

**CORTE DI GIUSTIZIA
DELLE COMUNITÀ
EUROPEE
GRANDE SEZIONE**

30 MAGGIO 2006

PRESIDENTE: SKOURIS

RELATORE: COLNERIC

AVV. GEN. LÈGER

(Cause riunite C-317/04 e
C-318/04)

**Tutela delle persone
fisiche con riguardo al
trattamento dei dati
personali • Trasporto
aereo • Decisione 2004/
496/CE • Accordo tra la
Comunità europea e gli
Stati Uniti d'America
• Schede nominative dei
passeggeri aerei trasferite
all'Ufficio delle dogane e
della protezione delle
frontiere degli Stati Uniti
d'America • Direttiva 95/
46/CE
• Art. 25 • Stati terzi
• Decisione 2004/535/CE
• Livello di protezione
adeguato**

Sono annullate la decisione del Consiglio 17 maggio 2004, 2004/496/CE, relativa alla conclusione di un accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (Passenger Name Record, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti, e la decisione della Commissione 14 maggio 2004, 2004/535/CE, relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti United States » Bureau of Customs and Border Protection.

1. Con il suo ricorso nella causa C-317/04, il Parlamento europeo chiede l'annullamento della decisione del Consiglio 17 maggio 2004, 2004/496/CE, relativa alla conclusione di un accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (Passenger Name Record, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti (GU L 183, pag. 83, e rettifica GU 2005, L 255, pag. 168).

2. Con il suo ricorso nella causa C-318/04, il Parlamento chiede l'annullamento della decisione della Commissione 14 maggio 2004, 2004/535/CE, relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti United States » Bureau of Customs and Border Protection (GU L 235, pag. 11; in prosieguo: la « decisione sull'adeguatezza »).

CONTESTO NORMATIVO. — 3. L'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, sottoscritta a Roma il 4 novembre 1950 (in prosieguo: la « CEDU »), così dispone:

« 1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.

2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese,

alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui ».

4. L'art. 95, n. 1, seconda frase, CE è del seguente tenore:

« Il Consiglio, deliberando in conformità della procedura di cui all'articolo 251 e previa consultazione del Comitato economico e sociale, adotta le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno ».

5. La direttiva del Parlamento europeo e del Consiglio 24 ottobre 1995, 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281, pag. 31), come modificata dal regolamento (CE) del Parlamento europeo e del Consiglio 29 settembre 2003, n. 1882, recante adeguamento alla decisione 1999/468/CE del Consiglio delle disposizioni relative ai comitati che assistono la Commissione nell'esercizio delle sue competenze di esecuzione previste negli atti soggetti alla procedura prevista all'articolo 251 del Trattato CE (GU L 284, pag. 1; in prosieguo: la « direttiva »), è stata adottata sul fondamento dell'art. 100 A del Trattato CE (divenuto, in seguito a modifica, art. 95 CE).

6. Al suo undicesimo « considerando » si afferma che « i principi della tutela dei diritti e delle libertà delle persone, in particolare del rispetto della vita privata, contenuti dalla presente direttiva precisano ed ampliano quelli enunciati dalla convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale ».

7. Ai sensi del tredicesimo « considerando » della direttiva:

« [L]e attività previste dai titoli V e VI del Trattato sull'Unione europea attinenti alla pubblica sicurezza, alla difesa, alla sicurezza dello Stato o alle attività dello Stato in materia di diritto penale non rientrano nel campo d'applicazione del diritto comunitario, fatti salvi gli obblighi che incombono agli Stati membri a norma dell'articolo 56, paragrafo 2, dell'articolo 57 e 100 A del Trattato (...) ».

8. Il cinquantasettesimo « considerando » della direttiva enuncia che:

« (...) deve essere vietato il trasferimento di dati personali verso un paese terzo che non offre un livello di protezione adeguato ».

9. L'art. 2 della direttiva prevede quanto segue:

« Ai fini della presente direttiva si intende per:

a) « dati personali »: qualsiasi informazione concernente una persona fisica identificata o identificabile (« persona interessata »); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale;

b) « trattamento di dati personali » (« trattamento »): qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi

automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione; (...)».

10. Ai sensi dell'art. 3 della direttiva:

« Campo d'applicazione

1. Le disposizioni della presente direttiva si applicano al trattamento di dati personali interamente o parzialmente automatizzato nonché al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi.

2. Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali[:]

— effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del Trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale;

(...)».

11. L'art. 6, n. 1, della direttiva enuncia:

« Gli Stati membri dispongono che i dati personali devono essere:

(...)

b) rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate;

c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali

vengono successivamente trattati;

(...)

e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati

(...)».

12. L'art. 7 della direttiva così dispone:

« Gli Stati membri dispongono che il trattamento di dati personali può essere effettuato soltanto quando: (...)

c) è necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento oppure

(...)

e) è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati, oppure

f) è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fonamen-

tali della persona interessata, che richiedono tutela ai sensi dell'articolo 1, paragrafo 1 ».

13. Ai sensi dell'art. 8, n. 5, primo comma, della direttiva:

« I trattamenti riguardanti i dati relativi alle infrazioni, alle condanne penali o alle misure di sicurezza possono essere effettuati solo sotto controllo dell'autorità pubblica, o se vengono fornite opportune garanzie specifiche, sulla base del diritto nazionale, fatte salve le deroghe che possono essere fissate dallo Stato membro in base ad una disposizione nazionale che preveda garanzie appropriate e specifiche. Tuttavia un registro completo delle condanne penali può essere tenuto solo sotto il controllo dell'autorità pubblica ».

14. L'art. 12 della direttiva così dispone:

« Gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento:

a) liberamente e senza costrizione, ad intervalli ragionevoli e senza ritardi o spese eccessivi:

— la conferma dell'esistenza o meno di trattamenti di dati che la riguardano, e l'informazione almeno sulle finalità dei trattamenti, sulle categorie di dati trattati, sui destinatari o sulle categorie di destinatari cui sono comunicati i dati;

— la comunicazione in forma intelligibile dei dati che sono oggetto dei trattamenti, nonché di tutte le informazioni disponibili sull'origine dei dati;

— la conoscenza della logica applicata nei trattamenti automatizzati dei dati che lo interessano, per lo meno nel caso delle decisioni automatizzate di cui all'articolo 15, paragrafo 1;

b) a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati;

c) la notificazione ai terzi, ai quali sono stati comunicati i dati, di qualsiasi rettifica, cancellazione o congelamento, effettuati conformemente alla lettera b), se non si dimostra che è impossibile o implica uno sforzo sproporzionato ».

15. L'art. 13, n. 1, della direttiva è del seguente tenore:

« Gli Stati membri possono adottare disposizioni legislative intese a limitare la portata degli obblighi e dei diritti previsti dalle disposizioni dell'articolo 6, paragrafo 1, dell'articolo 10, dell'articolo 11, paragrafo 1 e degli articoli 12 e 21, qualora tale restrizione costituisca una misura necessaria alla salvaguardia:

a) della sicurezza dello Stato;

b) della difesa;

c) della pubblica sicurezza;

d) della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate;

e) di un rilevante interesse economico o finanziario di uno Stato membro o dell'Unione europea, anche in materia monetaria, di bilancio e tributaria;

f) di un compito di controllo, ispezione o disciplina connesso, anche occasionalmente, con l'esercizio dei pubblici poteri nei casi di cui alle lettere c), d) ed e);

g) della protezione della persona interessata o dei diritti e delle libertà altrui ».

16. L'art. 22 della direttiva prevede quanto segue:

« Ricorsi Fatti salvi ricorsi amministrativi che possono essere promossi, segnatamente dinanzi all'autorità

di controllo di cui all'articolo 28, prima che sia adita l'autorità giudiziaria, gli Stati membri stabiliscono che chiunque possa disporre di un ricorso giurisdizionale in caso di violazione dei diritti garantitigli dalle disposizioni nazionali applicabili al trattamento in questione ».

17. Gli artt. 25 e 26 della direttiva formano il capo IV, relativo al trasferimento di dati personali verso paesi terzi.

18. L'art. 25 della direttiva, intitolato « Principi », prevede quanto segue:

« 1. Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva.

2. L'adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate.

3. Gli Stati membri e la Commissione si comunicano a vicenda i casi in cui, a loro parere, un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2.

4. Qualora la Commissione constati, secondo la procedura dell'articolo 31, paragrafo 2, che un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, gli Stati membri adottano le misure necessarie per impedire ogni trasferimento di dati della stessa natura verso il paese terzo in questione.

5. La Commissione avvia, al momento opportuno, negoziati per porre rimedio alla situazione risultante dalla constatazione di cui al paragrafo 4.

6. La Commissione può constatare, secondo la procedura di cui all'articolo 31, paragrafo 2, che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona.

Gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione ».

