Lotta al terrorismo, sicurezza del trasporto aereo e protezione dei dati personali nel recente contenzioso USA/UE

di Paola Puoti

Introduzione

L'accesso ai dati personali per motivi di pubblica sicurezza sta acquistando un'importanza sempre maggiore sia negli Stati Uniti che all'interno dell'UE, dato il carattere transnazionale del terrorismo, che determina il bisogno di una cooperazione sempre più stretta tra gli Stati, anche nell'attività di raccolta, conservazione, trattamento e trasferimento di dati personali[1].

D'altro canto, l'introduzione di misure di sicurezza basate sull'accesso ai dati personali per motivi di lotta al terrorismo ed al crimine organizzato, solleva profonde preoccupazioni in relazione alla tutela della *privacy* e dei dati delle persone coinvolte.

L'esigenza di far circolare liberamente ma in sicurezza le persone in tutto il mondo si scontra con il rischio di un controllo globale dei loro dati personali senza sufficienti garanzie di tutela.

Sotto questo profilo, gli Stati Uniti sono considerati all'avanguardia nell'uso di nuove tecnologie dell'informazione basate sull'accesso ai dati personali per motivi di sicurezza. Il loro approccio sembra favorire senz'altro la dimensione della sicurezza rispetto a quella della tutela dei dati personali, come è dimostrato dall'adozione dei sistemi di controllo dei dati PNR.

[1] Il Parlamento europeo, Direzione generale per le politiche interne dell'Unione, le libertà civili, la giustizia e gli affari interni, ha preparato uno *Study Concerning Data Protection from a Transatlantic Perspective: the EU and US Move Towards an International Data Protection Agreement?*, October 2008 (PE 408.320) disponibile nel sito dell'UE. Nello studio si afferma: «In the field of security and law enforcement, the request for data access are steadily multiplying» *(ibidem*, a p. 22).

L'Unione Europea sceglie un approccio più equilibrato nel coniugare *privacy* e sicurezza.

Lo scopo di realizzare la libera circolazione delle persone all'interno del territorio dell'Unione può essere conseguito, infatti, solo assicurando al contempo uno stretto controllo sulle persone che provengono sia da altri Stati europei che da paesi terzi, nel quadro di un unico spazio di libertà, sicurezza e giustizia che costituisce il contenuto del cosiddetto terzo pilastro dell'Unione.

A livello europeo, il controllo sulle persone che circolano nei confini dell'UE viene effettuato dalle polizie statali e da Europol utilizzando diverse banche dati, quali i sistemi VIS, SIS, SIS II, tutte soggette a severe norme di tutela della *privacy* e dei dati delle persone oggetto di controllo.

Il 4 novembre 2004 il Consiglio europeo ha adottato il Programma dell'Aja sul rafforzamento della libertà, sicurezza e giustizia nell'UE, in cui si invita la Commissione a presentare proposte entro la fine del 2005, per l'attuazione del principio della disponibilità dei dati. Questo, allo scopo di rafforzare lo scambio transfrontaliero di informazioni tra Stati membri. Il Programma dell'Aja sottolinea che le proposte della Commissione devono attenersi strettamente al principio del rispetto dei dati personali.

La necessità di conciliare sicurezza e libertà ha portato all'adozione, il 4 ottobre 2005, di una proposta della Commissione per una *Decisione-quadro del Consiglio sulla protezione dei dati personali trattati nel quadro della cooperazione di polizia e giudiziaria in materia penale*[2].

Da quanto appena detto si desume che, nonostante si possa riscontrare la stessa tendenza verso un utilizzo sempre crescente delle nuove tecnologie dell'informazione per la raccolta dei dati personali sia in Europa che negli USA, la normativa europea adotta un differente approccio rispetto a quella statunitense, per quanto riguarda il difficile equilibrio tra il bisogno di garantire la sicurezza delle persone e il loro diritto fondamentale alla *privacy* e alla tutela dei dati personali.

La necessità di conciliare le opposte esigenze di sicurezza delle persone, delle cose, degli Stati da atti di terrorismo internazionale e di criminalità organizzata da una parte, e di rispetto della vita privata e della riservatezza dei dati personali dall'altra, assume un ri-

[2] Brussels, 4.10.2005 COM(2005) 475 final 2005/0202 (CNS).

lievo del tutto particolare nella prassi statale relativa al flusso transfrontaliero dei dati dei passeggeri di voli aerei che si recano dall'Europa negli Stati Uniti e in altri paesi terzi come Australia e Canada e viceversa.

La controversia tra Unione Europea e USA relativa all'obbligo imposto dalle autorità statunitensi ai vettori aerei stabiliti nell'UE, di consentire l'estrazione dei dati PNR di chi voglia volare negli o dagli USA, da parte delle autorità di controllo delle frontiere, costituisce un chiaro esempio delle difficoltà legate al raggiungimento di un tale equilibrio.

Per comprendere meglio i termini della controversia sembra necessario richiamare in primo luogo le norme internazionali, europee e statunitensi, relative ai diritti ed agli obblighi degli Stati in materia di *privacy* e sicurezza del trasporto aereo.

Quindi si illustrerà il caso PNR e la sentenza della Corte di Giustizia del 30 maggio 2006.

Infine si darà conto dei più recenti sviluppi in materia di sicurezza e tutela dei dati personali nell'ordinamento dell'UE, analizzando in particolare la proposta di decisione relativa all'istituzione di un sistema europeo di raccolta dei dati PNR, e le prospettive aperte dal negoziato transatlantico su sicurezza e tutela dei dati personali attualmente in corso tra UE e Stati Uniti.

1. Le norme internazionali sulla protezione dei dati personali e sul loro flusso transfrontaliero

Il diritto internazionale contiene norme, alcune delle quali vincolanti, in materia di diritto alla vita privata ed alla riservatezza.

Nel quadro delle Nazioni Unite si possono ricordare l'articolo 12 della Dichiarazione universale dei diritti dell'uomo del 1948[3]; l'articolo 17 del Patto ONU sui diritti civili e politici del 1966[4]; le Linee

[3] Articolo 12: Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni. Testo in italiano in R. Luzzatto, F. Pocar, *Codice di diritto internazionale pubblico*, 2006, p. 160.

[4] L'articolo 17 riprende letteralmente l'articolo 12 della Dichiarazione universale.

guida dell'Assemblea generale dell'ONU del 14 dicembre 1990 sui sistemi computerizzati di dati personali[5].

L'OECD ha adottato, tra l'altro, la Raccomandazione del Consiglio del 23 settembre 1980 relativa alle Linee guida sulla tutela della riservatezza e i flussi transfrontalieri di dati[6].

Nel quadro del Consiglio d'Europa troviamo l'articolo 8 della CEDU[7] che è stato interpretato dalla Corte europea nel senso di ricomprendervi il diritto di ognuno alla tutela dei dati personali. Particolare rilievo assumono poi la *Convenzione del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato dei dati personali* e il *Protocollo addizionale alla Convenzione, relativo alle autorità di controllo ed al flusso transfrontaliero dei dati personali*.

Ai fini di questo lavoro interessano i principi generali contenuti nelle Linee guida dell'AG ONU, ai quali s'ispira la direttiva 95/46/CE, che costituisce l'atto generale di attuazione del principio della protezione dei dati personali nel diritto comunitario[8].

Le Linee guida ONU prevedono il principio della correttezza e legalità dei dati; quello di accuratezza con i conseguenti obblighi di aggiornamento, di completezza e revisione; il principio della finalità determinata del trattamento e del carattere proporzionato del trattamento a tale finalità; il diritto di accesso dell'interessato ai propri dati personali e alla correzione, rettifica, cancellazione dei dati processati illecitamente o inutilmente.

[5] *UN Guidelines Concerning Computerized Personal Data Files*, adopted by the General Assembly on 14 December 1990, in rete nel sito ufficiale dell'Organizzazione: www.un.org.

[6] *OECD Recommendation on 23 September 1980 Concerning Guidelines Governing the Protection of Privacy and the Transborder Flows of Personal Data*, disponibili nel sito ufficiale dell'Organizzazione: www.oecd.org.

[7] Articolo 8. *Diritto al rispetto della vita privata e familiare*.

1. Ogni persona ha diritto al rispetto della vita privata e familiare, del suo domicilio e della sua corrispondenza.

2. Non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto se non in quanto tale ingerenza sia prevista dalla legge e in quanto costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la difesa dell'ordine, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui. Testo in italiano in R. Luzzatto, F. Pocar, *Codice di diritto internazionale pubblico*, 2006, p. 185.

[8] *Direttiva 95/46 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*, pubblicata in *GUUE*, n. L 281 del 23.11.1995, p. 31 ss.

Particolare rilievo ha il principio n. 5 di non discriminazione, che stabilisce il divieto di trattare dati sensibili, ovvero dati personali che possano rivelare informazioni sull'origine razziale, etnica, sul colore, la vita sessuale, le opinioni politiche, religiose, filosofiche ed altre convinzioni così come l'appartenenza ad associazioni o sindacati.

Il successivo principio n. 6 specifica le deroghe ammesse al divieto di trattamento dei dati sensibili nel suo secondo comma, limitandole a quelle ammesse dal Patto internazionale sui diritti umani e da altri strumenti di garanzia dei diritti umani e di prevenzione della discriminazione.

Viene poi enunciato il principio di sicurezza dei trattamenti e si invitano gli Stati membri a predisporre leggi nazionali che istituiscano autorità indipendenti di controllo del diritto alla protezione dei dati personali, che prevedano l'erogazione di sanzioni penali per le violazioni e adeguati rimedi per i singoli individui.

Il principio n. 9 si occupa del flusso transfrontaliero dei dati e pone il principio della libertà di circolazione tra Stati che abbiano livelli equivalenti di tutela della riservatezza e, in caso di livelli diversi di tutela dei dati, stabiliscono che deroghe alla loro circolazione possono essere ammesse solo nella misura in cui ciò sia necessario alla tutela della *privacy*.

2. Gli standard internazionali in materia di flusso transfrontaliero di dati dei passeggeri di voli aerei

L'articolo 13 della Convenzione di Chicago che istituisce l'Organizzazione per l'aviazione civile internazionale riconosce agli Stati membri la libertà di disciplinare discrezionalmente le modalità e le condizioni di ammissione nei, o di partenza dai, loro territori, di passeggeri ed aerei. Queste leggi e regolamenti riguardano l'ingresso, la dogana, l'immigrazione, i passaporti, la quarantena.

Di conseguenza uno Stato gode di piena discrezionalità circa le informazioni che esige dalle persone che intendono fare ingresso sul suo territorio, e può chiedere al vettore aereo di inoltrare informazioni sui dati dei passeggeri, come i dati API e PNR, alle autorità di controllo delle frontiere.

Questi ultimi consistono in dati personali raccolti da operatori privati a fini commerciali per rafforzare la sicurezza dell'aviazione civile internazionale.

I dati API (Advanced Passenger Information), riguardano le informazioni biografiche essenziali di una persona richiesti da uno Stato ai vettori aerei prima del suo arrivo in un certo paese. In genere consistono nel nome completo del viaggiatore, data di nascita, sesso, cittadinanza o nazionalità e documento di viaggio, paese di rilascio e numero[9].

