IL DIRITTO DELL'INFORMAZIONE E DELL'INFORMATICA
Anno XXVI Fasc. 2 - 2010

Marco Botta - Mario Viola de Azevedo Cunha

LA PROTEZIONE DEI DATI PERSONALI NELLE RELAZIONI TRA UE E USA, LE NEGOZIAZIONI SUL TRASFERIMENTO DEI PNR

Estratto

MVLTA PAVCIS AG

Milano • Giuffrè Editore

MARCO BOTTA-MARIO VIOLA DE AZEVEDO CUNHA

LA PROTEZIONE DEI DATI PERSONALI NELLE RELAZIONI TRA UE E USA, LE NEGOZIAZIONE SUL TRASFERIMENTO DEI PNR

1. Introduzione, trasferimento transfrontaliero dei dati personali e pubblica sicurezza.

Sin dalle origini del dibattito sulla protezione dei dati personali nel corso degli anni '70 si è iniziato a discutere sul tema della « libera circolazione » dei dati personali. Lo sviluppo dell'informatica non ha portato soltanto alla nascita delle banche dati elettroniche, ma ha anche aumentato le possibilità di comunicazione di queste informazioni a livello transfrontaliero. I Paesi che garantiscono elevati standard di protezione dei dati personali si rifiutano di permettere il trasferimento d'informazioni riguardanti i propri cittadini verso Stati che, invece, non hanno nessuna forma di tutela in materia. Secondo il preambolo delle *Guidelines* dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) sulla protezione dei dati personali, « … c'è il pericolo che le differenze nelle legislazioni nazionali possano ostacolare il libero flusso di dati personali lungo le frontiere… Restrizioni a questi flussi potrebbero causare serie distorsioni in settori importanti dell'economia, come quello bancario e delle assicurazioni… »[2]. Sin dalla fine degli anni '70 il rischio che le regole nazionali

[1] Gli autori sono dottorandi nel Dipartimento di Giurisprudenza dell'Istituto Universitario Europeo di Firenze. Gli autori vorrebbero ringraziare Cesár Alonso Iriarte ed Alfonso Scirocco, ai cui questo articolo è dedicato. Ogni errore o mancanza è di esclusiva responsabilità degli autori.

[2] « *… there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers… Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance…* ».

nel settore della protezione dei dati personali potessero restringere la libera circolazione di quest'ultimi ha spinto i governanti europei ad intavolare trattative prima nel quadro dell'OCSE e del Consiglio d'Europa[3], e successivamente all'interno dell'Unione Europea, al fine di armonizzare le legislazioni nazionali in materia.

Negli ultimi anni il tema del trasferimento transfrontaliero dei dati personali non è più legato esclusivamente a ragioni di carattere commerciale. Sempre più spesso il trasferimento dei dati personali è connesso alla tematica della protezione della sicurezza pubblica. La condivisione tra le autorità di polizia di Paesi differenti dei dati personali relativi ai propri cittadini è divenuta un elemento essenziale nel quadro della cooperazione internazionale contro il terrorismo ed il crimine organizzato internazionale. Lo scambio di informazioni tra le polizie nazionali dei Paesi aderenti all'Europol[4] o dell'accordo Schengen[5] sono alcuni esempi di questa nuova giustificazione al flusso transnazionale di dati personali. Una delle sfide del XXI secolo nel settore della protezione dei dati personali è, pertanto, quella di proteggere il diritto alla riservatezza delle persone fisiche non soltanto quando i loro dati personali sono trasferiti per ragioni commerciali, ma anche quando sono trasferiti per ragioni di pubblico interesse. Nonostante la pubblica sicurezza sia un interesse della collettività, il diritto alla riservatezza, quale diritto fondamentale dell'individuo nella società dell'informazione, deve comunque essere tutelato. È quindi necessario raggiungere un equilibrio tra l'esigenza di sicurezza della collettività e l'esigenza di anonimato dell'individuo.

Il dibattito sulla protezione dei dati personali v. sicurezza pubblica ha molte sfaccettature. Questo lavoro analizza questo dibattito prendendo in considerazione le negoziazioni sul trasferimento dei Dati dei Passeggeri Aerei (*Passenger Name Records*, PNR) intavolate negli ultimi anni dalla Commissione Europea con le autorità federali statunitensi. Tali negoziazioni, conclusesi solo nel 2007 dopo oltre cinque anni di trattative, sono

---

Linee Guida sulla Protezione della Privacy e i Flussi Transfrontalieri dei Dati, approvate dall'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) il 23 settembre 1980. Il testo delle Linee Guida è disponibile a *http://www.oecd.org/document/18/0,3343, en_2649_34255_1815186_1_1_1_1,00.html* (19 febbraio 2010).

[3] Convenzione del Consiglio d'Europa n. 108 per la Protezione degli Individui in Relazione all'Elaborazione Automatica dei Dati Personali. Firmata a Strasburgo il 28 gennaio 1981, entrata in vigore il 1 ottobre 1985. Il testo della Convenzione è disponibile a: *http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm* (19 febbraio 2010).

[4] Europol è una delle agenzie dell'Unione Europea che ha il compito di funzionare da centrale di coordinamento per lo scambio di informazioni tra le polizie dei Paesi Membri dell'Unione Europea per favorire la lotta contro crimini con carattere transnazionale. Per ulteriori informazioni: *http://www.europol.europa.eu/index.asp?page=home&language=* (19 febbraio 2010).

[5] La convenzione di Schengen del 1990 abolì i controlli alle frontiere dei Paesi Membri della Comunità Europea che aderirono all'accordo. Tuttavia, al fine di evitare che l'abolizione dei controlli alle dogane favorisse le attività internazionali delle organizzazioni criminali europee, la convenzione prevedeva l'istituzione di un sistema centralizzato di scambio di informazioni tra le polizie nazionali chiamato « *Schengen Information System* ».

Convenzione di Schengen firmata il 19 giugno 1990, in vigore il 26 marzo 1995, in applicazione dell'Accordo di Schengen raggiunto il 14 giugno 1985 da Repubblica Federale Tedesca, Francia, Belgio, Lussemburgo e Paesi Bassi. Il testo della convenzione di Schengen è disponibile a: *http://www.hri.org/docs/Schengen90/* (19 febbraio 2010).

un ottimo esempio dello scontro tra l'esigenza di tutelare la pubblica sicurezza e quella di garantire la riservatezza dei dati personali dei cittadini. L'obbiettivo di questo lavoro e di condurre un'analisi delle varie tappe che hanno caratterizzato queste negoziazioni al fine di chiarire quale interesse, protezione dei dati personali o ragioni di sicurezza nazionale, sia prevalso al termine di queste negoziazioni.

2. Le origini delle negoziazioni sul trasferimento dei PNR.

Le ragioni che hanno condotto a queste negoziazioni sono da ricercarsi nel lontano 1996, l'anno in cui la compagnia Northwest Airlines introdusse per la prima volta un Sistema Computerizzato per Supportare il Monitoraggio del Passeggero (*Computer Assisted Passenger Pre-Screening System*, CAPPS) sui suoi voli[6]. Il CAPPS confrontava i dati dei passeggeri (PNR) presenti nel Sistema di Prenotazione Computerizzata (*Computer Reservation System*, CRS) della compagnia aerea con quelli inseriti in una banca dati contenente una *no-fly list*, una lista di persone considerate potenzialmente pericolose per la sicurezza del volo. Nel 1998 il CAPPS fu esteso a tutti gli aeroporti americani per tutti i voli interni.

In seguito ai tragici eventi dell'11 settembre, il 19 novembre 2001 il Congresso americano approvò una nuova Legge sull'Aviazione e la Sicurezza dei Trasporti (*Aviation and Transportation Security Act*)[7]. L'*Act* emendò la sezione 44909 del titolo 49 del Codice degli USA (*United States Code*), aggiungendo un nuovo paragrafo intitolato « Voli su Cieli Stranieri in Viaggio Verso gli Stati Uniti » (*Flights in Foreign Air Transportation to the United States*)[8]. Quest'ultimo paragrafo imponeva a tutte le compagnie aeree che operavano su rotte dall'estero verso gli aeroporti statunitensi di fornire i PNR dei propri passeggeri all'Amministrazione delle Dogane e per la Protezione dei Confini (*Customs and Border Protection Administration*, CBP) prima della partenza del volo[9]. La nuova normativa

[6] La prima versione del CAPPS confrontava i nomi dei passeggeri aerei con una lista di viaggiatori pericolosi stilata periodicamente dall'FBI. Alla luce dell'incapacità del CAPPS di identificare i dirottatori degli attentati dell'11 settembre 2001, nel 2003 la *Transportation Security Administration* (Ente alla Sicurezza dei Trasporti americana) iniziò a lavorare ad una seconda versione del CAPPS, la quale potesse verificare i PNR con vari dati contenuti negli archivi delle agenzie federali statunitensi. Tuttavia, il progetto fu abbandonato nell'estate del 2004 in seguito alle critiche di varie organizzazioni non governative (ONG) per la difesa della privacy e di un rapporto negativo del *General Accounting Office*. Nel 2005 la TSA iniziò a lavorare su di un nuovo progetto chiamato *Secure Flights* (Voli Sicuri), il quale non fu mai portato a termine a causa dell'opposizione del Congresso americano. Per ulteriori informazioni vedi il rapporto del *General Accounting Office* disponibile a: *http://www.gao.gov/new.items/d04385.pdf* (19 febbraio 2010).

[7] Aviation and Transportation Security Act, approvato il 19 novembre 2001. S. 1147, approvato dal 107imo Congresso degli Stati Uniti. Section 115. Il testo della legislazione è disponibile a: *http://www.tsa.gov/assets/pdf/Aviation_and_Transportation_Security_Act_ATSA_Public_Law_107_1771.pdf* (19 febbraio 2010).

[8] 49 USC 44909, par. *c*) disponibile a: *http://www4.law.cornell.edu/uscode/49/44909.html* (19 febbraio 2010).

[9] Le disposizioni dell'*Aviation and Transportation Security Act* a riguardo del trasferimento dei PNR da parte delle compagnie aeree alla CBP furono completate da un regolamento adottato nel giugno 2002 e poi aggiornato nell'aprile 2004.

Section 122.49.b, title 19 (Customs Regulation) Code of Federal Regulations, con-

aveva un chiaro valore extra-*ter*ritoriale, in quanto le compagnie aeree erano obbligate a fornire i PNR alla CBP quando l'aereo non era ancora decollato, e quindi si trovava al di fuori del territorio e della giurisdizione degli USA.

Le compagnie aeree di quasi tutti i Paesi del mondo accettarono la richiesta del governo americano, anche perché furono numerosi i Paesi che dopo l'11 settembre iniziarono ad introdurre nei propri aeroporti sistemi di monitoraggio simili al CAPPS. Situazione differente si presentava invece per le compagnie aeree europee, costrette a rispettare i vincoli della Direttiva 95/46/CE[10]. Quest'ultime si trovavano in una situazione di grande incertezza giuridica: le autorità statunitensi le minacciavano di privarle dei loro diritti di atterraggio nel territorio americano se non iniziavano a fornire i PNR alla CBP. Tuttavia, se avessero ottemperato a tali richieste, avrebbero probabilmente ricevuto sanzioni dai Garanti europei per la protezione dei dati personali, per aver violato le legislazioni nazionali che implementavano la Direttiva del 95/46/CE.

3. L'Articolo 25 della Direttiva 95/46/CE, la regolamentazione comunitaria in materia di trasferimento dei dati personali al di fuori della CE.

La Convenzione del Consiglio d'Europa del 1981 aveva introdotto il principio della protezione « equivalente », secondo il quale il trasferimento dei dati personali tra due Stati aderente alla Convenzione poteva aver luogo se il Paese di destinazione del flusso d'informazioni garantiva lo stesso livello di protezione dei dati personali assicurato dallo Stato di origine[11]. L'espressione « equivalente » richiedeva un elevato grado di compatibilità tra i due sistemi di protezione dei dati personali, rappresentando quindi un ostacolo *de facto* alla circolazione transfrontaliera dei dati personali.