19. Ai sensi dell'art. 26, n. 1, della direttiva, intitolato « Deroghe »: « In deroga all'articolo 25 e fatte salve eventuali disposizioni contrarie della legislazione nazionale per casi specifici, gli Stati membri dispongono che un trasferimento di dati personali verso un paese terzo che non garantisce una tutela adeguata ai sensi dell'articolo 25, paragrafo 2 può avvenire a condizione che:

a) la persona interessata abbia manifestato il proprio consenso in maniera inequivocabile al trasferimento previsto, oppure

b) il trasferimento sia necessario per l'esecuzione di un contratto tra la persona interessata ed il responsabile del trattamento o per l'esecuzione di misure precontrattuali prese a richiesta di questa, oppure

c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto, concluso o da concludere nell'interesse della persona interessata, tra il responsabile del trattamento e un terzo, oppure

d) il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, oppure per costatare, esercitare o difendere un diritto per via giudiziaria, oppure

e) il trasferimento sia necessario per la salvaguardia dell'interesse vitale della persona interessata, oppure

f) il trasferimento avvenga a partire da un registro pubblico il quale, in forza di disposizioni legislative o regolamentari, sia predisposto per l'informazione del pubblico e sia aperto alla consultazione del pubblico o di chiunque possa dimostrare un interesse legittimo, nella misura in cui nel caso specifico siano rispettate le condizioni che la legge prevede per la consultazione ».

20. Sulla base della direttiva, in particolare dell'art. 25, n. 6, la Commissione delle Comunità europee ha adottato la decisione sull'adequatezza.

21. L'undicesimo « considerando » di tale decisione così recita:

« Il trattamento da parte del CBP [United States Bureau of Customs and Border Protection (Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti)] dei dati personali contenuti nei PNR [« Passenger Name Records » (schede nominative dei passeggeri)] dei passeggeri aerei che gli sono inviati è disciplinato dalle disposizioni che figurano nella « Dichiarazione d'impegno del Ministero della Sicurezza interna (Department for Homeland Security) — Ufficio delle dogane e della protezione delle frontiere (CBP) dell'11 maggio 2004 » (nei prosieguo: « la dichiarazione d'impegno ») e dalla legislazione americana, alle condizioni previste dalla dichiarazione d'impegno ».

22. Ai sensi del quindicesimo « considerando » della stessa decisione, i dati PNR devono essere utilizzati al solo scopo di prevenire e di combattere il terrorismo e i reati collegati al terrorismo, altri reati gravi, compresa la criminalità organizzata, che, per natura, rivestono un carattere transnazionale, e la fuga in caso di mandato d'arresto emesso o di pena detentiva comminata per quei reati.

23. Ai sensi degli artt. 1-4 della decisione sull'adeguatezza:

« ARTICOLO 1

Ai fini dell'articolo 25, paragrafo 2, della direttiva 95/46/CE, l'Ufficio statunitense delle dogane e della protezione delle frontiere (CBP) è considerato in grado di garantire un livello di protezione adeguato dei dati delle schede nominative dei passeggeri (PNR) trasmessi dalla Comunità per quanto riguarda i voli con destinazione o partenza dagli Stati Uniti, conformemente alla dichiarazione d'impegno che figura nell'allegato.

ARTICOLO 2

La presente decisione riguarda il livello di protezione adeguato garantito dal CBP al fine di rispondere ai requisiti posti dall'articolo 25, paragrafo 1, della direttiva 95/46/CE e non incide sulle condizioni o restrizioni in attuazione di altre disposizioni della direttiva e che si applicano al trattamento di dati personali negli Stati membri.

ARTICOLO 3

1. Fatti salvi i poteri che consentono loro di adottare misure volte a garantire il rispetto delle disposizioni nazionali adottate conformemente alle disposizioni diverse dall'articolo 25 della direttiva 95/46/CE, le autorità competenti degli Stati membri possono esercitare i poteri di cui dispongono attualmente per sospendere la trasmissione di dati al CBP al fine di proteggere le persone fisiche per quanto riguarda il trattamento dei loro dati personali in uno dei casi seguenti:

a) quando un'autorità degli Stati Uniti competente ha accertato che il CBP non rispetta le norme in materia di protezione;

b) quando è probabile che le norme di protezione stabilite nell'allegato I non siano rispettate; quando vi sono motivi ragionevoli di credere che il CBP non adotta o non adotterà, in tempi opportuni, le misure che s'impongono per regolare il caso in questione; quando il proseguimento della trasmissione di dati comporterebbe un rischio imminente di grave pregiudizio per le persone interessate e le autorità competenti dello Stato membro si sono ragionevolmente sforzate, in tali circostanze, di avvertire il CBP e di dargli la possibilità di rispondere.

2. La sospensione della trasmissione cessa dal momento in cui è garantita l'applicazione delle norme di protezione e l'autorità competente interessata negli Stati membri ne è avvertita.

ARTICOLO 4

1. Gli Stati membri informano immediatamente la Commissione in merito alle misure adottate in forza dell'articolo 3.

2. Gli Stati membri e la Commissione si informano reciprocamente in merito a qualsiasi modificazione delle norme di protezione e ai casi nei quali le misure adottate dalle autorità incaricate di assicurare il rispetto da parte del CBP delle norme di protezione stabilite nell'allegato I non siano sufficienti a garantire tale rispetto.

3. Se le informazioni raccolte in virtù dell'articolo 3 e dei paragrafi 1 e 2 del presente articolo dimostrano che principi fondamentali necessari per assicurare un livello di protezione adeguato delle persone fisiche non sono più rispettati, o che un qualunque organismo incaricato di assicurare il rispetto da parte del CBP delle norme di protezione stabilite nell'allegato

non svolge efficacemente la sua missione, il CBP ne sarà informato e, se necessario, si applica la procedura di cui all'articolo 31, paragrafo 2, della direttiva 95/46/CE, al fine di revocare o sospendere la presente decisione ».

24. La « [d]ichiarazione d'impegno dell'Ufficio delle dogane e della protezione delle frontiere del Ministero della Sicurezza interna », allegata alla decisione sull'adeguatezza, enuncia quanto segue:

« A sostegno del progetto della Commissione europea per l'esercizio dei poteri che le sono conferiti dall'articolo 25, paragrafo 6, della direttiva 95/46/CE (...) e l'adozione di una decisione che riconosca che [il CBP] del Ministero della Sicurezza interna (Department of Homeland Security) fornisce una protezione adeguata ai fini delle trasmissioni da parte dei vettori aerei dei dati [PNR], che possono rientrare nell'ambito d'applicazione della direttiva, il CBP assume i seguenti impegni (...) ».

25. Tali impegni comprendono 48 punti, raggruppati sotto i titoli seguenti: « Fondamento giuridico del diritto di ottenere il PNR »; « Uso dei dati del PNR da parte del CBP »; « Requisiti relativi ai dati »; « Trattamento dei dati « sensibili » »; « Metodo di accesso ai dati del PNR »; « Conservazione dei dati del PNR »; « Sicurezza del sistema informatico del CBP »; « Trattamento e tutela dei dati del PNR da parte del CBP »; « Trasmissione dei dati del PNR ad altre amministrazioni pubbliche »; « Informazione, accesso ai dati e mezzi di ricorso per le persone interessate dal PNR »; « Rispetto delle regole »;

« Reciprocità »; « Revisione e durata di validità della dichiarazione d'impegno », e « Non sono creati diritti privati o precedenti ».

26. Tra i detti impegni figurano in particolare i seguenti:

« 1) In virtù della legge [titolo 49, sezione 44909(c)(3), dell'USC — United States Code — Codice degli Stati Uniti] e dei regolamenti di attuazione (provvisori) (titolo 19, sezione 122.49b, del codice dei regolamenti federali), ciascun vettore aereo che assicura il trasporto aereo internazionale di passeggeri da e per gli Stati Uniti deve fornire al CBP un accesso elettronico ai dati del PNR nella misura in cui essi sono raccolti e conservati nei sistemi automatici di prenotazione/controllo delle partenze (nel prosieguo: i « sistemi di prenotazione ») dei vettori aerei.

(...)

3) I dati del PNR sono utilizzati dal CBP al solo fine di prevenire e combattere: 1) il terrorismo e i crimini connessi; 2) altri reati gravi, compresa la criminalità organizzata transnazionale; e 3) la fuga dall'arresto o da pena detentiva per i suddetti crimini. L'uso dei dati del PNR a tali scopi consente al CBP di concentrare le proprie risorse su casi di elevato rischio, facilitando e salvaguardando i viaggi bona fide.

4) I dati richiesti dal CBP sono elencati nell'allegato A (...).

(...)

27) Nell'ambito di ogni ricorso amministrativo o giudiziario cui dia adito una richiesta, presentata in forza della legge sulla libertà di informazione, di dati del PNR raccolti dai vettori aerei, il CBP sosterrà che tali archivi non sono soggetti alla divulgazione prevista dalla legge sulla libertà di informazione.

(...)

29) Il CBP, nell'esercizio del suo potere discrezionale, trasmetterà i dati del PNR ad altre autorità governative, comprese le autorità degli altri paesi incaricate di far rispettare la legge o della lotta contro il terrorismo, previo esame del caso singolo, a fini di prevenzione e lotta contro i reati di cui al punto 3. Le autorità cui il CBP può trasmettere tali informazioni saranno in prosieguo denominate «autorità designate».

30) Il CBP esercita con prudenza il proprio potere discrezionale di trasmettere dati del PNR ai fini di cui al punto 3. Innanzitutto, esso determinerà se il motivo per la divulgazione dei dati a un'altra autorità designata sia conforme alle finalità indicate (cfr. punto 29). In caso affermativo, il CBP determinerà se tale autorità designata abbia il compito di prevenire la violazione di leggi o regolamenti connessi con tali finalità, di condurre indagini o esperire azioni giudiziarie a tal riguardo, o di attuare o far rispettare dette leggi o regolamenti, laddove il CBP venga a conoscenza di una violazione, concreta o potenziale, della legge. La fondatezza della divulgazione dovrà essere esaminata alla luce di tutte le circostanze presentate.

(...)