Le schede nominative dei passeggeri (Passenger Name Record, PNR) sono finalizzate alla raccolta di un numero di dati superiore a quelli disponibili con il sistema API[10]. In base all'Annesso 1 delle Linee guida ICAO[11], relativo agli elementi contenuti nei dati, un operatore di un sistema può includere fino ad un massimo di 22 gruppi o categorie di dati personali, che comprendono i dati API, l'indirizzo e-mail, l'indirizzo di casa, la forma di pagamento, il numero della carta di credito e soprattutto tutti i dati sensibili, come il cibo preferito dal passeggero o altre richieste che possono rivelare l'origine etni-

[9] L'Organizzazione mondiale delle dogane (the World Customs Organization) assieme all'Agenzia internazionale per il trasporto aereo (the International Air Transport Agency) e all'ICAO hanno adottato, nel marzo del 2003, le Linee guida WCO/IATA/ICAO: *Guidelines on Advance Passenger Information* (API), March 2003. Il punto 1.5. dell'introduzione auspica: «to stress the benefits that can be gained from the efficient use of Information Technology (i.e. computerized passenger screening/clearance systems). The deployment of such systems, incorporating passenger selection criteria developed on the basis of high quality intelligence, can and do have a very positive effect on enforcement activities. Information Technology can be further harnessed to ensure that details of arriving passengers are received in advance of the arrival of the flight – thus allowing the Border Control Agencies adequate time to determine their response. This advance notification to the Border Control Agencies by carriers (or other parties) using electronic data interchange (EDI), is the topic of this Guideline». Il documento è reperibile al seguente indirizzo: http://www.un.org/sc/ctc/pdf/APIGuidelines.pdf.

[10] Si veda la 12ª Sessione dell'ICAO Facilitation Division svoltasi al Cairo, Egitto, dal 22 marzo al 1° aprile 2004, dove per la prima volta è stata sollevata la questione della raccolta dei dati PNR da parte degli Stati. Durante quella Sessione la Divisione ha adottato la Raccomandazione B/5 che dispone come segue: «It is recommended that ICAO develops guidance for those States that may require access to Passenger Name Record (PNR) data to supplement identification data received through an API system, including guidelines for distribution, use and storage of data and a composite list of data elements that may be transferred between the operator and the receiving State». Di conseguenza l'ICAO ha sviluppato le Linee guida relative ai dati PNR che sono state approvate dal Segretario generale e pubblicate a sua cura nell'aprile 2006 (ICAO Cir309 AT/131).

[11] ICAO, *Guidelines on Passenger Name Record (PNR) Data*, April 2006 (Cir309 AT/131.

ca, le opinioni politiche, il credo religioso, così come dati relativi alla salute o alla vita e all'orientamento sessuale del viaggiatore.

Queste ultime informazioni sui dati sensibili si ricavano dalla categoria denominata «General remarks»[12].

In quanto dati sensibili, molti di quelli contenuti nel PNR non dovrebbero essere trasferiti dai vettori agli Stati a meno che ciò non sia necessario ai fini della lotta al terrorismo e sempre che sia assicurato un adeguato livello di tutela di questo genere di dati da parte della legislazione dello Stato richiedente.

Nel marzo del 2005 l'ICAO ha adottato una «Prassi raccomandata» (Recommended Practice) ai fini della sua inclusione nell'Annesso 9 della Convenzione di Chicago, intitolato «Facilitation» che invita gli Stati contraenti ad attenersi alle Linee guida ICAO ove esigano l'accesso alle schede nominative dei passeggeri[13].

Le Linee guida dell'ICAO si propongono di stabilire misure uniformi per il trasferimento dei dati PNR ed il successivo trattamento da parte degli Stati interessati, date le sostanziali differenze di condizioni per il trasferimento di questi dati imposte dai singoli Stati ai vettori aerei[14].

Le Linee guida raccomandano che la richiesta di traferimento di dati PNR sia disciplinata da chiare disposizioni legislative (*explicit legal provisions*).

Lo standard n. 12 enumera i principi generali relativi alla protezione dei dati personali, tra i quali:

– quello del livello adeguato di gestione e protezione da parte dell'autorità designata;
– quello del bilanciamento ragionevole dell'esigenza di protezione dei dati PNR e di quella di accesso alle informazioni dei passeggeri a rischio per la sicurezza del volo.

Le Linee guida accolgono quindi come regola generale *il principio di disponibilità dei dati PNR*: si suggerisce infatti di non restringere la

[12] Si vedano i gruppi e le categorie elencate nell'Annesso 1 (PNR data elements) delle *ICAO Guidelines*.

[13] «*Recommended Practice*. Contracting States requiring Passenger Name Record (PNR) access should conform their data requirements and their handling of such data to guidelines developed by ICAO».

[14] Punti 3.1 e 3.2 delle *ICAO Guidelines*.

loro circolazione tra Stati, a meno che uno di essi non abbia posto in essere un adeguato sistema di protezione dei dati.

I principi che gli Stati devono osservare nel trattare i dati PNR sono i seguenti[15]:

– principio della finalità limitata e specificata del trattamento;
– principio dell'uso dei dati limitato alla finalità per la quale sono trattati;
– principio della restrizione del diritto di accesso alle sole autorità o organismi autorizzati;
– principio dell'adeguata protezione dei dati da distruzioni o trattamenti illeciti;
– principio della durata limitata della conservazione dei dati;
– principio dell'accesso ai dati da parte delle persone fisiche interessate ai fini della loro correzione, rettifica o cancellazione[16];
– principio della garanzia di rimedi giurisdizionali a disposizione dei singoli i cui dati siano stati trattati in modo non corretto o illecito o errato[17].

Per quel che concerne il flusso transfrontaliero dei dati personali, le Linee guida ICAO riaffermano lo stesso principio enunciato nelle Linee guida dell'OECD e dell'ONU, vale a dire quello del *livello adeguato di protezione che lo Stato verso il quale i dati sono trasmessi deve garantire in base alla propria legislazione*.

3. I metodi di trasmissione dei dati PNR

Le Linee guida (standard 7.1.) chiariscono anche quali metodi siano utilizzabili per la trasmissione transfrontaliera dei dati, individuandoli nei due che seguono:

[15] Punto 6.1 delle *ICAO Guidelines*: 6. PNR Data Processing.

[16] Punto 1.4.3. delle Linee guida: States should provide for appropriate mechanisms, established by legislation where feasible, for passengers to request access to and consult personal information about them and request corrections of notations, if necessary.

[17] Punto 14.4. delle Linee guida: Redress mechanisms should be set up to enable passengers to obtain adequate remedy for the unlawful processing of their PNR data by public authorities.

– metodo di trasferimento dei dati PNR «*push*», in virtù del quale le autorità competenti dello Stato richiedente i dati PNR possono accedere direttamente nel sistema del vettore aereo ed estrarre copia dei dati richiesti dal suo archivio;
– metodo di trasferimento dei dati PNR «*pull*», dove è il vettore aereo che trasmette i dati PNR che gli vengono richiesti all'archivio informatico dell'autorità richiedente.

Le Linee guida invitano gli Stati a valutare i vantaggi di ognuno dei due metodi in termini di protezione dei dati e di valutazione del rischio così come dell'impatto economico sugli operatori e sugli Stati, prendendo però apertamente posizione a favore del secondo (metodo «*push*»), che assicura una maggiore protezione dei dati poiché essa è affidata all'operatore che è anche il responsabile del trattamento, il quale può filtrare in anticipo i dati sensibili vietati e trasmettere solo quelli consentiti.

Seguono indicazioni relative alla frequenza ed al momento della trasmissione dei dati, il loro filtraggio per trasmettere solo i dati richiesti, alla loro conservazione che deve avere carattere temporaneo dovendosi limitare al tempo necessario al conseguimento della finalità del trattamento o a finalità di controllo o di risarcimento secondo legge, alle modalità e ai limiti dell'inoltro dei dati a terzi, che possono essere soltanto altre autorità autorizzate al trattamento dello Stato ricevente o autorità di un altro Stato, dopo aver posto in essere i necessari accorgimenti concordati tra gli Stati richiedenti e riceventi.

4. La normativa del Consiglio d'Europa in materia di privacy e sicurezza del trasporto aereo

Gli Stati membri del Consiglio d'Europa prendono in considerazione il diritto alla *privacy* in diversi strumenti convenzionali, quali l'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali[18]; la Convenzione del Consiglio d'Europa n. 108 del 28 gennaio 1981 sulla *Protezione delle perso-*

[18] La Convenzione è stata firmata a Roma il 4 novembre 1950, si può leggere nel sito ufficiale del Consiglio d'Europa: http://conventions.coe.int, ed è in vigore dal 3 settembre 1953. Tutti gli Stati membri dell'UE vi partecipano.

ne con riguardo al trattamento automatico del dati personali[19]; il Protocollo addizionale alla Convenzione n. 108 relativo alle *Autorità di controllo ed al flusso transfrontaliero di dati* dell'8 novembre 2001[20].

La normativa del Consiglio d'Europa risulta applicabile a tutti gli Stati membri dell'UE, in quanto anche contraenti sia della CEDU che della Convenzione n. 108, mentre soltanto alcuni, tra i quali non figura l'Italia, fanno parte del Protocollo addizionale del 2001. Come si vedrà più avanti, le norme del Consiglio d'Europa sulla tutela dei dati personali svolgono una funzione importante soprattutto nel terzo pilastro, dove non esiste ancora una disciplina organica della tutela dei dati personali nelle attività di contrasto alla criminalità ed al terrorismo.

5. Le norme sulla protezione dei dati personali e sul loro flusso trasfrontaliero nel sistema UE/CE

Il diritto dell'Unione Europea prende in considerazione la protezione della *privacy* e dei dati personali *in primis* attraverso il richiamo operato dall'articolo 6 § 2 del TUE alla Convenzione di Roma del 1950, sopra ricordata. Inoltre, la tutela della vita privata e dei dati personali costituisce oggetto di due distinte disposizioni – gli articoli 7 e 8 – della Carta di Nizza, attribuendo così natura di diritti fondamentali a questi due princìpi[21].

[19] Firmata a Strasburgo il 28 gennaio 1981, la Convenzione si legge nel sito ufficiale del Consiglio d'Europa: http://conventions.coe.int, ed è entrata in vigore nel 1985. L'Italia partecipa.

[20] Il Protocollo si legge nel sito ufficiale del Consiglio d'Europa: http://conventions.coe.int, ed è entrato in vigore il 1° luglio 2004. L'Italia ha solo firmato ma non ratificato, per cui non partecipa.

[21] La Carta di Nizza distingue tra il rispetto per la vita privata e la protezione dei dati personali, disponendo in merito in due diversi articoli.

L'articolo 7 s'intitola al rispetto della vita privata e della famiglia e così dispone: Ognuno ha il diritto al rispetto per la sua vita privata e della famiglia, dell'abitazione e delle comunicazioni.

