

12. Samenvatting	75
12.1 Een juridische grondslag	75
12.2 Toepassing van biometrie	76
12.2.1 De wetgeving blijkt genegeerd te zijn	77
12.2.2 Inmenging persoonlijke levenssfeer	78
12.2.3 Het gebruik voor eigen agenda's	78
12.3 Risico's biometrie	
12.3.1 Inleiding	79
12.3.2 Een problematische situatie	79
12.3.3 Negatieve onderzoeksbevindingen	80
12.4 Wettelijke basis toegang tot gegevens ontbreekt	81
12.5 Naleving volgens het Unierecht	82
13. Mensenrechten	
13.1 Inleiding	83
13.2 Schending	84
13.3 De situatie	85
13.4 Aanpassing wetgeving	86
13.5 Tussenbalans	88
13.6 Conclusie	89
14. Toekomstige ontwikkelingen op Europees niveau	
14.1 Inleiding	91
14.2 Aantasting recht op privacy	91
14.3 De volle werking van de Verordening	92
14.4 Controverse	93
14.5 Nationale veiligheid	94
14.6 Verantwoording	95
15. Doelstelling	96
15.1 Beleidsmatig optreden	97
15.2 Een werkwijze	98
16. Slot	100
17. Conclusie	100
18. Nabeschuiving	103

12. Samenvatting

De Paspoortwet is sinds 21 september 2009 ingevoerd. En toen bleek de burger voor een voldongen feit te staan. "Wie een nieuw paspoort of nieuwe identiteitskaart haalt is verplicht vingerafdrukken af te geven." Maar wat zijn de risico's. Wat is het nut en is dit juridisch toelaatbaar?

Dit aanvullend stuk is nu voltooid. Aan het begin hadden we veel vragen. Maar nog niet alle antwoorden. Toen konden we geen conclusies trekken. Achteraf is alles helder. Het blijkt mogelijk om tot een conclusie te komen. De toedracht van de situatie zal duidelijk zijn.

12.1 De Juridische Grondslag

Het uitbrengen van de Nieuwe Paspoortwet gaat gepaard met de nodige kritiek. Haken en ogen levert dat op zullen we maar zeggen. Daartoe leidt het feitelijk alleen maar. Met name de realisering van een bepaalde doelstelling roept vraagtekens op. Een doelstelling wordt niet bereikt.

Aan de motieven van de Europese Commissie kan ook getwijfeld worden. Vooral omdat de gebruikte methodiek totaal onbruikbaar is. Het doel is nu voorbij gestreefd. Maar men gaat alleen gewoon verder. Niet zonder reden overigens. Te veel 'politieke' afwegingen zijn gemaakt.

Voor een zogeheten algemeen belang zijn daardoor mensenrechten gepasseerd. Een achtergrond is intussen duidelijk. In hoofdstuk 10.3 is dat ook omschreven. De volle werking heeft de Europese Verordening allang verloren. Opmerkelijk dat Rechter niet hebben willen ingrijpen.

In een democratie kon zoiets als vanzelfsprekend worden verondersteld. Deze wet is voor een correctie vatbaar. Zeker gelet op vaststaande feiten.

Een belang van de Europese Unie is niet gediend met zaken die zijn achterhaald. Het oude bestaande Paspoort blijkt op zich accurater te zijn. Fraude daargelaten. De nieuwe methodiek voorkomt fraude niet. Het werkt fraude nu letterlijk in de hand. Er is niet goed over nagedacht.

Het is duidelijk wat er niet klopt aan de Nieuwe Paspoortwet. Iedereen realiseert zich dat. Maar de Europese Commissie gaat gewoon verder. Zo'n verloop geeft geen aanwijzing om dezelfde koers na te streven. Op die manier weten we hoe het afloopt. Niet echt zoals het hoort. In Europa worden burgers zodoende voor anderen aangezien. Dat wijkt nogal af van de aanvankelijke bedoeling van de Verordening. Een juridische grondslag voor de Nieuwe Paspoortwet geeft te denken.

