

## PDF hosted at the Radboud Repository of the Radboud University Nijmegen

The following full text is a publisher's version.

For additional information about this publication click this link.

<http://hdl.handle.net/2066/73979>

Please be advised that this information was generated on 2021-09-23 and may be subject to change.

# Verantwoordelijkheden van vervoerders in grenscontrole. Nut en noodzaak van doorgifte van passagiersgegevens

195

## Trefwoorden:

passagiersgegevens, terrorismebestrijding, vervoerders

**Vervoersmaatschappijen worden meer en meer door overheden ingezet in het kader van controle op de reisbewegingen van burgers. Na 9 september 2001 en de aanslagen daarna is deze neiging versterkt onder het mom van terrorismebestrijding. Er is veel onduidelijkheid over deze verplichting om passagiersgegevens door te geven. Welke gegevens moeten worden doorgegeven en met welk doel? Wat kan men met deze gegevens? Wat betekent dit voor luchtvaartmaatschappijen?**

**Met dit artikel probeert de schrijfster meer duidelijkheid te geven over deze ontwikkelingen, waarbij zij zich vooral richt op de vraag wat het verschil is tussen soorten passagiersgegevens en wat nut en noodzaak zijn van het doorgeven ervan.**

## 1 Inleiding

Vervoersmaatschappijen zoals luchtvaartmaatschappijen en rederijen worden al langer door overheden gebruikt in het kader van grenscontroles.<sup>2</sup> Deze organisaties moeten controleren of hun passagiers beschikken over de benodigde geldige reisdocumenten, om zo te voorkomen dat zij 'inadmissibles' vervoeren – passagiers die niet voldoen aan de voorwaarden voor toegang.

De aanslagen in de Verenigde Staten in 2001 en in Madrid en Londen in 2004 en 2005 beïnvloedden in sterke mate de visie van overheden op migratie en migratiecontrole. Steeds meer worden reizigers als mogelijke terroristen en als bedreiging voor de openbare orde en binnenlandse veiligheid

gezien.<sup>3</sup> Coleman stelt dat de identificatie van de daders als 'buitenlands' het immigratiebeleid in de schijnwerpers zette.<sup>4</sup> Volgens Guild is het gezicht van de vreemdeling zelfs getransformeerd tot prima facie het gezicht van terrorisme.<sup>5</sup>

Deze zienswijze heeft gevolgen voor de wijze waarop grenscontrole wordt vormgegeven. Dit blijkt ook uit de veranderende verantwoordelijkheden van particuliere vervoersbedrijven. Naast het controleren van documenten om illegale migratie tegen te gaan, kregen vervoerders tevens verantwoordelijkheden in het kader van terrorismebestrijding. Zij zijn verplicht gegevens over hun passagiers te verzamelen en door te geven aan immigratieautoriteiten. In de hiernavolgende paragrafen wordt hierop verder ingegaan.

## 2 Nederland: de afschrijfplicht

Vervoerders zijn al langer verplicht om het vervoer van ongewenste vreemdelingen naar het grondgebied van de EU te voorkomen. Wanneer een vervoerder toch een passagier vervoert die aan de grens geweigerd wordt, moet de desbetreffende vervoersonderneming deze terugbrengen naar het land van herkomst. Ook kan een sanctie opgelegd worden aan de vervoerder. Dit beleid wordt dan ook vaak 'carrier sanctions' genoemd. In Nederland moeten luchtvervoerders sinds 1995 op vluchten vanaf bepaalde 'risico'-luchthavens een kopie of scan maken van documenten van passagiers. Dit is de zogenaamde afschrijfplicht.<sup>6</sup> Deze kopieën worden, desgevraagd, na aankomst in Nederland aan de autoriteiten overhandigd. Het doel van de afschrijfplichting is om van 'inadmissibles' vast te kunnen stellen waarvandaan en met welke vervoerder zij naar Nederland zijn gekomen. Op deze manier kunnen immigratieautoriteiten ook van ongedocumenteerde reizigers achterhalen vanuit welke land ze komen zodat eventuele asielaanvragen geëvalueerd en terugkeer makkelijker geëffectueerd kan worden, mede doordat een

1 Sophie Scholten is werkzaam bij het Instituut voor Rechtssociologie, Radboud Universiteit Nijmegen.

2 O.a. A.R. Zolberg, 'The Archaeology of "Remote Control"' en K. Wüstenbecker, 'Hamburg and the Transit of East European Emigrants', in: A. Fahrmeir a.o. (red.), *Migration Control in the North Atlantic World: the Evolution of State practices in Europe and the US from the French Revolution to the inter-war period*, Oxford: Berg-hahn, p. 195-222.