La Direttiva 95/46/CE ha semplificato il sistema di trasferimento transfrontaliero dei dati personali sotto tre punti di vista. Innanzitutto, la Direttiva del 1995 ha introdotto il principio della libera circolazione dei dati personali all'interno del mercato comune europeo in seguito all'armonizzazione delle legislazioni nazionali in questo settore. La Direttiva ha invece mantenuto un sistema preventivo di accertamento del livello di protezione dei dati personali solo per i Paesi extra-Comunitari. Inoltre, la Direttiva 95/46/CE ha garantito alla Comunità, piuttosto che ai singoli Stati Membri, il compito di decidere sul livello di adeguatezza della protezione dei dati personali nei Paesi esterni all'Unione Europea[12]. Infine, rispetto

cerning Passenger Name Record Information. Regolamento emanato il 25 giugno 2002 e poi aggiornato il 1 aprile 2004. Il testo del regolamento è disponibile a: *http://cfr.vlex.com/vid/122-passenger-name-record-pnr-information-19649183* (19 febbraio 2010).

[10] Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995, Relativa alla Tutela delle Persone Fisiche con Riguardo al Trattamento dei Dati Personali, nonché alla Libera Circolazione dei Dati. GUCE L-281/31.

Il testo della Direttiva è disponibile a: *http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm* (19 febbraio 2010).

[11] *Supra*, Convenzione Consiglio d'Europa n. 108, Art. 12(3)(a).

[12] O. Estadella Yuste, *The draft directive of the European Community regar-*

al precedente del Consiglio d'Europa del 1981, la Direttiva ha assunto un approccio più realistico, richiedendo ai Paesi extra-Europei un livello di protezione « adeguato » piuttosto che « equivalente » rispetto agli standard Comunitari[13].

Da un punto di vista pratico, esistono tre possibili modalità di trasferimento di dati personali all'esterno dello spazio Comunitario[14]:

1) I dati personali dei cittadini europei possono essere trasferiti da un *controller* (titolare del trattamento dei dati)[15] situato all'interno dell'Unione Europea ad un *processor* (responsabile del trattamento)[16] situato in un Paese terzo. In questo caso il *processor* elaborerà i dati sotto la responsabilità del *controller* europeo, a sua volta vincolato dal rispetto della normativa Comunitaria in materia.

2) Il *controller* situato all'interno della UE trasferisce i dati personali ad un altro *controller* situato in Paese extra-europeo, soggetto alla normativa di protezione dei dati personali del Paese terzo.

3) Infine, l'interessato (il *data subject*) trasferisce direttamente i suoi dati personali ad un *controller* situato in uno Stato extra-Comunitario. Da un punto di vista pratico quest'ultimo è probabilmente il caso più frequente. Infatti, ogni volta che un individuo rilascia i suoi dati personali ad una compagnia che ha la sua sede legale all'esterno della Comunità (ad esempio in seguito ad un acquisto su Internet), i dati personali del cittadino europeo sono istantaneamente trasferiti al di fuori dello spazio di protezione Comunitario.

La Direttiva 95/46/CE ha introdotto un sistema preventivo di controllo del livello di protezione dei dati personali nei Paesi extra-Comunitari solo per gli ultimi due tipi di trasferimenti. Infatti, nel primo caso il *controller* è direttamente vincolato al rispetto della legislazione nazionale che ha implementato la Direttiva 95/46/CE.

Una pluralità di attori intervengono nel processo di valutazione del livello di adeguatezza del sistema di protezione dei dati personali di un Paese terzo. Francesca Bignami ha definito tale procedura di « *mixed administration* » (amministrazione mista), in quanto coinvolge sia le istituzioni nazionali che Comunitarie[17]. La Direttiva del '95 attribuisce un'importante funzione ai Garanti nazionali. Infatti, in base all'Articolo 25(1) della Direttiva, se un singolo Garante nazionale ritiene che un trasferimento di dati verso l'esterno dello spazio Comunitario non sia conforme ai principi della Direttiva, lo può bloccare. Tuttavia, così facendo, si ritornerebbe ad una situazione simile a quella prevista della Convenzione del Consiglio d'Europa del 1981, in cui ogni Stato europeo godeva di una pro-

ding the protection of personal data. Vol. 41., No. 1, International and Comparative Law Quarterly 170-179 (1992).

[13] B. Havelange, A.C. Lacoste, *Les FluxTtransfrontaliers de Données à Caractère Personnel en Droit Européen*. Vol. 9, No 84, in *Journal des Tribunaux, Droit Européen*, 241-248 (2001).

[14] Gruppo di Lavoro 29, « First orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy ». Opinione adottata il 26 giugno 1997. Opinione 4/97, pagina 9. Il documento è disponibile a: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1997/wp4_it.pdf* (19 febbraio 2010).

[15] *Supra*, Direttiva 95/46/CE, Art. 2(d).

[16] *Supra*, Direttiva 95/46/CE, Art. 2(e).

[17] F. Bignami, *Mixed Administration in the European Data Protection Directive: The Regulation of International Data Transfers*. Vol. 1, in *Rivista Trimestrale di Diritto Pubblico*, 31-57 (2004).

pria discrezionalità nel decidere quali trasferimenti erano legittimi. Al fine di evitare una tale frammentazione, i Garanti nazionali sono tenuti ad informare la Commissione Europea della loro scelta[18]. Successivamente, il caso verrà dibattuto all'interno del comitato dei rappresentanti dei Paesi Membri introdotto dall'Articolo 31 della Direttiva[19]. Quest'ultimo potrà decidere di bloccare il trasferimento dei dati personali a partire da tutti i Paesi Membri dell'Unione Europea[20], oppure incaricare la Commissione di intavolare negoziazioni con il Paese terzo per « porre rimedio » alla situazione[21]. Se lo Stato extra-Comunitario, in seguito alle negoziazioni con la Commissione, s'impegna a garantire un livello di tutela « adeguata » ai dati personali dei cittadini europei, l'esecutivo di Bruxelles adotterà una decisione di « *adequacy finding* » nella quale dichiarerà che « la protezione adeguata è stata trovata »[22]. La decisione della Commissione Europea dovrà successivamente essere approvata dal Comitato 31, diventando quindi vincolante per tutti i Garanti nazionali[23].

Per quanto riguarda la natura giuridica della decisione di adeguatezza è importante sottolineare che non ci troviamo di fronte ad un vero e proprio trattato internazionale, il quale necessiterebbe della ratifica del Consiglio e dell'assenso del Parlamento Europeo[24]. L'accordo riceve semplicemente l'approvazione dei delegati dei Paesi Membri che partecipano ad un organo tecnico quale il Comitato 31. Il Parlamento Europeo è, pertanto, l'unica istituzione totalmente esclusa da tale processo decisionale, nonostante la rilevanza di una decisione di *adequacy finding* e nonostante la stessa Direttiva 95/46/CE sia stata approvata anche dal Parlamento Europeo per mezzo della procedura di co-decisione. Come vedremo nelle prossime pagine, il Parlamento Europeo ha assunto un atteggiamento molto critico nei confronti delle negoziazioni della Commissione Europea con le autorità statunitensi per il trasferimento dei PNR. Tuttavia, a causa di tale processo decisionale la sua voce è sempre rimasta inascoltata.

L'Articolo 25 non chiarifica il significato dell'espressione « protezione adeguata ». Il significato di tale espressione è stato chiarificato dall'ultima istituzione coinvolta all'interno del processo decisionale previsto dall'Articolo 25, il Gruppo di Lavoro 29. Questo comitato comprende i rappresentanti delle Autorità Garanti nazionali, e ha il compito di fornire pareri

---

[18] *Supra*, Direttiva 95/46/CE, Art. 25(3).

[19] Il Comitato 31 è uno dei comitati che fanno parte della così detta « comitologia ». In base all'Articolo 202 del Trattato della Comunità Europea il Consiglio delega alla Commissione l'autorità di adottare decisioni applicative delle legislazioni Comunitarie. Tuttavia, gli Stati Membri hanno voluto mantenere un certo controllo su tali decisioni, attraverso l'istituzione dei Comitati, che devono approvare ad unanimità o a maggioranza qualificata le decisioni della Commissione. Il Comitato 31 è presieduto da un rappresentante della Commissione e adotta le sue decisioni a maggioranza qualificata, nonostante la regola del consenso di solito prevalga.

[20] *Supra*, Direttiva 95/46/CE, Art. 25(4).

[21] *Supra*, Direttiva 95/46/CE, Art. 25(5).

[22] *Supra*, Direttiva 95/46/CE, Art. 25(6).

[23] A tale riguardo vedi J. Monducci, *La Circolazione Online dell'Individuo*. Vol. 1, in *Ciberspazio e Diritto*, 31-39 (2000).

[24] A riguardo del ruolo del Parlamento Europeo nelle fasi di stipulazione degli accordi internazionali della Comunità Europea vedi S. Di Paola, *International treaty-making in the EU: what role for the European Parliament?*. Vol. XXXVIII, No. 2, in *The International Spectator*, 75-90 (2003).

non vincolanti alla Commissione a riguardo della corretta applicazione della Direttiva 95/46/CE. In una delle sue prima opinioni consultive il Gruppo di Lavoro ha individuato una serie di principi che le legislazioni dei Paesi extra-europei dovrebbero rispettare al fine di poter essere considerate « adeguate »[25]. Il Gruppo di Lavoro ha dichiarato che i principali diritti dei *data subject* (diritto a fornire il consenso al fine della elaborazione dei dati, diritto di rettifica e cancellazione dei dati dall'archivio) ed i criteri di qualità e sicurezza dei dati previsti dalla Direttiva dovrebbero essere tutelati anche nei Paesi extra-Europei. Inoltre, il Paese di destinazione dei dati non può permettere che quest'ultimi siano « ri-esportati » verso Paesi terzi che non garantiscano un livello di tutela adeguato. Infine, il Gruppo di Lavoro ha sottolineato che il trasferimento di alcune specifiche categorie di dati merita un'attenzione particolare[26]. Si dovrebbe infatti concedere con molta cautela l'autorizzazione al trasferimento di « dati sensibili »[27], dei dati frutto delle « decisioni automatiche individuali » (ad esempio, i dati trasmessi attraverso Internet, in quanto l'individuo non sa esattamente dove verranno inviate le informazioni a suo riguardo), e i dati raccolti per fini di *marketing*. Nella sua opinione il Gruppo di Lavoro riconobbe che pochi Paesi al di fuori dell'Unione Europea erano dotati di un meccanismo di *enforcement* simile a quello Comunitario, basato sull'esistenza dei Garanti nazionali[28]. Secondo il Gruppo di Lavoro, anche i Paesi che non dispongono di un Garante nazionale possono comunque essere considerati « adeguati » se la legislazione locale prevede sanzioni abbastanza severe per i *controllers* che non tutelino i dati, e se i *data subjects* possono far valere i loro diritti in modo rapido ed effettivo, senza dover affrontare costi eccessivi (sistema di *redress* effettivo). Questi criteri mostrano l'intenzione del Gruppo di Lavoro 29 di andare oltre al criterio formalistico della protezione equivalente prevista dalla Convenzione del Consiglio d'Europa del 1981 e di trovare un giusto equilibrio tra la necessità di tutelare i diritti dei *data subjects* europei anche al di fuori dello spazio Comunitario e la necessità di permettere il trasferimento dei dati verso Paesi terzi che utilizzano sistemi di *enforcement* diversi da quello Comunitario. Tuttavia, come vedremo nelle prossime pagine in relazione alle negoziazioni sul PNR, non è sempre stato facile tradurre in casi concreti l'approccio funzionalista suggerito dal Gruppo di Lavoro.

---

[25] *Supra*, Opinione del Gruppo di Lavoro 29 n. 4/97. Pagina 6.

[26] P. Graham, N. Platten, *Orchestrating Transatlantic Approaches to Personal Data Protection: a European Perspective*. Vol. 22, No. 5, in *Fordham International Law Journal*, 2024-2051 (1999).

