

## I

(Risoluzioni, raccomandazioni e pareri)

## PARERI

## GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

**Parere del garante europeo della protezione dei dati relativo al progetto di decisione quadro del Consiglio sull'uso dei dati del codice di prenotazione (*Passenger Name Record*, PNR) nelle attività di contrasto**

(2008/C 110/01)

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 286,

vista la Carta dei diritti fondamentali dell'Unione europea, in particolare l'articolo 8,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati <sup>(1)</sup>,visto il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati <sup>(2)</sup>, in particolare l'articolo 41,

vista la richiesta di parere a norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001, ricevuta il 13 novembre 2007 dalla Commissione europea,

HA ADOTTATO IL SEGUENTE PARERE:

## I. INTRODUZIONE

**Consultazione del garante europeo della protezione dei dati (GEPD)**

1. A norma dell'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001, la Commissione ha trasmesso al GEPD, per consultazione, il progetto di proposta di decisione

quadro del Consiglio sull'uso dei dati del codice di prenotazione (*Passenger Name Record*, PNR) nelle attività di contrasto (nel prosieguo, «la proposta»).

2. La proposta attiene al trattamento dei dati PNR in seno all'UE ed è strettamente legata ad altri sistemi di raccolta ed uso dei dati dei passeggeri, in particolare l'accordo UE-Stati Uniti del luglio 2007. Tali sistemi rivestono grande interesse per il GEPD, che ha già avuto occasione di formulare alcune osservazioni preliminari sul questionario della Commissione relativo al sistema PNR previsto dall'UE, trasmesso alle pertinenti parti interessate nel dicembre 2006 <sup>(3)</sup>. Il GEPD si felicita che la Commissione lo consulti e ritiene che il presente parere debba essere menzionato nel preambolo della decisione del Consiglio.

**Contesto della proposta**

3. La proposta mira ad armonizzare le disposizioni degli Stati membri relative all'obbligo dei vettori aerei, che effettuano voli a destinazione del territorio di almeno uno Stato membro, o in provenienza dallo stesso, di trasmettere i dati PNR alle autorità competenti, al fine di prevenire e combattere i reati di terrorismo e la criminalità organizzata.
4. L'Unione europea ha concluso con gli Stati Uniti e il Canada accordi per la trasmissione dei dati PNR per finalità simili. Un primo accordo, concluso con gli Stati Uniti nel maggio 2004, è stato sostituito da un nuovo accordo

<sup>(1)</sup> GUL 281 del 23.11.1995, pag. 31.<sup>(2)</sup> GUL 8 del 12.1.2001, pag. 1.<sup>(3)</sup> In particolare gli Stati membri, le autorità per la protezione dei dati e le associazioni di compagnie aeree. La Commissione europea ha elaborato il questionario in vista della preparazione di una valutazione d'impatto sulla presente proposta.

nel luglio 2007 <sup>(1)</sup>. Un accordo analogo è stato concluso con il Canada nel luglio 2005 <sup>(2)</sup>. Inoltre, è previsto l'avvio di negoziati tra l'UE e l'Australia per la conclusione di un accordo sullo scambio di dati PNR e anche la Corea del Sud esige dati PNR per i voli a destinazione del suo territorio, benché nella presente fase non siano previsti negoziati a livello europeo.

5. In seno all'UE, la proposta va ad integrare la direttiva 2004/82/CE del Consiglio <sup>(3)</sup> concernente l'obbligo dei vettori aerei di comunicare i dati relativi alle persone trasportate, noti come dati API, per combattere efficacemente l'immigrazione clandestina e migliorare i controlli alle frontiere. Questa direttiva avrebbe dovuto essere recepita nella legislazione nazionale degli Stati membri entro il 5 settembre 2006. La sua attuazione, tuttavia, non è ancora assicurata in tutti gli Stati membri.

6. Contrariamente alle informazioni anticipate sui passeggeri (dati API), che dovrebbero agevolare l'identificazione dei passeggeri, i dati PNR menzionati nella proposta contribuirebbero a effettuare valutazioni di rischio sui passeggeri, ottenere informazioni e stabilire associazioni tra soggetti noti e non noti.

7. La proposta include i seguenti elementi principali:

- stabilisce che i vettori aerei mettano a disposizione delle autorità competenti degli Stati membri i dati PNR, al fine di prevenire e combattere i reati di terrorismo e la criminalità organizzata,
- prevede la designazione, in linea di principio in ciascuno Stato membro, di un'unità d'informazione sui passeggeri incaricata di raccogliere i dati PNR presso i vettori aerei (o gli intermediari da questi designati) ed effettuare una valutazione di rischio sui passeggeri,
- le informazioni così analizzate saranno trasmesse alle autorità competenti di ciascuno Stato membro e scambiate con altri Stati membri, caso per caso e per le finalità indicate in precedenza,
- il trasferimento verso paesi esterni all'Unione europea è soggetto a condizioni supplementari,

— i dati saranno conservati per tredici anni, di cui otto in una banca dati dormiente,

— il trattamento deve essere disciplinato dal (progetto) di decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (nel prosieguo, la «decisione quadro sulla protezione dei dati» <sup>(4)</sup>),

— un comitato, composto da rappresentanti degli Stati membri, assisterà la Commissione per quanto riguarda le questioni inerenti al protocollo e alla cifratura, nonché per i criteri e le pratiche da applicare nella valutazione del rischio,

— la decisione formerà oggetto di un riesame entro tre anni dalla sua entrata in vigore.

### Punto centrale del parere

8. La proposta su cui il GEPD viene consultato rappresenta un ulteriore passo verso la raccolta sistematica dei dati di passeggeri che, in linea di principio, non sono sospettati di alcun reato. Come accennato in precedenza, tale evoluzione è riscontrabile a livello sia internazionale che europeo.

9. Il GEPD osserva che anche il Gruppo dell'articolo 29 e il Gruppo «Polizia e giustizia» hanno presentato un parere congiunto sulla proposta <sup>(5)</sup>, che egli appoggia. Il presente parere mette in risalto e sviluppa una serie di elementi aggiuntivi.

10. Pur analizzando tutti i pertinenti aspetti della proposta, il GEPD si concentrerà nel suo parere su quattro questioni principali.

— La prima di tali questioni riguarda la legittimità delle misure previste. La finalità, necessità e proporzionalità della proposta saranno esaminate alla luce dei criteri enunciati nell'articolo 8 della Carta dei diritti fondamentali dell'Unione europea.

— Il parere analizzerà altresì la questione della legislazione applicabile al trattamento proposto. In particolare, una speciale attenzione merita il campo di applicazione della decisione quadro sulla protezione dei dati in relazione all'applicazione della legislazione in materia di protezione dei dati nell'ambito del primo pilastro. Si discuterà inoltre delle conseguenze del regime di protezione dei dati applicabile sull'esercizio dei diritti delle persone interessate.

<sup>(1)</sup> Accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e sul trasferimento dei dati del codice di prenotazione (*Passenger Name Record*, PNR) da parte dei vettori aerei al dipartimento per la sicurezza interna degli Stati Uniti (DHS) (Accordo PNR del 2007) (GU L 204 del 4.8.2007, pag. 18).

<sup>(2)</sup> Accordo tra la Comunità europea e il governo del Canada sul trattamento delle informazioni anticipate sui passeggeri e dei dati delle pratiche passeggeri (GU L 82 del 21.3.2006, pag. 15).

<sup>(3)</sup> Direttiva 2004/82/CE del Consiglio, del 29 aprile 2004, concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate (GU L 261 del 6.8.2004, pag. 24).

<sup>(4)</sup> L'ultimo progetto di questa proposta è disponibile nel registro dei documenti del Consiglio con la sigla 16397/07.

<sup>(5)</sup> Parere congiunto relativo alla proposta di decisione quadro del Consiglio sull'uso dei dati del codice di prenotazione (*Passenger Name Record*, PNR) nelle attività di contrasto, presentata dalla Commissione il 6 novembre 2007, adottato dal Gruppo dell'articolo 29 il 5 dicembre 2007 e dal Gruppo «Polizia e giustizia» il 18 dicembre 2007, WP 145, WPPJ 01/07.

— Il parere si incentrerà poi sulla qualità dei destinatari dei dati a livello nazionale. Specifiche preoccupazioni suscita, in particolare, la qualità delle unità d'informazione sui passeggeri, degli intermediari e delle autorità competenti designate per effettuare la valutazione del rischio e analizzare i dati dei passeggeri, in quanto la proposta non precisa nulla al riguardo.

— La quarta questione attiene alle condizioni di trasferimento dei dati ai paesi terzi. Non risulta chiaro quali condizioni si applicheranno a siffatti trasferimenti in presenza di complessi di norme differenti: le condizioni di trasferimento previste dalla presente proposta, quelle stabilite dalla decisione quadro sulla protezione dei dati o gli accordi internazionali esistenti (con gli Stati Uniti e Canada).

11. Nella parte finale saranno identificati altri punti sostanziali, in particolare le misure positive in termini di protezione dei dati, ma anche ulteriori motivi di preoccupazione derivanti dalla proposta.

## II. LEGITTIMITÀ DELLE MISURE PROPOSTE

12. Per analizzare la legittimità delle misure proposte conformemente ai principi fondamentali della protezione dei dati, in particolare l'articolo 8 della Carta dei diritti fondamentali dell'Unione europea e gli articoli da 5 a 8 della Convenzione n. 108 <sup>(1)</sup> del Consiglio d'Europa, è necessario individuare chiaramente la finalità del trattamento di dati personali previsto, nonché valutarne la necessità e proporzionalità. Occorre accertarsi che non siano disponibili altri mezzi, meno invasivi della vita privata, per raggiungere il fine perseguito.

