Rechtbank ‘s-Gravenhage
Zitting d.d. 29 november 2010

PLEITNOTITIES

Inzake

1. De stichting **STICHTING PRIVACY FIRST**, statutair gevestigd te (1013 JH) Amsterdam aan de Haarlemmerdijk 104 c, (verder ook te noemen: “Privacy First”); en **21 natuurlijke personen**;
eisers,

Advocaten: Mrs Chr.A. Alberdingk Thijm en V.A. Zwaan
Procesadvocaat: Mr W.P. den Hertog

tegen

De **STAAT DER NEDERLANDEN (MINISTERIE VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES)**,
zetelende te ‘s-Gravenhage,
gedaagde

Advocaten: Mrs C.M. Bitter en G.J.S. ter Kuile

Edelachtbaar College,

INLEIDING

1. Sinds de inwerkingtreding van de Nieuwe Paspoortwet in september 2009 hebben meer dan 3 miljoen Nederlanders een nieuw paspoort of identiteitskaart aangevraagd. Van al deze mensen (van 12 jaar en ouder) zijn 4 vingerafdrukken afgenomen en opgeslagen ten behoeve van de nog te ontwikkelen en in te richten centrale databank. Dat zijn dus al meer dan 12 miljoen vingerafdrukken.

2. Het doel van de (op termijn) centrale opslag van alle vingerafdrukken is de bestrijding van *look-alike fraude*, aldus de Staat (CvA 2.1 en 4.15). Dat is het gebruik van een paspoort door een persoon die lijkt op de paspoorthouder. Uit onderzoek van de Wetenschappelijke Raad voor het Regeringsbeleid ("WRR") blijkt dat look-alike fraude al jaren een relatief kleinschalig fenomeen is [**productie 24**]. Blijkens onderzoek van het Expertise Centrum Identiteitsfraude en Documenten van de Koninklijke Marechaussee op Schiphol is in 2009 slechts 63 keer look-alike fraude met een Nederlands reisdocument geconstateerd. De Staat heeft bij de totstandkoming van de Nieuwe Paspoortwet nagelaten het "probleem", het primaire doel van de Nieuwe Paspoortwet, te onderzoeken, laat staan te kwantificeren.

3. Op het moment is een verhit maatschappelijk debat gaande over nut en noodzaak van de (centrale) opslag van vingerafdrukken.

   - De PvdA en GroenLinks hebben de minister verzocht de bouw van de centrale Online Raadpleegbare Reisdocumentatie Administratie (ORRA) [**producties 30 & 31**] respectievelijk iedere databank met persoonsgegevens op te schorten;[1]
   - Meerdere partijen hebben tijdens een recent Algemeen Overleg hun bezorgdheid uitgesproken over het tot stand brengen van een centrale database, met name ook over de rol van het Franse bedrijf Sagem Identification (tegenwoordig Morpho) bij de opslag van vingerafdrukken en het feit dat er nog geen duidelijkheid bestaat over de beveiliging [**productie 32**];[2]
   - Europarlementariër In 't Veld heeft de Europese Commissie vragen gesteld over onder meer de proportionaliteit van de Nederlandse Nieuwe Paspoortwet en het recht op privacy en de bescherming van persoonsgegevens [**productie 29**].
   - Het weekblad De Groene Amsterdammer kwam deze maand met een themanummer over privacy, waarin meerdere deskundigen hun zorgen over de Nieuwe Paspoortwet uiten [**producties 26 en 27**], o.a. Jacob Kohnstamm, voorzitter van het College Bescherming Persoonsgegevens.
   - Ook het televisieprogramma VARA Ombudsman besteedde ruim aandacht aan het onderwerp [**producties 35 & 36**].

[1] http://www.nu.nl/politiek/2385996/groenlinks-wil-tijdelijk-verbod-databases.html
[2] *Kamerstukken II* 2010/11, 25 764, nr. 44, p. 3-4, 6, 8, 9-11 en 14.

4. Deze maand verschenen ook twee rapporten van de WRR over de Nieuwe Paspoortwet, die een tamelijk onthutsend beeld schetsen. Het rapport “Happy landings? Het biometrische paspoort als zwarte doos”, geschreven door Vincent Böhre [**productie 24**] en het rapport “Het biometrische paspoort in Nederland: Crash of zachte landing” van Max Snijder. Het rapport van Snijder, managing partner van the European Biometrics Forum en voorzitter van de International Biometrics Advisory Council (IBAC), verscheen afgelopen vrijdag (26 november 2010) en is te raadplegen op de website van de WRR.[3]

5. Enkele conclusies van de WRR-uitgaven luiden als volgt.

   - In de loop van de parlementaire geschiedenis van de Nieuwe Paspoortwet is er steeds minder aandacht voor de privacy van burgers en wordt deze steeds meer ondergeschikt aan terrorismebestrijding (Böhre, p. 48 en p. 147);
   - *“Bij de nieuwe Paspoortwet stelde men zich collectief ten doel om (vrijwel ongekwantificeerde) look-a-like fraude te gaan bestrijden en dit primaire doel heiligde blijkbaar de middelen, inclusief grootschalige, amper beproefde middelen waarvan algemeen werd toegegeven dat die een inbreuk op de privacy van alle burgers zouden maken.”* (Böhre, p. 148);
   - De effectiviteit van het gebruik van biometrie ter bestrijding van look-alike fraude is feitelijk niet onderzocht (Böhre, p. 54);
   - De totstandkoming van de Nieuwe Paspoortwet getuigt van een structureel gebrek aan transparantie bij het ministerie van BZK en agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (“BPR”), die niet ontvankelijk was voor kritiek, inderdepartementaal overleg en externe advisering (Böhre, p. 44 en p. 150-153);
   - BPR negeerde en archiveerde een zeer kritisch TNO-rapport uit 1999 over de toepassing van biometrie (Snijder, p. 91);
   - De Nederlandse overheid heeft de Nieuwe Paspoortwet aanvankelijk opgezet voor *verificatie*, maar is zich vanaf circa 2005 gaan concentreren op *identificatie* in verband met opsporing, vervolging en terrorismebestrijding (Snijder, p. 87 en p. 132);
   - Het opgezette systeem – het verificatiesysteem – is echter onbruikbaar voor identificatie (Snijder, p. 133);