L'articolo 8 riguarda la protezione dei dati personali e recita:

1. Ognuno ha il diritto alla protezione dei dati che lo/la riguardano.

2. Tali dati devono essere trattati lealmente per scopi specifici e sulla base del consenso delle persone interessate o su qualsiasi altra base fondata sulla legge. Ognuno ha il diritto di accesso ai dati che sono stati raccolti e che lo/la riguardano, e il diritto a che siano corretti.

Infine, molti atti della Comunità e dell'Unione Europea – questi ultimi fondati prevalentemente sul terzo pilastro – hanno per contenuto la tutela della *privacy* e dei dati personali.

Qui di seguito illustreremo in due distinti paragrafi la disciplina comunitaria e quella dell'Unione Europea, poiché entrambi rilevano ai fini della comprensione della controversia sul trasferimento di dati PNR tra Unione Europea e Stati Uniti. Così facendo sarà anche possibile mettere in evidenza le incongruenze connesse con l'articolazione della disciplina della tutela dei dati personali tra il primo ed il terzo pilastro. In questa prospettiva, il Trattato di Lisbona, se e quando entrerà in vigore, porterà un sostanziale cambiamento, unificando i due pilastri ed assoggettando tutta la relativa legislazione alla procedura ordinaria di codecisione, con il coinvolgimento del Parlamento europeo che attualmente, nel terzo pilastro, svolge un ruolo marginale.

5.1. La normativa comunitaria

La protezione dei dati personali nel primo pilastro è disciplinata innanzitutto dalla direttiva 95/46/CE del PE e del Consiglio del 24 ottobre 1995 sulla *Protezione degli individui rispetto al trattamento dei dati e sulla libera circolazione di tali dati*[22], e poi dalla direttiva 2002/58/CE del PE e del Consiglio del 12 luglio 2002 relativa al *trattamento dei dati personali ed alla protezione della privacy nel settore delle comunicazioni elettroniche*[23]. Quest'ultima è stata emendata dalla più recente direttiva 2006/24/CE del PE e del Consiglio 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*[24].

La direttiva 95/46/CE costituisce l'atto fondamentale in materia di obblighi degli Stati sulla tutela dei dati personali e si propone, come emerge dal suo terzo *considerando*, di assicurare la libera circolazione di questi dati nell'UE da uno Stato membro all'altro, e di salvaguardare al contempo i diritti fondamentali della persona.

3. Il rispetto di queste norme sarà soggetto a controllo da parte di un'autorità indipendente.

[22] *GUUE*, L 281, 23.11.1995, pp. 31-50.

[23] *GUUE*, L201, 31.07.2002, pp. 37-47.

[24] *GUUE*, L 105, p. 54.

La direttiva s'indirizza agli Stati membri che sono quindi i principali responsabili della realizzazione dei suoi obiettivi, come risulta dall'articolo 1[25].

Per quanto riguarda la sfera di applicazione della direttiva, essa non si applica, in base all'articolo 3, al trattamento di dati personali effettuato in base al secondo o al terzo pilastro ed in ogni caso in cui il trattamento abbia per oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato e le attività dello Stato in materia penale[26].

Il capo II della direttiva specifica poi i principi fondamentali applicabili al trattamento dei dati personali ed i relativi obblighi degli Stati membri, che consistono nella predisposizione di normative nazionali conformi alle condizioni di liceità dei trattamenti di dati personali stabiliti dagli articoli 6 e seguenti della direttiva.

L'articolo 6 specifica i principi relativi alla qualità dei dati che gli Stati membri devono garantire, e che riguardano il carattere lecito del trattamento; il carattere limitato ad una specifica finalità della loro rilevazione; il carattere proporzionato, e quindi adeguato, pertinente alla finalità della rilevazione dei dati e non eccedente; la necessità dell'esattezza e dell'aggiornamento periodico dei dati.

La disposizione in esame prevede poi l'obbligo di adottare le misure necessarie a cancellare o rettificare i dati inesatti o incompleti e quello di conservarli in modo da consentire l'identificazione delle persone interessate solo per un arco di tempo determinato e non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati.

L'articolo 7 stabilisce i requisiti che legittimano il trattamento dei dati, primo tra tutti il consenso della persona interessata o in alternativa la base legale di quest'ultimo, mentre particolare rilievo riveste il successivo articolo 8 che riguarda il *trattamento dei dati sensibili*, ossia quei dati che permettono di rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché i dati relativi alla salute ed alla vita sessuale.

In base al primo paragrafo della disposizione gli Stati membri

[25] L'art. 1 dispone: Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.

[26] Si rinvia al prossimo paragrafo.

vietano il trattamento di queste categorie di dati sensibili, con alcune *eccezioni* previste nel successivo paragrafo, dove il divieto cede di fronte al consenso dell'interessato al trattamento dei suoi dati sensibili, o quando tale trattamento sia necessario per l'assolvimento di diritti ed obblighi del responsabile in materia di diritto del lavoro; o ancora quando serva per costituire, esercitare o difendere un diritto in via giudiziaria o sia necessario per finalità connesse con la salute della persona.

Il paragrafo 5 dell'articolo 8 stabilisce poi il principio per il quale solo una pubblica autorità può effettuare o autorizzare i trattamenti dei dati personali relativi a infrazioni, condanne penali o misure di sicurezza.

La direttiva contiene, per finire, una disposizione di particolare rilievo per il nostro tema, l'articolo 25, che riguarda i principi relativi al trasferimento di dati personali verso paesi terzi.

Questa disposizione, sebbene riguardi in generale il trasferimento di dati personali verso paesi terzi per finalità commerciali oggetto del primo pilastro, costituisce altresì la base giuridica inizialmente utilizzata dalle Istituzioni anche per disciplinare la trasmissione di dati PNR, trasferimento che serve scopi diversi da quelli commerciali, proponendosi di garantire la sicurezza del trasporto aereo e di contribuire alla lotta al terrorismo ed alla criminalità organizzata.

In base al primo paragrafo dell'articolo 25 si accoglie il principio della libera circolazione dei dati personali tra Stati che assicurino un livello di protezione adeguato al loro trattamento, livello di adeguatezza che, in base al paragrafo 2, deve valutarsi con riferimento ad un insieme di circostanze quali la natura dei dati da trasferire, le finalità del trattamento, il paese d'origine ed il paese di destinazione finale, le norme di diritto, generali e settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate.

Spetta alla Commissione la decisione circa la valutazione del livello di adeguatezza del sistema di protezione dei dati personali garantito da uno Stato terzo, la quale agisce con procedura di comitato e può concludere in senso negativo e quindi chiedere agli Stati membri dell'UE di impedire il flusso dei dati verso il paese terzo e avviare negoziati con quest'ultimo per porre rimedio alla situazione; oppure può concludere in senso positivo, nel qual caso gli Stati membri devono conformarsi alla sua decisione imponendo ai vettori di trasmettere i

dati. In base all'articolo 26 sono possibili delle deroghe che permettono il trasferimento di dati personali a paesi terzi che non garantiscono un livello adeguato di protezione, se c'è il consenso inequivocabile dell'individuo interessato dal trattamento, oppure se il trattamento serve a concludere o eseguire un contratto o, infine, se il responsabile del trattamento garantisce la tutela dei dati che riceve.

Come vedremo più avanti, la Commissione ha adottato diverse decisioni sul livello di adeguatezza dei sistemi di protezione dei dati dei passeggeri assicurati da paesi terzi, quali gli Stati Uniti ed il Canada.

L'altro strumento in materia di trasferimento dei dati, questa volta specificamente indirizzato ai vettori aerei e relativo alla comunicazione dei dati cosiddetti API è la più recente direttiva 2004/82/CE concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate.

Questa direttiva trova la sua base giuridica non già, come la 95/46, nell'articolo 95 sul ravvicinamento delle legislazioni, bensì negli articoli 62 § 2 lettera a e 63 § 3 lettera b del TCE, relativi alla materia degli affari interni su visti, asilo e immigrazione ed altre politiche connesse con la circolazione delle persone, da poco «comunitarizzata» dal trattato di Amsterdam.

Si tratta di un atto comunitario complementare al sistema Schengen, poiché persegue la stessa finalità di quest'ultimo di controllare i flussi migratori e di combattere l'immigrazione illegale. Il suo articolo 1 prevede che gli Stati membri adottino entro il termine di trasposizione (fissato al 5 settembre 2006 dal suo articolo 7) «le disposizioni necessarie per istituire l'obbligo per i vettori di trasmettere, entro il termine delle procedure di accettazione, su richiesta delle autorità incaricate di effettuare i controlli delle persone alle frontiere esterne, le informazioni relative alle persone che saranno trasportate a un valico di frontiera autorizzato attraverso il quale tali persone entreranno nel territorio di uno Stato membro».

Il secondo paragrafo enumera le informazioni che compongono i dati API, che sono conformi alle Linee guida dell'IATA e dell'ICAO già richiamate.

L'articolo 6 disciplina il loro trattamento, stabilendo che i dati vanno trasmessi su richiesta delle autorità di frontiera da parte dei vettori entro il termine delle procedure di accettazione per via elettronica o altra modalità appropriata e che i dati ricevuti possono es-

sere detenuti sono temporaneamente e distrutti entro le 24 ore successive alla loro trasmissione. Lo stesso obbligo di cancellazione incombe sui vettori negli stessi termini[27].

Il parere 9/2006 sull'attuazione della direttiva 2004/82/CE adottato dal Gruppo di lavoro Articolo 29 il 28 settembre 2006[28], a proposito delle categorie dei dati passeggeri oggetto di trasmissione, ribadisce che essi dovrebbero limitarsi ai dati API e che: «gli Stati membri violerebbero la direttiva 95/46/CE se richiedessero tutti i dati dei passeggeri contenuti nei registri dei nomi dei passeggeri (PNR, Passenger Name Records) o negli elenchi di controllo delle partenze dei vettori aerei, dato che entrambi eccedono di gran lunga i dati menzionati dagli orientamenti e da altre norme internazionali pertinenti; occorre ricordare inoltre che i dati PNR non sono necessari per il controllo delle frontiere»[29].

5.2. La tutela dei dati personali nel terzo pilastro dell'Unione Europea

Il terzo pilastro si occupa della lotta al terrorismo e della criminalità: la direttiva 95/46 non si applica alle attività del terzo pilastro, come chiaramente stabilisce l'articolo 3 § 2 che dispone:

«Questa Direttiva non si applica al trattamento dei dati personali:

- nel corso di attività che non rientrano nella sfera di applicazione del diritto comunitario, quali quelle previste dai Titoli V e VI del Trattato sull'Unione Europea ed in ogni caso alle operazioni di trattamento dati relative alla pubblica sicurezza, alla difesa, alla sicurezza nazionale (compreso il benessere economico dello Stato quando l'operazione di trattamento riguarda materie di sicurezza dello Stato) ed alle attività dello Stato nel settore del diritto penale».

[27] Si ricorda anche il regolamento CE n. 229/89 del 24 luglio 1989 su un codice di condotta per i sistemi telematici e di prenotazione, che, nella versione emendata dal regolamento CE n. 323/1999, al suo articolo 6 § 1 lett. a) prevede che i dati personali devono essere cancellati dalla rete entro 72 ore dal completamento della prenotazione (cioè l'arrivo del volo) e possono essere archiviati per un massimo di tre anni e l'accesso ai dati è consentito solo per controversie sulla fatturazione).

