de reisdocumentenadministratie worden er geheel nieuwe identificerende gegevens beschikbaar gesteld die geraadpleegd gaan worden door een officier van Justitie. Zie punt 3.4.5..

Evenmin volgt uit de ""Memorie van Antwoord" dat een beveiliging voor de vingerafdrukken ook is gewaarborgd. In de praktijk is telkens sprake van falende beveiligingsmaatregelen. Een sprekend voorbeeld is de telecomdatabank. CIOT. Zie het kopje "Fraudegevoelig"op pagina 21.

De praktijk leert dat de veiligheid van databanken onder de maat is.

Thans is verder ondubbelzinnig komen vast te staan dat de afgifte en de opslag van vingerafdrukken in strijd is met artikel 8 van het (EVRM).

Ik mag aannemen dat een staatssecretaris weet waarover ze het heeft. Daarbij verwijs ik naar de 4e alinea van pagina 7 van die Memorie.

Het "Memorie van Antwoord"wordt ook als **(Productie 28)** toegevoegd.

3.6.1 EU - privacyrichtlijn / Art. 16 functioneren van EU

De toepasbare regelgeving krijgt ten aanzien van de nieuwe Paspoortwet geen correcte uitvoering. De Europese privacyrichtlijn 95/46 suggereert een degelijke bescherming van alle burgers. Vooral in verband met de verwerking van persoonsgegevens en het vrije verkeer van die gegevens.

Op het moment is het onduidelijk hoe gegevens precies zijn verwerkt.

Een samenhang met artikel 16 betreffende het functioneren van de Europese Unie ontbreekt ook in dit geval t.a.v. de nieuwe Paspoortwet.

3.6.2 Samenvatting

Hiervoor is gebleken dat het opnemen van vingerafdrukken en het opslaan ervan in een centraledatabank in strijd is met artikel 8 (EVRM).

Overigens vormt de Nieuwe Paspoortwet een inbreuk op de Resolutie inzake biometrie in paspoorten, identiteitskaarten en reisdocumenten. Die Resolutie is aangenomen in Montreux op 16 september 2005 door de Europese toezichthouders van gegevensbescherming. Zie punt 3.4.

De Europese Commissie treedt met dit voorstel volledig buiten haar bevoegdheden. Zij doet dit voorstel zonder het Europese Parlement ten gronde te betrekken. Het steunt op dubieuze rechtsgronden en schendt tal van fundamentele mensenrechten en internationale conventies.

Een strijd tegen terrorisme, illegale immigratie of valse documenten kan moeilijk gevoerd worden ten koste van deze fundamentele rechten.

Het is de vraag of de Nieuwe Paspoortwet juridisch te verantwoorden is.

3.7 Wet bescherming persoonsgegevens

De Wet (Wbp) regelt hoe organisaties moeten omgaan met persoonsgegevens. Iedereen mag zijn gegevens inzien en corrigeren. Organisaties moeten aan de burger laten weten wat zij met zijn gegevens doen. Ook mogen ze alleen gegevens verzamelen als daarvoor een goede reden is, of als de burger toestemming geeft.. **(Productie 29)**

Een aantal artikels zijn van toepassing op de ontstane situatie:

- artikel 16 Wbp (artikel 8 lid 1 Privacyrichtlijn): Het is verboden om bijzondere persoonsgegevens te verwerken. Vingerafdrukken worden aangemerkt als bijzondere gegevens. Met name omdat daaruit informatie over de gezondheid kan worden afgeleid.
- Artikel 36 Wbp: Een burger kan een verzoek doen om gegevens te verbeteren, aan te passen of te verwijderen of af te schermen.

Tegen deze achtergrond voldoen de handelingen van de Overheid niet.

Op de website Paspoortinformatie.nl is vermeld dat geen bezwaar kan worden gemaakt tegen de opname van vingerafdrukken in de databank. Vooral omdat er sprake is van een wettelijk voorschrift waarvan niet kan worden afgeweken. Het is de vraag of dat ook te rechtvaardigen is.