[3] http://www.wrr.nl/content.jsp?objectid=5545

- Hoe grootschaliger een systeem ter identificatie, hoe meer fouten er zullen optreden (Snijder, p. 133);
- De weinige voorbereidende studies en onderzoeken zijn onbruikbaar voor de beslissing het verificatiesyteem ook als identificatiesysteem te gebruiken (Snijder, p. 134);
- De veiligheid is bij geen enkele proef of studie grondig onderzocht (Snijder, p. 119), men heeft zich geconcentreerd op de inpassing van biometrie in bestaande processen (Snijder, p. 136);
- Technische voorzieningen en procedures zijn op het punt van veiligheid, betrouwbaarheid en integriteit niet getest, laat staan ontworpen (Snijder, p. 120)
- Het systeem zal juist tot meer identiteitsfraude leiden, omdat het eenvoudig is te manipuleren is (Snijder, p. 136).

6. Het is goed dat er op dit moment een maatschappelijk debat over de Nieuwe Paspoortwet wordt gevoerd, maar het is te laat. De wet is tamelijk geruisloos door het parlement geloodst en er wordt sinds september 2009 uitvoering aan gegeven. Minister Donner heeft al aangegeven niet van plan te zijn de bouw van de centrale reisdocumentenadministratie (ORRA) op te schorten. [4] We zijn begonnen aan een sociaal-biometrisch experiment waarvan de consequenties op zijn best onduidelijk en op zijn slechts rampzalig zijn. Dit proces is onomkeerbaar, tenzij uw Rechtbank intervenieert. Het belang van deze procedure is daarmee wel gegeven.

WAARTEGEN WORDT BEZWAAR GEMAAKT?

7. De teneur van de Conclusie van Antwoord (CvA) van de Staat is dat er in wezen niet zoveel verandert met de Nieuwe Paspoortwet. Er werden al gegevens opgeslagen en die gegevens konden ook voor opsporingsdoeleinden worden opgevraagd. Om die reden is het goed om aan te geven in hoeverre de situatie is veranderd en waar Privacy Bezwaar bezwaar tegen maakt:
   a. De creatie van een positief register, in plaats van het negatieve register waarin de oude Paspoortwet voorzag (alinea's 22-24 Dv).

[4] *Aanhangsel Handelingen II* 2010-11, nr. 456.

NB: De bezwaren tegen het positieve register zijn nadrukkelijk niet beperkt tot de opname van *vingerafdrukken* in dit register. Dat blijkt ook duidelijk uit alinea 24 Dv.

b. De *centrale* opslag van alle paspoortgegevens en de (al dan niet centrale) opslag van vingerafdrukken (alinea's 25-36 Dv);
c. Het verstrekkingenregime, zowel wat betreft vingerafdrukken als wat betreft overige paspoortgegevens (alinea's 37-46 Dv);
d. De veelheid aan (vage) delegatiewetgeving (alinea's 47-53 Dv);
e. De veelheid aan (open gefromuleerde en niet uitgewerkte) doeleinden waarvoor alle gegevens kunnen worden opgeslagen en gebruikt (alinea's 63-73 Dv);
f. De wijze waarop *uitvoering* wordt gegeven aan de Nieuwe Paspoortwet.

PRIVACY FIRST

8. Stichting Privacy First (hierna "Privacy First") stelt zich, kort gezegd, ten doel het bevorderen en behouden van het recht op privacy in de ruimste zin van het woord [**productie 15**].

9. Het belangrijkste dossier waarmee Privacy First zich bezighoudt, is de Nieuwe Paspoortwet. Privacy First staat desverzocht een ieder bij die gevraagd wordt vingerafdrukken te verstrekken bij het aanvragen van een reisdocument. In dat kader beantwoordt Privacy First veel juridische en praktische vragen. Ook heeft zij de zogenaamde GemeenteGarantieBrief opgesteld. Met behulp van deze standaard brief kunnen burgers de gemeente waar zij hun vingerafdrukken moeten afgeven, verzoeken te verklaren dat de nodige waarborgen in acht worden genomen ten aanzien van de verwerking van die gegevens.

BIOMETRIE

10. Biometrische kenmerken zijn meetbare patronen van het menselijk lichaam, zoals gezichts- en vingerafdrukken. Omdat geen twee opnames van dezelfde kenmerken identiek zijn, zal aan de hand van kansberekening moeten worden vastgesteld of het om één en dezelfde persoon gaat. Nadat biometrische kenmerken zijn afgenomen, moeten deze worden opgeslagen voor verificatie. Dat kan op een kaart of in een database. In Nederland gebeurt dat dus zowel op een kaart (de chip op het reisdocument) als in een database. Er is echter een belangrijk verschil in het vinden van een "match". In het ene geval gaat om een één-op-

één vergelijking, terwijl het bij een database gaat om een één-op-veel zoekactie (1:n search). Zie Snijder, p. 13.

11. Bij het bepalen van het doel van een biometrisch systeem dient een onderscheid te worden gemaakt tussen het vaststellen van de identiteit ("identificatie") en het verifiëren van de identiteit ("verificatie"). Bij identificatie wordt gebruik gemaakt van een database waarin naar de bekende identiteit gezocht. Hierbij is typerend dat hoe groter de database wordt, hoe groter de kans wordt dat meerdere identiteiten worden gevonden. Om die kans te verkleinen werken deze systemen, waarmee justitie vaak werkt, op basis van tien vingers. *Verificatie* met behulp van biometrie is echter een ander proces. Daarbij vindt eerst een identiteitsclaim plaats, bijvoorbeeld met een paspoort, die vervolgens wordt gecontroleerd door de biometrie. Deze is daarom opgeslagen op dezelfde informatiedrager die de identiteitsclaim bevat. Zie Snijder, p. 17.