[27] Secondo l'Articolo 8(1) della Direttiva 95/46/CE l'elaborazione di dati personali che rilevano l'origine etnica, razziale, le convinzioni politiche o religiose, o le condizioni di salute dell'individuo è vietata. Tali dati sono considerati « sensibili » in quanto possono causare una discriminazione dell'individuo se tali dati vengono a conoscenza di soggetti terzi. Tuttavia, il Paragrafo 2 dello stesso Articolo prevede una lista di eccezioni a tale divieto. Ad esempio, l'elaborazione è consentita quando il soggetto ha fornito il suo consenso esplicito o quando l'elaborazione è necessaria al fine di tutelare la salute del *data subject*.

A riguardo della tematica della protezione dei dati sensibili vedi: G. Bisso (eds.), *Dati Sensibili e Soggetti Pubblici: Commento Sistematico al D.Lgs. 135/1999: Commenti e Casi Pratici*, Giuffrè Editore, Milano (Italia), 2000.

[28] *Supra*, Opinione del Gruppo di Lavoro 29 n. 4/97, 7.

4. Le lunghe negoziazioni con le autorità USA; il primo accordo del maggio 2004.

Per un lungo periodo di tempo la Commissione Europea temporeggiò, ignorando l'esistenza delle disposizioni contenute nell'*Aviation and Transportaton Security Act* del novembre 2001 e delle loro conseguenze per le compagnie aeree europee. Infatti, solo nel febbraio 2003 la Commissione Europea e la CBP conclusero una dichiarazione congiunta (*joint statement*)[29] in base alla quale la Commissione avrebbe autorizzato le compagnie aeree europee a trasferire i PNR alla CBP. Tuttavia, tale soluzione era temporanea, in quanto era vincolata all'impegno d'intraprendere negoziazioni al fine di trovare una soluzione definitiva al problema.

Le negoziazioni tra la Commissione Europea e la CBS furono più complesse di quanto inizialmente previsto. Nel giugno 2003 il Gruppo di Lavoro 29 identificò una serie di aspetti delle richieste statunitensi che risultavano chiaramente in contrasto con i principi della Direttiva 95/46/CE[30]. In particolare, il Gruppo di Lavoro sottolineava che i dati dovevano essere trasferiti attraverso un sistema di *push*, in base al quale erano le compagnie aeree ad inviare direttamente i PNR alla CBP. Il sistema allora in vigore era, invece, di tipo *pull*, in base al quale la CBP otteneva i PNR attraverso l'accesso diretto ai CRS delle compagnie aeree prima della partenza del volo. Il sistema di *push* era più rispettoso della privacy dei cittadini europei, in quanto i dati sensibili venivano filtrati automaticamente dalle compagnie aeree prima di essere inviati alla CBP. Inoltre, secondo il Gruppo di Lavoro, i PNR dovevano essere utilizzati solo per identificare potenziali terroristi e non dovevano essere condivisi con altri dipartimenti federali americani. La CBP, invece, chiedeva l'utilizzo dei PNR per individuare criminali che si fossero macchiati di *serious criminal offences* (gravi crimini penali), espressione alquanto generica, e di poter condividere tali informazioni con tutte le istituzioni che si occupassero di *intelligence* negli USA. Tale approccio era profondamente in contrasto con la Direttiva 95/46/CE, che prevedeva che il *data subject* fossero messi al corrente di chi fosse il *controller* e di quali fossero le finalità dell'elaborazione dei propri dati personali[31]. Inoltre, la quantità di dati richiesti dalla CBP (inizialmente trentotto) e il tempo di ritenzione di quest'ultimi (7-8 anni) non rispettavano il principio di proporzionalità né quello della limitazione del tempo di ritenzione dei dati al periodo di elaborazione dei dati[32]. Infine, il passeggero europeo non godeva di alcun diritto di accesso, rettifica o cancellazione dei suoi dati;[33] i PNR erano comunicati alla CBP senza il consenso del *data subject* e quest'ultimo non godeva di alcun strumento di ricorso giudiziale contro potenziali abusi da parte del CBP[34].

---

[29] *Joint statement* approvato al termine della riunione tenutasi a Bruxelles il 17/18 febbraio 2003 tra i rappresentanti dalla Commissione Europea e del CBP.

[30] Gruppo di Lavoro 29, Opinion 4/2003 on the Level of Protection Ensured in the US for the Transfer of Passengers' Data. Opinione adottata il 13 giugno 2003. Documento n. 4/2003. Il testo dell'opinione è disponibile a: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp78_it.pdf* (19 febbraio 2010).

[31] *Supra*, Direttiva 95/46/CE, Art. 10(a).

[32] *Supra*, Direttiva 95/46/CE, Art. 6.

[33] *Supra*, Direttiva 95/46/CE, Art. 12(a)(b).

[34] *Supra*, Direttiva 95/46/CE, Art. 22.

Nonostante le difficoltà incontrate nel riconciliare posizioni tanto differenti, le quali enfatizzavano l'una la protezione dei dati personali e l'altra ragioni di sicurezza nazionale, nel dicembre 2003 la Commissione Europea annunciò l'intenzione di voler adottare una decisione di *adequacy finding* nei confronti delle richieste americane[35]. L'esecutivo europeo aggiunse che la decisione d'adeguatezza sarebbe stata accompagnata da un « *light international agreement* » (« accordo internazionale leggero »). Quest'ultimo serviva a vincolare gli Stati Uniti a rispettare le condizioni di trattamento dei PNR pattuite durante le negoziazioni. Inoltre, avrebbe autorizzato la CBP a prelevare, attraverso il sistema di *pull*, i dati dalle CRS delle compagnie aeree. Pertanto, la UE, attraverso l'accordo internazionale autorizzava le autorità americane ad « entrare », anche se solo virtualmente, all'interno del territorio Comunitario. La decisione di *adequacy finding* e l'accordo internazionale furono approvati dalla Commissione Europea nel 2004[36], e l'accordo internazionale fu successivamente ratificato dal Consiglio[37].

Durante i mesi di negoziazioni il CBP venne incontro ad alcune richieste della Commissione Europea. Ad esempio, i dati sensibili che potevano permettere l'identificazione di un passeggero sulla base della sua razza o religione vennero esclusi dalla lista dei PNR trasmessi alla CBP. Inoltre, i *data subject* avrebbero avuto diritto di rettifica dei loro dati. Tuttavia, secondo il Gruppo di Lavoro 29, le concessioni americane rimasero insufficienti sotto molti aspetti[38]. Ad esempio, il numero dei dati raccolti era sceso da trentotto a trentaquattro, una quantità di dati ritenuta eccessiva rispetto alla finalità di identificare potenziali terroristi prima della partenza di un volo. Similmente, il periodo di ritenzione dei dati era sceso da 7-8

[35] Commissione Europea, Communication from the Commission to the Council and the Parliament; Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach. Adottata il 16 dicembre 2003; documento n. COM(2003) 826 final. Il testo del documento è disponibile a: *http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/apis-communication/apis_en.pdf* (19 febbraio 2010).

[36] Commissione Europea, Decisione della Commissione 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). Adottata il 14 maggio 2004. Documento n. C(2004) 1914. Il testo della decisione è disponibile a: *http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32004D0535&model=guichett* (19 febbraio 2010).

[37] Consiglio dell'Unione Europea, Council Decision of 17 May 2004 on the Conclusion of an Agreement between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection. Adottata il 17 maggio 2004. Documento n. 2004/496/EC. Il testo della Decisione del Consiglio è disponibile a: *http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32004D0535&model=guichett* (19 febbraio 2010).

Il testo dell'accordo internazionale stipulato tra gli Stati Uniti e la Comunità Europea per permettere il trasferimento dei PNR è disponibile a: *http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/2004-05-28-agreement_en.pdf* (19 febbraio 2010).

[38] Gruppo di Lavoro 29: Parere 2/2004 sul Livello di Protezione Adeguato dei Dati a Carattere Personale Contenuti nelle Pratiche Passeggeri (PNR - Passenger Name Record) Trasferite all'Ufficio delle Dogane e della Protezione di Frontiera degli Stati Uniti (Bureau of Customs and Border Protection - US CBP). Adottato il 29 gennaio 2004. Documento n. 2/2004. Il testo dell'Opinione è disponibile a: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp87_it.pdf* (19 febbraio 2010).

anni a 3 anni e sei mesi, un periodo comunque troppo lungo per tale finalità. Infine, il CAPPS continuava a funzionare sulla base di un sistema *pull*, invece di un sistema *push*. Infine, il CBP, nonostante si impegnasse a mantenere confidenziali i dati ricevuti, poteva trasmettere a sua discrezione i PNR ad altre autorità statunitensi e straniere che si occupavano di lotta contro il terrorismo ed il crimine organizzato. Nella sua Opinione il Gruppo di Lavoro 29 sostenne di comprendere l'esigenza di sicurezza emersa negli Stati Uniti dopo i tragici eventi del « 9/11 ». Tuttavia, le richieste delle autorità americane non rispettavano un criterio di proporzionalità. L'inadeguatezza delle richieste americane era particolarmente evidente se paragonata alle richieste di altri Paesi, i quali dopo l'11 settembre avevano introdotto forme di controllo dei PNR sull'esempio degli USA. Tali richieste, pur mirando a tutelare la sicurezza pubblica, salvaguardavano la privacy dei passeggeri (e.g. il numero dei dati richiesti era molto inferiore rispetto a quelli richiesti dalla CBP, e i dati venivano conservati solo per il periodo di durata del volo e poi cancellati)[39]. In virtù della mancanza di proporzionalità delle richieste americane la conclusione del Gruppo di Lavoro 29 fu la seguente: « i limitati progressi che sono stati registrati non consentono di giudicare che sia stato raggiunto un livello adeguato di protezione dei dati »[40].

Nel maggio del 2004 la Commissione Europea approvò quindi una decisione di *adequacy finding* nei confronti delle richieste della CBP nonostante il parere contrario del comitato che rappresentava le Autorità Garanti nazionali. Nella conferenza stampa successiva all'approvazione della decisione di adeguatezza, il Commissario Bolkestein dichiarò che le autorità americane avevano applicato « una forte pressione politica » (uno « *strong political pressure* ») sulla Commissione, al fine di ricevere *l'adequacy finding*. Tuttavia, a giudizio del Commissario, il risultato negoziato era « equilibrato » (« *balanced* »)[41]. Il risultato di una negoziazione è sempre un compromesso, tuttavia, non era chiaro se l'accordo del maggio 2004 poteva essere considerato « adeguato » alla luce dell'Articolo 25 della Direttiva 95/46/CE.

5. La reazione del Parlamento Europeo e della Corte di Giustizia all'accordo del 2004.

Come è stato menzionato nelle pagine precedenti, il Parlamento Europeo è escluso dalla procedura di *adequacy finding*, nonostante le importanti implicazioni politiche di tale decisione in alcuni casi, come per il tra-

[39] Il Gruppo di Lavoro 29 nella sua Opinione si riferì all'esempio dell'Australia, la quale aveva anch'essa introdotto un sistema di monitoraggio dei PNR dopo l'11 settembre. Tuttavia, il Gruppo di Lavoro sottolineò che l'Australia richiedeva un numero inferiore di dati (18, invece dei 34 richiesti dalla CBP). Inoltre, i dati erano mantenuti nei *database* delle autorità di dogana australiane solo fino all'arrivo a destinazione del volo. Successivamente, « le dogane di questo paese conservano o immagazzinano dati su un passeggero solo se quest'ultimo ha commesso un atto illegale o se i dati sono necessari per le esigenze di un'inchiesta riguardante un presunto delitto ».

Ibid, 9.

[40] *Ibid*, 13.