12.2 Toepassing van biometrie

Het doel met de verzameling van vingerafdrukken wordt niet bereikt. Er is geen noodzaak meer tot gegevens zoals vingerafdrukken. Van belang is te onderkennen dat vingerafdrukken nutteloos zijn gebleken. Een uitspraak van de Hoge Raad te 's-Gravenhage bevestigt dit feitelijk. Op pagina 9 in het aanvullend stuk is dat onder de voetnoot 62 vermeld. De noodzaak van vingerafdrukken voor het eerder gekozen doel valt weg. Het veroorzaakt een bedreigende situatie. Fraude ontstaat gewoon. Tegen deze achtergrond is het verzamelen van vingerafdrukken verboden. In EU-Verordening 2252/2004 is dat in art. 4 lid 3 te lezen. Een vingerafdruk mag alleen voor identiteitsbewijzen worden toegepast. Voor andere doeleinden mogen vingerafdrukken niet gebruikt worden. In de praktijk worden nog steeds vingerafdrukken afgenomen voor reisdocumenten. De verplichting ertoe is ineffectief. Zonder enig doel.¹⁷⁵ 'Handig voor later' is een te magere rechtvaardiging volgens wetgeving. Later gebruik ervan moet verenigbaar zijn met het doel van verzamelen.

¹⁷⁵ Op bladzijde 57 is onder voetnoot 151 een verwijzarrest van het EHRM aangegeven waarin de effectiviteit van een betreffende maatregel wel is meegewogen. Wat door het EU-Hof is genegeerd.

12.2.1 De Wetgeving blijkt genegeerd te zijn

In wetgeving is dat ook vastgelegd. De grondslag "selecteer voor je verzamelt" omvat mede de eis van doelbinding uit artikel 7 van de Wbp. Alsmede het verbod van bovenmatige verwerking van artikel 11 van de Wbp. En artikel 9 bepaalt verder dat het gebruik van persoonsgegevens verenigbaar moet zijn met het doel waarvoor ze feitelijk verzameld zijn.

Kortom: 'Het betekent goed nadenken over het doel van de verzameling'.

Evenals goed nadenken over het type gegeven dat nodig is. Verder ook goed nadenken of het doel met verzameling van persoonsgegevens nog bereikt kan worden. En steeds nadenken of met verzamelen doorgedaan moet worden gelet op de aard van de veiligheidsbedreiging.

De verzamelaar moet de gegevens ook feitelijk gebruiken. '*Nice to know*' is niet genoeg, '*need to know*' is een minimumvoorwaarde. Het is van belang te onderkennen dat een 'doel' van tijdelijke aard kan zijn. Soms valt de noodzaak voor het eerder gekozen doel weg. Begrijpelijk: -

"Een bedreigende situatie kan zich zo lang niet hebben voorgedaan dat er geen noodzaak meer is tot gegevensverzameling met het oog daarop."

Voor een verzameling van persoonsgegevens dient een op basis van een risicoanalyse onderbouwde noodzaak te bestaan, Ook in het veiligheidsdomein. Door te waarborgen dat er niet meer gegevens worden verzameld dan nodig wordt voorkomen dat een onevenredige inmenging in de persoonlijke levenssfeer van de burgers plaatsvindt.

Ook zorgt de grondslag 'selecteer voor je verzamelt' er voor dat de gegevens die wél noodzakelijk zijn niet als een speld in een hooiberg verdwijnen. Ook de efficiency is gebaat bij een zorgvuldige selectie. Zo versterkt deze grondslag niet alleen de persoonlijke levenssfeer maar ook de veiligheid. Die veiligheid wordt nu aan de grenzen geschaad.

Het doel waarvoor vingerafdrukken gebruikt wordt is disproportioneel.

De Europese Commissie kan de gegevens niet gebruiken. Het werkt niet.

Verzamelen van vingerafdrukken was zodoende totaal ontoelaatbaar.

12.2.2 Inmenging persoonlijke levenssfeer

Tegen deze achtergrond is sprake van een onevenredige inmenging in de persoonlijke levenssfeer van burgers. Dat plaatst alles in perspectief.

Opvallend is immers dat vingerafdrukken geen rol spelen in dit dossier. Door de overheid wordt toevoeging van biometrie ook genuanceerd.¹⁷⁶

Het nieuwe concept waarmee men fraude probeert te voorkomen faalt.