JURIDISCH KADER

12. Privacy First beroept zich in deze procedure onder meer op schending door de Staat van diverse beginselen van het recht op privacy, zoals deze zijn verankerd in de Europese Privacyrichtlijn (Richtlijn 95/46/EG, hierna "Privacyrichtlijn"), de Wet bescherming persoonsgegevens, artikel 16 van het Verdrag betreffende de werking van de EU en artikel 8 van het EVRM. Een en ander is uitvoerig onderbouwd in de dagvaarding. Ik beperk mij in het navolgende tot het benoemen van deze privacybeginselen en een beknopte uiteenzetting op welke wijze deze beginselen met voeten worden getreden met de Nieuwe Paspoortwet. Het betreft de volgende beginselen:
    a. Legitimiteit en noodzaak;
    b. Proportionaliteit en subsidiariteit;
    c. Transparantie;
    d. Doelbinding;
    e. Zorgvuldigheid; en
    f. Verbod op verwerking van bijzondere gegevens.

a. Legitimiteit en noodzaak

13. Het bestrijden van look-alike fraude kan in beginsel een legitiem doel zijn voor een overheidsmaatregel. Het is daarbij echter wel van belang dat de noodzaak wordt

aangetoond. Die noodzaak volgt wat betreft de afname van biometrie en opslag op de chip in het paspoort of identiteitsbewijs uit de Verordening. Maar niet meer dan dat. Zie overweging 5 van Verordening 444/2009 [**productie 13**]:

> *"Verordening (EG) nr. 2252/2004 voorziet niet in een rechtsgrondslag voor het opzetten of bijhouden van gegevensdatabanken voor de opslag van deze gegevens in de lidstaten."* [onderstreping adv.]

14. Dat geldt met name nadrukkelijk *niet* voor de ontwikkeling van een centrale databank, het verstrekkingenregime en de wijze waarop de Nieuwe Paspoortwet wordt uitgevoerd, in afwachting van de creatie van de centrale databank. De Staat heeft nagelaten van al deze aspecten de legitimiteit of de noodzaak aan te tonen. Op een recent verzoek van Tweede Kamerlid Van Raak cijfers van look-a-like fraude aan de Kamer te verstrekken, antwoordde de verantwoordelijk staatssecretaris nota bene dat dergelijke cijfers haar niet bekend zijn dus dat zij deze ook niet aan de Kamer kan toesturen [**productie 30**].

15. Hiervoor gaf ik al aan dat er in 2009 slechts 63 keer look-alike fraude met een Nederlands reisdocument is geconstateerd. Ook als niet-gesignaleerde gevallen erbij op zouden worden geteld, zou het naar schatting slechts om 130 gevallen gaan. De geconstateerde gevallen betroffen bovendien fraude met sociaal-economische doeleinden en geen gevallen van zware criminaliteit of terrorisme. Het aantal gevallen van look-alike fraude met Nederlandse reisdocumenten neemt bovendien al jaren af [**productie 24**, p. 37].

16. Een ander doel genoemd door de Staat voor de maatregelen in de Nieuwe Paspoortwet betreft de wens het voor burgers mogelijk te maken ook in andere gemeenten dan hun woonplaats reisdocumenten aan te vragen (alinea 2.5 CvA). In april 2006 is echter uit onderzoek van het agentschap BPR (Basisadministratie Persoonsgegevens en Reisdocumenten) gebleken dat plaatsonafhankelijke aanvraag en uitgifte van paspoorten juist zou kunnen leiden tot een *toename* van look-alike fraude.

17. Bovendien is het aanleggen van een centrale database geen geschikt middel om look-alike fraude te bestrijden. Het gaat daarbij immers om verificatie, niet om identificatie. Opslag van de biometrische gegevens op het reisdocument voldoet daarvoor. Gelet op het feit dat look-alike fraude nauwelijks voorkomt en dat het aanleggen van een centrale datrabase geen

geschikt middel is om het te bestrijden, is geen sprake van enige legitimiteit of noodzaak om deze maatregelen door te voeren.

b. Proportionaliteit & subsidiariteit

18. Uit het feit dat de genoemde maatregelen niet noodzakelijk zijn vloeit voort dat deze ook buitenproportioneel zijn en daarmee, onder meer, strijdig met artikel 8 EVRM. De beoordeling van de proportionaliteit vereist een belangenafweging tussen de belangen van de Staat en die van de aanvragers van reisdocumenten.

19. De Staat heeft daarbij niet veel eigen beoordelingsruimte. Dat blijkt uit het Marper-arrest van het EHRM over de opname van onder meer vingerafdrukken van verdachten in een nationale database van Engeland [**productie 21**]. Het EHRM oordeelde dat het feit dat andere landen, ondanks de voordelen, niet tot een dergelijke maatregel over zijn gegaan, tot gevolg heeft dat er maar een beperkte *margin of appreciation* is (r.o. 112). Anders dan de Staat impliceert (alinea 4.25), vond het EHRM de opslag van *vingerafdrukken* in een databank wel degelijk een inbreuk op de privacy.

> *"While true, this consideration cannot alter the fact that fingerprints objectively contain unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances. They are thus capable of affecting his or her private life and retention of this information without the consent of the individual concerned cannot be regarded as neutral or insignificant. (…) … the retention of fingerprints constitutes an interference with the right of respect for private life."* (r.o. 84 & 86)

20. Opvallend is dat de Staat in de CvA concludeert dat de nieuwe reisdocumentenadministratie aan alle vereisten van artikel 8 EVRM voldoet, zonder dat überhaupt een belangenafweging wordt gemaakt. Volgens de Staat zijn diens belangen bij de administratie voldoende om te concluderen dat de maatregelen proportioneel zijn (alinea's 4.14-4.18 CvA). Die redenering gaat natuurlijk niet op.

21. Wanneer tot een belangenafweging wordt overgegaan, kan niet anders worden geconcludeerd dan dat geen sprake is van proportionaliteit. Zoals ik zojuist al aangaf, is het probleem dat de Staat wil oplossen door de Staat niet gekwantificeerd en blijkt uit andere

cijfers dat het een relatief klein probleem is. Bovendien kunnen de maatregelen niet leiden tot een oplossing van het probleem, terwijl de inbreuk op de privacy significant is.

22. Ook uit het Marper-arrest blijkt dat in casu geen sprake is van proportionaliteit. Het EHRM oordeelde dat het opzetten van een landelijke database voor opsporingsdoeleinden waarin onder meer vingerafdrukken voor onbeperkte tijd werden opgeslagen, niet voldeed aan het vereiste van proportionaliteit.