35) Nessuna disposizione della presente dichiarazione d'impegno può impedire l'uso o la divulgazione di dati del PNR nell'ambito di un procedimento penale o negli altri casi previsti dalla legge. Il CBP informerà la Commissione in ordine all'adozione, da parte delle autorità americane, delle leggi che incidono sulle dichiarazioni contenute nella presente dichiarazione d'impegno.

(...)

46) La presente dichiarazione d'impegno si applica per un periodo di tre anni e sei mesi a decorrere dalla data di entrata in vigore di un accordo tra gli Stati Uniti e la Comunità europea che autorizzi il trattamento dei dati del PNR da parte dei vettori aerei ai fini del trasferimento di tali dati al CBP, in conformità con la direttiva (...).

47) La presente dichiarazione d'impegno non crea o conferisce alcun diritto o beneficio a persone fisiche o giuridiche, private o pubbliche.

(...)».

27. L'allegato «A» della dichiarazione d'impegno contiene i «[d]ati del PNR» richiesti dal CBP ai vettori aerei. Fanno parte di tali dati, in particolare, il «[c]odice del documento PNR», la data di prenotazione, il nome, l'indirizzo, le modalità di pagamento, i recapiti telefonici, l'agenzia viaggi, la «fase di viaggio» del passeggero («travel status of passenger»), l'indirizzo di posta elettronica, le osservazioni generali, il numero del posto, l'informazione sulle precedenti assenze all'imbarco e le «informazioni APIS» eventualmente assunte.

28. Il Consiglio ha adottato la decisione 2004/496 in particolare sul fondamento dell'art. 95 CE, in combinato disposto con l'art. 300, n. 2, primo comma, prima frase, CE.

29. Ai sensi dei tre «considerando» di tale decisione:

«(1) Il 23 febbraio 2004 il Consiglio ha autorizzato la Commissione a negoziare, in nome della Comunità, un accordo con gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle prati-

che (Passenger Name Record, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti.

(2) Il Parlamento europeo non ha espresso il suo parere nel termine fissato dal Consiglio, ai sensi dell'articolo 300, paragrafo 3, primo comma del Trattato, dato l'urgente bisogno di porre rimedio alla situazione di incertezza in cui si trovano le compagnie aeree ed i passeggeri, nonché di proteggere gli interessi finanziari degli interessati.

(3) È opportuno approvare il presente accordo ».

30. L'art. 1 della decisione 2004/496 prevede quanto segue:

« L'accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti è approvato in nome della Comunità.

Il testo dell'accordo è accluso alla presente decisione ».

31. Il detto accordo (in prosieguo: l'« accordo ») recita come segue:

« La Comunità europea e gli Stati Uniti d'America,

Riconoscendo l'importanza di rispettare i diritti e le libertà fondamentali, in particolare il diritto alla vita privata, e l'importanza di rispettare tali valori nella prevenzione e nella lotta contro il terrorismo e i reati ad esso connessi, nonché altri reati gravi di natura transnazionale, tra cui la criminalità organizzata;

Visti le leggi e i regolamenti statunitensi che impongono a ciascun vettore aereo che assicura il trasporto di passeggeri da e per gli Stati Uniti nello spazio aereo estero di fornire [al CBP] del dipartimento per la sicurezza interna (Department of Homeland Security, in seguito denominato « DHS »), un accesso elettronico ai dati di identificazione [PNR] nella misura in cui questi sono raccolti e conservati nei sistemi automatici di prenotazione/controllo dei vettori aerei;

Vista la direttiva 95/46/CE G.), in particolare l'articolo 7, lettera c);

Viste le dichiarazioni di impegno del CBP dell'11 maggio 2004, che saranno pubblicate nel registro federale (in seguito denominate le « dichiarazioni di impegno »);

Vista la decisione 2004/535/CE della Commissione adottata il 14 maggio 2004, ai sensi dell'articolo 25, paragrafo 6 della direttiva 95/46/CE, con cui si ritiene che il CBP, conformemente alle dichiarazioni di impegno alligate, assicuri un livello di protezione adeguato dei dati PNR trasferiti dalla Comunità europea (in seguito denominata « Comunità ») in relazione ai voli da o per gli Stati Uniti (in seguito denominata la decisione);

Constatando che i vettori aerei dotati di sistemi di prenotazione/controllo situati nel territorio degli Stati membri della Comunità europea dovrebbero provvedere a trasmettere i dati PNR al CBP non appena ciò sia tecnicamente possibile, ma che, fino a quel momento, dovrebbe essere consentito alle autorità statunitensi di accedere direttamente a tali dati, ai sensi delle disposizioni del presente accordo;

(...)

Hanno convenuto quanto segue:

1) Il CBP può accedere elettronicamente ai dati PNR provenienti dai sistemi di prenotazione/controllo (« sistemi di prenotazione ») dei

vettori aerei situati nel territorio degli Stati membri della Comunità europea, in assoluta conformità della decisione, per tutto il periodo in cui la decisione è applicabile e solo finché non sia in vigore un sistema soddisfacente che permetta la trasmissione di tali dati da parte dei vettori aerei.

[La versione inglese recita come segue: « CBP may electronically access the PNR data from air carriers reservation/departure control systems ('reservation systems') located within the territory of the Member State of the European Community strictly in accordance with the Decision and for so long as the Decision is applicable and only until there is a satisfactory system in place allowing for transmission of such data by the air carriers ».]

2) Ciascun vettore aereo che assicura il trasporto di passeggeri da o per gli Stati Uniti nello spazio aereo estero tratta i dati PNR contenuti nei suoi sistemi automatizzati di prenotazione come richiesto dal CBP ai sensi della normativa statunitense, in assoluta conformità della decisione e per tutto il periodo in cui la decisione è applicabile.

3) Il CBP prende nota della decisione e attesta che sta attuando le dichiarazioni di impegno allegate a detta decisione.

4) Il CBP tratta i dati PNR ricevuti e i titolari dei dati interessati da tale trattamento in conformità delle leggi e degli obblighi costituzionali statunitensi applicabili, senza discriminazioni illegittime, in particolare in base alla nazionalità e al paese di residenza.

(...)

Il presente accordo entra in vigore all'atto della sua firma.

Ciascuna parte può denunciare il presente accordo in qualsiasi momento, mediante notifica per via diplomatica. In tal caso, l'accordo cessa di essere in vigore novanta (90) giorni dopo la data di tale notifica. Il presente accordo può essere modificato in ogni momento mediante consenso scritto di entrambe le parti.

8) Il presente accordo non intende derogare o apportare modifiche alla normativa delle parti; esso non crea né conferisce alcun diritto o beneficio ad altre persone o enti, pubblici o privati ».

32. Secondo l'informazione del Consiglio relativa alla sua data di entrata in vigore (GU 2004, C 158, pag. 1), l'accordo, firmato a Washington il 28 maggio 2004 da un rappresentante della presidenza in esercizio del Consiglio e dal Segretario del dipartimento per la sicurezza interna degli Stati Uniti, è entrato in vigore, in conformità del suo punto 7, il giorno della sua firma.

FATTI ALL'ORIGINE DELLA CONTROVERSIA. — 33. A seguito degli attacchi terroristici dell'11 settembre 2001, nel novembre dello stesso anno gli Stati Uniti hanno adottato una normativa che disponeva che i vettori aerei che assicuravano collegamenti con destinazione o partenza nel territorio degli Stati Uniti ovvero traversanti tale territorio fossero tenuti a fornire alle autorità doganali degli Stati Uniti un accesso elettronico ai dati contenuti nel loro sistema automatico di prenotazione e di controllo delle partenze, denominati « Passenger Name Records » (in prosieguo: i « dati PNR »). Pur riconoscendo la legittimità degli interessi di sicurezza in gioco, la Commissione, sin dal giugno 2002, ha informato le autorità statunitensi che tali disposizioni rischiavano di entrare in contrasto con la

legislazione comunitaria e con quella degli Stati membri in materia di tutela dei dati e con talune disposizioni del regolamento (CEE) del Consiglio 24 luglio 1989, n. 2299, relativo ad un codice di comportamento in materia di sistemi telematici di prenotazione (GU L 220, pag. 1), come modificato dal regolamento (CE) del Consiglio 8 febbraio 1999, n. 323 (GU L 40, pag. 1). Le autorità statunitensi hanno rinviato l'entrata in vigore delle nuove disposizioni, rifiutandosi però, in definitiva, di rinunciare ad infliggere sanzioni alle compagnie aeree che non si fossero conformate alla normativa sull'accesso elettronico ai dati PNR dopo il 5 marzo 2003. Da allora, numerose grandi compagnie aeree dell'Unione europea hanno fornito alle dette autorità un accesso ai propri dati PNR.

34. La Commissione ha avviato con le autorità statunitensi negoziati sfociati in un documento contenente determinati impegni (« undertakings ») assunti dal CBP, in vista dell'adozione da parte della Commissione, sulla base dell'art. 25, n. 6, della direttiva, di una decisione sull'adeguatezza.

35. Il 13 giugno 2003 il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'art. 29 della direttiva, ha pronunciato un parere in cui esprimeva dubbi circa il livello di tutela dei dati garantito dai detti impegni riguardo alle forme di trattamento dei dati previste. Tali dubbi sono stati da esso reiterati in un parere del 29 gennaio 2004.

36. Il 1 marzo 2004 la Commissione ha sottoposto al Parlamento il progetto di decisione sull'adeguatezza, in virtù dell'art. 25, n. 6, della direttiva, accompagnato dal progetto di impegno del CBP.