[28] Gruppo di lavoro Articolo 29 – Protezione dei dati – 01613/06/IT WP 127, *Parere 9/2006 sull'attuazione della direttiva 2004/82/CE*.

[29] Gruppo di lavoro Articolo 29 – Protezione dei dati, doc. n. 01613/06/IT – WP 127, *Parere n. 9/2006 sull'attuazione della direttiva 2004/82/CE del Consiglio concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate*, adottato il 28 settembre 2006, che si legge in inglese in rete nel sito ufficiale dell'UE.

Di conseguenza nel settore del terzo pilastro la Convenzione n. 108 del Consiglio d'Europa rappresenta tuttora la base giuridica alla quale le attività di cooperazione di polizia ed in materia penale devono uniformarsi in materia di protezione dei dati personali. La Convenzione contiene un elenco vincolante di princìpi in materia di tutela dei dati personali come quelli del trattamento leale e basato sulla legge; quello della finalità limitata del trattamento; quello dell'adeguatezza. L'articolo 6 vieta il trattamento di dati sensibili, a meno che tali dati così come quelli relativi alla materia penale non siano trattati secondo appropriate garanzie stabilite dalle legislazioni nazionali.

Per quel che riguarda il flusso transfrontaliero di dati la Convenzione lo favorisce senz'altro tra le parti contraenti. L'articolo 2 del Protocollo addizionale del 2001 introduce in proposito il concetto di «adeguato livello di protezione» quale condizione per il flusso transfrontaliero di dati verso paesi terzi non parti della Convenzione n. 108.

Nonostante queste innovazioni introdotte dal Protocollo addizionale, la Convenzione è stata adottata prima dell'imponente sviluppo delle tecnologie dell'informazione. Alcuni studiosi affermano che sia arrivato ormai il momento di adottare un nuovo quadro normativo nell'ambito dell'Unione Europea[30].

In effetti qualcosa nell'Unione si sta muovendo. La Convenzione Europol contiene delle norme che vanno a completare la Convenzione n. 108 del Consiglio d'Europa, mentre a livello di atti dell'Unione va ricordata l'adozione di un progetto di proposta della Commissione relativa ad una *Decisione del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione di polizia e giudiziaria in materia penal*e, resa pubblica nell'ultima versione del 24 giugno 2008, che potrebbe costituire in futuro uno dei principali strumenti in materia di protezione dei dati personali rispetto alle attività del terzo pilastro.

[30] «if not integrated or substituted at EU-wide level by a new frame, it risks becoming outdated and overwhelmed by the growing application of technological instruments», affermazione tratta dallo studio del PE (*Study concerning Data Protection from a Transatlantic Perspective…*, già citato), che riferisce il pensiero di De Hert, Papakostantinou, Van Riehle, *Data Protection in the Third Pillar: Cautios Pessimism*, in Mike (ed.) *Crime, Rights and the EU: the Future of Police and Judicial Cooperation*, Justice, London, 2008.

6. La tutela dei dati personali nel diritto degli USA

L'approccio del diritto statunitense alla protezione dei dati personali sembra andare nella direzione di un maggior favore per la sicurezza rispetto alla tutela della *privacy*.

La Costituzione americana tutela la vita privata in modo articolato e, secondo alcuni, insoddisfacente[31]. Il *Privacy Act* del 1974 disciplina la tutela dei dati personali ma riguarda esclusivamente quelli trattati dalle autorità federali statunitensi, ad esclusione quindi dei trattamenti effettuati da privati per fini commerciali. A seguito dei fatti dell'11 settembre 2001 gli USA hanno adottato alcune leggi, tra le quali il *Patriot Act*[32], l'*Aviation Transportation Security Act* (ATSA) del 19 novembre 2001 e l'*Enhanced Border Security and Visa Reform Act* (EBSV) del 5 maggio 2002, che aggiorna l'*Immigration and Nationality Act*, che hanno sensibilmente indebolito la tutela della *privacy*.

L'*Homeland Security Act* del 2002, che istituisce il Department of Homeland Security (DHS), è un'altra legge che incide negativamente sul diritto alla *privacy* ed alla protezione dei dati personali.

Il Dipartimento è incaricato dei controlli alle frontiere USA e, in base all'ATSA sopra ricordato, le autorità statunitensi hanno imposto ai vettori aerei che volano per/da gli USA, di permettere al DHS l'accesso diretto ai loro terminali per estrarne i dati personali dei passeggeri (PNR) (metodo «*pull*»), con la minaccia di sanzionare severamente chi non avesse acconsentito a tale accesso.

In sintesi è possibile condividere l'opinione di chi ritiene che la legislazione federale statunitense: «fails to provide a comprehensive regime for data privacy, and the state coverage is similarly patchy. Even when federal legislation exists, it is often so laden with exemptions as to virtually negate its purposes»[33].

Infine occorre sottolineare che in base al *Privacy Act* l'azione di ri-

[31] A. Terrasi, *Trasmissione dei dati personali e tutela della riservatezza: l'accordo tra Unione Europea e Stati Uniti del 2007*, in *Rivista di diritto internazionale*, 2007, p. 375 ss., specie 379.

[32] USA PATRIOT ACT è l'acronimo inglese per *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (Publ. L. n. 107-56, 2001). È stato adottato per rafforzare la lotta al terrorismo dopo l'11 settembre. Sull'impatto di questa legge sulla tutela dei dati personali si veda Osher, *Privacy, Computers and the Patriot Act: the Fourth Amendment Isn't Dead but No One Will Ensure It*, in *Florida Law Review*, 2002, p. 521 ss.

[33] Charlesworth, *Clash of Data Titans? US and EU Data Privacy Regulation*, in *European Public Law*, 2000, p. 259, citato in nota (12) a p. 379 dell'articolo di Terrasi.

sarcimento è riservata ai cittadini americani ed ai residenti permanenti, escludendo così ogni possibilità di tutela giurisdizionale negli USA per i cittadini ed i residenti dell'Unione Europea, per eventuali violazioni dei loro diritti alla tutela dei dati personali e della *privacy*.

Inoltre negli Stati Uniti non esiste una vera e propria Autorità indipendente incaricata del controllo del rispetto delle leggi sulla *privacy*, sebbene: «legislation is moving forward in Congress that would establish independence for the Privacy and Civil Liberties Oversight Board that currently reports to the President as well as establish new reporting requirements for data mining activities within the federal government»[34].

Vero è che la legge sulla sicurezza nazionale (Homeland Security Act) ha istituito l'Ufficio per la Privacy (the Privacy Office) diretto da un Chief Privacy Officer (DHS CPO), che può considerarsi l'agenzia più attiva nel settore dei controlli sulla *privacy* e sul trasferimento illecito di dati personali negli USA[35]. Tuttavia anche il controllo esercitato da quest'Ufficio è riservato ai cittadini americani ed ai residenti permanenti ed il suo direttore viene nominato politicamente, e come tale non può considerarsi strutturalmente indipendente se paragonato alle autorità europee di protezione dei dati personali.

7. Il contenzioso tra UE e USA sul trasferimento dei dati PNR e l'inadeguatezza del livello di protezione garantito dalle autorità statunitensi

Dopo l'11 settembre 2001 gli Stati Uniti, come si è detto, hanno intensificato le misure di sicurezza del trasporto aereo rispetto a tutti i voli provenienti da altri Stati, compresi i paesi dell'UE, con l'adozione di leggi finalizzate a garantire la loro sicurezza interna nel

[34] M. Rotemberg, *Recent Privacy Developments in the US, Particularly with Respect to Travelers Using Air Transportation*, Contribution to the European Parliament Public Seminar «*PNR/SWIFT/Safa Harbour: Are Transatlantic Data Protected?*», 26 March 2007. Rintracciabile in: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/rotemberg_/rotemberg_en.pdf.

[35] M. Rotemberg, *The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9/11,* in *Social Science Research Network,* September 2006, pp. 1-60, p. 59, cit. in *Study Concerning Data Protection from a Transatlantic Perspective*… del Parlamento europeo, cit.

settore dei trasporti, quali *l'Aviation Transportation Security Act* (ATSA) del 19 novembre 2001[36], e *l'Enhanced Border Security and Visa Reform Act* (EBSV) del 5 maggio 2002, che aggiorna *l'Immigration and Nationality Act*.

Dopo avere inizialmente richiesto alle compagnie aeree la trasmissione dei dati API, l'amministrazione USA e specificamente il Servizio Dogane hanno preteso, pena gravi sanzioni, l'accesso diretto ai sistemi di prenotazione elettronica, secondo il metodo *pull*, ai dati PNR che possono contenere molte più informazioni dei dati API.

La scheda nominativa passeggeri (PNR) può infatti contenere anche la cronistoria del PNR, ovvero i viaggi effettuati in passato, e dati di tipi religioso o etnico come la scelta del pasto, l'affiliazione ad un gruppo particolare, dati relativi alla residenza e ai mezzi per contattare un individuo, come l'indirizzo e-mail, le coordinate di un amico, il luogo di lavoro, i dati medici, come la richiesta di assistenza in volo, ossigeno, problemi di vista, udito o mobilità o qualsiasi altro problema che è bene conoscere per il buono svolgimento del volo. Molti di questi dati hanno natura sensibile e la loro trasmissione è vietata a norma dell'articolo 8 della direttiva CE 95/46 sulla tutela delle persone fisiche rispetto al trattamento dei dati personali e la loro libera circolazione[37].

[36] Sulla base dell'ATSA gli USA hanno adottato norme provvisorie del Dipartimento del Tesoro (dogane) in materia di dati relativi a passeggeri ed equipaggi richiesti per i voli passeggeri nel trasporto aereo dall'estero verso gli Stato Uniti (registro federale, 31 dicembre 2001) e trasmissione del registro dei nomi del passeggeri richiesta per i passeggeri di voli internazionali da o verso gli Stati Uniti (registro federale, 25 giugno 2002).

[37] L'articolo 8 riguarda il trattamento dei dati sensibili, ossia quei dati che permettono di rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché i dati relativi alla salute ed alla vita sessuale.

In base al primo paragrafo della disposizione gli Stati membri vietano il trattamento di queste categorie di dati sensibili, con alcune eccezioni previste nel successivo paragrafo, dove il divieto cede di fronte al consenso dell'interessato al trattamento dei suoi dati sensibili, o quando tale trattamento sia necessario per l'assolvimento di diritti ed obblighi del responsabile in materia di diritto del lavoro; o ancora quando serva per costituire, esercitare o difendere un diritto in via giudiziaria o sia necessario per finalità connesse con la salute della persona.

Il paragrafo 5 dell'articolo 8 stabilisce poi il principio per il quale solo una pubblica autorità può effettuare o autorizzare i trattamenti dei dati personali relativi a infrazioni, condanne penali o misure di sicurezza.

8. La posizione critica del PE sui trasferimenti dei dati PNR dall'UE agli USA

Di fronte a tali pretese forte è stata la reazione del Parlamento europeo che in più di un documento ha stigmatizzato l'inerzia della Commissione nel far fronte al conflitto tra le richieste statunitensi e la legislazione dell'UE in materia di protezione dei dati personali.