23. Ook belangrijk vond het hof het algemene en non-discriminatiore karakter van de Engelse maatregel. De vingerafdrukken en andere persoonsgegevens werden opgeslagen ongeacht de zwaarte van de verdenking, de leeftijd van de verdachte en voor onbepaalde tijd.

> *"In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society. This conclusion obviates the need for the Court to consider the applicants' criticism regarding the adequacy of certain particular safeguards, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data. Accordingly, there has been a violation of Article 8 of the Convention in the present case."*

24. De Staat betoogt dat het Marper-arrest niet van toepassing is, omdat het daar ging om opsporingsregister, waarin ook personen die niet langer van een strafbaar feit werden verdacht waren opgenomen. Maar dat is juist precies de situatie die zich hier voordoet. In de centrale databank zijn immers zowel verdachten opgenomen als personen die niet (langer) verdacht worden van een strafbaar feit. Onschuldige burgers worden op gelijke voet behandeld als verdachten. In wezen stigmatiseert het centrale register de gehele Nederlandse bevolking van 12 jaar en ouder met een reisdocument. Dat is juist wat het EHRM in strijd met artikel 8 EVRM achtte.

"Of particular concern in the present context is the risk of stigmatisation, stemming from the fact that persons in the position of the applicants, who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons."

Het verstrekkingenregime

25. Een aparte afweging dient gemaakt te worden ten aanzien van het verstrekkingenregime. Door de Staat wordt in alinea's 4.19-4.23 wel een erg summiere belangenafweging gemaakt ten aanzien van het verstrekkingenregime in de Nieuwe Paspoortwet. Deze maatregel zou, kort gezegd, proportioneel zijn, omdat

a. het eerder ook al mogelijk was gegevens uit reisdocumentenadministraties te verkrijgen;
b. het doel en de toegang beperkt zijn en er beveiligingsmaatregelen zijn getroffen; en
c. bevoegdheden zouden aansluiten bij artikel 126nc Sv.

26. Deze redenen kunnen echter niet leiden tot de conclusie dat sprake is van proportionaliteit.

Ad a)

27. In de eerste plaats geldt dat uit de "oude" reisdocumentenadministraties minder gegevens worden verkregen, omdat er minder gegevens werden opgeslagen. Met name in het kader van opsporingsdoeleinden kan men zich wel voorstellen dat vingerafdrukken nu juist zeer gevoelige gegevens zijn, die eerder niet konden worden opgevraagd en nu wel. Dat is nu juist waartegen bezwaar wordt gemaakt. Bij herhaling wordt gesteld dat de impact daarvan klein zou zijn, omdat de officier ook altijd zou moeten beschikken over een foto en een naam in combinatie met een vingerafdruk. In de praktijk zal er echter wel degelijk op vingerafdrukken kunnen worden gezocht, zoals ook door Snijder wordt uitgelegd:

"Deze waarborg hebben we vaker gehoord en klinkt geruststellend. Maar technisch gezien zitten er een paar onduidelijkheden in die daar potentieel afbreuk aan kunnen doen. Want de zoekfunctie op basis van de foto gaat in zo'n grote database niet werken. Studies hadden uitgewezen dat 1:1 verificatie op basis van het gelaat al niet goed genoeg presteert (zie paragraaf 8.6 Technical Survey). Bij een 1:n zoekactie in een database van 17.000.000 foto's van zeer matige kwaliteit zullen de fouten vele malen groter zijn. Het lezen van het geslacht is 50% kans. De uiteindelijke zoekactie zal dan toch gebaseerd moeten zijn op de vingerafdrukken. De verdachte hoeft dan niet fysiek

aanwezig te zijn: je neemt een hele slechte foto van een willekeurig iemand, van wie je weet dat daar honderden of duizenden hits op kunnen komen. Die kun je verder negeren. Je gokt het geslacht, waarmee je in elk geval ca. 8.500.00 hits hebt. Komt er geen hit uit, dan probeer je het nog eens op basis van het andere geslacht en dan heb je de gehele bevolking op basis van de vingerafdrukken doorzocht." (Snijder, p. 121)

Ad b)

28. Indien persoonsgegevens worden verwerkt, moeten altijd bepaalde waarborgen in acht worden genomen, waaronder beperking van de gebruiksdoelen en toegang en adequate beveiliging. Hierna zal nog aan de orde komen dat daaraan in casu niet is voldaan. Maar zelfs als dat wel zo zou zijn, kan dat op zichzelf niet de conclusie rechtvaardigen dat sprake is van proportionaliteit. Het zijn immers voorwaarden waaraan *altijd* moet worden voldaan.

Ad c)

29. Het verstrekkingenregime van de Nieuwe Paspoortwet kan niet worden vergeleken met artikel 126nc Sv, zoals de Staat doet voorkomen. Artikel 126nc heeft *verificatie* tot doel en niet *identificatie*, zoals het verstrekkingenregime in de Nieuwe Paspoortwet.[5] De administratieve kenmerken die kunnen worden opgevraagd, moeten iets zeggen over de relatie tussen de verdachte en de instelling van wie de gegevens worden opgevraagd. Bijvoorbeeld de vraag of een verdachte een bankrekening heeft bij een bepaalde bank. Bovendien biedt artikel 126nc de officier niet de mogelijkheid een vingerafdruk te vergelijken met de vingerafdrukken van alle Nederlandse burgers.

Subsidiariteit

30. Op grond van het beginsel van subsidiariteit had de Staat zichzelf de vraag moeten stellen of look-alike fraude ook op een andere manier kan worden bestreden, een manier waarbij de persoonlijke levenssfeer van de Nederlandse bevolking niet of minder vergaand wordt aangetast. Hierboven is al aangegeven dat opslag in de chip op het reisdocument afdoende is voor de verificatie die nodig is om look-alike fraude tegen te gaan. Voorzover aanvullende maatregelen zouden worden overwogen, is een centrale database niet een voor de hand liggende aanvulling. Andere en betere maatregelen zijn bijvoorbeeld strengere grenscontroles, het opleggen van hogere straffen of het opleggen van andere sancties. Met name gelet op het feit dat look-alike fraude voornamelijk om sociaal-economische redenen

[5] Kamerstukken II 2003/04, 29 441, nr. 3, p. 21.

wordt gepleegd, is het denkbaar dat sociaal-economische sancties effectief zijn. De Staat heeft echter in het geheel geen onderzoek gedaan naar alternatieven.