[41] Redazione, *Europe Bows to U.S. on Air Passenger Data*. International Herald Tribune, 18 maggio 2004.

sferimento dei PNR alle autorità americane. Il Parlamento Europeo fu inoltre escluso dall'approvazione dell'accordo internazionale « *light* » stipulato dalla Comunità Europea con gli USA nel maggio 2004 come corollario alla decisione di *adequacy finding* della Commissione. Infatti, l'accordo fu approvato sulla base dell'Articolo 300(3) del Trattato della Comunità Europea. In base a tale Articolo, i trattati internazionali approvati in settori in cui a livello interno si applichi la procedura di co-decisione prevista dall'Articolo 251 del Trattato erano ratificati dal Consiglio su proposta della Commissione. Il Parlamento svolgeva esclusivamente una funzione « consultiva »: il suo parere non era vincolante. Tuttavia, il secondo comma dell'Articolo 300(2) prevedeva che nel caso in cui il trattato internazionale emendasse una norma Comunitaria precedentemente approvata per mezzo della procedura di co-decisione il Parlamento doveva fornire il suo « assenso » (con valore vincolante) alla ratifica del Consiglio. Come vedremo nelle prossime pagine, lo sconto tra Parlamento e Commissione a riguardo dell'accordo per il trasferimento dei PNR si focalizzò maggiormente sulla base legale dell'accordo internazionale *light* stipulato nel maggio 2004 che sul contenuto della decisione di *adequacy finding*.

Durante il periodo delle negoziazioni tra la Commissione e la CBP il Parlamento Europeo, ed in particolare al suo interno il Comitato per i Diritti e le Libertà Civili dei Cittadini (LIBE), fu molto critico nei confronti della Commissione Europea. Il LIBE criticò l'intenzione della Commissione Europea di adottare una decisione di *adequacy finding* per le richieste della CBP nonostante le critiche mosse dal Gruppo di Lavoro 29[42]. Inoltre, secondo il Parlamento Europeo l'accordo internazionale *light* che la Commissione intendeva concludere con gli USA rappresentava una deroga ai principi della Direttiva 95/46/CE. Pertanto, quest'ultimo doveva essere ratificato con l'assenso del Parlamento Europeo e non soltanto con l'approvazione del Consiglio[43]. Dal canto suo l'esecutivo di Bruxelles voleva evitare questa strada per ovvie ragioni politiche, sapendo che il Parlamento Europeo, sotto l'influenza del LIBE, non avrebbe mai approvato un trattato internazionale con gli USA per permettere il trasferimento dei PNR.

A causa del rifiuto della Commissione di coinvolgere il Parlamento nella negoziazione di un vero trattato internazionale nel marzo 2004 il LIBE propose al plenario del Parlamento di « portare il caso davanti alla Corte di Giustizia al fine di verificare la legalità dell'accordo internazionale progettato (accordo in forma "*light*" proposto dalla Commissione) ed, in particolare, (di verificare) la compatibilità di tale accordo con la protezione dei diritti fondamentali (dei cittadini europei) »[44]. La proposta del LIBE

[42] Comitato per i Diritti e le Libertà dei Cittadini, e la Giustizia e gli Affari Interni (LIBE), Motion for a Resolution on the Draft Commission Decision Noting the Adequate Level of Protection Provided for Personal Data Contained in the Passenger Name Records (PNRs) Transferred to the US Bureau of Customs and Border Protection. Risoluzione adottata il 19 marzo 2004. Documento n. RE\339611EN.doc. Il documento è disponibile a: *http://www.edri.org/edrigram/number2.5/PNR* (19 febbraio 2010).

[43] Parlamento Europeo, European Parliament Resolution on Transfer of Personal Data by Airlines in the Case of Transatlantic Flights: State of Negotiations with the USA. Risoluzione adottata il 9 ottobre 2003. Punto 3 della risoluzione, comma C. Il documento è disponibile a: *http://www.statewatch.org/news/2003/oct/eppnrresol.pdf* (19 febbraio 2010).

[44] *Supra*, risoluzione del LIBE del 19 marzo 2004. Punto n. 8 delle conclusioni: « *... to bring an action before the Court of Justice in order to seek verification of*

di ricorrere alla Corte di Giustizia fu approvata a stretta maggioranza dalla seduta plenaria del Parlamento del 21 aprile 2004[45]. Senza considerare il ricorso alla Corte di Giustizia, il 14 maggio 2004 la Commissione adottò la sua decisione di *adequacy* e alcuni giorni dopo, il 17 maggio, il Consiglio adottò la Decisione 2004/496/CE, la quale approvava l'accordo di trasferimento dei PNR agli USA.

Il 30 maggio 2006 la Corte sentenziò che sia la decisione di *adequacy* che la decisione del Consiglio erano al di fuori dell'ambito di applicazione della Direttiva 95/46/CE, in quanto quest'ultime riguardavano problemi legati alla pubblica sicurezza. Di conseguenza, la Corte annullò la decisione di *adequacy*. In relazione alla decisione del Consiglio, che si riferiva ad un tema legato alla pubblica sicurezza, l'Articolo 95 CE non costituiva una base legale adeguata e, pertanto, la decisione doveva essere anch'essa annullata[46]. La Corte, tuttavia preservò in via transitoria gli effetti della decisione di *adequacy* per un periodo di 90 giorni (30 settembre 2006) per permettere alla Commissione di negoziare un nuovo accordo con le autorità americane sulla base di una base giuridica appropriata.

È importante sottolineare che la sentenza della Corte di Giustizia non chiarì completamente quale dovesse essere la base legale per il trasferimento dei dati, in quanto il semplice fatto che un'attività non ricadesse nell'ambito di applicazione della Direttiva 95/46/CE non implicava necessariamente che tale attività fosse regolata all'interno del terzo pilastro[47]. Il successivo accordo sul PNR del 2007 è stato approvato da una Decisione del Consiglio sulla base del terzo pilastro, senza alcun coinvolgimento del Parlamento Europeo[48]. In tal modo anche la giurisdizione della Corte di Giustizia è stata esclusa. Un altro interessante aspetto da sottolineare è che nella sua sentenza la Corte si limitò ad annullare l'accordo internazionale e la decisione di *adequacy* sulla base di una scorretta base legale, senza invece analizzare l'adeguatezza del trasferimento dei PNR con i di-

the legality of the projected international agreement and, in particular, the compatibility thereof with the protection of a fundamental right ».

[45] La riunione plenaria del Parlamento Europeo approvò il ricorso alla Corte di Giustizia con 276 voti a favore; 260 i contrari e 13 astensioni.

Redazione, Parliament Takes Commission to Court over Passenger Data. EurActive.com, 22 aprile 2004.

[46] Casi Congiunti C-317/04 e C-318/04, Parlamento Europeo c. Consiglio dell'Unione Europea e Commissione della Comunità Europea [2006] ECR I-04721 in questa *Rivista*, 2006, 761 con nota di D. Maffei, *« Legislazione dell'emergenza » e tutela dei dati personali dei passeggeri: il conflitto Europa-USA*..

Per un commento della sentenza vedi anche V. Papalonstantinou, P. De Hert, *The PNR Agreement and Transatlantic Anti-Terrorism Co-operation: No Firm Human Rights Framework on Either Side of the Atlantic*. Vol. 46, in *Common Market Law Review*, 885-919 (2009).

[47] EDPS Opinion on the Final Report by the EU-Us High Level Contact Group on Information Sharing and Privacy and Personal Data Protection. Paragrafo 22. Disponibile a: *www.edps.europa.eu* (19 febbraio 2010).

Y. Poullet, M.V. Peres Asinan, *Données des voyageurs aériens: le débat Europe - États-Unis*. N. 113 in *Journal des tribunaux, Droit Européen*, 269 (2004).

[48] Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the Signing, on Behalf of the European Union, of an Agreement Between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) (2007 PNR

Agreement). Pubblicato nella Gazzetta Ufficiale dell'Unione Europea L 204/16 il 4 agosto 2007.

Il testo della Decisione è disponibile a: *http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_204/l_20420070804en00160017.pdf* (19 febbraio 2010).

ritti dei soggetti dei dati personali garantiti dalla Direttiva 95/46/CE o dalla Convenzione 108 del Consiglio d'Europa. Questo sarà l'aspetto su cui questa ricerca si concentrerà invece nelle prossime pagine.

6. L'accordo del 2004, l'*interim agreement* e l'accordo del 2007 - cambio del contenuto o solo cambio della base giuridica?

Successivamente alla sentenza della Corte di Giustizia, un nuovo accordo sul PNR è stato concluso tra UE e USA nel 2007, preceduto da un *interim agreement* per permettere la continuazione del trasferimento dei PNR durante il corso delle nuove negoziazioni. L'obbiettivo di questo paragrafo è di confrontare i tre accordi sul PNR stipulati tra la UE e gli Stati Uniti, sottolineando le differenze esistenti tra i tali strumenti in relazione al livello di protezione garantito ai PNR. I temi di maggior rilevanza negli accordi sul PNR tra UE-USA sono stati i seguenti:

a) quali dati dovevano essere raccolti/trasferiti;
b) il trattamento dei dati sensibili;
c) i destinatari dei dati;
d) l'obbiettivo/finalità della raccolta;
e) il tempo di ritenzione dei dati;
f) le forme di raccolta ai dati-sistema di « *pull* » o « *push* »;
g) i diritti dei titolari dei dati personali.

Come menzionato nel paragrafo precedente, il primo accordo sul trasferimento dei dati del PNR tra UE-USA fu stipulato tra il Governo Americano e la Comunità Europea il 28 maggio 2004, a Washington, con l'obbiettivo di regolarizzare i trasferimenti delle informazioni dei PNR per le imprese aeree che operavano i voli dall'Europa agli USA[49]. L'accordo sul PNR del 2004 era inoltre accompagnato dalla decisione di *adeguacy finding* della Commissione Europea, adottata sulla base delle « *undertakings* » (« impegni ») assunti dalla CBP sulle modalità di raccolta e mantenimento dei PNR.

L'accordo del 2004 stabiliva che solamente il CBP aveva accesso ai dati ricevuti tramite tale trasferimento con l'obbiettivo di prevenire e combattere: 1) il terrorismo e i crimini connessi; 2) altri reati gravi, compresa la criminalità organizzata internazionale; e 3) la fuga dall'arresto o da pena detentiva per i suddetti crimini. Il CPB poteva trasferire le informazioni ricevute attraverso l'accordo PNR all'Amministrazione della Sicurezza Pubblica (*Transportation Security Administration*, TSE) con l'unico obbiettivo di permettere a tale istituzione di testare un nuovo sistema computerizzato di pre-screening dei passeggeri aerei, il CAPPS II. Tali limitazioni dell'uso dei PNR potevano essere esentate nei casi di situazioni di emergenza che coinvolgevano la identificazione di un terrorista conosciuto o di un individuo con legami al terrorismo[50]. Fu inoltre chiarito

[49] *Supra*, accordo tra Stati Uniti e Comunità Europea del maggio 2004 per regolare il trasferimento dei PNR.

[50] Undertakings del Department of Homeland Security e Bureau of Customs and Border Protection (CBP). Paragrafi 3 e 8. Il testo del documento è disponibile a *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0535:IT:HTML* (19 febbraio 2010).

che il CBP aveva accesso solo a 34 categorie di dati[51]. In relazione al trattamento dei dati sensibili, l'accordo stabiliva che quest'ultimi non sarebbero stati utilizzati dalla CBP fino all'introduzione di filtri automatici che impedissero il trasferimento di tali dati alla CBP. La CBP garantiva che avrebbe cancellato i dati sensibili accidentalmente raccolti e che non li avrebbe trasferiti alla TSA[52].

Secondo l'accordo, la CBP poteva consultare i PNR relativi ad un volo specifico non prima di 72 ore dalla partenza del volo e poteva ri-consultare il sistema non più di tre volte tra l'accesso iniziale e la partenza del volo. L'accordo prevedeva che sarebbe stata introdotta una procedura informatica che sostituisse il sistema di accesso diretto alla raccolta di dati (*pull*) con un sistema di invio diretto di informazioni alla CBP da parte delle imprese aeree (*push*). Nella ipotesi in cui il CBP fosse informata da altre fonti che una determinata persona potenzialmente pericolosa stesse volando verso gli USA, la CBP poteva consultare le informazioni del PNR in relazione ad uno specifico volo prima delle 72 ore prima della partenza del volo.

In relazione al periodo di ritenzione dei dati, l'accordo sul PNR del 2004 prevedeva che i dati fossero consultabili « online » per un periodo massimo di 7 giorni e che dopo tale periodo i funzionari della CBP autorizzati avrebbero comunque avuto accesso ai dati per un periodo massimo di 3 anni e mezzo. Se i dati non fossero stati consultati manualmente all'interno di tale periodo sarebbero stati distrutti, o in caso contrario sarebbero stati trasferiti in un archivio di « *deletion* », dove sarebbero rimasti fino ad 8 anni, momento in cui sarebbero stati distrutti.