3 Zie onder andere: A. Baldaccini and E. Guild (red.), *Terrorism and the Foreigner: A Decade of Tension around the Rule of law in Europe*, Leiden: Martinus Nijhoff Publishers 2007; E. Brouwer, P. Catz and E. Guild (red.), *Immigration, Asylum and Terrorism. A Changing Dynamic in European Law*, Nijmegen: Recht en Samenleving 2003; V. Mitsilegas 'Border Security in the European Union: Towards Centralised Controls and Maximum Surveillance', in: E. Guild, H. Toner and A. Baldaccini (red.), *Developments in EU Asylum and Immigration Law*, Oxford: Hart Publishing 2007 en H. Oosterom-

Staples, 'Using National Security and Public Policy to Combat Terrorism: The Case of the Netherlands', *European Journal of Migration and Law*, vol. 10, nr. 1, p. 51-75.

4 N. Coleman, 'From Gulf War to Gulf War' in: A. Baldaccini and E. Guild (red.), *Terrorism and the Foreigner: A Decade of Tension around the Rule of law in Europe*, Leiden: Martinus Nijhoff Publishers 2007, p. 49.

5 E. Guild in: E. Brouwer, P. Catz and E. Guild (red.), *Immigration, Asylum and Terrorism. A Changing Dynamic in European Law*, Nijmegen: Recht en Samenleving 2003, p. 7.

6 Art.4 (2) Vreemdelingenwet 2000 (VW 2000). Zie voor de lijst van risicoluchthavens bijlage 1 Vreemdelingenvoorschrift. Deze wordt iedere zes maanden bijgewerkt. Op deze lijst hebben onder andere steden gestaan als Londen, Toronto en Genève, steden die over het algemeen niet direct worden gezien als 'asiel producerend'.

claim tot terugvervoeren bij de desbetreffende vervoerder gelegd kan worden.<sup>7</sup>

### 3 Richtlijn 2004/82/EG: API-gegevens

Ook Europese regelgeving dwingt vervoerders gegevens over reizigers te verzamelen en door te geven. Richtlijn 2004/82/EG<sup>8</sup> schrijft voor dat lidstaten de nodige maatregelen moeten nemen om vervoerders te verplichten voor het eind van de instapcontroles, desgevraagd, informatie te verstrekken over de passagiers die zij zullen vervoeren. Deze gegevens moeten elektronisch worden doorgezonden aan de autoriteiten met het oog op het verbeteren van grenscontroles en het bestrijden van illegale immigratie.<sup>9</sup> Wanneer vervoerders deze gegevens niet doorgeven, of wanneer zij incomplete of onjuiste gegevens verstrekken, kan een boete worden opgelegd.

De informatie die luchtvervoerders volgens deze richtlijn moeten verstrekken, zijn gegevens over de vlucht, zoals aankomsttijd, aantal passagiers en vertrekpunt, in combinatie met 'Advanced Passenger Information' (API). API-gegevens zijn die gegevens waarmee iemands identiteit kan worden vastgesteld en die in een paspoort zijn opgenomen, zoals naam, nationaliteit, geboortedatum, paspoortnummer, et cetera. API-data worden verzameld en geverifieerd op het moment van inchecken. In steeds meer paspoorten staan deze gegevens in de scanbare zone van het paspoort, de zogenaamde 'Machine Readable Zone' (MRZ).