Er is totaal geen wenselijkheid om met biometrie de veiligheid van identiteitsbewijzen te garanderen. Het heeft slechts een averechts effect.

Een vervalser of de fraudeur heeft op deze manier gewoon vrijspel.¹⁷⁷

Op dat punt hoeft niet geïnvesteerd te worden qua overtuigingskracht.

12.2.3 Het gebruik voor eigen agenda's

In de praktijk zijn echter aanwijzingen dat noodzaak tot afname van vingerafdrukken hoog wordt gehouden. Terwijl dit wettelijk is verboden.

Onduidelijk is waarom dit zo'n verloop krijgt. Het is niet meer relevant.

Mogelijk speelde andere belangen daarin toch een doorslaggevende rol?

Een oorspronkelijk idee wilde de EU-Commissie blijkbaar niet loslaten. De realisering van een Europese databank moest er hoe dan ook komen.

Voor het circus van het realiseren van eigen agenda's is alles verzameld.

Het verloop is dat burgers feitelijk misleid zijn. Ofschoon alles een omslag had moeten betekenen in het voorkomen van 'look-alike' fraude.

¹⁷⁶ De beleidsmakers zijn onmiskenbaar niet verdacht geweest op de complicaties van grootschalige toepassing van een nog volop in ontwikkeling zijnde technologie. Rapport 21 februari 2012 bladzijde 33 van Prof. R. Bekker + brief Plasterk d.d. 12-02-2014. Ik citeer: "Op dit moment hebben we nog niet zoveel aan de vingerafdrukken in het paspoort" Zie onderste alinea, eerste pagina van die brief.

Toepassing van biometrie is ook door de Hoge Raad te 's-Gravenhage als middel voor de identificatie als ongeschikt verklaard. Op bladzijde 9 van dit aanvullend stuk is dat onder voetnoot 62 toegelicht.

¹⁷⁷ Zie daarvoor bladzijde 61 van dit aanvullend stuk onder het kopje 8.7, de vijfde alinea van onderen. Verder is gebleken dat terroristen na de aanslag in Parijs ongestoord reizen in Europa. (zie pagina 83).

12.3 Risico's biometrische gegevens

12.3.1 Inleiding

De Europese Commissie heeft geen greep op het steeds ingewikkelder wordende onderwerp rond biometrie. Aandacht was alleen gericht op een zo snel mogelijke uitvoering. Weinig ruimte blijkt er te zijn voor kritische vragen of de gekozen richting wel de beste is geweest.

Tekortkomingen moesten verbeterd worden. En dat is zeer zeker nodig.

In de praktijk baseert men zich op misvattingen rond de biometrie. Misvattingen die vandaag de dag nog leven onder de EU-Commissie.

Rond veel vragen omtrent de biometrie is geen sluitend antwoord. En daarop moest eerst een bevredigend antwoord komen gelet op de risico's.

Nu ambieert de Eu-Commissie ineens de realisering van een databank?

Door de onzorgvuldige selectie van het gekozen middel om fraude te voorkomen ontstaan problemen. Het besef van de lezer dringt natuurlijk in volle proporties door. We zien een glijdende schaal van de ernst van de situatie. Gegevens zijn nutteloos maar ze liggen wel op straat.

Vooraf doordat op afstand gegevens gewoon ingelezen kunnen worden.

Het is een grote dreiging voor de mensenrechten van burgers in Europa.

12.3.2 Een problematische situatie

Deze vingerafdrukken zijn opgeslagen in een op afstand uitleesbare RFID-chip in de reisdocumenten. Wat dat inhoudt is ook bekend?

Radio frequency identification (identificatie met radiogolven), is een technologie om van een afstand informatie op te slaan in en af te lezen van z.g. RFID-tags die in de paspoorten en identiteitskaarten zitten. De soort techniek ervoor is vanzelfsprekend erg zorgvuldig uitgekozen.

Op voorhand blijkt die optie voor andere doeleinden te zijn ingebouwd.