37. Il 17 marzo 2004 la Commissione ha trasmesso al Parlamento, nell'ottica della consultazione di tale organo ai sensi dell'art. 300, n. 3, primo comma, CE, una proposta di decisione del Consiglio avente ad oggetto la conclusione di un accordo con gli Stati Uniti. Con lettera datata 25 marzo 2004 il Consiglio, riferendosi alla procedura d'urgenza, ha chiesto al Parlamento di esprimere un parere su tale proposta entro il 22 aprile 2004.

In tale lettera il Consiglio ha sottolineato quanto segue: « La lotta contro il terrorismo, che giustifica le misure proposte, costituisce una priorità fondamentale dell'Unione europea, [attualmente] i vettori aerei e i passeggeri si trovano in una situazione di incertezza cui è urgente porre rimedio [e.] inoltre, [è] essenziale tutelare gli interessi economici delle parti interessate ».

38. Il 31 marzo 2004, in attuazione dell'art. 8 della decisione del Consiglio 28 giugno 1999, 1999/468/CE, recante modalità per l'esercizio delle competenze di esecuzione conferite alla Commissione (GU L 184, pag. 23), il Parlamento ha adottato una risoluzione in cui esprimeva un certo numero di riserve di carattere giuridico sulla proposta presentata. In tale risoluzione ha considerato, in particolare, che il progetto di decisione sull'adeguatezza eccedeva le competenze conferite alla Commissione dall'art. 25 della direttiva 95/46, ha invocato la conclusione di un accordo internazionale appropriato che rispettasse i diritti fonda-

mentali su un certo numero di punti specificati nella risoluzione stessa e ha chiesto alla Commissione di sottoporgli un nuovo progetto di decisione. Il Parlamento si è inoltre riservato di adire la Corte al fine di verificare la legittimità dell'accordo internazionale previsto e, in particolare, la sua compatibilità con la tutela del diritto al rispetto della vita privata.

39. Su richiesta del suo presidente, il 21 aprile 2004 il Parlamento ha approvato una raccomandazione della commissione giuridica e del mercato interno volta ad ottenere, ai sensi dell'art. 300, n. 6, CE, un parere della Corte sulla compatibilità dell'accordo previsto con le disposizioni del Trattato. Tale procedura è stata avviata lo stesso giorno.

40. Il Parlamento ha inoltre deciso in pari data di rinviare a tale commissione il rapporto sulla proposta di decisione del Consiglio, respingendo così implicitamente, in questa fase, la domanda di esame urgente della detta proposta presentata dal Consiglio il 25 marzo.

41. Il seguente 28 aprile il Consiglio, sulla base dell'art. 300, n. 3, primo comma, CE, ha inviato al Parlamento una lettera chiedendogli di emettere entro il 5 maggio 2004 il suo parere sulla proposta di decisione relativa alla conclusione dell'accordo. A giustificazione dell'urgenza di tale richiesta, il Consiglio ha ribadito i motivi indicati nella sua lettera del 25 marzo 2004.

42. Avendo avuto notizia della persistente mancanza di tutte le versioni linguistiche della proposta di decisione del Consiglio, il 4 maggio 2004 il Parlamento ha respinto la domanda di esame urgente della detta proposta che il Consiglio gli aveva presentato il 28 aprile.

43. Il 14 maggio seguente la Commissione ha adottato la decisione sull'adeguatezza, che forma oggetto della causa C-318/04. Il 17 maggio 2004 il Consiglio ha adottato la decisione 2004/496, che forma oggetto della causa C-317/04.

44. Con lettera del 4 giugno 2004, la presidenza in esercizio del Consiglio ha informato il Parlamento che la decisione 2004/496 prendeva in considerazione la lotta contro il terrorismo — prioritaria per l'Unione —, ma anche la necessità di affrontare una situazione di incertezza giuridica per le compagnie aeree, oltre che gli interessi finanziari di queste.

45. Con lettera del 9 luglio 2004 il Parlamento ha informato la Corte del ritiro della sua richiesta di parere registrata con il n. 1/04.

46. Nella causa C-317/04, con ordinanze del presidente della Corte 18 novembre 2004 e 18 gennaio 2005, sono stati ammessi gli interventi della Commissione e del Regno Unito di Gran Bretagna e Irlanda del Nord a sostegno delle conclusioni del Consiglio.

47. Nella causa C-318/04, con ordinanza del presidente della Corte 17 dicembre 2004, è stato ammesso l'intervento del Regno Unito a sostegno delle conclusioni della Commissione.

48. Con ordinanze della Corte 17 marzo 2005 è stato ammesso l'intervento del Garante europeo della protezione dei dati a sostegno delle conclusioni del Parlamento nelle due dette cause.

49. In considerazione della connessione tra tali cause, confermata nella fase orale, i procedimenti in esame vanno riuniti ai fini della sentenza a norma dell'art. 43 del regolamento di procedura della Corte.

SUL RICORSO NELLA CAUSA C-318/04. — 50. Il Parlamento deduce quattro motivi di annullamento, relativi, rispettivamente, ad un eccesso di potere, ad una violazione dei principi essenziali della direttiva, ad una violazione dei diritti fondamentali e ad una violazione del principio di proporzionalità.

Sulla prima parte del primo motivo, relativa ad una violazione dell'art. 3, n. 2, primo trattino, della direttiva.

ARGOMENTI DELLE PARTI. — 51. Il Parlamento sostiene che la decisione della Commissione è stata adottata *ultra vires*, in quanto non sarebbero state rispettate le disposizioni emanate con la direttiva e in violazione, in particolare, dell'art. 3, n. 2, primo trattino, della stessa, relativo all'esclusione delle attività che non rientrano nell'ambito di applicazione del diritto comunitario.

52. Non vi sarebbe dubbio che il trattamento dei dati PNR dopo il trasferimento all'autorità americana di cui alla decisione sull'adeguatezza è, e sarà, effettuato per l'esercizio di attività proprie degli Stati ai sensi del punto 43 della sentenza 6 novembre 2003, causa C-101/01, *Lindqvist* (Rec. pag. I-12971).

53. La Commissione, sostenuta dal Regno Unito, ritiene che le attività dei vettori aerei rientrino chiaramente nell'ambito di applicazione del diritto comunitario. Afferma che tali operatori privati trattano i dati PNR all'interno della Comunità e ne organizzano il trasferimento verso uno Stato terzo. Si tratterebbe dunque di attività dei privati e non dello Stato membro in cui operano i vettori interessati, o dei suoi pubblici poteri, come definito dalla Corte al punto 43 della citata sentenza *Lindqvist*. Nel trattamento dei dati PNR i vettori aerei perseguirebbero semplicemente lo scopo di rispettare le prescrizioni del diritto comunitario, compreso l'obbligo iscritto al punto 2 dell'accordo. L'art. 3, n. 2, della direttiva farebbe riferimento alle attività di autorità pubbliche che non rientrano nell'ambito di applicazione del diritto comunitario.

GIUDIZIO DELLA CORTE. — 54. L'art. 3, n. 2, primo trattino, della direttiva esclude dal suo ambito di applicazione i trattamenti di dati personali effettuati per l'esercizio di attività che non rientrano nell'ambito di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del Trattato sull'Unione europea e, comunque, i trattamenti aventi come og-

getto la pubblica sicurezza, la difesa, la sicurezza dello Stato e le attività dello Stato in materia di diritto penale.

55. La decisione sull'adeguatezza riguarda solamente i dati PNR trasmessi al CBP. Dal sesto «considerando» di questa decisione emerge che l'obbligo di tale trasmissione si basa su una legge adottata dagli Stati Uniti nel novembre 2001 e su regolamenti di attuazione adottati dal CBP in base a tale legge. Ai sensi del settimo «considerando» della stessa decisione, la legislazione statunitense in questione riguarda il rafforzamento della sicurezza, nonché le condizioni di ingresso negli Stati Uniti e di uscita dal paese. Ai sensi dell'ottavo «considerando», la Comunità sostiene pienamente gli Stati Uniti nella loro lotta contro il terrorismo nei limiti imposti dal diritto comunitario. Il quindicesimo «considerando» della stessa decisione enuncia che i dati PNR devono essere utilizzati al solo scopo di prevenire e di combattere il terrorismo e i reati collegati al terrorismo, altri reati gravi, compresa la criminalità organizzata, che, per natura, rivestono un carattere transnazionale, e la fuga in caso di mandato d'arresto emesso o di pena detentiva comminata per quei reati.

56. Ne risulta che il trasferimento dei dati PNR al CBP costituisce un trattamento avente come oggetto la pubblica sicurezza e le attività dello Stato in materia di diritto penale.

57. Se è giusto considerare che i dati PNR sono inizialmente raccolti dalle compagnie aeree nell'ambito di un'attività che rientra nel diritto comunitario, ossia la vendita di un biglietto aereo che dà diritto ad una prestazione di servizi, il trattamento dei dati che viene preso in considerazione nella decisione sull'adeguatezza, tuttavia, possiede una natura del tutto diversa. Infatti, tale decisione, come già ricordato al punto 55 della presente sentenza, non riguarda un trattamento di dati necessario alla realizzazione di una prestazione di servizi, ma ritenuto necessario per salvaguardare la pubblica sicurezza e a fini repressivi.