Het initiatief tot deze richtlijn werd in januari 2003 door Spanje genomen.<sup>10</sup> Volgens Spanje zou het doorgeven van API-data direct nadat de passagiers zijn ingestapt bijdragen tot een efficiëntere controle bij binnenkomst doordat er meer tijd zal zijn voor een grondig onderzoek.<sup>11</sup> In dit voorstel lag de nadruk op het tegengaan van illegale immigratie, al wilde een aantal lidstaten (Duitsland, Verenigd Koninkrijk en Nederland) meer aandacht besteden aan de bijdrage van deze richtlijn in de strijd tegen terrorisme. Nederland verwachtte zelfs alleen effect voor het bestrijden van terrorisme en niet voor het bestrijden van illegale migratie.<sup>12</sup>

Het oorspronkelijke voorstel bepaalde dat passagiersgegevens uitsluitend verstrekt moeten worden om de uitvoering van de controle aan de grens te vergemakkelijken. De lidstaten moeten de verstrekte gegevens vernietigen nadat de controle is uitgevoerd.<sup>13</sup> Deze termijn werd in latere versies op 24 uur gesteld. Dit betekende dat verzamelde gegevens alleen gebruikt mochten worden voor grenscontrole, zonder dat deze verder bewaard mochten worden. De Britse en Nederlandse delegatie maakten – in eerste instantie zonder succes – bezwaar tegen deze bepaling die de duur van de opslag beperkte en daardoor ook de mogelijkheid om gege-

vens met andere autoriteiten (politie, douane) te delen, beperkte.

In maart 2004 vonden de aanslagen in Madrid plaats. Onder invloed van deze aanslagen en onder druk van het Verenigd Koninkrijk werd de richtlijn op twee belangrijke punten wezenlijk uitgebreid: de bewaartermijn van passagiersgegevens is uitgebreid van 24 uur naar een onbepaalde tijd en het doel van de maatregel werd verruimd, waardoor autoriteiten passagiersgegevens nu ook mogen gebruiken voor wetshandhavingsdoeleinden, bijvoorbeeld terrorismebestrijding.

De invloed van de aanslagen in Madrid in maart 2004 blijkt ook uit de verklaring van de Europese Raad met betrekking tot het bestrijden van terrorisme van 26 maart 2004.<sup>14</sup> In deze verklaring, waarnaar wordt verwezen in de richtlijn, benadrukte de Raad dat de besprekingen over maatregelen op het gebied van terrorisme moeten worden bespoedigd en dat snel voortgang zal worden gemaakt met, onder andere, de richtlijn over het doorgeven van passagiersgegevens.<sup>15</sup> De Nederlandse Minister van Justitie stelt tevens dat deze richtlijn 'wel een zeker momentum [heeft] gekregen in het kader van terrorismebestrijding'.<sup>16</sup> Mitsilegas spreekt in deze context over 'post-Madrid urgency'.<sup>17</sup> Ondanks deze verschuiving naar terrorismebestrijding, wordt in considerans 1, 7 en 9 en in art. 1 van de richtlijn, evenals in latere documenten, deze maatregel nog altijd vooral als instrument tegen illegale migratie gepresenteerd.

De deadline voor de omzetting van de richtlijn liep af op 5 september 2006. De manier van omzetting is niet uniform en loopt uiteen van implementatie in de Terrorismewet (Frankrijk), de Politiewet (Duitsland), de Transportwet (Litouwen), of de Vreemdelingenwet (Bulgarije, Nederland, Finland). In Nederland is de richtlijn in wetgeving omgezet in juli 2007, bijna een jaar na het verstrijken van de deadline voor omzetting. Er is echter tot op heden nog geen sprake van het daadwerkelijk toepassen van deze regelgeving in Nederland, buiten de al bestaande afschriftplicht.

### 4 Terrorisbestrijding in de EU: ontwerp-kaderbesluit over het gebruik van PNR-gegevens

Terwijl in de meeste landen nog geen of weinig ervaring was opgedaan met de richtlijn presenteerde de Europese Commissie op 6 november 2007 een nieuw ontwerp-kaderbesluit om passagiersgegevens te gebruiken in de strijd tegen terrorisme en georganiseerde misdaad.<sup>18</sup> Luchtvaartmaatschappijen die van en naar de EU vliegen, moeten, volgens dit voorstel, 'Passenger Name Record' (PNR)-gegevens beschikbaar stellen aan een 'Passenger Information Unit' (PIU), die in

7 Terugkeernota maatregelen voor een effectievere uitvoering van het terugkeerbeleid 2003, *Handelingen II* 2003/04, 29 344, nr. 1.