### Individuazione della finalità

13. Dal testo della proposta e della relativa valutazione d'impatto si evince che l'obiettivo non è semplicemente quello di identificare terroristi o criminali noti implicati nella criminalità organizzata, confrontandone i nomi con quelli figuranti negli elenchi gestiti dalle autorità di contrasto, bensì di raccogliere informazioni sul terrorismo e la criminalità organizzata e, più precisamente, di «effettuare valutazioni di rischio sui passeggeri, ottenere informazioni e stabilire associazioni tra soggetti noti e non noti» <sup>(2)</sup>. Nello stesso spirito, la finalità enunciata nell'articolo 3, paragrafo 5, della proposta è innanzitutto di «identificare coloro che sono o *potrebbero essere* implicati in un reato di terrorismo o di criminalità organizzata, *nonché i loro complici*».
14. È questo il motivo addotto per spiegare che i dati API non sono sufficienti per raggiungere il fine perseguito. In effetti, come già accennato, mentre i dati API dovrebbero agevolare l'identificazione dei passeggeri, i dati PNR non

hanno alcuna finalità di identificazione, ma le informazioni in essi contenute contribuirebbero a effettuare valutazioni di rischio sui passeggeri, ottenere informazioni e stabilire associazioni tra soggetti noti e non noti.

15. Le misure previste non si prefiggono soltanto di catturare i soggetti noti, ma anche di localizzare i soggetti che *potrebbero* rispondere ai criteri stabiliti dalla proposta.

Per identificare tali persone, l'analisi del rischio e l'individuazione di modelli rivestono un'importanza centrale nel progetto. Il considerando 9 della proposta prevede esplicitamente che i dati devono essere conservati «per un periodo abbastanza lungo da permettere di elaborare indicatori di rischio e individuare modelli di spostamento e comportamento».

16. L'obiettivo perseguito comporta quindi due livelli: il primo livello consiste nell'obiettivo generale di combattere il terrorismo e la criminalità organizzata, mentre il secondo include i mezzi e le misure inerenti al conseguimento di tale obiettivo. Mentre l'obiettivo della lotta al terrorismo e alla criminalità organizzata appare abbastanza chiaro e legittimo, i mezzi utilizzati per conseguirlo sono più discutibili.

### Individuazione dei modelli e valutazione del rischio

17. La proposta non dà alcuna indicazione su come saranno individuati i modelli e sarà effettuata la valutazione del rischio. La valutazione d'impatto precisa che i dati PNR saranno utilizzati come segue: i dati dei passeggeri saranno confrontati «con una serie di caratteristiche e modelli di comportamento, per ottenere una valutazione di rischio. Quando rientra in un determinato profilo, un passeggero può quindi essere considerato ad alto rischio» <sup>(3)</sup>.
18. I passeggeri sospetti potrebbero essere selezionati in base ad elementi concreti giustificanti un sospetto contenuti nei loro dati PNR (ad esempio, contatto con un'agenzia di viaggio sospetta, riferimento di una carta di credito rubata), nonché sulla base di «modelli» o di un profilo astratto. In base ai tipi di spostamenti, si potrebbero effettivamente stabilire diversi profili standard per «passeggeri normali» o «passeggeri sospetti». Questi profili consentirebbero di approfondire le indagini sui passeggeri che non rientrano nella «categoria dei passeggeri normali», specie se il loro profilo è associato ad altri elementi sospetti, quali una carta di credito rubata.
19. Benché non si possa presumere che i passeggeri sarebbero selezionati in base alla religione o ad altri dati sensibili, appare tuttavia chiaro che sarebbero oggetto di un'indagine basata su una combinazione di informazioni *concrete e astratte, tra cui* modelli standard e profili astratti.

<sup>(1)</sup> Convenzione del Consiglio d'Europa, del 28 gennaio 1981, sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale.

<sup>(2)</sup> Relazione della proposta, punto 1.

<sup>(3)</sup> Valutazione d'impatto, punto 2.1, «Descrizione del problema».

20. Ci si potrebbe chiedere se tale tipo di indagine sia qualificabile come profilazione. La profilazione può essere definita come un metodo informatico che, attraverso l'attività di «data mining» in un magazzino di dati («data warehouse»), permette o mira a permettere di classificare, con una certa probabilità e quindi con un certo margine di errore, una persona in una determinata categoria al fine di prendere decisioni individuali nei riguardi di tale persona <sup>(1)</sup>.
21. Il GEPD è consapevole che la definizione di profilazione è tuttora oggetto di discussioni. Che si riconosca o meno ufficialmente che la proposta mira a *profilare* i passeggeri, ciò che importa veramente non è la definizione, bensì l'impatto sulle persone.
22. La principale preoccupazione del GEPD è legata al fatto che le decisioni relative alle persone saranno prese sulla base di modelli e criteri stabiliti utilizzando i dati relativi all'insieme dei passeggeri. Pertanto le decisioni riguardanti una singola persona potrebbero essere prese utilizzando come riferimento (almeno parzialmente) modelli derivati dai dati di *altre* persone. Le decisioni saranno quindi prese in relazione ad un contesto astratto, il che può avere ripercussioni enormi sugli interessati. È estremamente difficile, per i singoli, difendersi da tali decisioni.
23. Inoltre, la valutazione del rischio deve essere effettuata in mancanza di norme uniformi di identificazione dei sospetti. Il GEPD mette seriamente in dubbio la certezza giuridica dell'intero processo di filtraggio, dato il carattere non sufficientemente chiaro dei criteri in base ai quali ogni passeggero sarà controllato.
24. Il GEPD rammenta la giurisprudenza della Corte europea dei diritti dell'uomo, secondo cui il diritto interno deve essere sufficientemente preciso nell'indicare ai cittadini in quali circostanze e secondo quali modalità le autorità pubbliche sono autorizzate a conservare ed utilizzare le notizie relative alla loro vita privata. L'informazione

«dovrebbe essere accessibile alla persona interessata e prevedibile per quanto riguarda i suoi effetti». Una norma «è prevedibile se è formulata con sufficiente precisione al fine di permettere ad ogni individuo — se necessario, con appropriato avviso — di regolare la sua condotta» <sup>(2)</sup>.

25. In conclusione, è proprio a causa di questi tipi di rischi che la presente proposta richiede un attento esame. L'obiettivo generale della lotta contro il terrorismo e la criminalità organizzata è in se stesso chiaro e legittimo, ma gli elementi fondamentali del trattamento da porre in essere non risultano sufficientemente circoscritti e giustificati. Il GEPD esorta pertanto il legislatore UE ad affrontare chiaramente tale questione, prima dell'adozione della decisione quadro.

### Necessità

26. Le considerazioni fatte in precedenza mostrano chiaramente il carattere invasivo delle misure. D'altro canto, l'utilità delle misure è ben lungi dall'essere dimostrata.
27. La valutazione d'impatto relativa alla proposta mette l'accento più sulla maniera migliore di stabilire un sistema PNR dell'UE che sulla necessità di tale sistema. Nella valutazione <sup>(3)</sup> si fa riferimento ai sistemi PNR esistenti in altri paesi, segnatamente Stati Uniti e Regno Unito. Appare tuttavia deplorabile la mancanza di fatti e cifre precisi relativi a tali sistemi. Nel sistema «Semaphore» istituito dal Regno Unito si segnalano «numerosi arresti» in relazione a «vari reati», senza però precisarne il nesso con il terrorismo o la criminalità organizzata. Nessun particolare è fornito riguardo al programma americano, eccetto che «l'UE ha potuto valutare l'importanza dei dati PNR e rendersi conto del loro potenziale per le attività di contrasto».
28. Non solo *la proposta* non contiene informazioni precise sui risultati concreti dei suddetti sistemi PNR, ma le relazioni pubblicate *da altre agenzie*, quali il Government Accountability Office (GAO) negli Stati Uniti non confermano, nella presente fase, l'efficacia delle misure <sup>(4)</sup>.

<sup>(1)</sup> Questa definizione è tratta da un recente studio del Consiglio d'Europa sulla profilazione: *L'application de la Convention 108 au mécanisme de profilage, Éléments de réflexion destinés au travail futur du Comité consultatif (T-PD)*, Jean-Marc Dinant, Christophe Lazaro, Yves Pouillet, Nathalie Lefever, Antoinette Rouvroy, novembre 2007 (non ancora pubblicato). Si veda anche la definizione di Lee Bygrave, secondo cui la profilazione è, in termini generali, il procedimento che permette di inferire una serie di caratteristiche (tipicamente comportamentali) riguardo ad una singola persona o ad un'entità collettiva e, quindi, di trattare tale persona/entità (o altre persone/entità) alla luce di tali caratteristiche. In quanto tale, il procedimento di profilazione comporta due componenti principali: i) la generazione del profilo, ossia il processo d'inferenza di un profilo; ii) l'applicazione del profilo, ossia il processo di trattazione delle persone/entità alla luce del profilo determinato. L. A. BYGRAVE, *Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, *Computer Law & Security Report*, 2001, vol. 17, pagg. 17-24, <http://www.austlii.edu.au/journals/PLPR/2000/40.html>

<sup>(2)</sup> Rotaru contro Romania, n. 28341/95, punti 50, 52 e 55.

Si veda anche Amann contro Svizzera, n. 27798/95, punti 50 e seguenti.

<sup>(3)</sup> Punto 2.1, «Descrizione del problema».

<sup>(4)</sup> Si veda, ad esempio, la relazione pubblicata nel maggio 2007 dal Government Accountability Office, l'organo investigativo del Congresso degli Stati Uniti, in risposta alle richieste dei membri del Congresso, *Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues remain*, <http://www.gao.gov/new.items/d07346.pdf>

29. Il GEPD è del parere che occorra approfondire l'esame delle tecniche intese a valutare il rischio presentato dalle persone mediante strumenti di «data mining» e modelli comportamentali e che sia opportuno stabilirne chiaramente l'utilità nel quadro della lotta contro il terrorismo, prima di utilizzarle su una scala così vasta.