58. Al punto 43 della citata sentenza Lindqvist, invocato dalla Commissione nella sua difesa, la Corte ha dichiarato che le attività indicate, a mo' di esempio, nell'art. 3, n. 2, primo trattino, della direttiva sono, in tutti i casi, attività proprie degli Stati o delle autorità statali ed estranee ai settori di attività dei singoli. Tuttavia, non ne discende che, per il fatto che i dati PNR sono stati raccolti da operatori privati a fini commerciali e che sono questi ultimi ad organizzarne il trasferimento ad uno Stato terzo, tale trasferimento non rientri nell'ambito di applicazione della detta norma. Infatti, il trasferimento rientra in un ambito istituito dai poteri pubblici e attinente alla pubblica sicurezza.

59. Dalle precedenti considerazioni risulta che la decisione sull'adeguatezza riguarda un trattamento di dati personali ai sensi dell'art. 3, n. 2, primo trattino, della direttiva. Tale decisione non rientra pertanto nell'ambito di applicazione di quest'ultima.

60. La prima parte del primo motivo, relativa ad una violazione dell'art. 3, n. 2, primo trattino, della direttiva, è quindi fondata.

61. Conseguentemente, senza che sia necessario esaminare le altre parti del primo motivo o gli altri motivi invocati dal Parlamento, si deve annullare la decisione sull'adeguatezza.

Sul ricorso nella causa C-317/04.

62. Il Parlamento deduce sei motivi di annullamento, relativi alla scelta erronea dell'art. 95 CE come fondamento giuridico della decisione 2004/496 e alla violazione, rispettivamente, dell'art. 300, n. 3, secondo comma, CE, dell'art. 8 della CEDU, del principio di proporzionalità, del « obbligo di motivazione e del principio di leale cooperazione. Sul primo motivo, relativo alla scelta erronea dell'art. 95 CE come fondamento giuridico della decisione 2004/496

ARGOMENTI DELLE PARTI. — 63. Il Parlamento sostiene che l'art. 95 CE non costituisce, per la decisione 2004/496, un fondamento giuridico corretto. La decisione, infatti, non avrebbe né per oggetto né per contenuto l'instaurazione e il funzionamento del mercato interno contribuendo all'eliminazione di ostacoli alla libera prestazione dei servizi e non conterrebbe disposizioni volte alla realizzazione di tale scopo. Infatti, la sua finalità sarebbe piuttosto quella di legittimare il trattamento di dati personali imposto dalla legislazione statunitense. Del resto, l'art. 95 CE non potrebbe costituire il fondamento della competenza della Comunità a concludere l'accordo, giacché questo riguarda trattamenti di dati esclusi dall'ambito di applicazione della direttiva.

64. Il Consiglio sostiene che la direttiva, validamente adottata sul fondamento dell'art. 100 A del Trattato, all'art. 25 contiene disposizioni che prevedono la possibilità di un trasferimento di dati personali verso uno Stato terzo che garantisca un livello adeguato di protezione, compresa la possibilità di avviare, in caso di necessità, negoziati che conducano alla conclusione di un accordo tra la Comunità e tale paese. L'accordo riguarderebbe la libera circolazione dei dati PNR tra la Comunità e gli Stati Uniti in condizioni che rispettino le libertà e i diritti fondamentali delle persone, in particolare la vita privata. Sarebbe volto a sopprimere qualsiasi distorsione della concorrenza tra le compagnie aeree degli Stati membri e fra queste ultime e le compagnie degli Stati terzi, che possa risultare dalle condizioni imposte dagli Stati Uniti, per ragioni attinenti alla tutela dei diritti e delle libertà degli individui. Le condizioni della concorrenza fra le compagnie degli Stati membri che offrono un servizio di trasporto internazionale di passeggeri verso o dagli Stati Uniti avrebbero potuto essere falsate per il fatto che solo alcune di esse avrebbero accordato alle autorità statunitensi un accesso alle loro banche dati. L'accordo intenderebbe imporre obblighi uniformi a tutte le compagnie interessate.

65. La Commissione sottolinea l'esistenza di un « conflitto di leggi », nel senso del diritto internazionale pubblico, tra le leggi degli Stati Uniti e la normativa comunitaria oltre che la necessità di conciliarle. Rimprovera al Parlamento, che nega che l'art. 95 CE possa costituire il fondamento normativo della decisione 2004/496, di non aver proposto un fondamento normativo idoneo. Secondo la Commissione, tale articolo costituirebbe il « fondamento normativo naturale » della decisione, in quanto

l'accordo riguarderebbe la dimensione esterna della protezione dei dati personali nel momento del loro trasferimento all'interno della Comunità. Gli artt. 25 e 26 della direttiva fonderebbero una competenza esclusiva esterna a favore della Comunità.

66. Inoltre, la Commissione sostiene che il trattamento iniziale di quei dati da parte delle compagnie aeree viene effettuato a fini commerciali. L'uso che ne fanno le autorità statunitensi non li sottrarrebbe all'incidenza della direttiva.

GIUDIZIO DELLA CORTE. — 67. L'art. 95 CE, in combinato disposto con l'art. 25 della direttiva, non è idoneo a fondare la competenza della Comunità a concludere l'accordo.

68. Infatti, l'accordo riguarda lo stesso trasferimento di dati della decisione sull'adeguatezza e quindi trattamenti di dati che, come precedentemente esposto, sono esclusi dall'ambito di applicazione della direttiva.

69. Conseguentemente, la decisione 2004/496 non è stata validamente, adottata sul fondamento dell'art. 95 CE.

70. Senza che sia necessario esaminare gli altri motivi invocati dal Parlamento, si deve pertanto annullare la detta decisione.

SULLA LIMITAZIONE DEGLI EFFETTI DELLA SENTENZA. — 71. Dal punto 7 dell'accordo risulta che ciascuna parte può denunciarlo in qualsiasi momento e che esso cessa di essere in vigore 90 giorni dopo la data della notifica della denuncia all'altra parte.

72. Tuttavia, ai sensi dei punti 1 e 2 dell'accordo, il diritto di accesso del CBP ai dati PNR e l'obbligo imposto ai vettori aerei di trattarli come richiesto dal CBP esistono solo finché la decisione sull'adeguatezza è applicabile. Al punto 3 del detto accordo, il CBP ha dichiarato di stare attuando le dichiarazioni di impegno allegate alla detta decisione.

73. Dato che la Comunità non può invocare il proprio diritto per giustificare la mancata esecuzione dell'accordo che resta applicabile per 90 giorni dalla sua denuncia e dato che l'accordo e la decisione sull'adeguatezza sono strettamente collegati, appare giustificato, per ragioni di certezza del diritto e al fine di proteggere le persone interessate, mantenere gli effetti della decisione sull'adeguatezza durante tale periodo.

Inoltre, occorre tener conto del tempo necessario per adottare le misure che l'esecuzione della presente sentenza comporta.

74. Gli effetti della decisione sull'adeguatezza devono pertanto essere mantenuti fino al 30 settembre 2006, senza che, tuttavia, tali effetti siano mantenuti oltre la data di estinzione dell'accordo.

SULLE SPESE. — 75. Ai sensi dell'art. 69, n. 2, del regolamento di procedura, la parte soccombente è condannata alle spese se ne è stata fatta domanda. Poiché il Parlamento ha chiesto la condanna del Consi-

glio e della Commissione, questi ultimi, rimasti soccombenti, devono essere condannati alle spese. Ai sensi del n. 4, primo comma, dello stesso articolo, gli intervenienti nelle presenti cause sopportano le proprie spese.

Per questi motivi, la Corte (Grande Sezione) dichiara e statuisce:

1) Sono annullate la decisione del Consiglio 17 maggio 2004, 2004/496/CE, relativa alla conclusione di un accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (Passenger Name Record, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti, e la decisione della Commissione 14 maggio 2004, 2004/535/CE, relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti United States' Bureau of Customs and Border Protection.

2) Gli effetti della decisione 2004/535 sono mantenuti fino al 30 settembre 2006, senza che, tuttavia, tali effetti siano mantenuti oltre la data di estinzione dell'accordo.

3) Il Consiglio dell'Unione europea è condannato alle spese nella causa C-317/04.

4) La Commissione delle Comunità europee è condannata alle spese nella causa C-318/04.

5) La Commissione delle Comunità europee sopporterà le proprie spese nella causa C-317/04.

6) Il Regno Unito di Gran Bretagna e Irlanda del Nord e il Garante europeo della protezione dei dati sopporteranno le proprie spese.

IL CASO.

« *LEGISLAZIONE DELL'EMERGENZA* » E *TUTELA DEI DATI PERSONALI DEI PASSEGGERI: IL CONFLITTO EUROPA - USA*

A seguito degli attacchi terroristici dell'11 settembre 2001, gli Stati Uniti hanno adottato una normativa che obbliga i vettori aerei che assicurano collegamenti con destinazione o partenza nel territorio degli Stati Uniti ovvero traversanti tale territorio a fornire alle autorità doganali degli Stati Uniti l'accesso elettronico ai dati contenuti nel loro sistema automati-

co di prenotazione e di controllo delle partenze, denominati *Passenger Name Records* (PNR).

La Commissione, ritenendo che tali disposizioni fossero potenzialmente in contrasto con la legislazione comunitaria e con quella degli Stati membri in materia di tutela dei dati, ha avviato dei negoziati con le autorità americane. In esito a tali trattative, il 14 maggio 2004 la Commissione ha adottato una decisione (la decisione sull'adeguatezza) secondo cui l'Ufficio statunitense delle dogane e della protezione delle frontiere (*United States* » *Bureau of Customs and Border Protection*, CBP) garantisce un livello di protezione adeguato dei dati PNR trasmessi agli Stati Uniti. Il

17 maggio 2004 il Consiglio ha adottato una decisione che approva la conclusione di un accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati *PNR* al *CBP* da parte dei vettori aerei con sede nel territorio degli Stati membri della Comunità. Tale accordo è stato firmato a Washington il 28 maggio 2004 ed è entrato in vigore lo stesso giorno.