8 *PbEU* 2004, L 261/24-2, 6 augustus 2004.

9 Richtlijn 2004/82/EG, art. 3(1) en art. 1.

10 Doc. 5174/03, 9 januari 2003.

11 Doc. 5174/03, 9 januari 2003.

12 Doc. 13363/03, 15 oktober 2003.

13 *PbEU* C 82/23 (Doc. 7161/03), art. 4(1).

14 European Council Meeting 25 maart 2004.

15 Doc. 8078/04, 27 april 2003, overweging 2.

16 *Kamerstukken II* 2003/04, 23 490, nr. 325, p. 11.

17 V. Mitsilegas, 'Contrôle des étrangers, des passagers, des citoyens: surveillance et anti-terrorisme', *Cultures & Confl* 2005, no. 58, p. 155-181.

18 COM (2007) 645 definitief, 6 november 2007. Voorstel voor een kaderbesluit van de Raad over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor wetshandhavingsdoeleinden.

iedere lidstaat zal worden gevormd. PNR-data zijn gegevens die worden verzameld in het reserveringssysteem van een luchtvaartmaatschappij wanneer een vlucht geboekt wordt. Het gaat dan om betalingsgegevens, ticket-informatie, (veranderingen in) reisroutes, stoelinformatie, contactgegevens, et cetera. Deze gegevens moeten door luchtvaartmaatschappijen op twee momenten aan de PIU worden verzonden: 24 uur voor vertrek en na de check-in.<sup>19</sup> De PIU in de desbetreffende lidstaat zal de data analyseren en risicobeoordelingen uitvoeren. Gegevens van verdachte personen zullen door de PIU worden doorgestuurd naar de autoriteiten in die lidstaat.

PNR-gegevens zijn volgens de Europese Commissie een zeer belangrijk instrument in de aanpak van terrorisme, omdat met PNR-gegevens risicobeoordelingen kunnen worden uitgevoerd en verbanden tussen bekende en onbekende personen worden gelegd. De Europese Commissie stelt dat 'the conception and planning of terrorist attacks involves traveling by air.' 'Terrorists and organised criminals are mobile and increasingly more so. They travel abroad to plan and execute their sinister activities.'<sup>20</sup> Door 'unknown high-risk passengers' te identificeren, zo argumenteert de Commissie, kunnen deze onderworpen worden aan een tweede controle en eventuele ondervraging bij aankomst terwijl andere passagiers minder controles hoeven te ondergaan. Volgens de Europese Commissie zijn wetshandhavingautoriteiten in de hele wereld zich sinds 11 september 2001 bewust geworden van de toegevoegde waarde van het verzamelen en analyseren van PNR-gegevens bij bestrijding van het terrorisme.<sup>21</sup>

De afgelopen jaren zijn verschillende landen PNR-gegevens gaan verzamelen in het kader van terrorismebestrijding. Zo sloot de EU akkoorden over de overdracht van passagiersgegevens met de VS en Canada. Momenteel wordt door de Europese Commissie overleg gevoerd met Australië. Nieuw-Zeeland heeft hiervoor eveneens een verzoek ingediend. Ook Zuid-Korea heeft inmiddels PNR-data gevraagd van Europese luchtvaartmaatschappijen. Frankrijk, het Verenigd Koninkrijk en Denemarken zijn bezig met wetgeving op dit terrein.<sup>22</sup> Volgens de Commissie heeft de EU kunnen leren van ervaringen in de VS, Canada en het Verenigd Koninkrijk waar een soortgelijk systeem al bestaat. In het Verenigd Koninkrijk zou dit systeem verschillende arrestaties hebben opgeleverd en hebben bijgedragen tot de ontdekking van mensensmokkelnetwerken en het verkrijgen van waardevolle informatie met betrekking tot terrorisme. De Europese Commissie is dus optimistisch over de effectiviteit. Toch ontbreken tot op heden rapporten die dit succes ondersteunen. De mate van succes van reeds bestaande systemen en de mate waarin het analyseren van PNR- of API-gegevens hieraan heeft bijgedragen, is niet helder.