### Proporzionalità

30. Per valutare l'equilibrio tra l'ingerenza nella vita privata dell'individuo e la necessità della misura <sup>(1)</sup>, si tiene conto dei seguenti elementi:

- le misure si applicano a tutti i passeggeri, siano essi indagati o meno dalle autorità di contrasto; si tratta di una ricerca proattiva, su una scala senza precedenti,
- le decisioni relative alle persone possono basarsi su profili astratti, che comportano pertanto un significativo margine di errore,
- le misure da adottare nei riguardi della persona interessata sono di carattere repressivo; comportano pertanto un'ingerenza di gran lunga maggiore, in termini di esclusione o coercizione, rispetto ad altri contesti, quali la frode con carta di credito o il marketing.

31. Il rispetto del principio di proporzionalità implica non solo che la misura proposta sia efficace, ma anche che il fine perseguito dalla proposta non possa essere conseguito con mezzi meno invasivi della vita privata. L'efficacia delle misure previste non è stata dimostrata. Occorre esaminare attentamente l'esistenza di soluzioni alternative prima di istituire ulteriori/nuove misure per il trattamento delle informazioni personali. Secondo il GEPD, una siffatta valutazione globale non ha avuto luogo.

32. Il GEPD desidera ricordare che esistono altri sistemi su vasta scala, già operativi o in procinto di diventarlo, per monitorare gli spostamenti delle persone all'interno o alle frontiere dell'UE, incluso in particolare il sistema di informazione visti <sup>(2)</sup> e il sistema d'informazione Schengen <sup>(3)</sup>.

<sup>(1)</sup> In conformità dell'articolo 9 della Convenzione 108, «È possibile derogare alle disposizioni degli articoli 5, 6 ed 8 della presente Convenzione qualora una tale deroga, prevista dal diritto della Parte, costituisca una misura necessaria in una società democratica:

1) alla protezione della sicurezza dello Stato, alla sicurezza pubblica, agli interessi monetari dello Stato o alla repressione dei reati;

2) alla protezione della persona interessata e dei diritti e delle libertà altrui».

<sup>(2)</sup> Decisione 2004/512/CE del Consiglio, dell'8 giugno 2004, che istituisce il sistema di informazione visti (VIS) (GU L 213 del 15.6.2004, pag. 5); proposta di regolamento del Parlamento europeo e del Consiglio concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata, COM(2004) 835 defin.; proposta di decisione del Consiglio relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità degli Stati membri competenti in materia di sicurezza interna e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di atti terroristici e di altre gravi forme di criminalità, COM(2005) 600 defin.

<sup>(3)</sup> Si veda, in particolare, la decisione 2007/533/GAI del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) (GU L 205 del 7.8.2007).

Benché l'obiettivo principale di tali strumenti non sia quello di combattere il terrorismo o la criminalità organizzata, essi sono o saranno in certa misura accessibili alle autorità di contrasto nel quadro più ampio della lotta alla criminalità <sup>(4)</sup>.

33. Un altro esempio riguarda la disponibilità dei dati personali contenuti nelle banche dati della polizia nazionale — specialmente per quanto riguarda i dati biometrici — nel quadro del trattato di Prüm firmato nel maggio 2005, che viene attualmente esteso a tutti gli Stati membri dell'Unione europea <sup>(5)</sup>.

34. Tutti questi diversi strumenti hanno in comune il fatto che consentono un monitoraggio globale degli spostamenti delle persone, anche se da prospettive differenti. Il modo in cui essi possono già contribuire alla lotta contro determinate forme di criminalità, incluso il terrorismo, dovrebbe formare oggetto di un'analisi approfondita e completa, prima di decidere di istituire una nuova forma di controllo sistematico di tutte le persone in entrata o in uscita dall'Europa in aereo. Il GEPD raccomanda che la Commissione effettui tale analisi, che rappresenta una tappa necessaria nel processo legislativo.

### Conclusione

35. Tenuto conto di quanto precede, il GEPD trae le conclusioni seguenti sulla legittimità delle misure proposte. Fondarsi su diverse banche dati senza avere una visione globale dei risultati concreti e delle carenze:

— è contrario ad una politica legislativa razionale, che esige che non si adottino nuovi strumenti prima di aver pienamente attuato quelli esistenti e dimostrato la loro insufficienza <sup>(6)</sup>,

— potrebbe altrimenti portare ad una società basata sulla sorveglianza totale.

36. La lotta contro il terrorismo può certamente costituire un motivo legittimo per applicare deroghe ai diritti fondamentali alla vita privata e alla protezione dei dati. Tuttavia, per essere valida, la necessità dell'ingerenza deve poggiare

<sup>(4)</sup> Si veda al riguardo il parere del garante europeo della protezione dei dati sulla proposta di decisione del Consiglio relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità degli Stati membri competenti in materia di sicurezza interna e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di atti terroristici e di altre gravi forme di criminalità [COM(2005) 600 def.] (GU C 97 del 25.4.2006, pag. 6).

<sup>(5)</sup> Si vedano i pareri del GEPD sulle decisioni di Prüm: parere del 4 aprile 2007 sull'iniziativa di 15 Stati membri in vista dell'adozione di una decisione del Consiglio sul rafforzamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo ed alla criminalità transfrontaliera (GU C 169 del 21.7.2007, pag. 2) e parere del 19 dicembre 2007 sull'iniziativa della Repubblica federale di Germania in vista dell'adozione di una decisione del Consiglio relativa all'attuazione della decisione 2007/.../GAI sul rafforzamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera, disponibile sul sito: <http://www.edps.europa.eu>

<sup>(6)</sup> Questo punto è stato sollevato svariate volte dal GEPD, da ultimo nel parere del 25 luglio 2007 relativo all'attuazione della direttiva sulla protezione dei dati (GU C 255 del 27.10.2007, pag. 1).

su elementi chiari ed inconfutabili e la proporzionalità del trattamento deve essere dimostrata. Ciò risulta tanto più necessario nel caso di una forte ingerenza nella vita privata delle persone, quale prevista nella proposta.

37. Si può solo constatare che siffatti elementi giustificativi mancano nella proposta e che la necessità e la proporzionalità non sono state verificate.
38. Il GEPD insiste sul carattere essenziale dei criteri di necessità e proporzionalità di cui sopra, che rappresentano una condizione indispensabile per l'entrata in vigore della presente proposta. Tutte le altre osservazioni formulate dal GEPDF nel presente parere devono essere considerate alla luce di questa condizione preliminare.

### III. LEGISLAZIONE APPLICABILE — ESERCIZIO DEI DIRITTI DELLA PERSONA INTERESSATA

#### Legislazione applicabile

39. L'analisi seguente si concentrerà su tre punti:
- una descrizione delle diverse fasi del trattamento previsto nella proposta, al fine di determinare la legislazione applicabile in ciascuna fase,
  - le restrizioni, in termini di campo di applicazione e di diritti delle persone interessate, della proposta di decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale,
  - un'analisi più generale della misura in cui uno strumento del terzo pilastro possa applicarsi al trattamento di dati da parte di attori privati nel quadro del primo pilastro.

#### *Legislazione applicabile nelle diverse fasi del trattamento*

40. L'articolo 11 della proposta dispone che «gli Stati membri provvedono affinché la decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (...) si applichi al trattamento dei dati personali ai sensi della presente decisione quadro».
41. Tuttavia, malgrado tale disposizione, non è chiaro in quale misura la decisione quadro sulla protezione dei dati — uno strumento del terzo pilastro del trattato UE — si applicherà ai dati trattati dalle compagnie aeree, raccolti dalle unità d'informazione sui passeggeri e successivamente utilizzati da altre autorità competenti.
42. La prima fase del trattamento dei dati personali prevista dalla proposta consiste nel trattamento effettuato dalle compagnie aeree, che sono obbligate a comunicare i dati

PNR alle unità nazionali d'informazione sui passeggeri utilizzando, in linea di principio, un sistema «push». La formulazione della proposta e la valutazione d'impatto <sup>(1)</sup> lasciano intendere che le compagnie aeree potrebbero anche trasmettere in blocco i dati agli intermediari. Le compagnie aeree operano soprattutto in un contesto commerciale e sono soggette alla legislazione nazionale sulla protezione dei dati personali che attua la direttiva 95/46/CE <sup>(2)</sup>. I problemi relativi alla legislazione applicabile si porranno qualora i dati raccolti siano utilizzati per finalità di contrasto <sup>(3)</sup>.

43. I dati sarebbero quindi filtrati da un intermediario (per essere formattati ed escludere i dati PNR che non figurano nell'elenco dei dati richiesti dalla proposta) o trasmessi direttamente alle unità d'informazione sui passeggeri. Gli intermediari potrebbero anche essere attori del settore privato, come nel caso della SITA, che disimpegna tali funzioni nel quadro dell'accordo PNR con il Canada.
44. Quanto alle unità d'informazione sui passeggeri, responsabili della valutazione di rischio della totalità dei dati, non è chiaro a chi incomberà il trattamento. Potrebbero essere coinvolte le autorità doganali e di frontiera e non necessariamente i servizi di contrasto.
45. La successiva trasmissione dei dati filtrati alle autorità «competenti» avverrebbe probabilmente nel contesto di attività di contrasto. La proposta dispone che «le autorità competenti comprendono soltanto le autorità responsabili della prevenzione e della lotta contro i reati di terrorismo e la criminalità organizzata».
46. Con il succedersi delle fasi del trattamento, gli attori implicati e la finalità perseguita hanno sempre più attinenza con la cooperazione giudiziaria e di polizia in materia penale. Tuttavia, la proposta non indica esplicitamente in quale preciso momento si applicherà la decisione quadro sulla protezione dei dati. La formulazione sembrerebbe persino suggerire che essa si applichi all'intero processo e addirittura alle compagnie aeree <sup>(4)</sup>. Tuttavia, la decisione quadro sulla protezione dei dati personali contiene di per sé alcune restrizioni.