Il Parlamento europeo ha chiesto alla Corte di giustizia delle Comunità europee di annullare la decisione del Consiglio (causa C-317/04) e la decisione sull'adeguatezza (causa C-318/04), sostenendo, in particolare, che quest'ultima è stata adottata *ultra vires*, poiché l'art. 95 del trattato istitutivo della Comunità Europea non costituisce un fondamento giuridico appropriato per la decisione, e facendo valere, in entrambi i casi, una violazione dei diritti fondamentali.

La Corte di Giustizia, con la sentenza in questione, ha annullato entrambe le decisioni.

La vicenda ha trovato epilogo il 16 ottobre 2006, data in cui l'Unione Europea ha firmato un nuovo accordo provvisorio con gli Stati Uniti, prevedendo la raccolta dei dati solo per finalità di lotta al terrorismo e criminalità organizzata, la conservazione degli stessi per un lasso di tempo limitato, ed escludendo l'accesso automatico da parte delle agenzie statunitensi.

IL TRASFERIMENTO DEI DATI PERSONALI ALL'ESTERO.

La sentenza della Corte di Giustizia riapre il dibattito sul trasferimento dei dati personali, che, nato da una questione di natura economica legata per lo più alle transazioni commerciali internazionali telematiche, assume ora nuovi risvolti. Nel novembre 2001 l'Amministrazione statunitense, temendo il compimento di nuovi atti terroristici con l'uso di aerei provenienti da altri Paesi, ha emanato alcune disposizioni normative atte a realizzare più stringenti controlli sui passeggeri diretti verso gli Stati Uniti. Si tratta delle norme dell'*Aviation and Transportation Security Act*¹, che impongono a tutte le compagnie aeree che effettuano voli verso, da o attraverso gli Stati Uniti, di fornire all'Ufficio Statunitense delle dogane e della protezione delle frontiere, *United States Bureau of Customs and Border Protection (CBP)*, l'accesso elettronico ai dati dei passeggeri² per motivi di sicurezza e di protezione del

¹ *Aviation and Transportation Security Act*, Pub. L. No. 107-71, 115 Stat. 597 (2001) (codified as amended in scattered sections of 49 U.S.C.)

² I dati dei passeggeri cui si fa riferimento sono quelli contenuti nel codice di prenotazione, il *Passenger Name Record (PNR)*: la sequenza alfanumerica rilasciata dalle compagnie aeree all'atto della prenotazione del viaggio. L'Ufficio Statunitense delle Dogane e della Protezione delle Frontiere può avere accesso elettronico diretto, dunque, al nome del passeggero, al contatto telefonico dello stesso, ai dettagli

del volo (data del viaggio, origine e destinazione, numero del posto a bordo, numero dei bagagli, ecc.), nonché alla forma di pagamento scelta. I dati possono essere intercettati dallo *US CBP* all'interno dei sistemi di prenotazione fino a 48 ore prima della partenza del volo ed utilizzati per operare controlli dei passeggeri prima del loro arrivo sul territorio statunitense, con lo scopo di facilitare l'ingresso della maggior parte dei viaggiatori, focalizzando le risorse dello *US CBP* stesso solo su quel numero ristretto di passeggeri che potrebbe costituire un rischio reale per la sicurezza. 49 U.S.C.

territorio. Sono previste pesanti sanzioni, tra cui l'interdizione all'atterraggio in territorio statunitense, per le compagnie aeree che rifiutino l'adeguamento alla normativa.

Dal 5 marzo 2003, termine iniziale per le sanzioni penali, alcune grandi compagnie aeree hanno assicurato all'*US CBP* libero accesso alle proprie banche dati³, pur in violazione della normativa europea in materia, che vieta, entro certi limiti, la trasmissione dei dati personali verso Paesi, tra cui gli Stati Uniti, che non assicurano un adeguato livello di tutela dei dati personali⁴.

SAFE HARBOR AGREEMENT.

Il livello di protezione dei dati personali garantito dalla legislazione degli Stati Uniti è stato già in passato giudicato inadeguato, ed ha richiesto interventi di adattamento spesso limitati dalle profonde differenze nell'approccio alla materia: settoriale quello statunitense e più generale quello europeo⁵.

44909(c)(1), 44909(c)(2), (3), (5) (2001). MEGAN ROOS, *Safe on the Ground, Exposed in the Sky: The Battle Between the United States and the European Union Over Passenger Name Information*, 14 *Transnat'l L. & Contemp. Probs.* 1137, (2005) p.1138. K. KRAUSE, *Putting the Transportation Security Administration in Historical Context*, 68 *J. Air L. & Com.* 233, (2003) p. 242 e ss.

³ A. DI MARTINO, *La protezione dei dati personali. Aspetti comparatistici e sviluppo di un modello europeo di tutela*, in PANUZIO (a cura di) *I diritti fondamentali e le Corti in Europa*, Napoli, 2005, p. 448.

⁴ Direttiva 95/46/CE relativa alla tutela delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, art. 25.

⁵ Negli Stati Uniti, in assenza di una normativa generale, esistono *Statutes* federali che fissano norme a tutela dei dati personali per alcune determinate attività (quella relativa al credito bancario) o per alcune categorie di soggetti (i minori). I riferimenti normativi sono, dunque, il *Fair Credit Reporting Act* del 26 ottobre 1970, il *Family Educational Rights and Privacy Act* del 10 novembre 1978, il *Privacy Protection Act* del 13 ottobre 1980, il *Privacy Act* del 1974. Lo sviluppo delle tecnologie informative ha posto anche l'esigenza di ulteriori soluzioni legislative appropriate. Nel 1973 l'*U.S. Department of Health and Educational* ha elaborato le prime regole per disciplinare l'uso del computer con il rispetto della *privacy*. Nel 1977, a seguito di uno studio commissionato dal Congresso, l'*U.S. Privacy Protection Study*

Commission ha evidenziato l'esigenza di una normativa che tutelasse l'individuo dall'utilizzo arbitrario delle informazioni personali. Nel 1980, con l'approvazione delle linee guida per l'Organizzazione per la cooperazione economica e lo sviluppo della *privacy*, il governo ha riconosciuto le norme basilari necessarie al controllo del « commercio » delle informazioni. Pur considerando, dunque, le istanze di protezione dei dati personali, il sistema americano ha deciso di affidarsi a mezzi diversi dalla disciplina legislativa. Il riferimento è alla *self-regulation* che, senza l'intervento di regolamenti governativi, dovrebbe realizzare una significativa tutela della *privacy*, con la flessibilità necessaria ad assicurare l'adeguamento agli sviluppi tecnologici. In concreto, secondo la teoria della *self-regulation*, il mercato dovrebbe assicurare adeguata protezione ai dati personali al fine di conservare le utilità derivanti dal commercio delle informazioni. Si veda: K. ZAIDI, *Harmonizing U.S. — E.U. Online Privacy Laws: Toward a U.S. Comprehensive Regime for the Protection of Personal Data*, 12 *Mich. St. J. Int'l L.* 169, (2003), p. 171; J. R. REIDENBERG, *Symposium: Restoring Americans Privacy in Electronic Commerce*, *Berkley Tech. Law Journal*, 771 (1999) p. 774 e ss.; D. CASTOR, *Treading Water in the Data Privacy Age: An Analysis of Safe Harbor's First Year*, 12 *Ind. Int'l & Comp. L. Rev.* 265, (2002), p.267. A. DI MARTINO, *La protezione dei dati personali. Aspetti comparatistici e sviluppo di un modello europeo di tutela*, cit., p. 445.

Un primo intervento, volto a scongiurare la paralisi del flusso di dati legato alle attività di scambio commerciale, ha condotto l'Europa e gli Stati Uniti all'adozione, nel marzo 2000, del *Safe Harbor Agreement*.⁶

Non si tratta di un accordo nel senso tecnico del termine, ma piuttosto un insieme di linee guida, promosse ed elaborate dall'amministrazione americana, con un intervento negoziatorio dell'Unione europea, al fine di agevolare l'attività delle imprese americane nel mercato europeo⁷. Il *Safe Harbor* non ha il compito di dichiarare adeguato il grado di protezione effettivamente offerto dalle norme statunitensi, ma solo di considerare sufficiente la tutela derivante dall'adesione volontaria delle aziende ad un sistema di norme di sicurezza appositamente costruito.

Le imprese e le organizzazioni statunitensi che aderiscono a tale sistema attestano, tramite autocertificazione⁸, il rispetto dei principi indicati nel *Safe Harbor* che, naturalmente, ricalcano le norme di protezione dei dati previste dalla Direttiva Europea 95/46/CE. È, dunque, richiesto il consenso della persona interessata al trattamento, oltre ad una serie di diritti accessori quali l'informazione sulla finalità della raccolta, la sicurezza dei trasferimenti, la protezione dall'abuso e dalle perdite, i diritti

⁶ J. ASSEY, D. ELEFTHERIOU. *The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?* 9, CommLaw Conspectus 145 (2001) p.147 e ss. In Italia il Garante per la protezione dei dati personali ha dato attuazione alla decisione della Commissione con il rilascio, nel 2001, di un'autorizzazione generale. Cfr. Garante Per La Protezione Dei Dati Personali, *Autorizzazione al trasferimento dei dati personali verso organizzazioni aventi sede negli Stati Uniti secondo i principi di approdo sicuro in materia di riservatezza*, 10 ottobre 2001, G.U del 26.11. 2001.