Nella sua risoluzione del 13 marzo 2003[38], il PE esprime dubbi sulla conformità della pretesa statunitense di accedere ai dati PNR che possono contenere dati sensibili ai sensi dell'articolo 8 della direttiva 95/46/CE, con quest'ultima e con il diritto comunitario in materia di protezione dei dati personali. Per questo deplora la Commissione per non aver verificato per tempo se l'accesso ai dati dei sistemi di prenotazione abbia un fondamento legale nell'ordinamento statunitense, né aver verificato se la legislazione USA presenti un livello adeguato di protezione dei dati dei passeggeri ai sensi dell'articolo 25 della Direttiva 95/46; né ha informato i cittadini dell'uso che le compagnie aeree fanno delle loro informazioni[39].

Nell'ottobre 2003 il PE torna a pronunciarsi sull'argomento, questa volta con una risoluzione[40] in cui, sulla premessa dell'inadeguatezza della normativa USA sulla protezione dei dati, minaccia di utilizzare il ricorso in carenza (articolo 232/TCE) se la Commissione non provvederà immediatamente:

– a determinare quali dati possano essere legittimamente trasferiti a terzi dalle compagnie aeree e/o dai sistemi computerizzati d'informazione e a quali condizioni;
– a vietare alle compagnie aeree ed ai sistemi computerizzati d'informazione ogni accesso e/o trasferimento dei dati non conforme alla predetta decisione;

[38] *Risoluzione del PE del 13 marzo 2003 sulla trasmissione dei dati personali da parte delle compagnie aeree in occasione di voli transatlantici*: P5_TA-PROV (2003)0097 B5-0187/2003, in rete al seguente indirizzo: http://www.privacy.it/ceris20030313.html (ultimo accesso del 15/05/2008).

[39] Paragrafi 1 e 2 della risoluzione cit.

[40] *Risoluzione del PE sul trasferimento di dati personali da parte delle compagnie aeree in occasione di voli transatlantici: stato dei negoziati con gli Stati Uniti – Processo verbale del 9 ottobre 2003*, in rete al seguente indirizzo: http://www.privacy.it/ceris20031009.html (ultimo accesso del 15/05/2008).

– ad avviare immediatamente negoziati per un accordo internazionale conforme al diritto comunitario;
– a verificare la compatibilità con la direttiva 95/46 di progetti quale quello statunitense di introdurre nei passaporti piastrine elettroniche che contengono dati biometrici;
– a prendere le iniziative necessarie per agevolare l'applicazione di sistemi filtro computerizzati per controllare l'accesso ai dati dei passeggeri, quale il «Secured Short-Term PNR-Store», un progetto delle Austrian Airlines e delle Autorità austriache per la protezione dei dati.

Un terzo intervento, anch'esso fortemente critico, del PE, ha luogo in occasione dell'adozione da parte della Commissione della proposta di decisione sull'adeguatezza del sistema americano di protezione dei dati ai fini della trasmissione di quelli PNR alle autorità USA, basata sull'articolo 25 della direttiva 95/46 e sollecitata proprio dal PE.

Nella risoluzione del 31 marzo 2004[41] il PE esclude che il progetto di decisione della Commissione sia accettabile sotto più di un profilo.

In primo luogo si sottolinea che nell'ordinamento dell'UE non esiste una base giuridica per il trasferimento dei dati PNR, che sono dati commerciali, al diverso fine della sicurezza pubblica e quindi per autorizzarlo; che negli USA la protezione della vita privata non è considerata un diritto fondamentale, come accade invece nell'UE in base all'articolo 8 della CEDU; infine, che nell'ordinamento USA la protezione della vita privata è oggetto di leggi diverse dal trasporto aereo e che tutelano solo i cittadini americani e i residenti legali, mentre non c'è tutela per i passeggeri non americani né forme di garanzie giurisdizionali in caso di abusi nel trattamento dei loro dati personali.

In secondo luogo si sottolinea che il progetto di decisione della Commissione dovrebbe costituire una misura di esecuzione della direttiva 95/46, basandosi sul suo articolo 25, e che pertanto non po-

[41] *Risoluzione del PE sul progetto di decisione della Commissione che prende atto del livello di protezione adeguato dei dati a carattere personale contenuti nelle pratiche passeggeri (PNR-Passenger Name Records) trasferite all'Ufficio delle dogane e della protezione di frontiera degli Stati Uniti* (2004/2011(INI)), in *GUUE*, C 103 E/665 ss. del 29.04.2004.

trebbe avere l'effetto di ridurre i criteri di protezione dei dati garantiti da quest'ultima.

Tale effetto invece si realizzerebbe con l'adozione della decisione, secondo il PE, in quanto la Commissione nel redigere il progetto non ha tenuto conto dei suggerimenti del PE e del Gruppo di lavoro Articolo 29, relativi ai seguenti punti:

– definire i dati (massimo 19 categorie) che potrebbero essere trasferiti lecitamente senza rischi;
– sostituire il sistema *pull* col sistema *push* in considerazione del maggior rischio di trasferimento di dati sensibili non filtrati che comporta il primo;
– negoziare un accordo con gli USA in cui si garantiscano ai passeggeri europei gli stessi diritti di quelli statunitensi.

Il PE conclude pertanto nel senso che la decisione della Commissione esuli dalle sue competenze di esecuzione in quanto:

– non è una base giuridica idonea a modificare le finalità per cui si sono raccolti i dati PNR e permetterne il trasferimento a terzi da parte delle compagnie aeree;
– non costituisce un accordo internazionale in applicazione del quale la Commissione sarebbe tenuta ad autorizzare il trasferimento dei dati PNR;
– non è condivisibile nel contenuto perché misura il livello di adeguatezza della protezione dei dati garantito dall'amministrazione statunitense su semplici «impegni» di quest'ultima che non hanno base giuridica certa negli USA;
– neppure è condivisibile nel contenuto perché ammette il sistema di trasmissione dei dati PNR del tipo *pull* che non consente di filtrare e bloccare il trasferimento di dati sensibili;
– una decisione non costituisce lo strumento adatto per la soluzione di un problema del genere, che invece dovrebbe trovare rimedio nella stipulazione da parte dell'UE di un vero e proprio accordo internazionale con gli USA che definisca chiaramente le condizioni e le modalità del trasferimento dei dati PNR assoggettandoli ai principi di protezione stabiliti dall'ordinamento dell'UE.

In particolare il PE suggerisce di inserire nell'accordo i seguenti punti:

a) i dati che possono essere trasferiti in modo automatizzato e quelli che possono trasferirsi caso per caso;
b) l'elenco dei reati gravi per cui è possibile avanzare una richiesta supplementare;
c) l'elenco delle agenzie e delle autorità che potrebbero condividere i dati e le condizioni di tutela dei dati da rispettare;
d) il periodo di conservazione per i due tipi di dati;
e) il ruolo delle compagnie aeree nell'attività di trasferimento dati (API e PNR) a fini di sicurezza pubblica;
f) le garanzie per i passeggeri;
g) le responsabilità delle compagnie aeree nei confronti dei passeggeri;
h) il diritto di ricorso ad un'autorità indipendente ed i rimedi in caso di violazione dei diritti dei passeggeri.

Il parere del 31 marzo non si riferisce né alla procedura classica di adozione degli atti comunitari, né tantomeno a quella di stipulazione di accordi internazionali da parte della CE ai sensi dell'articolo 300.

Esso si fonda su di una disposizione della decisione del Consiglio 28 giugno 1999 n. 1999/468/CE che riguarda le modalità per l'esercizio delle competenze esecutive della Commissione, e revoca in dubbio la competenza della Commissione ad adottare una decisione come quella oggetto della proposta.

Invece, *il PE non risulta essersi mai espresso né sulla proposta di decisione della Commissione sul livello di adeguatezza del sistema USA di protezione dati dei passeggeri, né sul progetto di decisione che adotta l'accordo CE/USA sul trasferimento dei dati PNR*[42].

Nonostante la mancanza di parere del PE, che si rifiuta di nuovo nel

[42] Il 17 marzo la Commissione comunica al PE una proposta di decisione del Consiglio relativa alla conclusione di un accordo con gli USA. A sua volta il Consiglio il 25 marzo successivo sollecita il parere del PE entro il 22 aprile invocando la procedura d'urgenza e il 31 marzo il PE si è, come abbiamo visto, espresso negativamente. Il PE il successivo 21 aprile 2004 decide di rinviare alla commissione giuridica e del mercato interno il rapporto sulla proposta di decisione del Consiglio relativa alla conclusione di un accordo con gli USA e, così facendo, respinge la domanda di esame urgente del Consiglio.

Il 21 aprile 2004 il PE ha inoltre approvato una raccomandazione della commissione giuridica e del mercato interno, volta ad ottenere il parere preventivo della Corte di Giustizia ai sensi dell'articolo 300 § 6 TCE sull'accordo previsto CE/USA.

maggio 2004 di adottarne uno su nuova richiesta urgente del Consiglio, la Commissione e il Consiglio procedono con l'adozione, rispettivamente, della decisione della Commissione 2004/535/CE del 14 maggio 2004[43] e della decisione del Consiglio 2004/496/CE del 17 maggio 2004 relativa alla conclusione dell'accordo PNR con gli USA[44].

9. La decisione 2004/535/CE del 14 maggio 2004 e l'accordo CE/USA sul PNR

La decisione della Commissione, che ha come base giuridica l'articolo 25 § 6 della direttiva 95/46/CE, al suo articolo 1, considera adeguato il livello di protezione garantito dall'Ufficio statunitense delle dogane e della protezione delle frontiere (CBP) dei dati delle schede nominative dei passeggeri (PNR) trasmessi dalla Comunità per i voli con destinazione o partenza dagli Stati Uniti.

Alla decisione è allegata la *Dichiarazione d'impegno dell'ufficio delle dogane e della protezione delle frontiere del Ministero della Sicurezza interna degli Stati Uniti (CBP)*, in cui quest'ultima autorità si assume una serie di impegni, dal dubbio valore giuridico vincolante.

Essendo allegata ad un atto comunitario, e perciò interno a quest'ordinamento, tale Dichiarazione di impegni dell'ufficio CBP statunitense non può considerarsi un accordo internazionale vero e proprio.

Questo perché, da un lato, la Commissione non ha competenza a stipulare accordi, potendosi semmai considerare la Dichiarazione del CBP come un'intesa tra autorità amministrative; dall'altro, perché contenuto in un atto sempre revocabile a discrezione dell'istituzione che lo ha emanato.

Nel merito, la Dichiarazione contiene «impegni» che si pongono

[43] *Decisione della Commissione, del 14 maggio 2004 n. 2004/535/CE, relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti United States' Bureau of Customs and Border Protection*, in *GUUE*, n. L 235 del 6 luglio 2004, pp. 11-22.

[44] *Decisione del Consiglio del 17 maggio 2004 n. 2004/496/CE, relativa alla conclusione di un accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche Passenger Name Record (PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del Dipartimento per la Sicurezza interna degli Stati Uniti*, in *GUUE*, n. L 183 del 20 maggio 2004, p. 83.

senz'altro, a nostro avviso, in contrasto con il diritto comunitario in materia di protezione dei dati personali, specie con la direttiva 95/46, ed anche con le Linee guida ICAO in materia di trasferimento dei dati PNR.