De geschatte kosten van dit nieuwe voorstel zijn overigens aanzienlijk. Volgens de Impact Assessment zal het Europese Luchtvaartmaatschappijen ongeveer € 1 200 000 kosten om een systeem op te zetten om gegevens naar autoriteiten te sturen. Terugkerende kosten, waaronder onderhoud, personeel en het gebruiken van het systeem, schat de Commissie op € 5 435 321 per jaar.<sup>23</sup>

## 5 Verschil API- en PNR-data

Nu de Commissie zo snel na Richtlijn 2004/82/EG een nieuw plan lanceerde om passagiersgegevens te gebruiken, rijst de vraag wat eigenlijk de mogelijkheden zijn van het gebruik van passagiersgegevens.

### 5.1 PNR-data

Deze gegevens worden verzameld in de reserveringssystemen van luchtvaartmaatschappijen wanneer een vlucht geboekt wordt. In principe bevatten deze gegevens geen identificeerbare data-elementen zoals paspoortnummer en geboortedatum, die worden pas bij de check-in aan de passagier gevraagd. In het EU-PNR-plan gaat het om negentien datavelden die, mits ingevuld, doorgegeven moeten worden.<sup>24</sup> Hieronder vallen ook zogenaamde vrije-tekstvelden. Gemiddeld bestaat een PNR echter uit 6 – 10 data-elementen. PNR-data worden maar in een aantal gevallen rechtstreeks aan de vervoerder verstrekt. Een groot deel van de boekingen gaat via reisagenten, in welk geval de luchtvaartmaatschappij – uit commerciële overwegingen – vaak alleen die PNR-elementen van de reisagent krijgt, die nodig zijn om de vlucht uit te voeren. Ongeveer 48 uur voor de vlucht worden PNR-gegevens uit de reserveringssystemen in het 'Departure Control Systeem' (DCS) gezet. Op het moment van inchecken worden deze data aangevuld met gegevens als stoelnummer en hoeveelheid bagage.

### 5.2 API-gegevens

API-gegevens zijn paspoortgegevens die in steeds meer paspoorten in de MRZ van het paspoort staan en gescand kunnen worden (of anders handmatig worden ingevoerd). API-gegevens worden bij het inchecken verzameld en gecontroleerd. Onder andere Canada, de VS, Mexico, China en Zuid-Korea vragen deze informatie ten behoeve van de grenscontrole. De VS wil naast de paspoortgegevens ook het land van vestiging weten en het adres waar men in de VS verblijft. API-gegevens worden in de meeste gevallen gebruikt in het kader van migratiecontrole. Met behulp van de API-gegevens kunnen autoriteiten kijken of reizigers vermeld staan op terrorisme 'watch-lists' of gemeld staan in het Schengen Informatie Systeem.

Er zijn veel verschillen tussen systemen die API- of PNR-

matie; reisagent; informatie over bevestigingen, check-in status, 'no show'- of 'go show'-informatie; gesplitste PNR-data; opmerkingen (exclusief gevoelige informatie); ticket-informatie zoals ticket-nummer, datum van ticket-uitgifte, enkele tickets; stoelnummer en andere informatie over plaats; code share informatie; bagage-informatie; nummer en naam van andere reizigers op het PNR; verzamelde API-gegevens; veranderingen in bovenstaande gegevens.

19 Art. 5 voorstel-kaderbesluit. COM (2007) 654, 22 oktober 2007.

20 MEMO/07/449, 6 november 2007.

21 COM (2007) 654 definitief, 6 november 2007.

22 SEC (2007) 1453, 6 november 2007, p. 10.

23 SEC (2007) 1453, 6 november 2007.

24 PNR record locator; datum van reservering/uitgifte van ticket; reisdatum; naam; adres en contact informatie; informatie over betaling, inclusief adresgegevens; reisroute; frequent flyer infor-