In fine, in relazione ai diritti degli interessati, il CBP, in base alle sue « *undertakings* » si vincolava ad informare i passeggeri delle compagnie aeree a riguardo delle esigenze e dei temi legati al PNR per mezzo del suo sito web, volantini informativi per i passeggeri e altri mezzi di comunicazione. Ad esempio, la CBP avrebbe fornito un'informazione generale a riguardo dell'autorità che avrebbe raccolto i dati, le finalità di tale raccolta, le modalità di protezione e di condivisione dei dati, l'identità del funzionario responsabile, il meccanismo di risarcimento e le informazioni per l'invio di domande e lamentele.

---

[51] Le 34 categorie di PNR trasferite alla CBP erano i seguenti: data di prenotazione del biglietto; data prevista del viaggio; nome del passeggero; indirizzo; informazioni sulla modalità di pagamento del biglietto; indirizzo di fatturazione; recapiti telefonici; itinerario completo del viaggio; informazioni sui viaggiatori abituali « frequent flyer » (miglia percorse e indirizzo); agenzia di viaggi/agente di viaggio che ha venduto il biglietto; informazioni sul *code share* in relazione alla compagnia aerea che ha effettuato il volo in cooperazione con i suoi partners; fase di viaggio del passeggero; indirizzi di posta elettronica; data di emissione del biglietto; osservazioni generali della compagnia aerea sul passeggero; numero del biglietto; numero del posto a sedere; precedenti assenze all'imbarco da parte del passeggero; numero di etichetta dei bagagli; passeggero senza prenotazione; informazioni OSI; informazioni SSI/SSR; informazioni sulle modifiche cronologiche del PNR; indicazione dei biglietti di sola andata; informazioni APIS (Advanced Passenger Information System) e ATFQ (Automatic Ticketing Fare Quote Field).

Allegato A alle Undertakings del Department of Homeland Security Bureau of Customs and Border Protection (CBP). Il testo del documento è disponibile a: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0535:IT:HTML* (19 febbraio 2010).

[52] *Supra*, par. 8, 9, 10 e 11 delle Undertakings.

Sulla base delle *undertakings* del CBP, le richieste dei titolari dei dati per ottenere una copia dei dati del PNR mantenuti nell'archivio del CBP sarebbero state elaborate sulla base della legislazione americana in materia di accesso ai dati detenuti dalle istituzioni pubbliche (il *Freedom of Information Act*, FOIA)[53]. Questa legislazione permetteva al CBP di negare o posticipare l'accesso a tali informazioni in circostanze eccezionali, se tale accesso « sia tale da interferire con procedimenti penali o qualora essa sveli le tecniche e le procedure relative ad indagini, con il conseguente pericolo di elusione della legge »[54]. L'accordo sul PNR del 2004 prevedeva che il CBP avrebbe rettificato i dati personali raccolti, a richiesta dei titolari dei dati o delle autorità nazionali di protezione dei dati. Nel caso in cui la richiesta di rettifica presentata non fosse stata accolta, il titolare dei dati avrebbe potuto presentare un appello al « *Chief Privacy Officer* » del Dipartimento « dell'*Homeland Security* » (Dipartimento per la Sicurezza Nazionale, DHS, a cui il CBP era sottoposto). Il « *Chief Privacy Officer* » si sarebbe impegnato al fine di risolvere il reclamo presentato.

L'accordo descritto in queste pagine fu annullato dalla Corte Europea di Giustizia, in ragione della sua scorretta base legale. Tale sentenza obbligò gli USA e l'Unione Europea di adottare una misura « provvisoria » che permettesse la continuazione del trasferimento dei dati PNR da parte delle compagnie aeree agli USA. La misura provvisoria si concretizzò nella conclusione di un accordo temporaneo (« *interim agreement* ») tra UE e USA. L'accordo fu concluso nell'ottobre 2006, firmato il giorno 16 in Lussemburgo e il 19 a Washington[55].

L'*interim agreement*, prevedeva il cambiamento della base legale e conseguentemente il cambiamento di una delle parti (che passò ad essere l'Unione Europea in sostituzione della Comunità Europea). Tuttavia, da un punto di vista sostanziale l'accordo poco alterò il precedente accordo del 2004. È necessario sottolineare, tuttavia, che l'accordo transitorio allargò il numero dei destinatari dei dati, includendo tra quest'ultimi oltre al CBP, l'ufficio federale americano per l'immigrazione (« *US Immigration and Customs Enforcement Department* »), il Dipartimento di Stato e altre entità direttamente legate a quest'ultimo. Invece non furono inclusi tra i destinatari dei PNR gli altri dipartimenti inclusi nel DHS[56].

È importante sottolineare inoltre che l'*interim agreement* fu successivamente modificato in ragione di una lettera inviata dal DHS alla Presidenza del Consiglio e alla Commissione Europea[57]. Nella missiva il Dipartimento

[53] The Freedom of Information Act, 5 U.S.C. § 552, as amended by Electronic Freedom of Information Act of 1996, No. 104-231, 110 Stat. 3048.

Il FOIA regola il diritto di accesso dei cittadini americani ai documenti detenuti dale autorità federali americane.

[54] *Supra*, par. 37 e 38 delle Undertakings.

[55] Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security. Firmato a Washington il 19 ottobre 2006. Il testo dell'accordo è disponibile a: *http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/2006_10_accord_US_en.pdf* (19 febbraio 2010).

[56] Ad esempio, furono esclusi dal ricevimento dei dati il *Citizenship and Immigration Services, Transportation Security Administration, United States Secret Service, United States Coast Guard e Federal Emergency Management Agency*.

[57] Letter to the Council Presidency and the Commission from the Department of Homeland Security (DHS) of the United States of America, concerning the interpretation of certain provisions of the underta-

Americano per la Sicurezza Nazionale presentò una sua interpretazione di alcuni punti contenuti nelle *undertakings* del CBP del 2004 e comunicò l'adozione di alcuni nuovi strumenti normativi che avrebbero di fatto modificato il valore delle *undertakings* La Commissione ed il Consiglio hanno prontamente risposto a tale missiva, accettando senza alcuna restrizione le richieste americane[58]. A partire dal momento dello scambio di tale corrispondenza l'*interim agreement* doveva essere interpretato alla luce della nuova interpretazione offerta dal « *Department of Homeland Security* »[59].

Una prima modifica di rilievo apportata dallo scambio di missive rispetto al contenuto dell'*interim agreement* riguardava i destinatari dei PNR. Sulla base della missiva, il DHS avrebbe potuto condividere i PNR con ogni altra agenzia federale americana responsabile per prevenire e combattere il terrorismo e i crimini collegati[60]. Il DHS dichiarò che prima

---

kings issued by DHS on 11 May 2004 in connection with the transfer by air carriers of passenger name record (PNR) data (2006/C 259/01). La lettera è disponibile a: *http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/2006_10_letter_DHS_en.pdf* (19 febbraio 2010).

[58] Reply by the Council Presidency and the Commission to the Letter from the USA's Department of Homeland Security (2006/C 259/02). Il testo della lettera è disponibile a: *http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/pnr/2006_10_letter_council_reply_en.pdf* (19 febbraio 2010).

[59] *Supra*, V. Papakonstantinou, P. De Hert, Pag. 905: « *The Interim PNR Agreement contained essentially the same provisions as its predecessor of 2004; it is nevertheless its reading in combination with a Side Letter by the DHS (which was officially annexed to the Council's Decision adopting the Interim PNR Agreement, and was referred to in its text) which had raised substantial concerns on its actual effectiveness in protecting individual privacy.* » (« L'Accordo *Interim* sul PNR conteneva essenzialmente le stesse clausole del suo predecessore del 2004; tuttavia, è la sua lettura in combinazione con la Lettera inviata dal DHS (che è stata ufficialmente allegata alla Decisione del Consiglio di adottare l'Interim Agreement, e a cui la Decisione fa' riferimento nel suo testo) che ha creato numerose perplessità a riguardo della sua attuale effettività nella protezione della privacy dei passeggeri aerei »).

[60] « *Pursuant to Paragraph 35 of the Undertakings (which states that "No statement in these Undertakings shall impede the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law" and allows DHS to "advise the European Commission regarding the passage of any U.S. legislation which materially affects the statements made in these Undertakings"), the U.S. has now advised the EU that the implementation of the Information Sharing Environment required by the Act and the Executive Order described above may be impeded by certain provisions of the Undertakings that restrict information sharing among U.S. agencies, particularly all or portions of paragraphs 17, 28, 29, 30, 31, and 32. In light of these developments and in accordance with what follows, the Undertakings should be interpreted and applied so as to not impede the sharing of PNR data by DHS with other authorities of the U.S. government responsible for preventing or combating of terrorism and related crimes as set forth in Paragraph 3 of the Undertakings* ».

« Sulla base del Paragrafo 35 delle Undertakings della CBP del 2004 (che afferma che "Le Undertakings non impediranno l'uso o la divulgazione dei PNR in ogni procedimento penale o dove così richiesto dalla legge americana" e permette al DHS di "informare la Commissione Europea a riguardo dell'adozione di ogni legislazione americana che materialmente ha un impatto su queste Undertakings") gli Stati Uniti hanno così comunicato all'Unione Europea che l'applicazione dell'Information Sharing Environment richiesto dall'Act e dell'Executive Order descritti sopra possono essere impediti da alcune clausole delle Undertakings che restringono la possibilità di condividere informazioni tra le agenzie americane, in particolare in relazione ai paragrafi 17,28, 29, 30, 31 e 32 delle Undertakings. Alla luce di questi sviluppi le Undertakings dovrebbe essere interpretate e applicate in modo da non ostacolare il trasferimento dei PNR da parte del DHS alle altre agenzie parte del Governo americano responsabili per la prevenzione e la lotta contro il terro-

di condividere le informazioni del PNR si sarebbe assicurato che le istituzioni che avrebbero ricevuto i dati avrebbero garantito un livello di protezione dei dati comparabile a quello offerto dal DHS. In particolare, il DHS avrebbe controllato il rispetto della limitazione degli usi, tempi di mantenimento dei dati, utilizzo dei dati per altre finalità da quelle della raccolta, il livello di sicurezza e le sanzioni per punire abusi, e l'introduzione di un procedimento per permettere ai titolari dei dati di esercitare i diritti previsti dall'*undertaking* del 2004.

Inoltre, il DHS avrebbe potuto tramite il sistema di « *push* » ottenere informazioni sui PNR illimitatamente, anche in relazione ad un momento anteriore rispetto alle 72 ore prima della partenza del volo. Il DHS chiarificò che in relazione alle informazioni relative ai programmi di « *Frequent Flyer* », il DHS avrebbe raccolto non solo il conto delle miglia e gli indirizzi dei passeggeri, ma anche i numeri di telefono, le emails, il numero del programma di « *Frequent Flyer* », in quanto tali informazioni potevano avere un importante valore per la lotta contro il terrorismo[61]. Tale alterazione « unilaterale » pose alla luce il fatto che la limitazione a 34 PNR raccolti inclusa nella precedente *undertakings* del CBP del 2004 aveva un valore puramente indicativo[62].

Infine, il DHS sottolineò nella sua lettera che avrebbe collezionato ed elaborato informazioni relative alle condizioni di salute dei passeggeri. Tali informazioni « sensibili » erano raccolte al fine di proteggere « gli interessi vitali dei titolari dei dati e delle altre persone ». In tale contesto, il

rismo e i crimini connessi elencati nel paragrafo 3 delle Undertakings ».

Supra, Lettera inviata dal DHS alla Commissione e al Consiglio dell'Unione Europea del 2006.