In particolare l'ufficio CBP USA, s'impegna al trattamento dei dati PNR ottenuti dalle compagnie aeree (*34 categorie contro le 19 considerate lecite dal PE*) secondo il principio della limitazione della finalità del trattamento (lotta al terrorismo e crimini connessi, altri reati gravi della criminalità organizzata a carattere transnazionale; la fuga dall'arresto o da pena detentiva); a non divulgare i dati sensibili ai sensi dell'articolo 8 della direttiva 95/46; a garantire la sicurezza del sistema informatico del CBP attraverso rigide norme di limitazione all'accesso diretto dei dati PNR al solo personale autorizzato.

La Dichiarazione prevede però che *l'ufficio CBP possa inoltrare in blocco i dati PNR all'Amministrazione per la sicurezza dei trasporti (TSA)*, previa selezione e cancellazione ad opera del BP dei dati sensibili.

Inoltre è previsto dalla dichiarazione *il potere per il CBP di inoltrare i dati PNR ad altre Amministrazioni pubbliche*, anche se con modalità diverse rispetto a quelle usate per l'inoltro alla TSA, *nonché ad autorità di paesi terzi* che svolgano compiti di lotta al terrorismo.

Per quanto riguarda il metodo di trasmissione dei dati la Dichiarazione fa chiaramente riferimento al *metodo «pull», che il PE considera invece inappropriato perché non garantisce il filtraggio dei dati sensibili*. Con riferimento a questi ultimi, poi, la Dichiarazione si limita ad impegnare l'ufficio CBP, «fintantoché un sistema automatizzato di selezione non sarà operativo, a non usare i dati sensibili, ossia i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche o religiose o filosofiche, l'appartenenza ai sindacati o dati riguardanti la salute e la vita sessuale delle persone.

Infine, con riguardo alla *conservazione dei dati*, la Dichiarazione prevede che l'accesso in linea ai dati PNR sarà consentito al personale autorizzato dal CBP per sette giorni e poi ulteriormente limitato ad alcuni soltanto dei funzionari autorizzati, per un periodo di tre anni e sei mesi a decorrere dalla data dell'accesso o del ricevimento delle informazioni dal vettore.

Al termine di quest'ultimo periodo i dati PNR per i quali non si sia avuto un accesso manuale saranno distrutti; *i dati ai quali si è effettuato un accesso manuale, invece, vengono immagazzinati in un file di dati cancellati, in cui rimarranno per otto anni prima di essere distrutti*.

Sulla base di questa decisione, che considera adeguato il livello di protezione dei dati PNR garantito dal CBP statunitense, la Comunità europea ha concluso il primo accordo PNR con gli USA, già citato sopra (decisione del Consiglio 2004/496/CE).

10. L'annullamento dei due atti da parte della Corte di Giustizia

Entrambi questi atti sono stati oggetto d'impugnazione per farne dichiarare l'annullamento in due cause portate davanti alla Corte di Giustizia dal PE, sostenuto dal Garante europeo per la protezione dei dati (GEDP) nei confronti del Consiglio, sostenuto dalla Commissione e dal Regno Unito da un lato (causa C-317/04); e dal PE contro la Commissione sostenuta dal Regno Unito dall'altro (causa C-318/04).

La Corte, dopo aver riunito le due cause, si è pronunciata il 30 maggio 2006 con una sentenza[45] con la quale ha accolto il ricorso del PE, annullando i due atti ma prorogando per un periodo gli effetti della decisione della Commissione.

La Corte esclude che la materia oggetto dei due atti rientri nella sfera di applicazione del diritto comunitario.

Più precisamente la Corte si fonda, per la sua decisione, sull'articolo 3 § 2 della direttiva 95/46, che esclude espressamente di volersi applicare ai trattamenti dei dati personali effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario come quelle previste dai titoli V (PESC) e VI (CGPG) del TUE, e comunque ai trattamenti aventi per oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato e le attività dello Stato in materia di diritto penale.

La Corte giustifica l'annullamento dei due atti argomentando con il fatto che il trasferimento dei dati PNR agli USA esuli dalla sfera di applicazione del primo pilastro, sebbene inizialmente essi siano stati raccolti e trattati dai vettori e dalle agenzie di viaggio come dati commerciali e quindi potessero considerarsi come rientranti nella competenza della CE.

[45] *Sentenza della Corte di Giustizia delle CE del 30 maggio 2006 nelle cause riunite C-317/04 e C-318/04 (PE c. Consiglio* e *PE contro Commissione)*, in rete nel sito ufficiale della Corte.

L'esclusione dal diritto comunitario e quindi l'infondatezza e la nullità delle basi giuridiche fondate sul TCE e su atti comunitari deriverebbe per la Corte dal fatto che i dati PNR sarebbero trasferiti al CBP USA per finalità di lotta al terrorismo ed alla criminalità che esulano dal campo di applicazione dell'articolo 3 § 2 della direttiva 95/46/CE.

Del pari, secondo la Corte, si deve escludere che l'articolo 95, che mira al ravvicinamento delle legislazioni per la realizzazione del mercato interno, coordinato con l'articolo 25 della direttiva 95/46, che si occupa del flusso transfrontaliero dei dati personali, possano costituire la base giuridica idonea a fondare la competenza della CE a concludere l'accordo con gli USA.

La Corte annulla le due decisioni, prorogando però l'efficacia della decisione della Commissione fino al 30 settembre 2006 per scongiurare un vuoto giuridico e per evitare l'inadempimento dell'accordo, che può essere denunciato in ogni momento da ogni contraente e che cessa di avere vigore 90 giorni dopo la notifica della denuncia. La Corte precisa infatti che la necessità di mantenere in vigore la decisione sull'adeguatezza trova ragione nel fatto che in base all'accordo PNR CE/USA il diritto di accesso dell'ufficio USA CBP ai dati PNR e l'obbligo imposto ai vettori aerei di trattarli come richiesto dall'amministrazione americana esistono solo finché la decisione sull'adeguatezza è applicabile.

11. Portata e valutazione critica della sentenza del 30 maggio 2006

Questa sentenza della Corte ha per risultato quello di escludere ogni futuro controllo giurisdizionale da parte sua in relazione ad accordi sul trasferimento dei dati PNR, che, dopo l'annullamento del primo, dovranno necessariamente essere conclusi dall'UE nel quadro della PESC e del terzo pilastro, come infatti è accaduto per gli accordi con gli USA del 2006 e del 2007.

Questa esclusione non aiuta la causa della protezione dei dati PNR trasferiti dal territorio degli Stati membri, dove il relativo diritto è considerato fondamentale e tutelato al massimo livello, al territorio di paesi, come gli Stati Uniti, dove tale diritto riceve una tutela minore rispetto alle esigenze di sicurezza nazionale.

In tal modo viene meno la possibilità che i futuri accordi siano

impugnati davanti alla Corte per farne valere l'annullamento perché in contrasto con il diritto fondamentale alla protezione dei dati.

In effetti gli accordi successivamente adottati dall'UE (e non più dalla CE) con gli USA hanno come base giuridica gli articoli 24 e 38 del TUE, relativi alla competenza dell'Unione a stipulare accordi internazionali in materia di PESC (art. 24) e CPGP (art. 38). Tali accordi si pongono tutti in contrasto con alcuni principi fondamentali in materia di protezione dei dati personali.

In particolare l'ultimo accordo concluso nel luglio del 2007 consente alle autorità statunitensi di confine:

- di accedere direttamente ai dati PNR dei vettori con il metodo *pull* che non garantisce il filtraggio dei dati sensibili, la cui diffusione e trattamento sono vietati dall'articolo 8 della direttiva 95/46 e dalle Linee guida ICAO sui dati PNR del 2006, a meno che l'interessato non vi consenta espressamente ed inequivocabilmente o non sia necessario per legge o esigenze mediche. Vero è che l'accordo prevede il passaggio al metodo *push*, più conforme alla protezione dei dati, specie di quelli sensibili, ma esclude in ogni caso che siano i vettori a decidere quali dati PNR filtrare e quindi escludere e quali inviare, attribuendo alle autorità USA tale potere;
- di garantire l'adeguatezza della protezione dei dati ricevuti solo sulla base di intese amministrative di corretto trattamento, senza che vi siano garanzie legali e giurisdizionali per i passeggeri non cittadini o residenti negli USA;
- di inoltrare ad altre autorità sia USA che di paesi terzi i dati PNR ottenuti a piena discrezione delle autorità USA e caso per caso;
- di conservare i dati PNR, tra gli archivi cosiddetti attivi e dormienti per un periodo totale di quindici anni, periodo eccessivo che per giunta viene applicato retroattivamente anche ai dati raccolti in base agli accordi PNR precedenti del 2004 e del 2006.

Il nuovo accordo del 2007 è stato oggetto di critiche da parte del PE nel suo parere del 12 luglio 2007[46], dove l'Istituzione, pur prendendo atto della sua esclusione dalla procedura di stipulazione in base al secondo e al terzo pilastro, invita con forza i parlamenti de-

[46] *Risoluzione del PE del 12 luglio 2007 sull'accordo PNR con gli Stati Uniti d'America* – P6_TA(2007)0347.

gli Stati membri ad esercitare il controllo sulla conformità dell'accordo con i diritti fondamentali in materia di protezione dei dati personali garantiti nell'UE.

Un altro inconveniente che deriva dalla decisione di escludere la materia del trasferimento dei dati PNR dal primo pilastro riguarda il fatto che, in contrasto con il principio generale dell'UE di coerenza delle azioni nei vari pilastri, resta tuttora in vigore l'accordo CE/Canada sul trasferimento dei dati PNR, concluso poco prima della sentenza della Corte del 30 maggio 2006 che ha annullato l'accordo con gli USA.

Questo accordo con il Canada si fonda, come faceva quello del 2004 con gli USA, sugli articoli 95 e 300 TCE e sulla Direttiva 95/46, articolo 25, per cui, a differenza di quelli conclusi dopo la sentenza di annullamento, ha natura giuridica comunitaria e la sua efficacia si estende, a norma dell'articolo 300 § 7, a tutti gli Stati membri ed è soggetto al controllo giurisdizionale della Corte di Giustizia.

Ora è piuttosto strana la situazione creatasi nel sistema UE/CE con la coesistenza di due accordi che, pur avendo lo stesso oggetto e lo stesso scopo, risultano stipulati secondo procedure diverse, con una sfera di efficacia soggettiva diversa, e con un diverso regime di controllo giurisdizionale.

L'accordo con il Canada peraltro risulta molto più conforme alla normativa comunitaria ed ai principi fondamentali dell'UE sulla protezione dei dati personali di quelli conclusi con gli USA[47].

È questa l'opinione della Commissione per le libertà civili, la giustizia e gli affari interni del PE espressa nella sua relazione del 4 luglio 2005 sul progetto di risoluzione del PE in sede di consultazione sulla proposta di decisione del Consiglio relativa alla conclusione di un accordo PNR con il Canada[48].