<sup>(1)</sup> Articolo 6, paragrafo 3, della proposta e valutazione d'impatto, allegato A, «Metodo di trasmissione dei dati da parte dei vettori».

<sup>(2)</sup> Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU L 281 del 23.11.1995, pag. 31.

<sup>(3)</sup> Si vedano al riguardo le conseguenze della sentenza PNR. Sentenza della Corte del 30 maggio 2006, Parlamento europeo contro Consiglio (C-317/04) e Commissione (C-318/04), cause riunite C-317/04 e C-318/04, Racc. [2006], punto 56.

<sup>(4)</sup> Articolo 11 della proposta. Si veda anche il considerando 10 del preambolo: «La decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (...) deve applicarsi a tutti i dati trattati conformemente alla presente decisione quadro. I diritti degli interessati in relazione al trattamento, cioè il diritto all'informazione, il diritto di accesso, il diritto di rettifica, cancellazione o congelamento, così come i diritti al risarcimento e all'impugnazione dovrebbero essere gli stessi previsti nella richiamata decisione quadro».

47. In tale contesto, il GEPD rimette sostanzialmente in questione il fatto che il titolo VI del trattato UE possa servire da base giuridica per imporre obblighi giuridici sistematici e per finalità di contrasto ad attori del settore privato. Inoltre, occorre chiedersi se il titolo VI del trattato UE possa servire da base giuridica per imporre obblighi giuridici ad autorità pubbliche che, in linea di principio, non rientrano nel quadro della cooperazione tra autorità di contrasto. Tali questioni saranno sviluppate nel prosieguo del presente parere.

*Restrizioni previste dalla decisione quadro sulla protezione dei dati*

48. Il testo della proposta di decisione quadro del Consiglio sulla protezione dei dati trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale contiene almeno due importanti restrizioni in termini di campo di applicazione.

49. In primo luogo, il campo di applicazione della decisione quadro sulla protezione dei dati è ben definito nella stessa decisione quadro: questa si applica «soltanto ai dati raccolti o trattati da autorità competenti ai fini della prevenzione, dell'indagine, dell'accertamento o del perseguimento dei reati o dell'esecuzione delle sanzioni penali»<sup>(1)</sup>.

50. In secondo luogo, non è previsto che la decisione quadro sulla protezione dei dati si applichi ai dati trattati esclusivamente a livello nazionale, ma si limita ai dati scambiati tra Stati membri ed al loro trasferimento a paesi terzi<sup>(2)</sup>.

51. La decisione quadro sulla protezione dei dati presenta pure alcuni inconvenienti rispetto alla direttiva 95/46/CE, in particolare un'ampia deroga al principio della limitazione della finalità. Riguardo a tale principio, la proposta limita chiaramente la finalità del trattamento alla lotta contro il terrorismo e la criminalità organizzata. Tuttavia, la decisione quadro sulla protezione dei dati permette trattamenti per finalità più ampie. In tale caso, la *lex specialis* (la proposta) dovrebbe prevalere sulla *lex generalis* (la decisione quadro sulla protezione dei dati)<sup>(3)</sup>. Ciò andrebbe esplicitato nel testo della proposta.

52. Per tale motivo, il GEPD raccomanda di aggiungere alla proposta la seguente disposizione. «I dati personali trasmessi dalle compagnie aeree in conformità della decisione quadro non possono essere trattati per fini diversi dalla lotta contro il terrorismo e la criminalità organizzata. Le deroghe al principio della finalità previste nella decisione quadro sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale non si applicano».

<sup>(1)</sup> Considerando 5 bis, versione dell'11 dicembre 2007 della decisione quadro sulla protezione dei dati.

<sup>(2)</sup> Articolo 1.

<sup>(3)</sup> Su questo punto, bisognerebbe esaminare attentamente e discutere il testo dell'articolo 27 ter dell'ultimo progetto di decisione quadro sulla protezione dei dati nell'ambito del terzo pilastro.

53. In conclusione, il GEPD constata che esiste una grave incertezza giuridica riguardo al regime di protezione dei dati applicabile ai diversi attori implicati nel progetto, in particolare le compagnie aeree e altri attori del primo pilastro: possono applicarsi le norme della proposta, quelle della decisione quadro sulla protezione dei dati o la legislazione nazionale che attua la direttiva 95/46/CE. Il legislatore dovrebbe chiarire in quale preciso momento del trattamento si applicheranno queste differenti norme.

*Condizioni d'applicazione delle norme del primo e terzo pilastro*

54. Il GEPD rimette sostanzialmente in questione il fatto che uno strumento del terzo pilastro crei obblighi giuridici sistematici e per finalità di contrasto a carico di attori del settore privato o pubblico che, in linea di principio, non rientrano nel quadro della cooperazione tra autorità di contrasto.

55. Si potrebbe comparare tale situazione ad altri due casi in cui il settore privato è intervenuto nella conservazione o nel trasferimento di dati per finalità di contrasto:

— *Il caso Stati Uniti/PNR, in cui era previsto il trasferimento sistematico di dati PNR da parte delle compagnie aeree alle autorità di contrasto.* La Corte di giustizia, nella sentenza sulla causa PNR, ha escluso la competenza della Comunità a concludere l'accordo PNR. Uno dei motivi adottati consisteva nel fatto che il trasferimento di dati PNR all'Ufficio doganale e di protezione dei confini (CBP) degli Stati Uniti costituiva un trattamento avente ad oggetto la pubblica sicurezza e le attività dello Stato attinenti al diritto penale<sup>(4)</sup>. In questo caso, il trattamento consisteva nel trasferimento di dati al CBP *in forma sistematica*, il che distingue questa causa dal caso seguente:

— *Conservazione generale di dati da parte degli operatori di comunicazioni elettroniche.* Per quanto riguarda la competenza comunitaria a stabilire un siffatto periodo di conservazione, è possibile distinguere questo caso da quello Stati Uniti/PNR, dato che la direttiva 2006/24/CE<sup>(5)</sup> prevede un obbligo di conservazione solo per i dati che restano sotto il controllo degli operatori. Non è previsto alcun trasferimento sistematico di dati alle autorità di contrasto. Si può concludere che, finché i dati restano sotto il controllo dei fornitori di servizi, questi sono pure responsabili, nei riguardi degli interessati, del rispetto degli obblighi in materia di protezione dei dati personali.

<sup>(4)</sup> Sentenza della Corte del 30 maggio 2006, Parlamento europeo contro Consiglio (C-317/04) e Commissione (C-318/04), cause riunite C-317/04 e C-318/04, Racc. [2006], punto 56.

<sup>(5)</sup> Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (GU L 105 del 13.4.2006, pag. 54).

56. Nella presente proposta, le compagnie aeree sono tenute a rendere sistematicamente disponibili i dati PNR di tutti i passeggeri. Tuttavia, tali dati non sono trasferiti direttamente in blocco alle autorità di contrasto: possono essere inviati ad un intermediario e sono valutati da una parte terza, il cui status resta incerto, prima che le informazioni selezionate siano trasmesse alle autorità competenti.
57. La parte principale del trattamento si svolge in una zona d'ombra, che presenta nessi concreti sia con il primo che con il terzo pilastro. Come vedremo nella parte IV, la qualità degli attori che trattano i dati non è chiara. Le compagnie aeree non sono ovviamente autorità di contrasto e gli intermediari potrebbero essere attori del settore privato. Anche per quanto riguarda le unità d'informazione sui passeggeri, che sarebbero autorità pubbliche, va rilevato che non tutte le autorità pubbliche hanno la qualità e le competenze per assolvere compiti di contrasto su base sistematica.
58. Tradizionalmente esiste una netta separazione tra attività di contrasto e attività del settore privato, dove i compiti di contrasto sono eseguiti da autorità specificamente preposte, in particolare le forze di polizia, e gli attori privati sono sollecitati caso per caso a comunicare dati personali alle autorità di contrasto. Si registra attualmente una tendenza ad imporre ad attori privati di cooperare sistematicamente per finalità di contrasto, il che solleva la questione del quadro di protezione dei dati (primo o terzo pilastro) che si applica alle condizioni di tale cooperazione: le norme dovrebbero basarsi sulla qualità del responsabile del trattamento (settore privato) o sulla finalità perseguita (attività di contrasto)?
59. Il GEPD ha già ricordato il rischio di un vuoto giuridico tra le attività del primo e del terzo pilastro <sup>(1)</sup>. Non è assolutamente chiaro se le attività svolte da società private, in qualche modo collegate all'applicazione del diritto penale, siano incluse nel campo d'azione previsto dal legislatore dell'Unione europea ai sensi degli articoli 30, 31 e 34 del trattato UE.
60. Se il quadro generale (primo pilastro) non fosse d'applicazione, un fornitore di servizi dovrebbe operare complesse distinzioni nelle sue banche dati. Sotto l'attuale regime, è chiaro che il responsabile del trattamento deve rispettare, nei riguardi degli interessati, le stesse norme in materia di protezione dei dati, indipendentemente dalle finalità che giustificano la conservazione dei dati stessi. Si dovrebbe pertanto evitare di arrivare ad una situazione in cui, a seconda della finalità perseguita, il trattamento da parte di fornitori di servizi sia soggetto a differenti quadri di protezione dei dati.

<sup>(1)</sup> Si veda il parere del garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati (GU C 255 del 27.10.2007, pag. 1). Si veda anche la relazione annuale 2006, pag. 47.