Overigens zijn een gezichtsscan en andere gegevens ook opgeslagen. Heel ondoordacht waarop gegevens in reisdocumenten zijn verwerkt. De gegevens kunnen door toevallige voorbijgangers worden ingelezen. Ik noemde het al eerder: "De wijze van verwerking is bewust bepaald". Een gezichtsscan is ondertussen al misbruikt voor doelen die niet zijn toegestaan. Ik wijd er niet verder over uit. Daaraan heb ik al aandacht besteed in het hoofdstuk 4.1 tot en met 4.3.4. van dit aanvullend stuk. Het gevaar is feitelijk dichterbij dan iemand zich überhaupt realiseert. Op termijn zullen de biometrische gegevens wellicht tot in de verste uithoeken van de wereld te vinden zijn. Als een speld in een hooiberg. Het probleem dat aan biometrie kleeft is dat niets is terug te vinden. De chaos is niet te overzien wanneer burgers er slachtoffer van worden.

12.3.3 Negatieve onderzoeksbevindingen

Een lange lijst met negatieve gevolgen van de komst van de RFID-chip is op zijn minst afschrikwekkend. De burger kan het ergste ook vrezen.

In onderzoeken zijn de bijkomende nadelen ervan opgesomd, zoals: -

- a) Opgeslagen gegevens zijn onvoldoende beschermd;
- b) Het is een hackers-gevoelig medium;
- c) Beroving van gegevens op afstand is mogelijk;
- d) Een bom is door terroristen te maken die afgaat om iemand van een bepaalde nationaliteit te vermoorden.

Deze informatie is in deel 1 van beroepschrift 09 mei 2011 terug te vinden. En wordt ook met producties onderbouwd. Zie blad 9, 23 en 24.

Identiteitsruil is op blad 19 van beroepschrift 22-03-2012 ook vermeld.

Het blootstellen van burgers aan die gevaren kan nooit de bedoeling zijn.

Verder is op het internet ook nog de nodige informatie te vinden.¹⁷⁸ Deze informatie zal menigeen vast niet zijn ontgaan. Het is zeer ernstig. Opvallend is dat de overheid in antwoord op vragen over misbruik van de RFID-technologie stelt het gebruik van deze techniek niet te staken. Een bewijs daarvoor is de productie 27 van beroepschrift 09 mei 2011. Feitelijk een goed voorbeeld hoe het middel erger is dan de kwaal. Omgekeerd blijkt de backdoor straks eigenlijk de voordeur te zijn voor bestuurders met een foute persoonlijk / ideologische agenda. Alles onder voorwendsel om paspoorten tegen fraude beter te beveiligen. Het papieren paspoort had tegen deze achtergrond meer opgeleverd. Burgers waren dan totaal gevrijwaard van enig gevaar. Nu helaas niet.

12.4 Wettelijke basis toegang tot gegevens ontbreekt

Een RFID-chip biedt de mogelijkheid van een routinematige toegang tot reisdocumenten door onbevoegden. Zoiets is niet in overeenstemming met de doelstelling. Krachtens artikel 13 van Richtlijn 95/46/EC kan toegang niet stelselmatig worden verleend. Maar alleen op ad-hoc basis in specifieke omstandigheden. Mits passende garanties worden geboden. Toegang tot reisdocumenten kan alleen worden verleend voor operaties die met de doelstelling van het "voorkomen van fraude" te verenigen is. Het beheer van gegevens wordt op deze manier draadloos vrijgegeven. De evenredigheid en de noodzaak tot de draadloze toegang is verboden. Alleen geautoriseerde mensen zijn bevoegd om deze gegevens in te zien. In het geval van de Nieuwe Paspoortwet is dat beginsel echter genegeerd.

¹⁷⁸ - De beschrijving techniek en problemen. https://en.wikipedia.org/wiki/Biometric_passport
 - Biometrie is te klonen en te kopiëren <http://www.pcworld.com/article/151734/article.html>
 - Data niet veilig opgeslagen, gevaar voor diefstal / misbruik <http://www.dexlab.nl/epassports.html>
<http://simplyrfid.typepad.com/simplyrfid1/2008/07/read-range-how-far-can-we-track-you-with-passive-rfid.html> - De data is op afstand uitleesbaar
 - Een personen traceersysteem wil men realiseren <https://edri.org/edriqramnumber2-4tracktrace/>

Het gebruik van biometrie en de toegang daartoe impliceert een zeer omvangrijke en bijzonder ernstige inmenging in de fundamentele rechten op eerbiediging van het privéleven en op bescherming van persoonsgegevens. Vooral gelet op wat zich in de praktijk voordoet.