[47] Si veda la relazione citata in nota successiva, punto 5 intitolato: I miglioramenti dell'accordo CE/Canada rispetto a quello CE/USA, a p. 5 di 10 del documento html.

[48] Relazione della Commissione per le libertà civili, la giustizia e gli affari interni del PE espressa nella sua relazione del 4 luglio 2005 sul progetto di risoluzione del PE in sede di consultazione sulla *Proposta di decisione del Consiglio relativa alla conclusione di un accordo tra la CE e il governo del Canada sul trattamento delle informazioni anticipate sui passeggeri (Advanced Passenger Information, API) e dei dati delle pratiche dei passeggeri (Passenger Name Record, PNR)* – COM (2005)0200-C68209; 0184/2005 -2005/0095 (CNS) (Procedura di consultazione) – Relatrice Sophia T. Veld, in rete al seguente indirizzo: http://www.privacy.it/cecA62005-226.html.

Nel progetto di risoluzione si legge che il PE, pur non approvando l'accordo PNR con il Canada, fonda questa opinione non certo sul fatto che la sua procedura di stipulazione non si debba basare sull'articolo 300 TCE, ma, al contrario, invoca quest'ultima disposizione per pretenderne l'applicazione più puntuale, invitando il Consiglio a coinvolgerlo con la procedura di parere conforme e non, come invece ha fatto, semplicemente consultandolo.

Sebbene le Istituzioni abbiano continuato il processo di adozione sia della decisione sull'adeguatezza della legislazione canadese sulla protezione dei dati, sia dell'accordo PNR, senza tener conto del parere contrario del PE – solo consultato in quelle sedi –, a noi sembra che l'accordo con il Canada sia correttamente fondato sul diritto comunitario.

Il carattere misto della natura e della finalità del trattamento dei dati PNR (commerciali all'inizio quando sono raccolti dai vettori e dalle agenzie, e necessari a garantire la sicurezza pubblica se richiesti da autorità di frontiera di paesi terzi) avrebbe a nostro avviso permesso alla Corte di mantenere la base giuridica comunitaria – maggiormente garantista sotto il profilo generale della tutela dei dati personali e delle deroghe ammesse –, anche con riferimento all'accordo stipulato dalla CE con gli USA nel 2004.

In casi dubbi, nei quali è possibile adottare un atto utilizzando basi giuridiche comunitarie e dell'UE, dovrebbe infatti trovare applicazione l'articolo 47 del TUE, che stabilisce il principio della prevalenza della base giuridica comunitaria, rispetto alle rilevanti disposizioni del quinto o quarto pilastro.

In un caso recente, relativo all'interpretazione ed applicazione della direttiva 2006/24/CE relativa alla conservazione dei dati personali, caso analogo a quello che stiamo esaminando, è in discussione la correttezza della base giuridica comunitaria sulla quale l'atto è fondato, alla luce dell'articolo 47 del TUE.

L'avvocato generale Bot suggerisce alla Corte, nelle sue Conclusioni, di distinguere tra trasferimenti dei dati personali effettuati da operatori privati e quelli effettuati da pubbliche autorità. I primi rientrerebbero senz'altro nel diritto comunitario, che costituirebbe pertanto la corretta base giuridica, mentre i dati trasferiti da autorità pubbliche di contrasto alla criminalità ed al terrorismo andrebbero disciplinati in base al secondo e/o terzo pilastro dell'UE.

Vero è che l'avvocato generale Bot, per giustificare il diverso orientamento assunto rispetto alla decisione della Corte del 30 maggio

2006 che è l'oggetto del nostro esame critico, afferma che i vettori e gli operatori del settore aereo, quando trasferiscono i dati PNR alle autorità statunitensi, vanno considerati alla stregua di pubbliche autorità, ma questa argomentazione appare del tutto artificiosa nel suo scopo, appunto, di salvare capra (la precedente decisione della Corte) e cavoli (l'attuale diversa conclusione dell'AG).

È chiaro infatti che i vettori aerei non sono pubbliche autorità. E l'attività loro richiesta di trasferimento dei dati PNR alle autorità USA è senz'altro finalizzata a scopi commerciali, quali quello di vendere i biglietti aerei a passeggeri che intendono recarsi negli, o tornare dagli, USA.

La Corte, nel caso PNR, aveva annullato la base giuridica comunitaria, in applicazione dell'articolo 3 § 2 della direttiva 95/46 che esclude dalla propria sfera di applicazione i trattamenti di dati personali «effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del Trattato sull'UE, e comunque ai trattamenti aventi per oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato».

L'avvocato generale Bot riprendendo questa pronuncia distingue a sua volta tra attività commerciali, che rientrerebbero senz'al-tro nella sfera di applicazione della direttiva 95/46 e del diritto comunitario, e attività finalizzate alla difesa ed alla sicurezza dello Stato, che invece ricadrebbero nella sfera di competenza dell'Unione, tra il secondo e il terzo pilastro.

L'aver considerato i vettori aerei quali pubbliche autorità è senz'altro, nella nostra opinione, una forzatura, così come l'aver escluso il carattere commerciale della loro attività, il cui fine principale è e resta quello di vendere biglietti aerei.

A noi sembra che la Corte ben avrebbe potuto mantenere la base giuridica comunitaria per l'adozione dell'accordo PNR con gli USA. Con la sua decisione, invece, si apre una grave lacuna nella protezione dei cittadini e residenti UE che vogliano recarsi negli, o tornare dagli, USA.

Inoltre, in considerazione delle diverse basi giuridiche adottate per la conclusione degli accordi PNR con USA e Australia da un lato e Canada dall'altro, si prospetta senz'altro una violazione del principio generale di non discriminazione, a causa del diverso livello di protezione dei dati personali che i singoli accordi riconoscono in ragione, appunto, della diversità delle loro basi giuridiche.

In conclusione, in assenza di disposizioni chiare applicabili nel quadro del terzo pilastro (attività di contrasto del crimine e del terrorismo), sarebbe stato meglio sottoporre il trasferimento di dati personali da operatori privati (i vettori aerei) a pubbliche autorità (gli USA) al diritto comunitario, in quanto maggiormente garante sul piano della protezione dei soggetti ai quali tali dati si riferiscono.

12. Soluzione di breve termine proposta dal Gruppo Articolo 29

Dall'analisi che precede un punto risulta particolarmente chiaro: chi fa le spese di questa situazione sono da una parte i passeggeri, i cui dati personali, anche sensibili, circolano da uno Stato all'altro del mondo e da un'autorità all'altra di ogni Stato senza sicure garanzie di protezione; dall'altro i vettori, le agenzie e sistemi telematici di prenotazione, che si trovano tra l'incudine del rispetto degli obblighi comunitari di protezione dei dati personali dei passeggeri, ed il martello delle pretese statunitensi. Quest'ultimo paese pretende infatti di accedere direttamente, *pena l'erogazione di gravi sanzioni*, a una serie categorie di dati che il PE, il Garante europeo e quelli nazionali, così come il Gruppo di lavoro Articolo 29 istituito dalla direttiva 95/46 ritengono per numero e per contenuto sproporzionati rispetto alla finalità di lotta al terrorismo ed alla criminalità.

I due accordi tra l'UE e gli USA del 2006 e del 2007 non migliorano la situazione.

Occorre allora individuare una soluzione di immediato effetto tesa alla protezione dei soggetti ai quali si riferiscono i dati PNR. *L'unico modo, conforme peraltro ai principi generali in materia di protezione dei dati personali, per superare le perplessità e le incertezze, resta quello di procurarsi il consenso dei soggetti interessati dal trattamento, ossia dei passeggeri*.

È questa del resto la linea che suggerisce il *Gruppo di lavoro Articolo 29 nel suo parere 2/2007 sull'informazione dei passeggeri in merito al trasferimento di dati PNR alle autorità statunitensi* del 15 febbraio 2007, parere reso dopo la stipulazione dell'accordo PNR UE/USA del 2006 ed espressamente rivolto alle compagnie aeree, agli agenti di viaggio ed altre organizzazioni che prestino servizi di trasporto passeggeri per voli da o per gli USA, con lo scopo di chiarire quali obblighi spettino loro in materia di trasferimento di dati PNR.

Il parere suggerisce di informare i passeggeri con due tipi di note informative, una breve ed una lunga.

Questa soluzione viene accolta e ripresa dall'ultimo accordo PNR UE/USA, quello del 2007, che contiene in allegato una Dichiarazione di impegni che al punto IV prevede quello dell'amministrazione statunitense di fornire al pubblico informazioni sul trattamento dei dati personali PNR effettuato in occasione dell'arrivo e della partenza di passeggeri sul territorio statunitense, mediante la pubblicazione nel registro federale, e predisponendo anche un modello di nota informativa per le compagnie aeree, con tutte le informazioni relative alle modalità di raccolta dei dati PNR, alle possibilità per i passeggeri anche non statunitensi, soprattutto dell'UE, di accedere ai loro dati per chiederne la rettifica.

13. Sviluppi recenti nell'ordinamento dell'Unione

Il sistema UE/CE disciplina, come si è visto, il trattamento dei dati personali in modo diverso a seconda che questi ultimi siano trattati per fini commerciali oppure di contrasto al crimine organizzato ed al terrorismo. Nel primo caso si utilizzano, come base giuridica, le disposizioni del Trattato CE, nel secondo caso invece ci si rifà a quelle del secondo, ma, più frequentemente, del terzo pilastro.

Questa situazione comporta un problema di coordinamento tra le diverse basi giuridiche, come si è chiaramente visto nell'analisi critica della sentenza della Corte relativa al caso PNR.

Una volta esclusa l'applicabilità del diritto comunitario al trattamento dei dati PNR, sorge il problema di individuare il diritto applicabile al trattamento dei dati personali ed al loro trasferimento per motivi di sicurezza nel quadro del terzo pilastro.

Si è già detto, in proposito, che l'unico strumento applicabile resta la Convenzione n. 108 del Consiglio d'Europa, che però non appare sufficiente alla luce degli attuali sviluppi delle tecnologie dell'informazione, mentre non esiste ancora alcun atto interno all'Unione applicabile nella materia.

In questa prospettiva la Commissione ha pubblicato, il 24 giugno 2008, l'ultima versione del progetto di Proposta relativa ad una *Decisione quadro del Consiglio sulla protezione dei dati personali trattati nel contesto della cooperazione di polizia e giudiziaria in materia penale*. Que-

sta decisione quadro potrebbe diventare uno dei principali strumenti di protezione dei dati personali rispetto alle attività del terzo pilastro.

Per quanto riguarda il trattamento dei dati dei passeggeri di voli aerei, la Commissione ha presentato una seconda Proposta per una Decisione quadro del Consiglio *sull'uso dei dati PNR in attività di contrasto*[49].

La proposta da ultimo ricordata è stata oggetto di critiche da parte di autorità indipendenti, istituzioni ed altri enti a livello europeo[50].