L'Information Sharing Environment era una nuova strategia adottata dal DHS per rafforzare la cooperazione tra le varie agenzie di intelligence americane rafforzando lo scambio di informazioni tra quest'ultime. L'accordo sul PNR del 2004 impediva al DHS di condividere i PNR con altre agenzie governative e si poneva quindi in contrasto con la nuova strategia di lotta contro il terrorismo. Per tale ragione gli USA cercarono di re-interpretare le clausole delle Undertakings del 2004 per mezzo della lettera inviata nel 2006 dal DHS. Ulteriori informazioni sulla strategia di Information Sharing Environment sono disponibili a: *http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf* (19 febbraio 2010).

[61] « *The frequent flyer field may offer addresses, telephone numbers, email addresses; all of these, as well as the frequent flyer number itself, may provide crucial evidence of links to terrorism. Similarly, information about the number of bags carried by a passenger may have value in a counterterrorism context. The Undertakings authorize DHS to add data elements to the 34 previously set forth in Attachment A of the Undertakings, if such data is necessary to fulfill the purposes set forth in paragraph 3. With this letter the U.S. has consulted under Paragraph 7 with the EU in connection with item 11 of Attachment A regarding DHS's need to obtain the frequent flier number… ».*

« Il campo di frequent flyer può offrire indirizzi, numeri di telefono, indirizzi emails; queste informazioni, insieme al numero di frequent flyer, possono offrire prove cruciali di collegamenti al terrorismo. Allo stesso modo, le informazioni riguardanti il numero di bagagli del passeggero possono avere valore in un contesto di anti-terrorismo. Le Undertakings permettono al DHS di aggiungere dati alle 34 categorie di dati elencate nell'Allegato A delle Undertakings, se tali dati siano necessari per soddisfare gli obbiettivi elencati nel paragrafo 3. Per mezzo di questa lettera il Governo americano ha consultato sulla base del Paragrafo 7 l'Unione Europea in relazione all'undicesimo tipo di PNR menzionato nell'Allegato A riguardante la necessità del DHS di ottenere il numero di frequent flyer… ».

Supra, Lettera inviata dal DHS alla Commissione e al Consiglio dell'Unione Europea del 2006.

[62] *Supra*, V. Papakonstantinou, P. De Hert, 906.

DHS avrebbe iniziato a raccogliere i dati che potevano « identificare, localizzare, informare e respingere, le persone che erano esposte a pericolose malattie contagiose … »[63].

Nel 2007 gli UE e gli USA hanno concluso un accordo definitivo sul trasferimento del PNR; accordo attualmente in vigore[64]. Nell'accordo del 2007 si possono identificare alcune alterazioni nel contenuto dell'accordo rispetto al precedente *interim agreement* e alla successiva lettera del DHS.

Una prima alterazione contenuta nell'accordo del 2007 rispetto all'accordo del 2004 ha riguardato l'uso dei PNR. Secondo il nuovo accordo, i PNR potevano essere utilizzati per proteggere gli interessi vitali dei titolari dei dati o di altre persone, o in qualsiasi procedimento penale, o quando « così richiesto per legge »[65]. La missiva allegata all'accordo prevedeva che il DHS avrebbe comunicato all'Unione Europea qualunque nuova legge americana che avrebbe materialmente modificato le condizioni di uso dei PNR elencati nella missiva. Pertanto, gli Stati Uniti erano di fatto liberi di modificare unilateralmente i termini dell'accordo sul PNR del 2007.

Inoltre il numero dei possibili destinatari delle informazioni contenute nei PNR aumentò significativamente rispetto all'accordo del 2004 e all'*interim agreement*. Il DHS poteva condividere i PNR con tutte le agenzie governative americane che avevano funzioni di « applicazione della legge » (« *law enforcement* ») e compiti di tutela della pubblica sicurezza. Ad esempio, il DHS poteva trasferire i PNR alle agenzie federali che si occupavano di lotta o prevenzione del terrorismo e crimini transnazionali, includendo minacce, voli, individui e « rotte aeree di preoccupazione » (« *routes of concern* ») sui cui tali agenzie stavano indagando[66].

L'accordo del 2007 ha inoltre introdotto la possibilità che tali informazioni fossero trasmesse a Paesi terzi, in seguito alla verifica degli usi che sarebbero stati fatti dei dati da parte dei destinatari e della loro capacità di proteggere tali informazioni. Il DHS dichiarò che, con l'eccezione di situazioni di emergenza, qualsiasi trasferimento dei dati a Paesi terzi sa-

---

63 « *Recognizing the potential importance of PNR data in the context of infectious disease and other risks to passengers, DHS reconfirms that access to such information is authorized by paragraph 34, which provides that the Undertakings must not impede the use of PNR for the protection of the vital interests of the data subject or of other persons or inhibit the direct availability of PNR to relevant authorities for the purposes set forth in Paragraph 3 of the Undertakings…* ».

« Riconoscendo la potenziale importanza dei PNR nel contesto delle malattie infettive e di altri rischi per i passeggeri, il DHS conferma che l'accesso a tali informazioni è autorizzato dal paragrafo 34, che prevede che le Undertakings non devono impedire l'uso dei PNR per la protezione degli interessi vitali del soggetto dei dati e di altre persone o inibire la disponibilità diretta dei PNR alle autorità pubbliche interessate per le finalità menzionate nel paragrafo 3 delle Undertakings… ».

Supra, Lettera inviata dal DHS alla Commissione e al Consiglio dell'Unione Europea del 2006.

64 Agreement Between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement). L'accordo fu firmato a Bruxelles il 23 luglio 2007 e a Washington il 26 luglio 2007.

Il testo dell'accordo è disponibile a: *http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_204/l_20420070804en00180025.pdf* (19 febbraio 2010).

65 *Supra*, lettera del DHS allegata all'accordo sul PNR del 2007. Par. I.

66 *Supra*, lettera del DHS allegata all'accordo sul PNR del 2007. Par. II.

rebbe dipeso da le « *understandings* » tra le parti contraenti, e doveva incorporare lo stesso sistema di protezione dei dati applicato dal DHS nell'accordo UE-USA sul PNR[67].

Per quanto riguarda le informazioni che dovevano essere raccolte, i campi furono ridotti a 19 rispetto ai 34 contenuti nei precedenti PNR[68]. Tuttavia, in realtà, tale riduzione corrispose ad un allargamento delle informazioni in quanto si riferivano a campi più generici. Pertanto, non ci fu alcuna riduzione reale del volume (se non un accrescimento) delle informazioni a cui il governo americano poteva avere accesso per mezzo dell'accordo EU-US[69]. Reiterando ciò che era stato incluso nella lettera allegata all'accordo ad interim sul PNR, l'accordo del 2007 prevedeva la possibilità per il DHS di avere accesso anche ad ulteriori dati personali rispetto alle informazioni elencate nell'accordo sul PNR, inclusi dati sensibili, in situazioni eccezionali nelle quali la vita del titolare dei dati o di soggetti terzi fosse stata in pericolo (« imperilled or seriously impaired »). In tal caso il DHS avrebbe informato la Commissione Europea che tali dati erano stati consultati.

Il periodo di raccolta dei dati fu ugualmente modificato. I dati sarebbero stati mantenuti nella banca dati del DHS per un periodo di 7 anni[70]. Successivamente, sarebbero stati trasferiti in un'ulteriore banca dati il cui accesso era maggiormente ristretto (dati dormienti) per un periodo di 8 anni. Pertanto, il DHS avrebbe conservato ogni PNR per un periodo totale di 15 anni. Tuttavia, i dati relativi ad un caso specifico sotto inchiesta, erano ritenuti nella banca dati fino al completamento dell'inchiesta o alla sua archiviazione. Tale modifica aveva valore retroattivo, in quanto si applicava anche ai dati raccolti sulla base del primo accordo del 2004[71].

Si può concludere, pertanto, dal primo accordo sul PNR del 2004 all'accordo sul PNR del 2007 attualmente in vigore ci sono state alcune significative modifiche del contenuto dell'accordo, con un ampliamento del numero dei destinatari delle informazioni, dei tipi di informazioni rese disponibili (incluso l'accesso ai dati sensibili), delle finalità di raccolta e trattamento di tali dati, e in relazione alla possibilità che tali dati siano resi disponibili a Paesi terzi. Tali modifiche espongono inevitabilmente a maggiori rischi di abusi i dati personali dei cittadini europei che viaggiano verso gli USA[72].

---

[67] *Supra*, lettera del DHS allegata all'accordo sul PNR del 2007. Par. II.

[68] *Supra*, lettera del DHS allegata all'accordo sul PNR del 2007. Par. III.

[69] Gruppo di Lavoro 29, Parere 5/2007 Relativo al Nuovo Accordo tra l'Unione Europea e gli Stati Uniti d'America sul Trattamento e sul Trasferimento dei Dati del Codice di Prenotazione (Passenger Name Record, PNR) da Parte dei Vettori Aerei al Dipartimento per la Sicurezza Interna degli Stati Uniti Concluso nel luglio 2007. Pag. 10. Disponibile a: *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp138_it.pdf* (19 febbraio 2010).

« Mentre il Gruppo di lavoro ha chiesto insistentemente di ridurre il numero degli elementi di dati considerati necessari nella lotta contro il terrorismo e la criminalità correlata, il nuovo accordo amplia l'elenco chiedendo maggiori informazioni sugli interessati. Questa modifica non si giustifica in alcun modo e deve essere considerata sproporzionata ».

[70] *Supra*, lettera del DHS allegata all'accordo sul PNR del 2007. Par. VII.

[71] « The above mentioned retention periods also apply to EU PNR data collected on the basis of the Agreements between the EU and the U.S., of May 28, 2004 and October 19, 2006 ».

Ibid.

[72] *Supra*, Gruppo di Lavoro 29, Parere 5/2007. Pag. 2, 3.

7. L'adeguatezza dell'accordo PNR 2007 alla Convenzione 108 del Consiglio d'Europa.

Nell'ultima parte dell'analisi si valuteranno la compatibilità dell'accordo sul PNR del 2007 con la Convenzione n. 108 del Consiglio d'Europa del 1981 relativa alla protezione dei dati personali trattati tramite processi automatizzati. La Convezione 108/81, nonostante non sia un documento della UE, ha incidenza nel trasferimento dei dati oggetto dell'accordo sul PNR, in quanto tutti gli Stati Membri della UE sono firmatari e hanno ratificato tale Convenzione. Di conseguenza, secondo Poulet e Peres Asinan, nonostante l'accordo sul PNR del 2007 non dovesse più necessariamente rispettare i principi della Direttiva 95/46/CE, in quanto adottato sulla base di una Decisione del Consiglio del terzo pilastro del Trattato dell'Unione Europea, tale accordo doveva comunque rispettare i principi contenuti nella Convenzione del Consiglio d'Europa 108/81[73]. Inoltre, la Convenzione tiene applicazione a qualsiasi tipo di trattamento automatico dei dati personali, sia nella sfera pubblica che privata. Nel corso delle prossime pagine si considererà inoltre la Raccomandazione R (87) 15 del Comitato dei Ministri del Consiglio d'Europa, la quale regola il trattamento dei dati personali nell'attività di polizia, includendo anche misure relative al trasferimento dei dati personali a Paesi terzi per tale proposito[74]. Nonostante la Raccomandazione 87/15 non abbia valore vincolante, è stata firmata da tutti gli Stati Membri dell'Unione Europea. Secondo l'opinione del Garante Europeo per la Protezione dei Dati questo fattore fornisce autorevolezza a questo documento, che deve essere usato come strumento interpretativo del contenuto della Convenzione 108/81 in relazione allo scambio di dati personali per le attività di cooperazione tra organi di polizia[75].

I contenuti di maggiore rilevanza della Convezione 108/81 e della Raccomandazione 87/15 in riferimento agli accordi sul PNR tra UE e USA sono i seguenti:

a) quali dati devono essere raccolti/trasferiti;
b) il trattamento dei dati sensibili;
c) i destinatari dei dati;
d) il proposito/finalità della raccolta;
e) il tempo di raccolta dei dati;

---

[73] *Supra*, Y. Poullet, M.V. Peres Asinan, 274.

[74] Council of Europe, Recommendation No. R (87) 15 of The Committee of Ministers to Member States Regulating The Use of Personal Data in the Police Sector. Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies. Il testo della Raccomandazione è disponibile a: *http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Rec_1987_15.pdf* (19 febbraio 2010).