gegevens gebruiken. Hoe deze zich tot elkaar verhouden wordt in het ontwerp-kaderbesluit PNR nog niet uitgelegd. De status van Richtlijn 2004/82/EG in dit voorstel is dan ook niet duidelijk. Volgens de Commissie kunnen de gegevens die in het kader van de API-Richtlijn moeten worden doorgegeven, slechts gebruikt worden om reeds bij de autoriteiten bekende terroristen en criminelen te identificeren. De verplichtingen voor vervoerders in het nieuwe EU-PNR-plan moeten dan ook gescheiden blijven van verplichtingen in het kader van Richtlijn 2004/82/EG.<sup>25</sup> Betekent dit dat deze gegevens niet gebruikt zullen worden in het kader van terrorismebestrijding? Of kan juist een combinatie van PNR- en API-gegevens waardevol zijn? De uitleg van het EU-PNR-plan is in die zin summier.

Enkele belangrijke verschillen bij het gebruik van API- of PNR-gegevens zijn:

- Betrouwbaarheid van gegevens: PNR-gegevens worden door de passagier aangeleverd en zijn dus manipuleerbaar en niet erg betrouwbaar. Kwaadwillende passagiers zullen er waarschijnlijk voor zorgen dan hun PNR-gegevens geen aanleiding geven tot verder onderzoek. API-data worden weliswaar later aangeleverd dan PNR-gegevens omdat ze pas bij de check-in verzameld kunnen worden, maar zijn betrouwbaarder.
- Systeem van gegevensuitwisseling: PNR-data worden verzameld in een reeds bestaand systeem, het reserveringssysteem, dat luchtvaartmaatschappijen en reisagenten gebruiken voor het boeken van vluchten. Luchtvaartmaatschappijen verzamelen PNR-data dus al, maar voor een ander doel. API-gegevens moeten nog verzameld worden, en werden niet eerder door luchtvaartmaatschappijen verzameld zoals bij PNR-data.
- Tijdstip: API-gegevens kunnen pas worden verzameld bij het inchecken, en kunnen dus pas worden verstuurd wanneer het inchecken is voltooid. PNR-gegevens worden verzameld wanneer de vlucht geboekt wordt. Deze PNR-data moeten volgens het EU-PNR-plan 24 uur voor de vlucht en net na het inchecken worden verzonden, zodat er meer tijd is om gegevens te analyseren dan bij API-data.
- Doel: API-gegevens worden meestal gebruikt in het kader van grensbewaking, zo ook in Richtlijn 2004/82/EG. Volgens het EU-PNR-voorstel zullen PNR-data gebruikt worden voor wetshandavingsdoeleinden, waaronder terrorismebestrijding. Met API-data wordt gecontroleerd bij bestaande watch lists: verdachte reizigers zijn dan al bekend. PNR-gegevens worden gebruikt om risicobeoordelingen uit te voeren en om zo ook onbekende 'high risk'-passagiers te identificeren. Hoe analyses gemaakt zullen worden op basis van PNR-gegevens én of API- en PNR-gegevens gecombineerd zullen worden wordt niet duidelijk in het voorstel-kaderbesluit.
- Risico: Bij beide systemen spelen vragen met betrekking tot databescherming van burgers. Gegevens worden voor een zeer lange tijd bewaard en kunnen zelfs met andere

instanties en in het nieuwe PNR-voorstel zelfs met andere (lid)staten gedeeld worden. PNR-gegevens kunnen bovendien gevoelige informatie bevatten die inzicht kunnen geven in politieke stroming, etniciteit, medicatie, seksuele voorkeur, et cetera. Ook al schrijft het concept-kaderbesluit voor dat deze gegevens niet gebruikt zullen worden door de PIU's, het doorgeven van deze gegevens blijft vanuit privacy-oogpunt bezwaarlijk.<sup>26</sup> Een risico voor overheden is dat PNR-data door de reiziger worden aangeleverd en daardoor niet betrouwbaar hoeven te zijn.