31. Dat is te meer opmerkelijk nu Nederland binnen de EU betrekkelijk alleen staat in de centrale opslag van biometrie. In Duitsland is het zelfs verboden.

32. Volgens het EHRM had Engeland in het Marper-arrest niet aangetoond dat de betreffende doelen alleen op deze manier konden worden bereikt (116). In deze zaak heeft de Staat ook geenszins aangetoond waarom de bestrijding van look-alike fraude juist op deze manier moet worden aangepakt.

c. Transparantie

33. Alle privacywetgeving verplicht tot transparantie ten aanzien van een beperking op de privacy cq. een verwerking van persoonsgegevens. Op grond van artikel 8 EVRM moet een beperking op de privacy *voorzienbaar* zijn. In de Dv is al aangegeven dat de maatregelen in de Nieuwe Paspoortwet niet voldoende voorzienbaar zijn in de zin van artikel 8 EVRM. Veel regels moeten immers nog nader worden uitgewerkt bij AMv(R)B. Het betreft hier belangrijke aspecten zoals de beveiliging van de centrale database ten behoeven waarvan nu al zoveel vingerafdrukken zijn afgenomen en de termijn dat de vingerafdrukken zullen worden bewaard (zie ook alinea 4.44 CvA). Uit het Marper-arrest [**productie 21**] blijkt dat daarom niet aan de vereiste voorzienbaarheid is voldaan:

> *"It reiterates that it is as essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness."* (r.o. 99)

34. Op grond van artikel 6b lid 1 sub b Privacyrichtlijn (artikel 7 Wbp) mogen persoonsgegevens alleen worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Op grond van artikel 10 Privacyrichtlijn (art. 33 lid 2 Wbp) moet de betrokkene worden geïnformeerd over de doeleinden van de verwerking.

35. Aan deze vereisten van transparantie wordt in de Nieuwe Paspoortwet en de uitvoering daarvan niet voldaan. De Staat heeft in de zomer van 2009 huis-aan-huis een folder verspreid [**productie 25**]. Daarin is louter aangegeven dat vanaf 21 september 2009 vingerafdrukken moeten worden afgegeven bij aanvraag van een paspoort of identiteitskaart. Er staat vermeld dat de Europese Unie hiervoor in 2004 een verordening heeft opgesteld en dat het doel daarvan is misbruik van reisdocumenten zoveel mogelijk tegen te gaan. Over de vele andere doeleinden waarvoor de gegevens kunnen worden gebruikt (zoals opsporing en vervolging) is niets opgenomen. Bij het aanvragen van een paspoort bij lokale gemeenten wordt evenmin enige informatie aan burgers verstrekt. Daar bestaat geen enkel beleid voor, laat staan een informatiefolder.

36. Bovendien worden burgers ontmoedigd om gebruik te maken van hun wettelijke recht (artikel 36 Wbp) om te verzoeken de gegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Op de website Paspoortinformatie.nl is vermeld dat geen bezwaar kan worden gemaakt tegen de opname van vingerafdrukken in de reisdocumentenadministratie, omdat sprake is van een wettelijk voorschrift waarvan niet kan worden afgeweken.

d. Doelbinding

37. Het primaire doel van de creatie van centrale database, zo geeft de Staat aan, is het tegengaan van look-alike fraude. Voorzover andere doeleinden worden nagestreefd dienen deze op grond van het beginsel van doelbinding verenigbaar te zijn met dit oorspronkelijke doel. In artikel 4b van de Nieuwe Paspoortwet worden tal van (nieuwe) doeleinden opgesomd, die betrekking hebben op *identificatie* (o.a. identificatie van slachtoffers en de opsporing en vervolging van strafbare feiten). Bovendien, zo heeft de staatssecretaris aangegeven, moeten de doeleinden voor verstrekking nog worden vastgesteld bij AMvB [zie **productie 19**]. De database zal voornamelijk worden gebruikt voor identificatie (waartoe het niet geschikt is), terwijl verificatie om look-alike fraude te bestrijden het oorspronkelijke doel is.

38. In de Dv is daarnaast uitgebreid gewezen op het risico van het verschuiven van de doeleinden waarvoor de persoonsgegevens in de nieuwe reisdocumentenadministratie mogen worden gebruikt (alinea's 68-71), ook wel *function creep* genoemd. Zoals Kamerlid Van Raak in het Algemeen Overleg van 7 oktober dit jaar terecht zei: het creëren van het

databestand zal straks het gebruik creëren.[6] Daarvoor wordt ook nog eens expliciet gewaarschuwd door de senior consultant public security van TNO Defence in het WRR Rapport van Böhre.

> *"Met betrekking tot de centrale database is sprake van een glijdende schaal. In eerste instantie zou de database worden afgeschermd en alleen bestemd zijn voor duplicate checks; net als bij het RAAS. De doelstelling was slechts het checken van 1:1; het kunnen verifiëren of iemand de eigenaar is van een bepaald reisdocument. (…) Maar als het nu alleen in heel uitzonderlijke gevallen [ook strafvorderlijk] geraadpleegd mag worden, dan mag het over 10 jaar voor een winkeldiefstal."* [onderstreping adv.] [**productie 24**, p. 92]

39. Volgens de Staat kan van function creep geen sprake zijn, nu daarvoor de wet zou moeten worden gewijzigd. Die stelling berust op een onjuist begrip van het verschijnsel function creep. Puur het feit dat de database bestaat, doet het risico ontstaan dat deze later voor andere dan de oorspronkelijke doeleinden kan worden gebruikt. Als deze niet wordt aangelegd, kan hij later immers ook niet voor andere doelen worden gebruikt. Dat voor ander gebruik een wetswijziging nodig zou zijn, is irrelevant. Dat is overigens ook nog maar de vraag, nu verstrekkingsdoeleinden ook nader bij AMvB kunnen worden uitgewerkt.