De gevoelige persoonsgegevens zijn opgevraagd op basis van duidelijke informatie. Alleen voor identiteitsdoeleinden mogen ze worden gebruikt. Maar dat wordt nu genegeerd.¹⁷⁹ En een toereikende waarborg om een doeltreffende beveiliging van gegevens te verzekeren ontbreekt totaal.

Een gevaar van onrechtmatige toegang tot gegevens en onrechtmatig gebruik ervan is onbelangrijk gevonden door de Europese Commissie.

12.5 Naleving volgens het Unierecht

In dit verband waarborgt de Europese Commissie aldus niet volledig dat toezicht wordt gehouden op naleving van de vereisten van bescherming en beveiliging. Wat het Handvest nu verlangt. Toezicht vormt onderdeel van de eerbiediging van de bescherming van personen aangaande de verwerking van de persoonsgegevens. Vooral op basis van het Unierecht.

Op 08 april 2014 is dat in een arrest van het Europese Hof bepaald.¹⁸⁰

Gegevens moet men ook op het grondgebied van de Unie bewaren. Zoiets is een vereiste voor naleving van de bescherming en beveiliging.

Voor het beheer van de afgegeven paspoorten wil men een “Europees register” realiseren. Dat gebeurt om na te gaan of het reisdocument oorspronkelijk wel is afgegeven aan de persoon die aan de grens verschijnt. Een dergelijk voornemen roept ‘desalniettemin’ vragen op.

Hoe zijn gegevens beschermd die worden uitgewisseld tussen landen?

¹⁷⁹ In mijn beroepschrift van 22-03-2012 is op de bladzijden 19 tot en met 24 vermeld dat sprake is van doelverschuiving. Dat vingerafdrukken feitelijk ook totaal ergens anders voor zijn gebruikt.

¹⁸⁰ Het gaat om arrest C-293/12 en C-594/12 Digital Rights Ireland en Seitlinger e.a. Onder kopje 8.6.2.2 “Inzage door onbevoegden” op bladzijde 59 in dit aanvullend stuk is de achtergrond uiteengezet.

Een volgende vraag is hoe dit “Europees register” de controles aan de grens zal gaan vergemakkelijken? Niet zoals verwacht wellicht. Biometrie werkt immers niet voor het identificeren van een burger. De technologie voor uitlezen van biometrie is ontoereikend gebleken. Tegen deze achtergrond is het verzamelen van vingerafdrukken verboden. De verzamelaar moet gegevens gebruiken. Nu lukt dit niet. Het toevoegen van biometrie aan paspoorten levert geen verbetering.

13. Mensenrechten zijn geschonden

13.1 Inleiding

Voor invoering van de biometrische gegevens in 2009 is het motief duidelijk. Dat gebeurde vanwege fraudebestrijding en de voorkoming van de illegale binnenkomst van personen op het grondgebied van de Europese Unie. Aan de grenzen wordt alleen niet gecontroleerd. Momenteel is in Europa nog steeds sprake van paspoortvrij reizen. Een dergelijk feit kan niet als een welkom effect worden beschouwd. Zeker gelet op de gevolgen ervan. Terroristen kunnen gewoon reizen. Niet speculatief. “In januari 2015 kon een terrorist na een aanslag in Parijs ongestoord Frankrijk verlaten en naar Spanje vertrekken om daar naar Turkije te vliegen. Waarna zij is doorgereisd naar Syrië.”¹⁸¹

De Europese Commissie zou de buitengrenzen van de Europese Unie beter gaan controleren. Maar die belofte blijkt niet te zijn nagekomen. Opstellen van regels is één. Handhaving ervan is iets anders. Nu dus niet. Het pakket van maatregelen om fraude te voorkomen is feitelijk een lege huls en een tandeloze tijger. Maar mensenrechten zijn wel geschonden.

¹⁸¹ http://www.telegraaf.nl/buitenland/23552054/Doek_Schengen_op_.html