- Gegevensverstrekking 'push'- versus 'pull'-systeem. Bij een 'pull'-systeem kunnen de autoriteiten zelf gegevens halen uit reserveringssystemen van luchtvaartmaatschappijen. Bij een 'push'-systeem sturen vervoerders de gegevens naar de autoriteiten. Vanuit het oogpunt van privacybescherming heeft het de voorkeur gegevens via de 'push'-methode uit te wisselen, volgens het concept-kaderbesluit zal dat systeem dan ook verplicht worden voor Europese luchtvervoerders. In het geval van API-gegevens is er altijd sprake van 'push'.
- Bewaartermijn: Zowel in Richtlijn 2004/82/EG als in het ontwerp-kaderbesluit PNR kunnen gegevens geruime tijd bewaard worden. In de API-Richtlijn moeten de gegevens in principe na 24 uur worden vernietigd 'tenzij deze later nodig zijn voor de uitoefening van de wettelijke taken van de autoriteiten die belast zijn met de controle van personen aan de buitengrenzen', in welk geval er geen beperking meer geldt. PNR-data worden in het ontwerp-kaderbesluit vijf jaar bewaard in een actieve database en daarna nog eens acht jaar in een minder toegankelijke databank.

## 6 Reacties op het voorstel-kaderbesluit

Het voorstel-kaderbesluit is door verschillende organisaties en instanties met gemengde gevoelens ontvangen. In een informele JBZ-Raad op 25 januari 2008 bleek er in de Raad 'zeer brede steun' voor dit voorstel te zijn.<sup>27</sup> Volgens de meeste lidstaten zouden de verplichtingen in de toekomst zelfs moeten gelden voor meer vervoersorganisaties dan alleen luchtvervoerders. Tevens werd de wens uitgesproken dat op termijn ook intra-EU-vluchten onderworpen zouden worden aan deze verplichting en dat de reikwijdte van het voorstel uitgebreid zou worden naar zware (in plaats van alleen georganiseerde) criminaliteit. Ook de Nederlandse regering staat positief ten opzichte van het EU-PNR-plan en verwijst naar het succes van bestaande soortgelijke systemen in het Verenigd Koninkrijk, de VS en Canada.<sup>28</sup> Wel vraagt de Nederlandse regering zich af waarom niet is gekozen voor gebruik van API-gegevens ten behoeve van terrorismebestrijding en wat de betekenis is van API na de invoering van een EU-PNR-systeem.

De Europese Data Toezichthouder (EDPS) onderschrijft het doel van het plan maar vindt dat onvoldoende aandacht is

25 COM (2007) 654 definitief, 6 november 2007, considerans 5, p. 9.

26 Een aantal lidstaten pleit ervoor deze data toch te gebruiken in uitzonderlijke omstandigheden. Doc. 7656/2/08 Rev. 2, 17 april 2008, p. 6.

27 Doc. 9514/08, 23 mei 2008.

28 BNC-fiche 1 Kaderbesluit persoonsgegevens van passagiers (PNR-gegevens).

29 PbEU 2008, C 110/1-15, 1 mei 2008.



besteed aan de noodzaak van het verzamelen van PNR-gegevens.<sup>29</sup> De EDPS noemt de maatregel 'intrusive' terwijl de 'utility' nog lang niet is aangetoond. Volgens de EDPS worden de behaalde resultaten in de VS en het Verenigd Koninkrijk onvoldoende aangetoond en bevestigen andere rapporten evenmin het geclaimde succes. Ook de Artikel 29-werkgroep, een onafhankelijk adviserend orgaan van de EU met betrekking tot databescherming en privacy, concludeert dat nut en noodzaak nog niet voldoende zijn aangetoond. Deze werkgroep oordeelt dat het voorstel disproportioneel is en dat het fundamentele principes van gegevensbescherming schaadt. Het is een stap verder in de richting van een 'European surveillance society'.<sup>30</sup>

Het Nederlandse parlement vroeg in een motie de regering pas op de plaats te maken met het EU-PNR-plan in verband met de vele onduidelijkheden met betrekking tot de effectiviteit van het verzamelen van PNR-gegevens.<sup>31</sup> Ook de Duitse Bundesrat (Bondsraad) redeneert kritisch dat, 'eine Ausweitung der Erhebung und Speicherung von Fluggastdaten nicht beschlossen werden [soll] solange nicht feststeht, dass sich die bisherigen Rechtsinstrumenten als unzureichend erwiesen haben. Es wird deshalb angeregt, zunächst die Wirkungen der Richtlinie 2004/82/EG zu untersuchen'.<sup>32</sup>