40. Ook uit het arrest Marper blijkt dat vrees voor gebruik in de toekomst wel degelijk relevant is.

> *In Van der Velden, the Court considered that, given the use to which cellular material in particular could conceivably be put in the future, the systematic retention of that material was sufficiently intrusive to disclose interference with the right to respect for private life (see Van der Velden cited above). The Government criticised that conclusion on the ground that it speculated on the theoretical future use of samples and that there was no such interference at present.*
> *The Court maintains its view that an individual's concern about the possible future use of private information retained by the authorities is legitimate and relevant to a determination of the issue of whether there has been an interference. Indeed, bearing in mind the rapid pace of developments in the field of genetics and information technology,*

[6] *Kamerstukken II* 2010/11, 25 764, nr. 44, p. 15.

the Court cannot discount the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today. Accordingly, the Court does not find any sufficient reason to depart from its finding in the Van der Velden case. (r.o. 70-71) [onderstreping adv.]

e. Zorgvuldigheid

41. Dat de risico's van het creëren van een positief register, het (centraal) opslaan van (biometrische) gegevens en het verstrekken van dergelijke gegevens aan politie en justitie en andere partijen enorme risico's inhoudt, behoeft weinig betoog. Juist daarom moet extra zorgvuldigheid worden betracht. Daarvan is echter geen sprake.

Valse vingerafdrukken en vingerafdrukken van slechte kwaliteit

42. In de eerste plaats is het eenvoudig om op basis van de vingerafdruk van iemand anders een paspoort aan te vragen. Dat geeft Snijder ook aan in de uitzending van VARA Ombudsman [**productie 36**]. Je kunt binnen tien minuten een siliconenafdruk maken van de vingerafdruk van een ander, die nauwelijks te zien is als je hem over je eigen vinger legt. In de hierboven aangehaalde WRR-publicatie van Snijder gaat hij verder uitgebreid in op de vele technische manco's van het gecreëerde systeem.

43. In de tweede plaats zijn niet alle afgenomen vingerafdrukken van voldoende kwaliteit, mede omdat het baliepersoneel bij de gemeentes geen verplichte training hebben gevolgd. Opmerkelijk is verder dat de staatssecretaris heeft besloten dat bij ouderen boven de 70 jaar slechts één vingerafdruk zal worden opgenomen, terwijl de kwaliteit van die ene afdruk slechter is.

44. Als gevolg daarvan kan de eigenaar van de vingerafdruk voor iemand anders worden aangezien (bijvoorbeeld degene wiens vingerafdrukken op een plaats delict worden aangetroffen) of kan hij juist voor iemand anders doorgaan (bijvoorbeeld degene die juist niet op een plaats delict aanwezig was). Volgens Snijder is dat - vanuit technologisch oogpunt – de tweede fout van de Nieuwe Paspoortwet. Hij geeft aan dat het systeem fouten gaat maken als een opgeslagen vingerafdruk van slechte kwaliteit is.

45. Ondanks deze gevaren, zijn gemeenten niet bevoegd de vingerafdrukken controleren van degene die een paspoort komt afhalen. Dat is volgens een brief van de staatssecretaris van 17 september 2009 alleen toegestaan als er twijfel bestaat over de identiteit van de persoon.[7] Dat wordt ook bevestigd op de website van BPR:

> *"Let wel: Het verifiëren van de vingerafdrukken bij de uitgifte van een reisdocument moet alleen plaatsvinden als wordt getwijfeld of de persoon die het document komt ophalen ook de aanvrager van dat document is geweest."*[8]

b. Hacking & beveiliging

46. Als wordt ingebroken in een database waarin persoonsgegevens, en met name biometrische gegevens, van mensen zijn opgeslagen dan zijn de gevolgen zeer ernstig. Die gevolgen zijn nog veel groter als het gaat om een centrale database, omdat men met één inbraak dan meteen over de gegevens van iedereen beschikt. Ook CBP voorzitter Kohnstamm wijst er in de uitzending van VARA Ombudsman op dat de centrale database riskeert gebruikt te worden door mensen die hacken [**producties 35 & 36**].

47. De veiligheid van de (centrale) opslag van biometrische gegevens is door de regering in de parlementaire geschiedenis steeds gesteld, maar nooit bewezen [**productie 24**, p.148]. De staatssecretaris heeft wel toegegeven dat nooit 100% kan worden uitgesloten dat onbevoegden toegang krijgen tot de database en dan niet op voorhand kan worden aangegeven wat voor gevolgen dat zal hebben voor de mensen van wie gegevens in de database zijn opgenomen. Als een burger schade zou leiden als gevolg van onrechtmatige toegang, dan moet dan worden bekeken wie aansprakelijk is voor die schade, zo wordt gesteld.[9]

48. Ondanks dat de centrale database nog niet tot stand is gebracht, worden zoals gezegd wel al sinds september 2009 vingerafdrukken ten behoeve van de centrale database afgenomen en decentraal opgeslagen bij de verschillende gemeenten. De wijze waarop de meer dan 12 miljoen opgeslagen vingerafdrukken zijn beveiligd, is geregeld in de

[7] *Kamerstukken II* 2009/10, 31 324 (R1844), nr. 23.
[8] http://www.bprbzk.nl/Reisdocumenten/Nieuws/Retourdocumenten_in_verband_met_mislukte_verificatie_vingerafdruk
[9] *Kamerstukken I* 2008/09, 31 324, nr. C, p. 2.

Paspoortuitvoeringsregelingen 2001. Daarin is geen enkele beveiligingsmaatregel opgenomen die speciaal is gericht op de beveiliging van vingerafdrukken.

49. De Staat beweert dat het CBP zich in 2007 lovend zou hebben uitgelaten over de voorgestelde beveiliging van de centrale database. Dat is een onjuiste voorstelling van zaken. Het CBP heeft aangegeven waardering te hebben voor de voorgestelde maatregelen, maar waarschuwt daarbij expliciet dat bij elke vorm van grootschalige collecties onvoorzien veel mogelijkheden tot onterechte toegang zullen bestaan. Ook waarschuwt het CBP dat grote collecties gegevens van belang een aantrekkelijk aanvalsobject zijn voor hackers en/of criminelen en dat het CBP een nadere uitwerking mist van maatregelen die getroffen worden als het systeem feitelijk gehacked wordt.

f. Verbod op verwerking bijzondere persoonsgegevens

50. Op grond van artikel 16 Wbp (artikel 8 lid 1 Privacyrichtlijn) is het verboden om *bijzondere persoonsgegevens* te verwerken. Vingerafdrukken moeten worden aangemerkt als bijzondere gegevens, omdat daaruit informatie over de gezondheid kan worden afgeleid.