⁷ K. ZAIDI, in *Harmonizing U.S. — E.U. Online Privacy Laws: Toward a U.S. Comprehensive Regime for the Protection of Personal Data*, cit., p. 169 definisce il *Safe Harbor Agreement* un accordo di e-commerce per colmare le differenze tra la protezione garantita dagli Stati Uniti e quella prevista dall'Europa, con finalità meramente commerciali, di interesse per le aziende americane. Dalla Relazione del 2002, il discorso del Garante per la protezione dei dati personali (Roma, 20 Maggio 2003): « Nell'ambito delle attività economiche assume rilievo particolare il trasferimento dei dati fuori dell'Unione Europea, che coinvolge sia l'interesse delle imprese alla fluidità della circolazione delle informazioni, sia il diritto dei cittadini a mantenere intatte le loro garanzie. » D. CASTOR: in *Treading Water in the Data Privacy Age: An Analysis of Safe Harbor's First Year*, cit., p.266, esprime efficacemente

l'interesse statunitense alla conclusione dell'accordo, affermando che, dopo lunghe trattative nel luglio 1999 gli Stati Uniti finalmente convinsero la Commissione Europea ad accettare il *Safe Harbor*.

⁸ K. ZAIDI, *Harmonizing U.S. — E.U. Online Privacy Laws: Toward a U.S. Comprehensive Regime for the Protection of Personal Data*, op. cit., p.179: « L'adesione al Safe Harbor da parte delle organizzazioni statunitensi si basa su una semplice autocertificazione da effettuarsi mediante notificazione al Department of Commerce a seguito della quale, senza che venga esperito nessun controllo aggiuntivo, l'ente è inserito nell'elenco delle organizzazioni che possono beneficiare dei vantaggi connessi all'approdo sicuro ». Sembra potersi affermare che gli Stati Uniti non rinunciano alla concezione, sia pure mitigata dall'accordo, che nel campo dei dati personali la self — regulation o self — certification sia la strategia più efficace. Si veda: J. ASSEY, D. ELEFTHERIOU. *The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?*, op. cit.; G. P. CIRILLO (a cura di) *Il codice sulla protezione dei dati personali*, Milano Giuffrè, 2004; M. ROOS, in *Safe on the Ground, Exposed in the Sky: The Battle Between the United States and the European Union Over Passenger Name Information*, cit., p. 1154, afferma che l'approccio corrente alla protezione dei dati è frammentato ed inconsistente, veicolato da segmenti economici.

di opposizione all'utilizzo, di accesso ed eventuale rettifica e cancellazione dei dati⁹.

Manca, nella disciplina dell'«approdo sicuro», un'autorità indipendente di controllo a livello federale che abbia una fisionomia, con i relativi poteri, prossimi a quelli garantiti dal modello europeo¹⁰.

Un impianto lasciato essenzialmente all'autoregolamentazione delle imprese, unito anche alla perplessità sugli organi di controllo, aveva indotto il Palamento europeo a procedere con cautela, sollecitando la Commissione a subordinare la decisione positiva sul progetto *Safe Harbor* alla operatività pratica di esso. La Commissione, tuttavia, nonostante la richiesta del Parlamento ed il parere critico del gruppo 29¹¹, ha adottato la decisione di adeguamento ancor prima che il meccanismo entrasse in funzione, sfruttando il «potere» attribuitole dall'art. 25, sesto comma della Direttiva 95/46/CE¹².

LA DECISIONE DELLA CORTE DI GIUSTIZIA.

I paragrafi uno e due dell'art 25 della Direttiva 95/46/CE stabiliscono che i dati personali possono essere trasferiti in un Paese non appartenente all'Unione Europea solo qualora il Paese terzo garantisca un livello di protezione adeguato¹³. Il paragrafo sei dello stesso articolo stabilisce,

⁹ La presunzione di adeguamento alle finalità della Direttiva comporta il rispetto di sette principi nel trattamento dei dati: *Notice, Choice, Onward Transfer, Security, Data integrity, Access, Enforcement*. Si veda: D. CASTOR, *Treading Water in the Data Privacy Age: An Analysis of Safe Harbor's First Year*, 12 Ind. Int'l & Comp. L. Rev. 265 (2002), p. 276 e ss. Parallelamente la Direttiva Europea 95/46/CE, prevede: obbligo di informativa, autodeterminazione, sicurezza dei trasferimenti e dall'abuso e da perdite, integrità, diritto di accesso, correzione (artt. 7 e ss.) Cfr. G. P. CIRILLO (a cura di) *Il codice sulla protezione dei dati personali*, cit.

¹⁰ L'art. 28 della Direttiva Europea 95/46/CE prevede la presenza di autorità pubbliche di controllo incaricate di sorvegliare l'applicazione delle disposizioni di attuazione della direttiva stessa. Il compito di verificare l'effettiva osservanza dell'accordo da parte delle aziende statunitensi e di infliggere eventualmente sanzioni è stato affidato alla *Federal Trade Commission* ed al *Department of Transportation*. La *Federal Trade Commission* può anche avviare un'iniziale fase inibitoria con un formale invito a conformarsi al contenuto dell'accordo, e in caso di flagrante e persistente comportamento non conforme, procedere alla espulsione dal sistema del *Safe Harbor*, nonché alla condanna al risarcimento dei danni derivanti dal reiterato inadempimento. G. P.

CIRILLO (a cura di) *Il codice sulla protezione dei dati personali*, cit.

¹¹ Il Gruppo 29, istituito in forza dell'articolo 29 della Direttiva 95/46/CE assume funzioni di organo consultivo europeo indipendente in materia di protezione dei dati e della privacy, ed «è composto da un rappresentante della o delle autorità di controllo designate da ciascuno Stato membro e da un rappresentante della o delle autorità create per le istituzioni e gli organismi comunitari, nonché da un rappresentante della Commissione» (art. 29, comma 2). Si veda: A. DI MARTINO, *La protezione dei dati personali. Aspetti comparatistici e sviluppo di un modello europeo di tutela*, cit., p. 446.

¹² La decisione in questione è 2000/520/CE. Si veda: A. DI MARTINO, *La protezione dei dati personali. Aspetti comparatistici e sviluppo di un modello europeo di tutela*, cit., p. 446.

¹³ A tale riguardo, la Commissione europea ha deciso che Canada, Ungheria, Svizzera, Argentina, Guernsey e l'Isola di Man garantiscono un livello adeguato di protezione dei dati personali, autorizzando il trasferimento. (Decisioni 2002/2/CE; 2000/519/CE; 2000/518/CE; 2003/1731CE; 2004/411CE). A. DI MARTINO, *La protezione dei dati personali. Aspetti comparatistici e sviluppo di un modello europeo di tutela*, cit. p. 451: «L'adeguatezza va valutata con riguardo a tutte le circo-

però, che la Commissione europea può constatare che un Paese terzo garantisce un livello di protezione adeguato, ai fini della tutela della vita privata o dei diritti e delle libertà fondamentali della persona, autorizzandone, così, il trasferimento¹⁴.

Come nel caso del *Safe Harbor*, la Commissione europea, nell'intento di assicurare sia la continuità dei voli verso gli Stati Uniti che un'adeguata protezione dei dati dei passeggeri¹⁵, ha intrapreso negoziati con il Dipartimento per la Sicurezza Interna degli Stati Uniti¹⁶ al fine di concludere un accordo, da sottoporre a decisione sull'adeguatezza in virtù dell'art. 25, n. 6 della Direttiva 95/46.

Nel marzo 2004 la Commissione ha presentato al Parlamento il progetto di decisione sull'adeguatezza, accompagnato dal progetto di impegno del CBP, ottenendo tuttavia dal Parlamento un parere sfavorevole¹⁷, pienamente condiviso dal « Gruppo 29 ».¹⁸

stanze relative ad un trasferimento o ad una categoria di trasferimento dei dati, secondo quanto dispone l'art. 25, comma 2 della Direttiva. »

¹⁴ La salvaguardia di un interesse pubblico rilevante, o un interesse vitale dell'interessato (art. 26, comma 1, lett. d ed e), o ipotesi di consenso della persona interessata (art. 26, comma 1, lett. a) e ipotesi in cui i dati personali siano necessari per la conclusione o l'esecuzione di un contratto (art. 26 co. 1, lett. b e c), permettono il trasferimento pur in mancanza di un livello adeguato di protezione. Si veda: A. DI MARTINO, *La protezione dei dati personali. Aspetti comparatistici e sviluppo di un modello europeo di tutela*, cit., p. 439. « ...nella prassi, infatti, non è tanto la valutazione di adeguatezza ex art. 25 a giustificare giuridicamente siffatti trasferimenti, bensì le eccezioni di cui all'art. 26, segnatamente i gruppi descritti alle lettere a), b) e c). In pratica, solo quando i trasferimenti non sono coperti né dal consenso della persona interessata, né da trattative o adempimenti contrattuali, l'autorità garante dovrà verificare se il paese destinatario disponga di misure di protezione adeguate. »

¹⁵ F. BIGNAMI, *Transgovernmental Networks vs. Democracy: the Case of the European Information Privacy Network*, 26 Mich. J. Int'l L. 807 (2005), p. 807. C. FRIEDEMANN, *Legislative Development: Council Decision Regarding Agreement Between the European Community and the United States on the Use of Passenger Name Record Data*, 11 Colum. J. Eur. L. 207, (2004-2005) p. 208; « In a Communication dated December 16, 2003, the Commission described its goal of attaining the best possible protection for PNR data under Article 25 of the Data Protection Directive while

keeping in mind the objectives of combating terrorism and ensuring fair conditions for European Union airlines. »

¹⁶ Un primo risultato delle trattative è una « dichiarazione congiunta », un documento contenente determinati impegni assunti dal CBP, in vista dell'adozione da parte della Commissione di una decisione sull'adeguatezza. Si tratta del *Joint Statement, European Commission/U.S. Customs, Talks on PNR Transmission* 3, (Brussels, Feb. 17-18, 2003) in http://europa.eu.int/comm/internal_market/privacy/docs/adequacy/declaration_en.pdf. Si veda: A. GUBITZ *The U.S. Aviation and Transportation Security Act of 2001 in Conflict with the E.U. Data Protection Laws: How Much Access to Airline Passenger Data Does the United States Need to Combat Terrorism?* 39 New Eng. L. Rev. 431 (2005), p. 452.