De 'Association of European Airlines' (AEA) benadrukte in een reactie dat 'security of citizens cannot be the responsibility – financially or otherwise – of airlines (...) should remain the exclusive task of national authorities'.<sup>33</sup> Ook betwijfelt de AEA of PNR-data betrouwbaar genoeg zijn, in tegenstelling tot API-gegevens. Ten slotte vreest de AEA dat het ontwerp-kaderbesluit van de Europese Commissie, waarin staat dat iedere lidstaat zijn eigen PIU moet organiseren, de zogenaamde decentrale aanpak, zal betekenen dat luchtvaartmaatschappijen straks met 27 verschillende systemen zullen moeten gaan werken. Dit is volgens de AEA een 'operationele en technische nachtmerrie'.<sup>34</sup>

Volgens het Platform Beveiliging en Publieke Veiligheid Schiphol (BPVS), een samenwerkingsverband tussen publieke en private actoren, verraadt de toelichting op het kaderbesluit een zekere onbekendheid met de beschikbaarheid en waarde van PNR-gegevens. Volgens de BPVS kan, gezien de beperkingen van PNR, niet worden verwacht dat het doel, het bestrijden van terrorisme en georganiseerde criminaliteit, wordt bereikt.

## 7 Tot besluit

De verantwoordelijkheden voor vervoerders in het kader van de grensbewaking zijn de afgelopen jaren veranderd. Nut en

noodzaak van het verzamelen van passagiersgegevens zijn niet onbetwist. Analyses van het gebruik van PNR-gegevens in de strijd tegen terrorisme en duidelijke resultaten ontbreken. Kritiek richt zich dan ook vaak op het feit dat ondanks die onduidelijkheid de Commissie in een hoog tempo nieuwe voorstellen presenteert om passagiersgegevens in te zetten in de strijd tegen terrorisme.<sup>35</sup> Ook is het verwonderlijk dat Richtlijn 2004/82/EG weinig aandacht krijgt in dit voorstel en dat onduidelijk is wat de status hiervan zal zijn in relatie tot de nieuwe maatregelen.

Het lijkt erop dat het gebruiken van passagiersgegevens een ontwikkeling is die niet zal verdwijnen maar eerder zal toenemen. In februari 2008 verschenen alweer twee nieuwe plannen van de commissie voor een 'entry-exit'-systeem van biometrische kenmerken en een systeem waarbij alle reizigers zich moeten registreren voordat zij werkelijk naar de EU komen.<sup>36</sup> Als het voorstel voor een EU-PNR-plan wordt aangenomen zal dat betekenen dat in de EU private vervoerders naast het uitvoeren van immigratiecontroles tevens als inlichtingendiensten zullen functioneren in de strijd tegen terrorisme. Vervoerders en vooral luchtvaartmaatschappijen dreigen op die manier een verlengstuk te worden van overheden in het immigratie- en antiterrorismebeleid.

30 Joint Opinion on the Proposal for a Council Framework Decision on the use of PNR for law enforcement purposes, 5 december 2007, 02422/07/EN WP 145.

31 Kamerstukken II 2007/08, 23 490, nr. 499.

32 Beschluss 826/07, 15 februari 2008.

33 AEA Comments on the European proposal to the Council of the European Union for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, 5 december 2007 en AEA Policy Paper on transfer of airline passenger data to governments, april 2008.

34 Persbericht *European airline body dismayed at proposal for EU-PNR*

*system*, 8 november 2007, <[www.aea.be/assets/documents/press/Pr07-029.pdf](http://www.aea.be/assets/documents/press/Pr07-029.pdf)>.

35 F. Geyer, *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, CEPS Research Paper No. 9, Brussel: Centre for European Policy Studies 2008.

36 COM (2008) 69 final, 13-02-2008. Zie hierover ook E. Guild, S. Carrera en F. Geyer, *The Commission's new Border Package: Does it take us one step closer to 'Cyber Fortress Europe'?*, CEPS Policy Brief No. 154, Brussel: Centre for European Policy Studies 2008.