51. Vingerafdrukken zijn bijzondere persoonsgegevens, omdat ze in verband kunnen worden gebracht met iemands gezondheid. De volgende aandoeningen kunnen worden gedetecteerd aan de hand van vingerafdrukken: syndroom van Down, syndroom van Hunter (ontbrekend X-chromosoom bij vrouwen), syndroom van Klinefelter (extra X-chromosoom bij mannen), aangeboren verstoppingen van het maag-darmkanaal, aangeboren rodehond (door infectie van de moeder), aanleg voor borstkanker, aanleg voor een hartinfarct.

52. Gezondsheidsgegevens mogen alleen worden verwerkt door partijen als hulpverleners, verzekeraars en scholen. Bestuursorganen mogen gezondsheidsgegevens alleen verwerken voorzover dat *noodzakelijk* is voor een goede uitvoering van wettelijke voorschriften. In casu is dus geen sprake van uitzonderingssituaties waardoor bijzondere persoonsgegevens zouden mogen worden verwerkt.

ONTVANKELIJKHEID

53. De Staat heeft zich in zijn CvA op het standpunt gesteld dat zowel Privacy First als de 21 eisers/natuurlijke personen niet ontvankelijk zijn. De ontvankelijkheidsverweren van de Staat ten aanzien van Privacy First en de 21 natuurlijke personen zal ik gezamenlijk bespreken.

54. Volgens de Staat heeft Privacy First geen *eigen* belang bij deze procedure, maar zou zij slechts optreden ter behartiging van de gebundelde belangen van natuurlijke personen die een reisdocument aanvragen. In een dergelijk geval, zo betoogt de Staat, brengt een behoorlijke taakverdeling tussen bestuursrechter en burgerlijke rechter mee dat Privacy First niet in haar vorderingen bij de burgerlijke rechter wordt ontvangen. Het verweer van de Staat gaat in deze zaak niet op.

55. Ten eerste treedt Privacy First niet op in het kader van een *groepsactie*. De collectieve actie die Privacy First met deze procedure in heeft gesteld op grond van artikel 3:305a BW, moet worden aangemerkt als a*lgemeen belangactie*. De personen om wie het hier gaat zijn immers niet te individualiseren. De actie is gericht op de behartiging van het privacybelang van alle Nederlanders boven de 12 jaar die een paspoort of identiteitskaart aanvragen. Het belang heeft daarmee een dermate algemeen karakter, dat het een facet vormt van ieders bestaan. Privacy First treedt op in het algemeen belang van de bescherming van de privacy van alle Nederlandse burgers.

56. Privacy First heeft ten tweede wel degelijk een *eigen* belang naast het belang van Nederlanders die een reisdocument wensen aan te vragen. Haar belang is allereerst ideëel van karakter, hetgeen evenzeer als eigen belang kan worden aangemerkt als een vermogensrechtelijk belang.[10] Privacy First is opgericht met als doel het bevorderen en behouden van het recht op privacy. De Nieuwe Paspoortwet is naar mening van Privacy First op belangrijke onderdelen in strijd met het recht op privacy en alleen al vanuit haar ideële belang tegen inbreuken op de privacy op te treden, is Privacy First ontvankelijk in haar vorderingen. Ten tweede heeft Privacy First echter eveneens een vermogensrechtelijk belang. Zij staat een ieder bij die gevraagd wordt vingerafdrukken te verstrekken bij de aanvraag van een reisdocument. Indien al die individuen Privacy First benaderen voor hulp bij een gang naar de bestuursrechter, wordt het de Stichting financieel en feitelijk onmogelijk gemaakt haar werk te doen en haar statutaire doel na te streven. Daarnaast vertrekt zij advies over de Nieuwe Paspoortwet, hetgeen een kostbare en tijdsintensieve activiteit is.

[10] *Kamerstukken II* 1991-1992 , 22 486, nr. 3, p. 22 (*MvT*).

Het eigen belang van Privacy First is dan ook daarin gelegen dat in één procedure de onrechtmatigheid van de Nieuwe Paspoortwet aan de orde wordt gesteld in plaats van dat individuele burgers de onverbindendheid van de wet in ieder concreet geval aan de orde moeten stellen bij de bestuursrechter. Nu Privacy First derhalve in deze procedure een eigen belang heeft (gesteld), is zij ontvankelijk, zelfs indien zou worden aangenomen dat sprake is van een groepsactie en niet van een algemeen belangactie zo oordeelde de Hoge Raad.[11]

57. Overigens stellen ook de gemeenten dat de gang naar de burgerlijke de juiste weg is. De Nederlandse Vereniging van Burgerzaken (NVVB) en de Vereniging van Nederlandse Gemeenten (VNG) schrijven aan de privacyorganisatie Vrijbit het volgende:

> *"Wij zijn van mening dat er tegen overheidsbesluiten zoals in casu aan de orde, een sluitend systeem van rechtsbescherming voor belanghebbenden bestaat. Wij denken dan ook dat de weg die door 'Privacy First' is ingeslagen, de juiste is. NVVB en VNG wachten daarom de uitkomsten van de bodemprocedure af."*[12]

58. Ten derde kunnen de 21 eisers/natuurlijke personen hun belangen niet behartigen in de rechtsgang bij de bestuursrechter, zodat tevens het ontvankelijkheidsverweer van de Staat ten aanzien van hen niet opgaat. Ook zij vorderen in deze procedure immers (onder meer) een verklaring voor recht dat de Nieuwe Paspoortwet jegens hen een onrechtmatige daad oplevert hetgeen een belang is dat zij niet in de rechtsgang bij de bestuursrechter kunnen dienen. Zij kunnen bij een rechtsgang naar de bestuursrechter slechts de onverbindendheid van de Nieuwe Paspoortwet in hun concrete geval trachten te bewerkstelligen.