[75] « *For activities within the area of police and judicial cooperation all Member States have subscribed to Recommendation No R (87) 15, which specifies Convention 108 to a certain extent for the police sector, but it is not a binding legal instrument* ».

« In relazione alle attività di polizia e di cooperazione giudiziaria tutti gli Stati Membri hanno firmato la Raccomandazione No R (87) 15, che chirarifica il contenuto della Convenzione 108 per le attività di polizia, nonostante quest'ultimo non sia uno strumento legale vincolante ».

European Data Protection Supervisor, Third Opinion on the Proposal for a Council Framework Decision on the Protection of Personal Data Processed in the Framework of Police and Judicial Co-operation in Criminal Matters. 2007/C 139/01.

f) i diritti dei titolari dei dati;

g) il sistema di consultazione dei dati (sistema di « pull » o « push »).

Tali elementi rappresentano i cardini della nostra analisi per la verifica dell'adeguatezza dell'accordo sul PNR del 2007 alla Convezione 108/81 e alla Raccomandazione 87/15.

Per quanto riguarda i dati sensibili, che sono stati raccolti a partire dall'accordo ad interim sul PNR, la Convenzione 108/1981 prevede salvaguardie speciali per il trattamento di tali dati. Il trattamento dei dati sensibili doveva essere proibito come regola generale nelle legislazioni nazionali, con un'eccezione prevista per l'utilizzo dei dati per la conduzione di procedimenti penali. La Raccomandazione 87/15 prevede che il trattamento dei dati sensibili nel settore penale « deve essere assolutamente necessario per i fini di una specifica indagine »[76]. L'accordo sul PNR del 2007 prevede come regola generale che i dati sensibili non siano utilizzati, salvo nel caso eccezionale « nel quale la vita del titolare dei dati o di altri individui possa essere in pericolo o seriamente minacciata »[77]. A prima vista tale utilizzazione « eccezionale » dei dati sensibili pare essere compatibile tanto con la Convenzione quanto con la Raccomandazione. Tuttavia, ad un'analisi più accurata della clausola che regola il trattamento dei dati sensibili nell'accordo sul PNR del 2007, si nota che tali dati sarebbe sempre disponibili per il DHS. Il DHS, infatti, rimane libero di decidere quando avere accesso a tali informazioni. Pertanto, esiste un rischio di abusi dell'utilizzo di tale eccezione. Sulla base dell'accordo del 2007 la UE non possiede alcun mezzo per limitare il possibile uso indebito di tali dati da parte del DHS. L'unica soluzione ad una possibile « violazione » dei termini dell'accordo da parte delle autorità americane sarebbe la rescissione dell'accordo e la revoca del riconoscimento di « adeguatezza » del livello di protezione dei PNR trasferiti alle autorità americane.

Per quanto riguarda i diritti dei *data subjects* la Convenzione riconosce nel suo articolo 8 il diritto di accesso, rettifica, cancellazione e la necessità di creare rimedi che garantiscano l'esercizio di tali diritti. È importante sottolineare che la Convenzione nel suo articolo 9 prevede la possibilità di restringere le garanzie previste dagli articoli 5, 6 e 8 (relativi alla qualità dei dati, alle categorie speciali di dati, e alle salvaguardie previste per l'interessato) se tali restrizioni siano un mezzo necessario in una società democratica con l'obbiettivo di « proteggere la sicurezza nazionale, la sicurezza pubblica, gli interessi monetari dello Stato o per combattere i crimini ». In relazione alle attività di polizia, la Raccomandazione 87/15 stabilisce che i diritti degli interessati non possono essere ristretti, a meno che « tale restrizione sia indispensabile per l'esecuzione di un compito legale della polizia o sia necessaria per la protezione del soggetto dei dati o per la protezione dei diritti e le libertà di soggetti terzi)[78]. Nell'accordo del 2007 il Governo Americano ha esteso ai cittadini non americani l'applicazione del FOIA il quale non era menzionato negli accordi precedenti, eliminando quindi la discriminazione precedentemente esistente tra i cittadini americani e non americani. Tuttavia, l'accordo sul PNR del 2007 non

[76] *Supra*, Raccomandazione 87/15, par. 2.4.

[77] *Supra*, lettera inviata dal Governo Americano all'Unione Europea e allegata all'accordo sul PNR del 2007.

[78] *Supra*, Raccomdnazione 87/15, par. 6.4.

ha previsto alcun mezzo pratico per permettere agli interessati di poter esercitare effettivamente i loro diritti di rettifica e cancellazione nei casi in cui i propri dati siano non corretti. Pertanto, in relazione a questo aspetto l'accordo del 2007 sembra non soddisfare adeguatamente i principi di protezione dei dati previsti dalla Convenzione 108/1981 e dalla Raccomandazione 87/15.

L'Articolo 5(e) della Convezione 108/1981 prevede che i dati siano trattenuti nella banca dati solo per il tempo necessario per raggiungere la finalità per la quale i dati sono stati raccolti. Anche la Raccomandazione prevede che i dati personali raccolti per fini di attività di polizia debbano essere cancellati quando il loro utilizzo non sia più necessario ai fini delle indagini. Il secondo paragrafo dell'Articolo 7(1) della Raccomandazione prevede dei criteri per valutare se un dato non sia più necessario e, pertanto, se quest'ultimo debba essere cancellato. In particolare, « regole che mirino a fissare i periodi massimi di immagazzinamento per le varie categorie di dati personali, così come regole che stabiliscano verifiche regolari della qualità dei dati, devono essere fissate dalla legislazione nazionale e il loro rispetto deve essere controllato dalle autorità di controllo nazionali »[79]. L'accordo sul PNR del 2007 stabilisce, in conformità a quanto previsto dagli accordi precedenti, che i dati siano archiviati per un periodo di sette anni in una banca dati consultabile, e per un ulteriore periodo di otto anni in una banca dati non consultabile direttamente (dati dormienti). I dati consultati per la finalità di condurre una specifica indagine possono essere archiviati per un periodo di tempo maggiore, « fino a quando il caso sotto inchiesta non sia archiviato », non esistendo quindi un tempo massimo al mantenimento di tali dati. Tale norma appare chiaramente in contrasto con quanto previsto dalla Convenzione e dalla Raccomandazione. Il fatto che i dati di tutti i passeggeri europei che volano verso gli USA siano trattenuti per un periodo totale di 15 anni, indipendentemente dal fatto che siano utilizzati per un'indagine o meno, a nostro avviso non si inquadra nella definizione di « necessità » prevista dalla Raccomandazione 87/15 e dalla Convezione 108/1981[80].

Un altro elemento da analizzare riguarda il trasferimento dei dati personali raccolti per la finalità di combattere la criminalità a soggetti terzi, distinti dal soggetto che ha raccolto tali dati. Nel caso dell'accordo sul PNR tale trasferimento è svolto dal Governo Americano. I dati sono raccolti all'interno del territorio della UE da parte di soggetti privati quali le compagnie aeree, e successivamente trasferiti alle autorità americane. L'Articolo 13(3)(a) della Convenzione 108/81 prevede che i dati possano essere trasferiti all'esterno del territorio dei Paesi Membri solo sulla base del principio di « equivalenza » del livello di protezione dei dati personali assicurato nel Paese di destinazione rispetto al livello di protezione garantito dalla legislazione del Paese da cui i dati sono stati trasferiti. La Raccomandazione 87/15 prevede che il trasferimento dei dati personali ad auto-

---

[79] *Supra*, Risoluzione 87/15, par. 7.2, § 2°.

[80] *Supra*, Gruppo di Lavoro 29, Parere 5/2007. Pag. 12.

« Il Gruppo di lavoro ha già giudicato eccessivo conservare i dati per tre anni e sei mesi tenuto conto delle finalità per cui sono conservati. Non è stato dimostrato in alcun modo che tale periodo è necessario (come prescrive l'articolo 8 della Convenzione europea dei diritti dell'uomo), o che è troppo breve ».

rità straniere di Paesi non Membri del Consiglio di Europea debba essere limitata solo ai casi in cui: *a*) tale trasferimento sia previsto da una « normativa nazionale o internazionale »; o *b*) « se il trasferimento sia necessario per la prevenzione di un serio e imminente pericolo o sia necessario per la soppressione di un grave reato penale, e che tale comunicazione non pregiudichi la regolamentazione nazionale per la protezione dei diritti dell'individuo »[81]. La Raccomandazione prevede inoltre che i dati possano essere utilizzati per fini distinti da quelli inizialmente raccolti, se l'autorità che trasferisce i dati è d'accordo con tale utilizzo[82], nonostante questa possibilità costituisca un'eccezione rispetto alla regola generale che proibisce l'utilizzazione dei dati per fini distinti da quelli per i quali i dati sono stati inizialmente raccolti[83]. Nel caso del trasferimento dei PNR non si tratta di una cooperazione tra due organi di polizia o di autorità pubbliche di Paesi differenti, ma piuttosto di un obbligo legale di trasferimento dei PNR dei passeggeri imposto da un Paese terzo (gli USA) alle imprese private che operano i voli verso gli Stati Uniti e che hanno raccolto tali dati all'interno del territorio della UE. Inoltre, tali informazioni sono state inizialmente raccolte dalle compagnie aeree per fini commerciali, piuttosto che con l'obbiettivo di combattere attività criminali. A nostro giudizio, il trasferimento dei dati personali verso Paesi terzi che non assicurano livelli di protezione esattamente compatibili con quelli previsti dalla Convenzione 108/81 rappresenterebbe un'eccezione, piuttosto che una regola, come invece sembra essere il caso nell'accordo tra UE ed USA per il trasferimento dei PNR.

Come menzionato precedentemente, l'accordo sul PNR del 2007 allargò notevolmente il numero dei destinatari delle informazioni, rendendolo quasi illimitato. Infatti, i PNR potevano essere ri-trasferiti dal DHS verso altre autorità americane o verso Paesi terzi, pregiudicando pertanto l'esercizio dei propri diritti agli interessati. Inoltre, le finalità per le quali i dati sarebbero trattati sono state anch'esse allargate. Di conseguenza, i PNR potrebbero essere potenzialmente utilizzati per finalità molto distinte rispetto ai fini per quali sono stati trasferiti al DHS. I PNR, infatti, potrebbero essere utilizzati « quando necessario per la protezione degli interessi vitali degli interessati o di altre persone, o in qualsiasi procedimento penale, o quando previsto dalla legge ». Pertanto, il Governo americano deciderà per quali fini i PNR trasferiti potranno essere ri-utilizzati sulla base di una legislazione federale americana[84]. La Convenzione 108/81 stabilisce chiaramente che i dati personali devono essere « raccolti per specifici e legittime finalità e non utilizzati in modo incompatibile con tali finalità ». I dati raccolti devono essere « adeguati, rilevanti e non eccessivi in relazione alle finalità per le quali sono stati raccolti ». Il ri-utilizzo dei PNR per finalità non precedentemente determinate e non compatibili con le finalità per le quali tale dati sono stati raccolti dimostra ulteriormente l'incompatibilità dell'accordo sul PNR del 2007 con la Convenzione 108/81 e con la Raccomandazione 87/15.

Nonostante gli aspetti negativi dell'accordo sul PNR del 2007 in relazione al livello di protezione dei dati dei passeggeri aerei, un aspetto posi-

[81] *Supra*, Raccomandazione 87/15, par. 5.4.
[82] *Supra*, Raccomdnazione 87/15, par. 5.5.
[83] *Supra*, raccomandazione 87/15, par. 5.5.iii.
[84] *Supra*, lettera inviata dal Governo Americano all'Unione Europea e allegata all'accordo sul PNR del 2007.

tivo di tale accordo deve comunque essere sottolineato. L'accordo ha permesso la transizione da un sistema di « pull » di trasferimento dei PNR ad un sistema di « push ». Tuttavia, l'accordo del 2007 non prevede tempi certi né un meccanismo di controllo per assicurarsi che tutte le compagnie aeree implementeranno il nuovo sistema di trasferimento di PNR. Tale mancanza limita pertanto la rilevanza del nuovo sistema di trasferimento dei dati previsto dall'accordo del 2007 in relazione al livello di protezione dei dati trasferiti[85].