### Esercizio dei diritti delle persone interessate

61. I diversi regimi giuridici che si applicherebbero a livello nazionale avrebbero un impatto importante innanzitutto sull'esercizio dei diritti da parte delle persone interessate.
62. Nel preambolo della proposta è precisato che «il diritto all'informazione, il diritto di accesso, il diritto di rettifica, cancellazione o congelamento, così come i diritti al risarcimento e all'impugnazione dovrebbero essere gli stessi previsti nella richiamata decisione quadro». Tuttavia, tale indicazione non chiarisce chi sia il responsabile del trattamento incaricato di rispondere alle richieste delle persone interessate.
63. Le informazioni sul trattamento potrebbero essere comunicate dalle compagnie aeree, ma riguardo all'accesso ai dati o alla loro rettifica la questione è più complessa. Questi diritti sono infatti limitati ai sensi della decisione quadro sulla protezione dei dati. Come indicato in precedenza, è dubbio che un fornitore di servizi come una compagnia aerea possa essere obbligato a fornire diritti di accesso e rettifica differenziati ai dati detenuti, a seconda della finalità (commerciale o di contrasto) perseguita. Si potrebbe eccepire che tali diritti debbano essere esercitati rivolgendosi alle unità d'informazione sui passeggeri o alle autorità competenti altrimenti designate. La proposta non fornisce, tuttavia, indicazioni in proposito e, come già segnalato, non chiarisce neppure se dette autorità (almeno le unità d'informazione sui passeggeri) saranno autorità di contrasto normalmente incaricate di procedure di accesso limitate (eventualmente indirette).
64. Per quanto riguarda le unità d'informazione sui passeggeri, l'interessato rischia altresì di essere confrontato a differenti destinatari dei dati: i dati sono infatti trasmessi alle unità d'informazione sui passeggeri del paese di partenza/arrivo dei voli, ma eventualmente anche alle unità d'informazione sui passeggeri di altri Stati membri, a seconda dei casi. Inoltre, è possibile che vari Stati membri possano istituire o designare un'unica unità d'informazione sui passeggeri comune. La persona interessata potrebbe, in tal caso, dover esercitare i suoi diritti rivolgendosi ad un'autorità di un altro Stato membro. Ancora una volta non è chiaro se si applicheranno le norme nazionali sulla protezione dei dati (presumibilmente armonizzate all'interno dell'UE) o se si dovrà tenere conto di una specifica normativa per finalità di contrasto (data la mancanza di armonizzazione totale nel quadro del terzo pilastro a livello nazionale).
65. La questione è la stessa per quanto riguarda l'accesso ai dati trattati da intermediari, il cui status non è chiaro, e che potrebbero anche essere comuni a compagnie aeree di diversi paesi dell'UE.



66. Il GEPD deplora l'incertezza che caratterizza l'esercizio di tali diritti fondamentali delle persone interessate. Rileva che tale situazione è dovuta principalmente al fatto che queste responsabilità siano conferite ad attori il cui compito principale non è l'attività di contrasto.

### Conclusione

67. Il GEPD è del parere che la proposta dovrebbe precisare il regime giuridico applicabile in ogni fase del trattamento e l'attore o l'autorità a cui la persona interessata deve rivolgersi per esercitare il diritto di accesso o rettifica. Il GEPD ricorda che, ai sensi dell'articolo 30, paragrafo 1, lettera b), del trattato UE, le disposizioni sulla protezione dei dati dovrebbero essere appropriate e includere l'intera gamma di trattamenti previsti dalla proposta. Un semplice riferimento alla decisione quadro sulla protezione dei dati non basta, dato il limitato campo di applicazione di tale decisione quadro e la restrizione dei diritti che essa comporta. Per quanto concerne le autorità di contrasto, le norme della decisione quadro sulla protezione dei dati dovrebbero applicarsi almeno all'insieme del trattamento previsto nella proposta, al fine di garantire la coerente applicazione dei principi sulla protezione dei dati.

### IV. QUALITÀ DEI DESTINATARI

68. Il GEPD rileva che la proposta non precisa nulla riguardo alla qualità dei destinatari dei dati personali raccolti dalle compagnie aeree, siano essi intermediari, unità d'informazione sui passeggeri o autorità competenti. Va rilevato che la qualità del destinatario è in diretto rapporto con il tipo di garanzie in materia di protezione dei dati che si applica al destinatario. La differenza tra le garanzie previste, in particolare, dalle norme del primo e del terzo pilastro è già stata menzionata. È essenziale che il regime applicabile sia chiaro per tutti gli attori implicati, inclusi i governi nazionali, i servizi di contrasto, le autorità per la protezione dei dati, nonché i responsabili del trattamento e le persone interessate.

### Intermediari

69. La proposta non precisa nulla riguardo alla qualità degli intermediari<sup>(1)</sup>. Non specifica neppure il ruolo degli intermediari come responsabili o incaricati del trattamento. Per esperienza, sembra che un'entità del settore privato, si tratti di un sistema informatico di prenotazione o di un'altra entità, potrebbe benissimo essere incaricata di raccogliere i dati PNR direttamente presso le compagnie aeree per poi comunicarli alle unità d'informazione sui passeggeri. È infatti questo il modo in cui i dati sono trattati nell'ambito dell'accordo PNR con il Canada. La

SITA<sup>(2)</sup> è la società incaricata del trattamento delle informazioni. Il ruolo dell'intermediario è decisivo, in quanto potrebbe essere incaricato del filtraggio/della riformattazione dei dati che le compagnie aeree trasmettono in blocco<sup>(3)</sup>. Anche se gli intermediari sono obbligati a sopprimere le informazioni trattate dopo averle trasferite alle unità d'informazione sui passeggeri, il trattamento è di per sé estremamente sensibile: una conseguenza dell'intervento degli intermediari è la creazione di una banca dati supplementare contenente ingenti quantitativi di dati e, addirittura, in base alla proposta, dati sensibili (che gli intermediari sono poi obbligati a sopprimere). Per tali motivi, il GEPD raccomanda che nessun intermediario intervenga nel trattamento dei dati dei passeggeri, a meno che non ne siano rigorosamente specificati la qualità e i compiti.

### Unità d'informazione sui passeggeri

70. Le unità d'informazione sui passeggeri svolgono un ruolo determinante nell'identificazione dei passeggeri che sono o potrebbero essere implicati o associati al terrorismo o alla criminalità organizzata. Secondo la proposta, esse saranno incaricate di elaborare indicatori di rischio e di fornire informazioni sui tipi di spostamento<sup>(4)</sup>. Qualora la valutazione del rischio si basi su tipi di spostamento standardizzati e non su prove materiali legate ad un caso concreto, l'analisi può essere considerata un'indagine proattiva. Il GEPD rileva che questo tipo di trattamento (se non è vietato) è, in linea di principio, rigorosamente disciplinato dalla legislazione degli Stati membri ed incombe a specifiche autorità pubbliche, il cui funzionamento è anch'esso rigidamente regolamentato.
71. Le unità d'informazione sui passeggeri sono pertanto incaricate di un trattamento molto sensibile delle informazioni, senza che la proposta specifichi nulla sulla loro qualità e sulle condizioni in cui eserciterebbero tale competenza. Anche se è probabile che tale compito sarà assolto da un organo pubblico, eventualmente le autorità doganali o le autorità preposte ai controlli di frontiera, la proposta non impedisce esplicitamente agli Stati membri di incaricare della sua esecuzione le agenzie d'informazione o addirittura un qualsiasi tipo di entità di trattamento. Il GEPD sottolinea che la trasparenza e le garanzie che si applicano alle agenzie d'informazione non sono sempre identiche a quelle applicabili alle tradizionali autorità di contrasto. Precisazioni sulla qualità delle unità d'informazione sui passeggeri sono decisive, in quanto avranno conseguenze dirette sul quadro giuridico applicabile e sulle condizioni di controllo. Secondo il GEPD, la proposta deve includere una disposizione aggiuntiva che specifichi le peculiarità delle unità d'informazione sui passeggeri.

<sup>(2)</sup> La SITA è stata creata nel 1949 da 11 compagnie aeree. Le soluzioni a valore aggiunto sono fornite all'industria del trasporto aereo attraverso la società commerciale SITA INC (Information, Networking Computing) e i servizi di rete attraverso la SITA SC su base cooperativa.

<sup>(3)</sup> Valutazione d'impatto, allegato A, «Metodo di trasmissione dei dati da parte dei vettori».

<sup>(4)</sup> Articolo 3 della proposta.

<sup>(1)</sup> Articolo 6 della proposta.

**Autorità competenti**

72. Dall'articolo 4 della proposta si evince che qualsiasi autorità incaricata della prevenzione o della lotta contro i reati di terrorismo e la criminalità organizzata può ricevere dati. Mentre la finalità è chiaramente definita, la qualità dell'autorità non è precisata. La proposta non prevede alcuna limitazione dei destinatari alle autorità di contrasto.

Come accennato in precedenza riguardo alle unità d'informazione sui passeggeri, è fondamentale che le informazioni sensibili in questione siano trattate in un contesto caratterizzato da un quadro giuridico chiaro. Ciò è tanto più importante, ad esempio, per le autorità di contrasto che per le agenzie d'informazione. Se si tiene conto degli elementi di data mining e ricerca proattiva inclusi nella proposta, non si può escludere che dette agenzie d'informazione o qualsiasi altro tipo di autorità siano associati al trattamento dei dati.

**Conclusione**

73. In via generale, il GEPD osserva che l'applicazione di un sistema PNR dell'UE è resa ancora più ardua dal fatto che le competenze delle autorità di contrasto si diversificano a seconda della legislazione nazionale degli Stati membri, includendo o meno l'intelligence, la fiscalità, l'immigrazione o la polizia. Ciò costituisce un ulteriore motivo per raccomandare che la proposta sia molto più precisa riguardo alla qualità degli attori menzionati e alle garanzie necessarie per controllarne l'esecuzione dei compiti. È necessario inserire nella proposta disposizioni supplementari che specifichino rigorosamente le competenze e gli obblighi giuridici di intermediari, unità d'informazione sui passeggeri e altre autorità competenti.