Een burger is in de positie om bezwaar te maken tegen de opname van vingerafdrukken in een databank.. De individuele beoordeling bestaat. Artikel 36 Wbp waarborgt die keuzevrijheid voor een burger terdege. Het gaat daarbij om Internationale regelgeving. Een hogere wet feitelijk.

De toepassing van de Nieuwe Paspoortwet door de Nederlandse Overheid verliest onder de internationale wetgeving dus zijn kracht. Anders gezegd: "deze Paspoortwet is onverenigbaar met het gemeenschapsrecht." Afgezien van hetgeen onder punt 3.6.2. is gesteld.

3.8 Aansprakelijkheid voor de schade indien in strijd gehandeld wordt met de (Wbp)

In de voorgaande paragrafen is in het kader van de nieuwe Paspoortwet aandacht besteed aan een aantal zaken. Tot dusver heeft de Overheid veel zaken rond de uitvoering van de nieuwe Paspoortwet laten liggen. De Overheid toont zich gewoon niet verantwoordelijk en betrokken.

Een aantal zaken worden niet in de beleidsdoelstelling opgenomen. Het gaat daarbij om: "voorlichting, zorgvuldigheid, transparantie, adviezen, beveiliging en de internationale regelgeving." Deze zaken ontbraken op de agenda van de Overheid. Zeker uitgaande van hetgeen is gebleken.

Op welke wijze invulling wordt gegeven aan de verantwoordelijkheid van de Overheid indien de burger schade ondervindt wordt uiteengezet.

De staatssecretaris, mevr. A. Th. B. Drs. Bijleveld stelt, dat in het geval van onrechtmatige toegang tot gegevens van geval tot geval zal moeten worden gekeken wie verantwoordelijk is als de burger schade lijdt. Hierover spreekt mevr. Bijleveild zich uit in de Memorie van Antwoord..

Wat er in de praktijk gebeurt weerspreekt die uitlating alleen. Een slachtoffer van identiteitsfraude staat er alleen voor. Zie ook punt 3.2.7.

3.8.1 Een burger in de knel

Een rapport van de Nationale Ombudsman beschrijft het schrijnend voorbeeld van iemand die op naam van een ander talloze strafbare feiten gepleegd had. Het rapportnummer is 2008/232. Een zakenman is zo bekeken 13 jaar lang slachtoffer geweest van identiteitsfraude.

Deze zakenman stond geregistreerd als drugshandelaar en ongewenst vreemdeling. Het was dankzij een oude vriend die zijn naam leende. De vele foute registraties bij politie en marechaussee had zijn privacy ernstig gezonden. Hij was tientallen keren vastgezet en miste orders.

Pogingen om de databanken van de Overheid te corrigeren mislukte. Totdat de ombudsman in oktober 2008 orde op zaken ging stellen.

In oktober 2008 beval de Nationale Ombudsman de Overheid aan diens naam te zuiveren excuses aan te bieden en de zakenman te compenseren.

Een schadeclaim tegen de Overheid werd door de rechtbank te 's-Gravenhage niet gehonoreerd. De rechter vond dat de Overheid niet aansprakelijk is voor de foute registraties bij de politiekorpsen. Voor een claim moet de burger zich bij de afzonderlijke politiekorpsen melden.

De politie valt dus onder de verantwoordelijkheid van de Overheid. Maar dat wil niet zeggen dat ze ook aansprakelijk is als de politie daar een potje van maakt. De Overheid heeft geen zeggenschap over politiekorpsen als ze werken met onjuiste informatie uit hun computers.

Een slachtoffer van identiteitsfraude staat nog meer in de kou dan al werd gedacht. Dat is dankzij de Haagse rechtbank duidelijk geworden.

3.8.2 Tussenbalans

In de vorige paragraaf stond de aansprakelijkheid van de Overheid centraal. Hieraan wordt echter geen invulling gegeven. Een burger is aan zijn lot overgelaten. Krijgt problemen door foute justitie-informatie. Het is onmogelijk om gegevens te corrigeren. Medewerking blijft uit.