8. Conclusioni e prospettive sul futuro dell'accordo.

Come sottolineato nell'introduzione, nel mondo attuale esiste una costante necessità di raggiungere un equilibrio tra l'esigenza di sicurezza della collettività con il diritto alla protezione dei dati personali. Le negoziazioni sul trasferimento del PNR rappresentano un chiaro esempio in cui l'esigenza di sicurezza della collettività ha prevalso sul diritto individuale alla protezione della propria privacy e dei propri dati personali. Come sottolineato nelle pagine precedenti, dal primo accordo del 2004 a quello attualmente in vigore del 2007 l'esigenza di protezione della sicurezza nazionale è via via prevalsa rispetto al diritto dei passeggeri aerei in volo verso gli Stati Uniti di proteggere i propri dati personali. In particolare, il DHS ha ottenuto una maggiore discrezione in relazione alla possibilità di trasferire i PNR anche ad altre agenzie governative americane e a Paesi terzi con finalità di lotta al terrorismo. Inoltre, l'accordo del 2007 ha di fatto allargato le categorie di PNR a cui il DHS poteva avere accesso rendendo i campi del PNR più generici, includendo anche l'accesso ai dati sensibili in determinati casi, e allungato i tempi di ritenzione dei dati fino a 15 anni. Il fatto che l'accordo del 2007 sia stato concluso sulla base di una Decisione del Consiglio all'interno del terzo pilastro del Trattato dell'Unione Europea piuttosto che sulla base di un atto Comunitario come nel 2004 non giustifica comunque un tale rilassamento della protezione del diritto alla privacy dei passeggeri aerei europei. La Convenzione 108 del Consiglio d'Europea resta comunque applicabile a tutti i Paesi Membri dell'Unione Europea che hanno ratificato la Convenzione e firmato la Raccomandazione 87/15.

Il dibattito sul trasferimento dei PNR non si è concluso con l'accordo del 2007. L'accordo resterà in vigore per un periodo di sette anni dal momento della sua entrata in vigore[86]. L'accordo sarà quindi in vigore fino al 2013. Nel mentre, l'accordo sarà soggetto a revisioni periodiche da parte della Commissione Europea e del DHS[87]. La speranza è che nelle future

---

[85] *Supra*, Gruppo di Lavoro 29, Parere 5/2007. Pag. 11.

[86] *Supra*, Accordo sul PNR 2007, par. 9.

[87] Communication from the Commission to the Council, the European Parliament, the European Economic And Social Committee and the Committee of the Regions Justice, Freedom and Security in Europe since 2005: An Evaluation Of The Hague Programme And Action Plan - General overview of instruments and deadlines provided in the Hague Programme and Action Plan in the fields of justice, freedom and security.

È disponibile a: *http://ec.europa.eu/justice_home/doc_centre/doc/sec_2009_767_en.pdf* (19 febbraio 2010).

Secondo la tabella inclusa a 64 della Comunicazione, la Commissione Europea do-

revisioni dell'accordo si possa raggiungere un migliore equilibrio tra l'esigenza di protezione della sicurezza nazionale e dei dati personali. Almeno tre fattori sembrano indicare che ci possano essere migliori prospettive future per raggiungere un accordo più bilanciato.

Innanzitutto, la nuova amministrazione americana sembra oggi maggiormente consapevole che la protezione della sicurezza nazionale non può annullare la protezione di un diritto fondamentale come il diritto alla privacy. Il nuovo Segretario dell'US Department of Homeland Security, Janet Napolitano, ha recentemente espresso parole concilianti in relazione ad una revisione dell'accordo sul PNR con la UE: « Prevedevamo questa revisione (dell'accordo sul PNR). Sono a vostra completa disposizione per fissare una data (per iniziare le negoziazioni con la Commissione Europea) per chiarire una serie di incomprensioni e per superare i problemi relativi al trasferimento del PNR »[88].

In secondo luogo, l'entrata in vigore del Trattato di Lisbona il 1 dicembre 2009 ha apportato due cambiamenti importanti. Da un punto di vista istituzionale, l'abolizione della struttura a pilastri permetterà un maggiore coinvolgimento del Parlamento Europeo nelle future negoziazioni per una revisione dell'accordo. Sulla base dell'Art. 87(2) del Trattato sul Funzionamento dell'Unione Europea, il Consiglio ed il Parlamento adotteranno sulla base della procedura legislativa ordinaria le misure riguardanti « la raccolta, l'archiviazione, il trattamento, l'analisi e lo scambio di pertinenti informazioni » tra le autorità di polizia dei Paesi Membri[89]. La procedura legislativa ordinaria, che di fatto sostituisce la precedente procedura di co-decisione, diventa lo strumento legislativo principale per adottare gli atti riguardanti la cooperazione tra le autorità giudiziarie e di polizia[90]. Pertanto, un futuro accordo sul PNR dovrà essere probabilmente approvato con il voto favorevole della seduta plenaria del Parlamento Europeo, dopo essere stato valutato dal LIBE. Tendendo in considerazione l'opposizione del LIBE al trasferimento dei PNR fin dal primo accordo del 2004, la Commissione Europea dovrà in futuro tener maggiormente in considerazione l'opinione ora divenuta vincolante del Parlamento. La recente opposizione del Parlamento Europeo all'accordo SWIFT con gli USA riguardante il trasferimento dei dati bancari alle autorità americane ai fini della lotta contro il terrorismo dimostra che il Parlamento non sarà timoroso di esercitare il suo potere di veto su un possibile nuovo accordo sul PNR[91].

---

veva condurre una prima revisione dell'accordo del 2007 nel 2009, anche se al momento tale revisione sembra sia stata posticipata.

[88] « *We anticipated this revision. I am fully at your disposal to set a date to clarify a number of misunderstandings and to move this PNR forward together.* » *http://www.library.sso.ep.parl.union.eu/lis/site/newsContent.form?src=3&agId=14&id=24764&fileName=aeen1107.htm#tag20* (19 febbraio 2010).

[89] Versione Consolidata del Trattato sul Funzionamento dell'Unione Europea. Gazzetta ufficiale n. C 115 del 9 maggio 2008 0001-0388. Art. 87(2)(a). Il testo del Trattato è disponibile a: *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0001:01:IT:HTML* (19 febbraio 2010).

[90] *Ibid.*, Art. 294.

[91] Comunicato stampa del Parlamento Europeo, SWIFT: MEPs To Vote on Backing or Sacking EU/US Data Sharing Deal. Il testo del comunicato è disponibile a: *http://www.europarl.europa.eu/news/public/story_page/019-68537-039-02-07-902-20100205STO68536-2010-08-02-2010/default_en.htm* (19 febbraio 2010).

Infine, l'entrata in vigore del Trattato di Lisbona ha segnato anche una svolta in relazione alla protezione del diritto alla privacy e dei dati personali. Questi due diritti fondamentali sono espressamente menzionati dagli Art. 7 e 8 della Carta dei Diritti Fondamentali dell'Unione Europea[92]. Il testo della Carta era stata inserito nella Parte II della Costituzione dell'Unione Europea. Il Trattato di Lisbona, che ha sostituito la Costituzione Europea dopo la sua mancata ratifica, fa' riferimento nell'Art.6 del Trattato dell'Unione Europea alla Carta dei Diritti Fondamentali. Secondo l'Art. 6, « l'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati ». Pertanto, nonostante il testo della Carta non sia stato inserito nel Trattato di Lisbona, quest'ultima è diventata vincolante. Secondo l'Art. 51(1) della Carta, quest'ultima garantisce una serie di diritti ai cittadini europei che devono essere rispettati dalle istituzioni europee nello svolgimento della propria attività legislativa. Di conseguenza, nelle future revisioni dell'accordo sul PNR la Commissione Europea dovrà tenere in considerazione gli Art. 7 e 8 della Carta. La protezione dei dati personali non sarà più garantita soltanto da una trattato internazionale esterno al quadro normativo europeo quale la Convenzione del Consiglio d'Europa 108 e da un atto secondario quale la Direttiva 95/46/CE, ma dall'atto giuridico primario nell'Unione Europea. Inoltre, anche la recente Decisione Quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale dovrà essere tenuta in considerazione dalla Commissione Europea nelle future negoziazioni su di un nuovo accordo sul PNR[93].

I tre fattori menzionati sopra non avranno solo un impatto in relazione all'accordo con gli USA, ma anche in relazione al progetto di introdurre un sistema di controllo dei PNR di tutti i passeggeri dei voli in entrata nel territorio europeo. L'introduzione di tale sistema, ispirata al americano, è stata proposta negli ultimi anni dalla Commissione, ma alcun accordo è stato raggiunto al momento[94].

---

[92] Articolo 7. — Rispetto della vita privata e della vita familiare

Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.

Articolo 8. — Protezione dei dati di carattere personale

1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Carta dei Diritti Fondamentali dell'Unione Europea, proclamata a Nizza il 7 dicembre 2000 dalla Commissione, Parlamento e Consiglio dell'Unione Europea. Il testo della Carta è disponibile a *http://www.europarl.europa.eu/charter/pdf/text_it.pdf* (19 febbraio 2010).

[93] Decisione Quadro 2008/977/Gai del Consiglio del 27 novembre 2008 sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale. Pubblicata nella Gazzetta Ufficiale L 350/60 il 30 dicembre 2008. Il testo della Decisione è disponibile a *http://www.ejpd.admin.ch/etc/medialib/data/staat_buerger/gesetzgebung/datenschutz_schengen.Par.0021.File.tmp/rahmenbeschluss-i.pdf* (20 febbraio 2010).

[94] Un progetto di creazione di un sistema di controllo dei PNR è stato proposto dalla Commissione Europea negli ultimi anni, ma finora sempre posticipato. Il Parlamento Europeo, in particolare, ha più

La minaccia del terrorismo globale rende oggi giorno necessaria l'adozione di misure per tutelare la sicurezza pubblica quali il controllo dei PNR. Tuttavia, limiti in relazione al numero di dati controllati, al periodo della loro ritenzione, alle finalità dell'elaborazione dei dati, all'utilizzo di dati sensibili e al successivo trasferimento di tali dati a soggetti terzi dovrebbero essere sempre rispettati. Tali limiti impediscono alla pubblica autorità di godere di una totale discrezione in relazione all'utilizzo dei dati dei propri cittadini in nome della sicurezza nazionale; discrezione che può inevitabilmente condurre ad un numero di abusi e discriminazioni nella moderna società dell'informazione dove gli individui non sono solo cittadini ma anche soggetti di dati.

Il cammino da percorrere è dunque ancora lungo. È quindi necessario riprendere al più presto il dibattito sul trasferimento dei PNR al fine di raggiungere un migliore equilibrio tra i due opposti interessi della protezione della sicurezza pubblica con la protezione dei dati personali rispetto al risultato raggiunto con l'accordo sul PNR del 2007. Il fatto che il Consiglio dell'Unione Europea abbia deciso lo scorso 15 Febbraio 2010 d'inviare al Parlamento Europeo, per discussione ed approvazione, di alcuni accordi conclusi tra l'Unione Europea e Paesi terzi, incluso l'accordo sul PNR tra UE e USA, dimostra che il dibattito sull'accordo sul PNR sarà presto riaperto[95].

volte richiesto di posticipare l'adozione di tale sistema fino all'entrata in vigore del Trattato di Lisbona in modo da essere pienamente coinvolto nelle negoziazioni di tale progetto.

Comunicato stampa del Parlamento Europeo, EU Passenger Name Record Talks on Hold in Council Until Lisbon Treaty Is Ratified. Pubblicato il 6 ottobre 2009. Il testo del comunicato è disponibile a: *http://www.europarl.europa.eu/news/expert/infopress_page/019-61958-279-10-41-902-20091006IPR61955-06-10-2009-2009-false/default_it.htm* (19 febbraio 2010).

[95] *http://www.europolitics.info/europolitics/ep-asked-to-approve-eu-us-passenger-name-record-agreement-artb263317-46.html* (19 febbraio 2010).