Prima di illustrarle sembra opportuno dare conto in estrema sintesi del contenuto della proposta. Essa intende armonizzare le disposizioni degli Stati membri relative agli obblighi dei vettori che effettuano voli aerei da/verso il territorio di almeno uno Stato membro, di trasferire i dati PNR alle autorità competenti per la lotta al terrorismo ed alla criminalità organizzata di un altro Stato membro, per il tramite di una Unità d'Informazione passeggeri. Quest'ultima entità dovrebbe avere il compito di ricevere i dati personali dai vettori e di trasmetterli, dopo averli controllati ed eventualmente filtrati, appunto alle autorità di contrasto di altri Stati membri. Tuttavia la proposta resta molto vaga sulla struttura, i compiti e le responsabilità di questo organismo, non precisando, in particolare, entro quali limiti normativi potrà agire.

In linea generale, il contenuto della proposta segue molto da vicino quello dell'accordo PNR concluso con gli USA nel 2007, che ha già costituito oggetto di critiche, come si è visto, da parte del Parla-

[49] 2008/C110/01.

[50] Si ricordano i seguenti documenti adottati in lingua inglese rispettivamente dal Gruppo di lavoro Articolo 29, dal Gruppo di lavoro su Polizia e giustizia, dal Garante europeo per la protezione dei dati personali, dalla neonata Agenzia europea per i diritti fondamentali: *Joint Opinion on the Proposal for a Council Framework Decision on the Use of PNR for Law Enforcement Purposes*, presented by the Commission on 6 November 2007, adopted on 5 December 2007 by the Article 29 Working Party and on 18 December 2007 by the Working Party on Police and Justice; the *Opinion of the European data protection supervisor on the draft Proposal for a Council Framework Decision on the use of PNR data for law enforcement purposes* published on 1 May 2008; the *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of PNR for law enforcement purposes* of 3 December 2008.

Una risoluzione critica è stata adottata infine dal PE il 20 novembre 2008: *The European Parliament Resolution of 20 November 2008 on the Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes*.

mento europeo e del Garante europeo per la *privacy* perché non in linea con gli standard europei di protezione dei dati personali. La proposta peraltro, rispetto alla questione della tutela dei dati PNR, contiene un rinvio all'altra proposta della Commissione relativa alla *Decisione quadro sulla protezione dei dati personali nel terzo pilastro*, proposta, quest'ultima, tuttora in fase di elaborazione e che pertanto non può costituire un utile fondamento per la protezione dei dati PNR almeno fino a quando non sarà approvata ed entrerà in vigore.

Ma le critiche maggiori alla proposta di un PNR europeo s'indirizzano alla sua incapacità di adempiere le tre condizioni cumulativamente richieste dall'articolo 8 della CEDU e dall'articolo 7 della Carta di Nizza, affinché sia legittima una restrizione al diritto fondamentale alla vita privata: la legittimità dello scopo della misura proposta; la sua conformità alla legge e la sua prevedibilità ed accessibilità da parte degli individui interessati dalla misura; infine, la proporzionalità di quest'ultima.

Il Garante europeo, l'Agenzia europea per i diritti fondamentali così come altri organismi indipendenti di controllo, oltre al Parlamento europeo, considerano tutti la proposta per un PNR europeo nelle attività di contrasto come legittima nel suo scopo di prevenire e lottare contro il terrorismo ed il crimine organizzato, ma non pienamente compatibile con i requisiti della legalità e della proporzionalità.

Sotto quest'ultimo profilo, in particolare, sorge il problema di come il trattamento dei dati PNR possa costituire un utile strumento nella lotta al terrorismo ed alla criminalità, poiché questo punto non risulta dimostrato. Al contrario, la reale utilità del ricorso al sistema PNR può essere confutata sotto un duplice punto di vista.

In primo luogo non esistono prove di concreti risultati derivati dall'uso di dati PNR nella lotta al terrorismo: è quanto emerge in particolare dalle opinioni espresse dalla House of Lords e dal Parlamento europeo.

In secondo luogo è dubbio che il ricorso ai dati PNR sia effettivamente utile, dal momento che sia nell'Unione che all'esterno esiste già un numero consistente di sistemi di banche dati finalizzate proprio allo scopo di combattere il terrorismo e la criminalità organizzata, quali i sistemi API, VIS, SIS, SIS II nell'UE ed i sistemi PNR messi in atto da paesi terzi come Canada, USA e Australia.

L'Agenzia europea per i diritti fondamentali esprime in particolare i suoi dubbi nel suo parere del dicembre 2008, reso sulla conformità

della Proposta di PNR europeo con i diritti fondamentali garantiti nell'Unione. In quest'ultimo si afferma che prima di procedere all'adozione di un sistema europeo di raccolta dati PNR occorrerebbe effettuare: «a detailed review of *existing measures which already provide for the processing of personal data* in order to specify why these measures do not suffice to provide the additional intelligence required»[51].

Conclusioni

In conclusione vorrei proporre alcuni spunti di riflessione.

Il primo riguarda l'opportunità di adottare atti, quali la decisione quadro sulla protezione dei dati personali nel terzo pilastro, e quella relativa all'istituzione di un sistema europeo di raccolta dati PNR, quando ancora non risulta chiaro quale sarà il destino del Trattato di Lisbona.

Il Garante europeo dei dati personali ha espresso, in più di un parere, l'opinione che sarebbe meglio attendere l'entrata in vigore del Trattato di revisione prima di procedere alla regolamentazione della materia. Infatti il Trattato di Lisbona introdurrà maggiori garanzie sotto più profili anche dal punto di vista dell'applicazione del principio fondamentale della protezione dei dati personali.

La prevista fusione tra il primo ed il terzo pilastro contribuirà, in particolare, ad evitare l'attuale frammentazione normativa con atti che oggi sono adottati su basi giuridiche differenti e che hanno sfere diverse di applicazione. In futuro gli atti adottati in base al Trattato UE come revisionato a Lisbona potranno rispondere meglio ed in modo uniforme alla necessità di armonizzare le legislazioni nazionali degli Stati membri. La base giuridica per l'adozione di ogni atto relativo alla protezione ed al trattamento dei dati personali dovrà effettuarsi sulla base di un'unica disposizione, l'articolo 16 del Trattato sul funzionamento dell'Unione.

Inoltre il nuovo contesto giuridico, eliminando le attuali differenze tra primo e terzo pilastro sugli aspetti procedurali di adozione degli atti, offrirà al Parlamento europeo piena competenza come

[51] *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the Use of PNR for Law Enforcement Purposes* of 3 December 2008, cit.

co-legislatore secondo la procedura ordinaria di co-decisione, attualmente esclusa per il terzo pilastro, e la procedura di voto passerà dall'attuale unanimità – richiesta per le decisioni di terzo pilastro, alla maggioranza qualificata.

La Corte di Giustizia avrà giurisdizione sulla legittimità degli atti così adottati, alla luce dei princìpi fondamentali sulla *privacy* e la tutela dei dati personali contenuti nella Carta di Nizza, come riproclamata nel 2007, che acquisterà finalmente valore giuridico vincolante.

Un secondo ordine di riflessioni riguarda il fatto che potrebbe mettersi in discussione la reale utilità dell'adozione di un sistema europeo di raccolta dati PNR, sotto il profilo della sua capacità di rispondere efficacemente al problema della lotta al terrorismo.

Si potrebbe infatti obiettare che sarebbe meglio adottare uno strumento internazionale multilaterale che coinvolga gli Stati terzi, in modo da provvedere ad una migliore armonizzazione delle garanzie poste a tutela dei dati personali nei sistemi di raccolta e trattamento.

Sotto questo profilo degni di nota (anche se insufficienti trattandosi di strumenti bilaterali) appaiono, oltre agli accordi già stipulati tra gli Stati Uniti ed Europol ed Eurojust, agli accordi PNR conclusi dall'UE con USA, Canada ed Australia e agli scambi di lettere tra USA e UE sul caso SWIFT, i recenti negoziati condotti dal Gruppo di contatto di alto livello UE-USA sulla condivisione delle informazioni e sulla *privacy* e la protezione dei dati personali. Il Gruppo ha adottato il rapporto il 28 maggio 2008, rendendolo pubblico il successivo 26 giugno.

L'11 novembre 2008 il Garante europeo per la protezione dei dati personali ha espresso un Parere sul Rapporto finale del gruppo di contatto di alto livello USA-UE.

Non è possibile in questa sede soffermarsi diffusamente sul parere, tuttavia sembra interessante l'indicazione del Garante che invita a non legittimare nel futuro accordo il trasferimento di dati personali da operatori privati a pubbliche autorità.

In linea generale, sempre con riguardo ai negoziati transatlantici e al previsto accordo UE-USA, il ricorso a strumenti bilaterali sembra meno utile rispetto all'adozione di un più ampio accordo multilaterale finalizzato all'armonizzazione delle legislazioni nazionali informata al rispetto di standard minimi di protezione dei dati personali.

Potrebbe ipotizzarsi per esempio la negoziazione di un accordo quadro generale e multilaterale sulla protezione dei dati personali,

che potrebbe includere, tra l'altro, specifiche disposizioni o capi sul trasferimento dei dati PNR o sul trasferimento di altri dati personali per scopi specificati di contrasto al crimine e al terrorismo o altro.

Per quel che riguarda i dati PNR, il futuro accordo quadro potrebbe essere formulato in modo tale da contenere una disposizione che inviti gli Stati contraenti ad adottare le Linee guida ICAO sull'uso del PNR, precisando che le legislazioni nazionali che si conformeranno ai detti standard ICAO saranno presunte legittime in quanto conformi con i princìpi generali di protezione dei dati personali garantiti da strumenti internazionali quali la CEDU o la Carta di Nizza. Questa formula potrebbe avere un effetto indiretto duplice: rendere vincolanti gli standard ICAO attraverso la loro adozione da parte degli ordinamenti interni ed armonizzare questi ultimi.

In conclusione, nel campo della protezione dei dati personali è necessario evitare ogni proliferazione di atti di primo e/o terzo pilastro, così come preferire al ricorso ad accordi bilaterali quello a strumenti multilaterali a carattere generale.

Abbiamo infatti avuto modo di verificare come l'adozione di accordi bilaterali sui dati PNR fondati su basi giuridiche diverse pongano problemi di coordinamento a livello internazionale, e possano determinare un abbassamento nel livello di protezione previsto dall'ordinamento di uno dei due Stati contraenti. È questo, secondo noi, il caso dell'accordo PNR tra Stati Uniti e UE, dove gli standard di protezione dei dati personali risultano molto inferiori a quelli garantiti dall'ordinamento comunitario e dell'Unione.

La minore tutela dell'accordo bilaterale rispetto all'ordinamento interno di uno dei due contraenti investe anche gli aspetti procedurali, eliminando ad esempio, come è accaduto nel caso PNR con gli USA, la possibilità per i cittadini ed i residenti dell'UE di far valere i loro diritti al rispetto dei dati personali ed al loro corretto trattamento davanti al giudice statunitense in caso di loro violazione.

Il ricorso allo strumento multilaterale per conseguire un effetto indiretto di armonizzazione attraverso l'invito agli Stati contraenti ad adottare nei loro ordinamenti interni gli standard internazionali elaborati da organizzazioni quali l'OCDE, l'ONU e l'ICAO sembra senz'altro l'opzione migliore.