59. Ten vierde is in deze zaak wel degelijk sprake van een onnodige omweg indien Privacy First de betrokken natuurlijk personen de bestuursrechtelijke rechtsgang in zou sturen met als doel de onverbindendheid van de Nieuwe Paspoortwet aan de orde te stellen. Anders dan de Staat stelt in 3.3 van zijn CvA, zijn de 21 eisers/natuurlijke personen namelijk niet genoodzaakt reisdocumenten aan te vragen. Dat maakt deze zaak ook anders dan die in het door de Staat aangehaalde arrest van de Hoge raad van 9 juli 2010, waarin het ging om de aanvraag van een verblijfsvergunning de situatie in het door de Staat genoemde arrest van

[11] Hoge Raad 3 september 2004, LJN: AO7808, *NJ* 2006, 28 (*Staat/VJAN en NJCM*) en Hoge Raad 9 juli 2010, LJN: BM2314 (*Staat/Vreemdelingenorganisaties*).
[12] Brief van 4 augustus 2010 aan Vrijbit, aangehaald bij Böhre, p. 137.

–. De eisen van een doeltreffende rechtsbescherming tegen de overheid brengen mee dat de burger een geschil omtrent de verbindendheid van het voorschrift aan de burgerlijke rechter moet kunnen voorleggen, zolang de beslechting van het geschil niet aan de bestuursrechter is opgedragen.

60. Zie in dit verband ook het arrest van de Hoge Raad in de zaak Leenders/Ubbergen, dat volledig van toepassing is op de onderhavige zaak:

> *"Indien de overheid het standpunt inneemt dat een burger voor het verrichten van bepaalde handelingen, zoals het uitoefenen van een bepaalde vorm van bedrijf of beroep, ingevolge een algemeen verbindend voorschrift een vergunning nodig heeft, maar die burger dit voorschrift onverbindend en daarom het inroepen en handhaven ervan jegens hem onrechtmatig acht, brengen de eisen van een doeltreffende rechtsbescherming tegen de overheid mee dat hij het geschil omtrent de verbindendheid van het voorschrift aan de rechter moet kunnen voorleggen. Zolang de beslechting van een dergelijk geschil niet aan de bestuursrechter is opgedragen — hetgeen destijds, ingevolge art. 2 van de hier toepasselijke Wet Arob niet het geval was, en thans, zolang art. 8:2 Awb nog niet is vervallen, evenmin het geval is — moet die burger de vraag of het voorschrift verbindend is, in beginsel door middel van een vordering gegrond op onrechtmatig overheidsoptreden kunnen voorleggen aan de burgerlijke rechter. Dit laatste wordt niet anders doordat, indien de burger zonder de vereiste vergunning handelt en tegen hem — aangenomen dat handelen zonder vergunning strafbaar is gesteld — een strafvervolging wordt ingesteld of bestuursdwang wordt toegepast, de verbindendheid van de desbetreffende regeling kan worden getoetst in een procedure voor de strafrechter resp. de bestuursrechter. Niet kan immers van de burger worden verlangd dat hij, hoezeer ook ervan overtuigd dat de regeling onverbindend is, het op een strafvervolging of toepassing van bestuursdwang laat aankomen om die onverbindendheid in rechte te doen vaststellen.*
>
> *Evenmin kan in voormelde situatie van de burger worden gevergd dat hij, uitsluitend teneinde de vraag of de regeling onverbindend is, aan het oordeel van de rechter te kunnen onderwerpen, de vergunning voor zover nodig en onder aantekening van zijn zienswijze omtrent de verbindendheid van de regeling aanvraagt, vervolgens tegen de beschikking waarbij de vergunning wordt*

verleend, een bezwaarschrift indient en zo nodig tegen de beslissing daarop beroep instelt bij de bestuursrechter. Met het oog op een doeltreffende, waarborgen tegen misverstanden biedende regeling van rechtsbescherming tegen de overheid moet worden aangenomen dat ook het openstaan van deze weinig voor de hand liggende weg blokkering van de toegang tot de burgerlijke rechter niet kan rechtvaardigen. Dit brengt mee dat deze toegang ook openblijft wanneer de burger — zoals hier — slechts de eerste stadia van voormelde weg heeft afgelegd, d.w.z. desgevraagd een vergunning heeft verkregen en een bezwaarschrift heeft ingediend, maar zich nadien, in stede van deze weg te vervolgen tot de burgerlijke rechter wendt teneinde deze voormelde vraag te doen beslissen. Daarom kan in een dergelijk geval, óók indien ervan zou moeten worden uitgegaan dat de formele rechtskracht van de beschikking waarbij de vergunning is verleend, zich mede uitstrekt tot het oordeel van de verlenende instantie dat de desbetreffende regeling verbindend is, niet worden aanvaard dat de burgerlijke rechter in het in voege als voormeld door de burger tegen de overheid aangespannen geding op grond van die formele rechtskracht aan dat oordeel van de overheid is gebonden."[13]

VORDERINGEN

61. Eisers hebben hun vorderingen aangepast in de eerste plaats om deze te verduidelijken, nu de Staat in haar CvA ten onrechte stelde dat deze onbegrijpelijk waren. In de tweede plaats is een vordering toegevoegd die ziet op de wijze waarop uitvoering wordt gegevens aan de Nieuwe Paspoortwet. Zoals in de dagvaarding uitgebreid aan de orde is gekomen, heeft de Staat in het kader van de Nieuwe Paspoortwet niet in voldoende waarborgen voorzien ter bescherming van de persoonlijke levenssfeer van burgers.

62. Voor de volledigheid benadruk ik dat eisers de rechtbank verzoeken, voorzover er onverhoopt enige twijfel zou bestaan over het toewijzen van de vorderingen, vragen van uitleg te stellen aan het Hof van Justitie van de Europese Gemeenschappen.

CONCLUSIE

[13] Hoge raad 11 oktober 1996, LJN: ZC2169, *NJ* 1997, 165 (*Leenders/Ubbergen*) rov. 3.4.3 en 3.4.4.

Ik concludeer tot toewijzing van de vorderingen met veroordeling van de Staat in de kosten van de procedure.

Deze procedure wordt behandeld door
Mrs. Chr.A. Alberdingk Thijm & V.A. Zwaan
SOLV Advocaten
Postbus 75538, 1070 AM Amsterdam
T: 020-5300160, F: 020-5300170