**V. CONDIZIONI PER IL TRASFERIMENTO AI PAESI TERZI**

74. La proposta stabilisce alcune misure di salvaguardia riguardo al trasferimento dei dati PNR ai paesi terzi <sup>(1)</sup>. In particolare, essa prevede esplicitamente l'applicazione della decisione quadro sulla protezione dei dati ai trasferimenti di dati, limita espressamente la finalità e precisa che il consenso dello Stato membro interessato è necessario in caso di ulteriore trasferimento. Il trasferimento dovrebbe inoltre rispettare la normativa nazionale dello Stato membro interessato e gli accordi internazionali eventualmente applicabili.
75. Rimangono tuttavia aperte molte questioni, segnatamente riguardo alla qualità del consenso, alle condizioni d'applicazione della decisione quadro sulla protezione dei dati e alla questione della «reciprocità» nella trasmissione dei dati ai paesi terzi.

<sup>(1)</sup> Articolo 8 della proposta.

**Qualità del consenso**

76. Lo Stato membro di origine deve dare il suo esplicito consenso all'ulteriore trasferimento dei dati da un paese terzo ad un altro paese terzo. La proposta non specifica a quali condizioni e da chi sarà dato tale consenso, né se le autorità nazionali per la protezione dei dati dovrebbero essere associate alla decisione. Il GEPD è del parere che il modo in cui il consenso sarà dato dovrebbe almeno essere conforme alla legislazione nazionale che disciplina le condizioni di trasferimento dei dati personali ai paesi terzi.
77. Inoltre, il consenso dello Stato membro non dovrebbe prevalere sul principio secondo cui il paese destinatario deve prevedere un adeguato livello di protezione per il trattamento previsto. Tali condizioni dovrebbero essere cumulative, come nella decisione quadro sulla protezione dei dati (articolo 14). Il GEPD propone pertanto di aggiungere al paragrafo 1 dell'articolo 8 una lettera c) così formulata: «e c) lo Stato terzo assicura un adeguato livello di protezione per il trattamento dei dati previsto». Il GEPD rammenta al riguardo che occorre istituire meccanismi che garantiscano norme comuni e decisioni coordinate riguardo al principio di adeguatezza <sup>(2)</sup>.

**Applicazione della decisione quadro sulla protezione dei dati**

78. La proposta fa riferimento alle condizioni e misure di salvaguardia contenute nella decisione quadro sulla protezione dei dati, specificando inoltre esplicitamente alcune condizioni, segnatamente il menzionato consenso dello Stato membro interessato e la limitazione della finalità alla prevenzione e lotta contro i reati di terrorismo e la criminalità organizzata.
79. La decisione quadro sulla protezione dei dati prevede anch'essa le condizioni per il trasferimento dei dati personali ai paesi terzi, ossia la limitazione della finalità, la qualità dei destinatari, il consenso dello Stato membro e il principio di adeguatezza. Tuttavia, contempla anche deroghe a tali condizioni di trasferimento: interessi legittimi superiori, soprattutto interessi pubblici importanti, possono essere una base sufficiente per il trasferimento anche quando le condizioni elencate sopra non sono soddisfatte.
80. Come già accennato nella parte III del presente parere, il GEPD ritiene che il testo della proposta debba chiaramente indicare che le garanzie più precise della proposta stessa prevalgono sulle condizioni generali — e sulle eccezioni — della decisione quadro sulla protezione dei dati, ove d'applicazione.

<sup>(2)</sup> Parere del GEPD, del 26 giugno 2007, relativo alla proposta di decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, punti da 27 a 30, GU C 139 del 23.6.2007, pag. 1.

**Reciprocità***Paesi che hanno concluso un accordo bilaterale con l'UE*

81. La proposta affronta la questione delle eventuali «richieste a titolo di reciprocità» di paesi che potrebbero chiedere all'UE dati PNR per i voli provenienti dall'UE e diretti al loro territorio. Quando l'UE chiede dati provenienti da banche dati di compagnie aeree di questi paesi terzi, poiché effettuano un volo a destinazione dell'UE o da questa proveniente, tali paesi terzi potrebbero chiedere le stesse informazioni alle compagnie aeree stabilite nell'UE, inclusi i dati di cittadini dell'UE. Benché la Commissione consideri tale eventualità «molto remota», essa l'ammette. La proposta fa riferimento in proposito al fatto che gli accordi con gli Stati Uniti e Canada prevedono tale trattamento reciproco «che può essere applicato automaticamente»<sup>(1)</sup>. Il GEPD si interroga sulla rilevanza di tale reciprocità automatica e sull'applicazione delle misure di salvaguardia a detti trasferimenti, segnatamente in considerazione dell'esistenza di un adeguato livello di protezione nel paese interessato.
82. Bisognerebbe operare una distinzione tra i paesi terzi che hanno già concluso un accordo con l'UE e quelli che non l'hanno ancora fatto.
- Paesi che non hanno concluso alcun accordo con l'UE*
83. Il GEPD rileva che la reciprocità potrebbe condurre a trasferire dati personali a paesi che non possono offrire garanzie in termini di norme democratiche e di adeguato livello di protezione.
84. La valutazione d'impatto offre ulteriori elementi in ordine alle condizioni di trasferimento di dati ai paesi terzi: è sottolineato il vantaggio del sistema PNR dell'UE, in cui i dati sono filtrati dalle unità d'informazione sui passeggeri. Solo i dati selezionati riguardanti persone sospette (e non i dati in blocco) sarebbero trasferiti alle autorità competenti degli Stati membri e presumibilmente anche ai paesi terzi<sup>(2)</sup>. Il GEPD raccomanda di chiarire questo punto nel testo della proposta. Una semplice dichiarazione nella valutazione d'impatto non assicura la protezione necessaria.
85. Se la selezione dei dati contribuirebbe a minimizzare l'impatto sulla vita privata dei passeggeri, va ricordato che i principi della protezione dei dati vanno ben al di là della limitazione dei dati, includendo principi quali la necessità, la trasparenza e l'esercizio dei diritti delle persone interessate, tutti principi di cui occorre tenere conto nel determinare se un paese terzo offre un adeguato livello di protezione.
86. La valutazione d'impatto indica che tale trattamento consentirà all'UE di insistere su determinate norme e assicurare la coerenza in siffatti accordi bilaterali con i paesi terzi. Permetterà inoltre di chiedere un trattamento reciproco ai paesi terzi con i quali l'UE ha concluso un accordo, cosa che oggi non è possibile<sup>(3)</sup>.
87. Queste osservazioni sollevano la questione dell'impatto della proposta sugli accordi esistenti con gli Stati Uniti e Canada. Le condizioni di accesso ai dati previste in tali accordi sono in effetti molto più ampie, in quanto i dati non sono soggetti ad una selezione analoga prima di essere trasferiti a detti paesi terzi.
88. La valutazione d'impatto indica che nel caso in cui l'UE abbia concluso accordi internazionali con paesi terzi in materia di scambio/trasmissione di dati PNR a tali paesi, occorre tener debito conto di tali accordi. I vettori dovrebbero trasmettere i dati PNR alle unità d'informazione sui passeggeri conformemente alla normale prassi prevista dalle misure vigenti. L'unità d'informazione sui passeggeri che riceve tali dati li trasmette all'autorità competente del paese terzo con il quale è stato concluso l'accordo<sup>(4)</sup>.
89. Se da un lato la proposta sembra mirare al trasferimento *esclusivamente* dei dati *selezionati* alle autorità competenti, all'interno o al di fuori dell'UE, dall'altro la valutazione d'impatto, il preambolo della proposta (considerando 21) e lo stesso articolo 11 ricordano che occorre tenere in debito conto gli accordi esistenti. Ciò potrebbe far concludere che solo il filtraggio possa essere una valida misura per gli accordi che si concluderanno in futuro. In tale prospettiva, si potrebbe prevedere che l'accesso in blocco continuerà a costituire la norma di accesso, ad esempio, delle autorità americane ai dati PNR, conformemente alle disposizioni dell'accordo UE-Stati Uniti, ma che parallelamente e a seconda dei casi si potrebbero trasferire agli Stati Uniti dati specifici identificati dalle unità d'informazione sui passeggeri, inclusi, ma non solo, i dati relativi ai voli diretti in Stati Uniti.
90. IL GEPD deplora la mancanza di chiarezza su questo punto decisivo della proposta. Considera particolarmente importante che le condizioni di trasferimento dei dati PNR ai paesi terzi siano coerenti e soggette ad un livello armonizzato di protezione. Inoltre, per motivi di certezza giuridica, le garanzie che si applicano al trasferimento di dati dovrebbero essere precisate nella proposta stessa e non solo, come avviene adesso, nella valutazione d'impatto.

<sup>(1)</sup> Relazione della proposta, punto 2.

<sup>(2)</sup> Valutazione d'impatto, punto 5.2, «Protezione della vita privata».

<sup>(3)</sup> Valutazione d'impatto, punto 5.2, «Relazioni con i paesi terzi».

<sup>(4)</sup> Valutazione d'impatto, allegato A, «Organi che ricevono i dati dalle unità d'informazione sui passeggeri».