De verwachting dat dit patroon zich blijft herhalen is gerechtvaardigd.

Het gaat in de praktijk immers om precies dezelfde Overheid. Een nuance moet gemaakt worden. In het genoemde voorbeeld spraken we over heel eenvoudige NAW-gegevens. Geheel anders wordt het wanneer sprake is van vingerafdrukken die in een databank zijn opgenomen.

De gevolgen zullen in dat laatste geval ernstigere vormen aannemen. Vooral vanwege de gevoelige aard van deze biometrische gegevens.

In de "Memorie van Antwoord" van de Staatssecretaris wordt dat laatste daarentegen ontkend. Op pagina 7 4e alinea van die memorie staat dat een centrale databank geen echte negatieve gevolgen heeft voor het niveau van privacybescherming. Voor wat dat waard zal mogen zijn.

Vooralsnog geeft de Overheid niet thuis als de privacy geschaad wordt.

Het ziet er naar uit dat de invoering van de Nieuwe Paspoortwet het plegen van identiteitsfraude nu eerder zal bevorderen dan voorkomen.

3.8.3 Slotopmerking

Zoals hierboven al uiteengezet neemt de Overheid niet haar verantwoording. Een daadkrachtig optreden blijft uit. Als gevolg waarvan de persoonlijke levenssfeer van een burger wordt geschaad. Terwijl de Overheid uitvoering moest geven aan daadwerkelijk beleid.

Niemand heeft tot nu toe antwoord gegeven op de vraag wie verantwoordelijk is voor fouten als een burger feitelijk schade lijdt..

Het belang van de persoonlijke levenssfeer lijkt te worden voorbehouden aan diegenen die zich opwerpen als verdedigers van de waarden van de rechtstaat (en zijn afzonderlijke burgers) en de daarbij behorende ruimte voor het individu.

****

4. DE PRODUCTIES

Bijlage 1: Trouw 21-09-09 / NRC Handelsblad 09-04-11
Bijlage 2: De Pers 31-03-10
Bijlage 3: NRC.nl 19-03-09
Bijlage 4: Webwereld 19-04-10
Bijlage 5: Nu.nl.politiek 19-11-10
Bijlage 6: Minobel.nl / Webwereld 23-11-10
Bijlage 7: Nu.nl 26-07-10
Bijlage 8: Liga 16-11-07
Bijlage 9 NRC Handelsblad 19-09-09
Bijlage 10: Platform bescherming burgers 2010
Bijlage 11: Webwereld 28-07-10
Bijlage 12: Nu.nl 03-02-09 / Groen links zin in de toekomst 03-02-09
Bijlage 13: Brief gemeente Voorburg d.d. 30-12-10
Bijlage 14: Webwereld 23-03-11 / 24-12-10
Bijlage 15: Webwereld 29-10-10
Bijlage 16: Privacybarometer 03-02-11
Bijlage 17: Nu.nl 24-12-10
Bijlage 18: Nu.nl 23-03-11

Bijlage 19: Rijksoverheid 22-03-11
Bijlage 20: Ministerei van Veiligheid en Juistiei 21-03-11
Bijlage 21: Webwereld.nl 24-12-10 / Bof.nl 17-04-11 / 18-04-11
Bijlage 22: Nu.nl 25-01-11/ Automatiseringsgids.nl 16-04-11/ NRC 15-04-11
Bijlage 23: Nu.nl 19-03-08
Bijlage 24: Nu.nl 10-12-10 / 10-12-10
Bijlage 25: Nu.nl 07-11-08
Bijlage 26: Trouw 27-04-11
Bijlage 27: Zibb.nl 05-08-06
Bijlage 28: Memorie van antwoord van de staatssecretaris 28-04-09
Bijlage 29: Rijksoverheid persoonsgegevens
Bijlage 30: Gewijzigd voorstel van Rijkswet d.d. 20 januari 2009