## VI. ALTRI PUNTI SOSTANZIALI

**Trattamento automatico**

91. Il GEPD rileva che la proposta esclude esplicitamente che le unità d'informazione sui passeggeri e le autorità competenti degli Stati membri intraprendano azioni di contrasto soltanto sulla base del trattamento automatico dei dati PNR o a motivo dell'origine razziale o etnica di un cittadino, delle sue convinzioni religiose o filosofiche, delle sue opinioni politiche o del suo orientamento sessuale <sup>(1)</sup>.
92. Tale precisazione è positiva in quanto limita i rischi di misure arbitrarie nei riguardi delle persone. Tuttavia, il GEPD fa rilevare che la portata della stessa si limita alle *azioni di contrasto* delle unità d'informazione sui passeggeri o delle autorità competenti, senza escludere, nell'attuale formulazione, il filtraggio automatico delle persone in base a profili standard, né impedire la costituzione automatica di elenchi di persone sospette e l'adozione di misure quali l'estensione della sorveglianza, fintantoché tali misure non sono considerate azioni di contrasto.
93. Il GEPD è del parere che la nozione di *azioni di contrasto* sia troppo vaga e che, per principio, non bisognerebbe prendere *alcuna decisione* nei riguardi delle persone solo in base al trattamento automatico dei loro dati <sup>(2)</sup>. Il GEPD raccomanda di modificare il testo di conseguenza.

**Qualità dei dati**

94. L'articolo 5, paragrafo 2, della proposta offre un'importante precisazione in quanto chiarisce che le compagnie aeree non sono tenute a raccogliere o conservare dati supplementari rispetto a quelli raccolti per i fini commerciali iniziali.
95. Vari aspetti del trattamento di tali dati meritano ulteriori osservazioni:
- I dati da mettere a disposizione, elencati nell'allegato 1 della proposta, sono molto numerosi e l'elenco è simile a quello dei dati messi a disposizione delle autorità americane nell'accordo UE-Stati Uniti. In varie occasioni, le autorità per la protezione dei dati, e in particolare il Gruppo dell'articolo 29, hanno messo in discussione la qualità di alcuni dei dati richiesti <sup>(3)</sup>.

<sup>(1)</sup> Considerando 20 e articolo 3, paragrafi 3 e 5, della proposta.

<sup>(2)</sup> Si veda al riguardo l'articolo 15, paragrafo 1, della direttiva 95/46/CE. La direttiva vieta tali decisioni automatizzate qualora esse abbiano effetti sulla persona interessata. Riguardo al contesto della proposta, le decisioni adottate nel quadro delle attività di contrasto verosimilmente comportano comunque effetti gravi sugli interessati. Anche il fatto di essere soggetti a controlli supplementari può incidere sull'interessato, specie se tali azioni sono ripetute.

<sup>(3)</sup> Si veda, in particolare, il parere n. 5/2007, del 17 agosto 2007, sul nuovo accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati del codice di prenotazione (PNR) da parte di vettori aerei al dipartimento per la sicurezza interna degli Stati Uniti, concluso nel luglio 2007, WP 138.

- Dalla formulazione della valutazione d'impatto <sup>(4)</sup> e dell'articolo 6, paragrafo 3, della proposta sembra evincersi che le compagnie aeree potrebbero trasmettere i dati agli intermediari anche in blocco. In una prima fase, i dati trasmessi ad una parte terza non si limiterebbero neppure ai dati PNR elencati nell'allegato 1 della proposta.
- Per quanto riguarda il trattamento dei dati sensibili, anche se tali dati potessero essere filtrati nella fase degli intermediari, resta ancora da stabilire se sia strettamente necessario che le compagnie aeree trasferiscano il campo aperto.

Il GEPD appoggia le osservazioni formulate in proposito dal Gruppo dell'articolo 29 nel suo parere.

**Metodo di trasferimento dei dati PNR**

96. I vettori aerei stabiliti fuori dell'UE sono obbligati ad utilizzare il metodo «push» per trasmettere i dati alle unità d'informazione sui passeggeri o agli intermediari, sempreché dispongano della necessaria architettura tecnica. In caso contrario, devono permettere l'estrazione dei dati mediante il metodo «pull».
97. La coesistenza di diversi metodi di comunicazione dei dati in funzione delle compagnie aeree interessate servirà solo a rendere più difficoltoso il controllo della conformità del trasferimento dei dati PNR con le norme sulla protezione dei dati e rischia altresì di falsare la concorrenza tra le compagnie aeree UE e non-UE.
98. Il GEPD ricorda che il metodo «push», che consente alle compagnie aeree di mantenere il controllo sulla qualità dei dati trasferiti e sulle circostanze di tali trasferimenti, è l'unico metodo ammissibile per quanto riguarda la proporzionalità del trattamento. Inoltre, deve trattarsi di un vero e proprio «push», cioè i dati non dovrebbero essere trasmessi in blocco all'intermediario, ma filtrati già in questa primissima fase del trattamento. Non è ammissibile che dati non necessari — e dati non inclusi nell'allegato 1 della proposta — siano trasmessi ad una parte terza, anche nel caso in cui questa debba cancellarli immediatamente.

**Conservazione dei dati**

99. L'articolo 9 della proposta prevede un periodo di conservazione dei dati PNR di cinque anni e un periodo supplementare di 8 anni durante il quale i dati devono essere conservati in una banca dati «dormiente», accessibile solo a determinate condizioni.

<sup>(4)</sup> Valutazione d'impatto, allegato A, «Metodo di trasmissione dei dati da parte dei vettori».

100. Il GEPD rimette in questione la differenza tra questi due tipi di banche dati: nulla garantisce che la banca dati «dormiente» sia un vero archivio, con metodi diversi di conservazione ed estrazione dei dati. In effetti, la maggior parte delle condizioni poste all'accesso alla banca dati dormiente consiste in requisiti di sicurezza che potrebbero applicarsi anche alla «banca dati in cui i dati sono conservati per cinque anni».

101. La durata totale di conservazione — 13 anni — risulta comunque eccessiva. La valutazione d'impatto la giustifica con la necessità di elaborare indicatori di rischio e individuare modelli di spostamento e comportamento <sup>(1)</sup>, la cui efficacia resta da dimostrare. Se è evidente che i dati possono essere conservati, in un caso specifico, per tutto il tempo necessario ad un'indagine in corso, nessuna giustificazione può addursi per la conservazione dei dati di tutti i passeggeri per 13 anni in mancanza del minimo sospetto.

102. Il GEPD rileva inoltre che tale periodo di conservazione non trova riscontro nelle risposte al questionario della Commissione fornite dagli Stati membri, secondo le quali la durata media di conservazione richiesta sarebbe di tre anni e mezzo <sup>(2)</sup>.

103. Inoltre, il periodo di 13 anni è equiparabile al periodo di conservazione di 15 anni previsto nell'ultimo accordo con gli Stati Uniti. Il GEPD ha sempre inteso che tale lungo periodo di conservazione era stato accettato esclusivamente a motivo delle forti pressioni esercitate dal governo americano, che voleva disporre di un periodo molto più lungo dei tre anni e mezzo e non perché lo avessero difeso, in una qualche fase, il Consiglio o la Commissione. Non c'è ragione di recepire in uno strumento giuridico dell'UE il compromesso in questione, giustificato soltanto dalla necessità di concludere i negoziati.

### Ruolo del comitato degli Stati membri

104. Il Comitato degli Stati membri istituito a norma dell'articolo 14 della proposta sarà competente non solo per le questioni inerenti alla sicurezza, inclusi il protocollo e la cifratura dei dati PNR, ma anche per quanto riguarda l'elaborazione di orientamenti relativi ai criteri generali comuni, ai metodi e alle pratiche inerenti alla valutazione del rischio.

105. Oltre a queste indicazioni, la proposta non prevede alcun elemento o criterio circa le condizioni concrete e il contesto del processo di valutazione del rischio. La valutazione d'impatto indica che i criteri dipenderanno in definitiva dalle informazioni in possesso di ciascuno Stato

membro, che sono in costante evoluzione. La valutazione di rischio deve essere effettuata in mancanza di norme uniformi di identificazione dei sospetti. Ci si può quindi chiedere in quale misura il Comitato degli Stati membri sarà in grado di svolgere un ruolo al riguardo.

### Sicurezza

106. La proposta specifica una serie di misure di sicurezza <sup>(3)</sup> che le unità d'informazione sui passeggeri, gli intermediari e le altre autorità competenti devono adottare per assicurare la protezione dei dati. Data l'importanza della banca dati e il carattere sensibile del trattamento, il GEPD è del parere che, oltre alle misure previste, l'entità che tratta i dati dovrebbe essere altresì obbligata a notificare ufficialmente qualsiasi violazione della sicurezza.

107. Il GEPD è al corrente del progetto di instaurare una procedura di notifica di questo tipo nel settore delle comunicazioni elettroniche a livello europeo. Raccomanda di includere tale misura di salvaguardia nella presente proposta e rimanda, a tale riguardo, al sistema istituito negli Stati Uniti per combattere le violazioni della sicurezza negli enti statali <sup>(4)</sup>. Gli incidenti inerenti alla sicurezza possono infatti verificarsi in qualsiasi campo d'attività, nel settore sia pubblico che privato, come ha dimostrato la recente perdita dell'intera banca dati dei cittadini britannici da parte dell'amministrazione del Regno Unito <sup>(5)</sup>. Anche dati su vasta scala, come quella prevista nella proposta, dovrebbero essere le prime, in un elenco delle priorità, a beneficiare di tale sistema di segnalazione.

### Riesame e clausola di caducità

108. Il GEPD prende atto che un riesame avrà luogo entro tre anni dall'entrata in vigore della decisione quadro, sulla scorta di una relazione della Commissione. Riconosce che tale riesame, basato sulle informazioni fornite dagli Stati membri, presterà particolare attenzione alle misure di salvaguardia della protezione dei dati e includerà l'attuazione del metodo «push», la conservazione dei dati e la qualità della valutazione di rischio. Per essere esaustivo, il riesame dovrebbe includere i risultati dell'analisi dei dati statistici elaborati in base al trattamento dei dati PNR. Tali statistiche dovrebbero includere, oltre agli elementi menzionati nell'articolo 18 della proposta, dati statistici sull'identificazione delle persone ad alto rischio, quali i criteri utilizzati per tale identificazione e i risultati concreti delle azioni di contrasto conseguenti all'identificazione.

<sup>(3)</sup> Articolo 12 della proposta.

<sup>(4)</sup> Si vedano, in particolare, i lavori della task force americana contro il furto d'identità, <http://www.idtheft.gov/>

<sup>(5)</sup> Si consulti il sito web dell'HM Revenue and Customs (HMRC, agenzia delle entrate fiscali e doganali) britannica: <http://www.hmrc.gov.uk/childbenefit/update-faqs.htm>  
Si consulti anche il sito: [http://news.bbc.co.uk/1/hi/uk\\_politics/7103566.stm](http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm)

<sup>(1)</sup> Valutazione d'impatto, allegato A, «Periodo di conservazione dei dati».

<sup>(2)</sup> Valutazione d'impatto, allegato B.

109. Nel parere, il GEPD ha già insistito sulla mancanza di elementi concreti che dimostrino la necessità del sistema proposto. Ritiene tuttavia che, qualora la decisione quadro entri in vigore, essa debba essere almeno integrata da una clausola di caducità. Al termine del periodo di tre anni, la decisione quadro dovrebbe essere abrogata qualora non vi siano elementi a favore del suo mantenimento.

### Impatto su altri strumenti giuridici

110. Nelle disposizioni finali, la proposta pone una condizione all'ulteriore applicazione degli accordi o intese bilaterali o multilaterali già esistenti. Questi strumenti possono essere applicati solo nella misura in cui sono compatibili con gli obiettivi della decisione quadro proposta.

111. Il GEPD nutre dubbi riguardo alla portata di tale disposizione. Come già accennato nella parte V sulla reciprocità, non è chiaro quale sarà l'impatto di tale disposizione sul contenuto degli accordi con i paesi terzi, come l'accordo con gli Stati Uniti. Per altro verso, non è chiaro neppure se la disposizione in questione possa avere un impatto sulle condizioni d'applicazione di strumenti di portata più ampia, come la Convenzione n. 108 del Consiglio d'Europa. Per quanto possa apparire improbabile in considerazione della diversità di contesto istituzionale e di attori implicati, bisognerebbe evitare qualsiasi rischio di interpretazione errata e precisare nella proposta che quest'ultima è ininfluente su strumenti di portata più ampia, segnatamente quelli aventi per oggetto la protezione dei diritti fondamentali.

## VII. CONCLUSIONE

112. Il GEPD rileva l'impatto importante della presente proposta in termini di protezione dei dati. Ha incentrato la sua analisi sulle quattro questioni fondamentali che suscita la proposta e insiste sulla necessità di affrontare globalmente le questioni sollevate. Nelle attuali circostanze, la proposta non è conforme ai diritti fondamentali, in particolare all'articolo 8 della Carta dei diritti fondamentali dell'Unione europea, e non dovrebbe essere adottata.

113. Nell'eventualità in cui si volesse dare seguito alle osservazioni fatte in precedenza, specie riguardo al criterio di legittimità, si sono formulate nel presente parere alcune proposte redazionali di cui il legislatore dovrebbe tenere conto. Si rinvia, in particolare, ai punti 67, 73, 77, 80, 90, 93, 106, 109 e 111 del parere.

### Legittimità delle misure proposte

114. Mentre l'obiettivo generale della lotta contro il terrorismo e la criminalità organizzata è di per sé chiaro e legittimo, l'elemento chiave del trattamento da porre in essere non risulta sufficientemente circoscritto e giustificato.

115. Il GEPD è del parere che occorra esaminare ulteriormente le tecniche intese a valutare il rischio presentato dalle persone mediante strumenti di «data mining» e modelli comportamentali e che sia opportuno stabilirne chiaramente l'utilità nel quadro della lotta contro il terrorismo, prima di utilizzarle su una scala così vasta.

116. Fondarsi su diverse banche dati senza avere una visione globale dei risultati concreti e delle lacune:

— è contrario ad una politica legislativa razionale, che esige che non si adottino nuovi strumenti prima di aver pienamente attuato quelli esistenti e dimostrato la loro insufficienza,

— potrebbe altrimenti portare ad una società basata sulla sorveglianza totale.

117. La lotta contro il terrorismo può certamente costituire un motivo legittimo per applicare deroghe ai diritti fondamentali alla vita privata e alla protezione dei dati. Tuttavia, per essere valida, la necessità dell'ingerenza deve poggiare su elementi chiari ed inconfutabili e la proporzionalità del trattamento deve essere dimostrata. Ciò è tanto più necessario nel caso di forte ingerenza nella vita privata delle persone, quale prevista nella proposta.

118. Siffatti elementi giustificativi mancano nella proposta e la necessità e proporzionalità non sono state verificate.

119. Il GEPD insiste sul carattere essenziale dei criteri di necessità e proporzionalità enunciati in precedenza, che rappresentano una condizione indispensabile per l'entrata in vigore della proposta.

### Quadro giuridico applicabile

120. Il GEPD rileva una grave incertezza giuridica riguardo al regime applicabile ai diversi attori implicati nel progetto, in particolare alle compagnie aeree e altri attori del primo pilastro; possono applicarsi le norme della proposta, quelle della decisione quadro sulla protezione dei dati o la legislazione nazionale che attua la direttiva 95/46/CE. Il legislatore dovrebbe chiarire in quale preciso momento del trattamento si applicheranno queste differenti norme.

121. L'attuale tendenza ad imporre in forma sistematica la cooperazione per finalità di contrasto ad attori del settore privato solleva la questione del quadro di protezione dei dati (primo o terzo pilastro) che si applica alle condizioni di tale cooperazione: non è chiaro se le norme debbano basarsi sulla qualità del responsabile del trattamento (settore privato) o sulla finalità perseguita (attività di contrasto).

122. Il GEPD ha già evidenziato il rischio di un vuoto giuridico tra le attività del primo e le attività del terzo pilastro <sup>(1)</sup>. Non è assolutamente chiaro se le attività svolte da società private, in qualche modo collegate all'applicazione del diritto penale, siano incluse nel campo d'applicazione previsto dal legislatore dell'Unione europea ai sensi degli articoli 30, 31 e 34 del trattato UE.
123. Si dovrebbe evitare di arrivare ad una situazione in cui, a seconda delle finalità perseguite, il trattamento da parte di fornitori di servizi sia soggetto a differenti quadri di protezione dei dati, soprattutto per le difficoltà che ciò comporterebbe in termini di esercizio dei diritti delle persone interessate.

#### Qualità dei destinatari

124. La proposta dovrebbe contenere una precisazione riguardo alla qualità dei destinatari dei dati personali raccolti dalle compagnie aeree, siano essi intermediari, unità d'informazione sui passeggeri o autorità competenti.
125. La qualità del destinatario, che in alcuni casi potrebbe essere un attore del settore privato, è in diretto rapporto con il tipo di garanzie in materia di protezione dei dati che si applica al destinatario stesso. È essenziale che il regime applicabile sia chiaro per tutti gli attori interessati, inclusi il legislatore, le autorità per la protezione dei dati, nonché i responsabili del trattamento e le persone interessate.

#### Trasferimento di dati a paesi terzi

126. Il GEPD rileva la necessità di garantire che il paese destinatario assicuri un adeguato livello di protezione. Si interroga anche sull'importanza del principio di «reciprocità» menzionato nella proposta e sulla sua applicazione a paesi già legati da un accordo con l'UE, come il Canada e gli Stati Uniti. Considera particolarmente importante che le condizioni di trasferimento dei dati PNR ai paesi terzi siano coerenti e soggette ad un livello armonizzato di protezione.

#### Altri punti sostanziali

127. Il GEPD attira altresì l'attenzione del legislatore su specifici aspetti della proposta che richiedono maggiore precisione o una migliore considerazione del principio della protezione dei dati. Si tratta, in particolare, dei seguenti aspetti:
- occorre limitare le condizioni in cui le decisioni automatizzate possono essere prese,
  - la quantità dei dati trattati dovrebbe essere ridotta,
  - il metodo di trasferimento dei dati dovrebbe basarsi unicamente sul metodo «push»,
  - il periodo di conservazione dei dati è giudicato eccessivo e ingiustificato,
  - occorre precisare il ruolo del comitato degli Stati membri per quanto riguarda gli orientamenti sulla «valutazione di rischio»,
  - le misure di sicurezza dovrebbero includere una procedura di «notifica delle violazioni della sicurezza»,
  - il riesame della decisione dovrebbe prevedere una clausola di caducità,
  - nella proposta si dovrebbe precisare che essa è ininfluente sugli strumenti di portata più ampia, segnatamente quelli aventi per oggetto la protezione dei diritti fondamentali.

#### Osservazioni finali

128. Il GEPD osserva che la presente proposta è presentata in un momento in cui il quadro istituzionale dell'Unione europea è sul punto di subire profondi mutamenti. Le conseguenze del trattato di Lisbona in termini di processo decisionale saranno fondamentali, specie per quanto riguarda il ruolo del Parlamento.
129. Tenuto conto dell'impatto senza precedenti della proposta in termini di diritti fondamentali, il GEPD raccomanda di non adottarla nel quadro del trattato attuale, ma di far sì che essa segua la procedura di codecisione prevista dal nuovo trattato. Ciò rafforzerebbe i fondamenti giuridici sui cui sarebbero prese le misure cruciali previste nella proposta.

---

<sup>(1)</sup> Si veda il parere del garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul seguito dato al programma di lavoro per una migliore applicazione della direttiva sulla protezione dei dati, GU C 255 del 27.10.2007, pag. 1. Si veda anche la relazione annuale 2006, pag. 47.