¹⁷ In precedenza vi era stata una comunicazione della Commissione al Parlamento ed al Consiglio, sullo stesso argomento: COM(2003)826, definitivo, in http://europa.eu.int/comm/internal_market/privacy/docs/adequacy/apis-communication/apis_en.pdf.

¹⁸ Il gruppo di lavoro, nel parere 4/2003 sul livello di tutela assicurato negli USA rispetto al trasferimento di dati relativi a passeggeri si esprime efficacemente: « Non è possibile compiere una valutazione dell'adeguatezza del livello di tutela rispetto a quei settori dell'amministrazione statunitense in cui il quadro normativo relativo al trattamento dei dati PNR non può ritenersi stabile o adeguatamente delineato sul piano dell'accesso ai dati e della legittimazione al loro trattamento. Né è possibile effettuare una valutazione dell'adeguatezza del livello di tutela per quei sistemi in grado di compiere un trattamento

Successivamente, nel maggio 2004, nonostante l'invito del Parlamento europeo ad una sostanziale rinegoziazione con gli USA¹⁹, la Commissione ha concluso un accordo « *sul trattamento e trasferimento dei dati di identificazione delle pratiche (Passenger Name Record, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti d'America*, » che il Consiglio dell'Unione Europea ha approvato con Decisione 2004/496/CE²⁰.

L'accordo in questione ha, naturalmente, i requisiti del compromesso: gli stati Uniti hanno accettato di raccogliere e conservare un numero di dati minore di quello originariamente previsto dall'ATSA e per un tempo inferiore; hanno previsto, inoltre, specifiche misure di filtraggio e cancellazione dei dati sensibili, nel tentativo di rispettare il principio di finalità caro alla legislazione europea, che nel concreto assume, però, il contenuto piuttosto vago di lotta al terrorismo²¹.

L'accordo, tuttavia, non può sottrarsi alle censure del Parlamento e del « Gruppo 29 »²², delle cui riserve la Commissione, al momento della conclusione, ha tenuto conto solo in parte.

massivo dei dati, il cui esatto funzionamento e configurazione denotano ampie problematiche ancora in via di definizione. » Il Gruppo propone, inoltre, un esplicito invito alla cautela ed alla massima attenzione in considerazione dell'ingente flusso di dati richiesto dalle autorità statunitensi, tendendo presente i rischi di schedatura di massa e controlli generalizzati.

¹⁹ Il 31 marzo 2004, in attuazione dell'art. 8 della decisione del Consiglio 28 giugno 1999, 1999/468/CE, recante modalità per l'esercizio delle competenze di esecuzione conferite alla Commissione (GU L184, pag.23), il Parlamento ha adottato una risoluzione in cui esprimeva un certo numero di riserve di carattere giuridico sulla proposta presentatagli, invocando la conclusione di un accordo internazionale appropriato, che rispettasse i diritti fondamentali su un certo numero di punti specificati nella risoluzione stessa.

²⁰ Decisione della Commissione del 14 maggio 2004 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*, pubblicata sulla G.U.U.E. n. L/235 del 6 luglio 2004.

²¹ L'accordo prevede la raccolta di un numero massimo di 34 informazioni, che possono essere conservate per un massimo di tra anni e mezzo, ad eccezione dei dati che nel corso di questi tre anni vengano consultati, suscettibili di una conservazione fino ad otto anni. È prevista la filtrazione o cancellazione di dati relativi alle ordinazioni dei pasti, capaci di rivelare infor-

mazioni sulla razza, la religione o la salute. I dati sono utilizzati unicamente per combattere e prevenire il terrorismo, i reati ad esso collegati e i reati gravi, inclusa la criminalità organizzata, a carattere transnazionale, e non per consentire una più ampia repressione dei reati, così come auspicato in precedenza dagli USA. Il CBP si impegna a scambiare i dati PNR raccolti soltanto su base individuale e unicamente ai fini convenuti; nel caso i dati provenienti da un Paese dell'Unione Europea fossero trasmessi alle autorità competenti a reprimere i reati di un Paese terzo, ne verrà data informazione ad un'autorità designata nell'Unione Europea. Le autorità garanti della protezione dei dati dell'Unione Europea potranno esaminare, assieme al direttore dell'ufficio responsabile per la protezione della vita privata (*Chief Privacy Officer*) del DHS, i casi di quei passeggeri le cui rimostranze — relative ad esempio a possibili abusi di dati o alla mancata correzione di inesattezze — non sono esaminate in maniera soddisfacente dal DHS. Si veda Allegato alla Decisione della Commissione del 14 maggio 2004: *Dichiarazione di impegno dell'ufficio delle dogane e della protezione delle frontiere del ministero della sicurezza interna*. Cfr: A. GUBITZ *The U.S. Aviation and Transportation Security Act of 2001 in Conflict with the E.U. Data Protection Laws: How Much Access to Airline Passenger Data Does the United States Need to Combat Terrorism?* cit., p. 461 e ss.

²² A. GUBITZ in *The U.S. Aviation and Transportation Security Act of 2001 in Conflict with the E.U. Data Protection Laws: How Much Access to Airline Pas-*

Con riguardo ai dati sensibili (in particolare, le informazioni sul cibo suscettibili di rivelare il credo religioso) il CBP si è impegnato esclusivamente ad introdurre programmi filtro, nonostante il « Gruppo 29 » chiedesse che tali dati non fossero neanche trasmessi²³. Inoltre, pur ottenendo l'eliminazione, tra le finalità di raccolta, della prevenzione di *serious criminal offences*²⁴, oltre che di reati terroristici, la durata dell'archiviazione dei dati raccolti, ridotta a tre anni e mezzo piuttosto che gli iniziali cinquanta, è ancora troppo lunga rispetto alle richieste del « Gruppo 29 ».²⁵

Oggetto di censura del Parlamento è, inoltre, la trasmissione sistematica di dati personali alle autorità doganali americane, poiché viola il principio di finalità nella raccolta dei dati (art. 25, 2 comma Direttiva 95/46/CE). « Lo scopo della raccolta dei dati non è la prevenzione o la repressione dei reati, quanto la facilitazione delle operazioni relative al trasporto aereo »²⁶.

Al CBP è poi attribuito il potere, sia pure nell'intento di prevenire il terrorismo, di comunicare i dati ricevuti ad altri rami dell'amministrazione. L'unica garanzia contro l'abuso di tale potere è la raccomandazione di agire « *judiciously* » (paragrafi 28-32 della Dichiarazione).

La terza critica operata dal Parlamento riguarda il momento del controllo. I soggetti controllanti sarebbero, infatti, lo stesso CBP insieme al

senger Data Does the United States Need to Combat Terrorism? cit., p. 465: indica analiticamente le critiche mosse dai Garanti Europei all'accordo: « *Many of the Member States Data Commissioners find the E.U. Commission's agreement with the United States deficient. Stefano Rodotà, who chairs the E.U. privacy 'watch-dogs', claimed that the agreement watered down Directive 95/46 and lowered global privacy standards. One of their major concerns was the lack of a binding redress system. In their opinion, while the Department of Homeland Security allowed E.U. citizens to address privacy concerns to its Chief Privacy Officer, this option failed E.U. independency requirements because the Chief Privacy Officer was attached to the Department of Homeland Security. Further, the U.S. requirement of collecting thirty-four items of PNR data was still excessive and unreasonable. The German data privacy official, Peter Schaar, voiced similar concerns, but expressly stated that U.S. rules concerning passenger data still breached E.U. laws. He felt strongly about reducing the extensive catalogue of data requested and wanted the United States to completely exclude sensitive data.* »

²³ Parere 4/2003 sul livello di tutela assicurato negli USA rispetto al trasferimento di dati relativi a passeggeri: « Deve essere esclusa la trasmissione di dati in

senso lato sensibili, protetti dall'Art. 8 della Direttiva. »

²⁴ Parere 4/2003: « *Le finalità per cui i dati potranno essere utilizzati devono rimanere circoscritte alla lotta agli atti terroristici, senza allargarne l'ambito ad altri non meglio precisati « serious criminal offences » (gravi reati penali). Gli USA dovrebbero fornire una lista chiara e delimitata di gravi reati direttamente connessi al terrorismo.* »

²⁵ Il Gruppo di lavoro, nel Parere 4/2003 esprime le proprie riserve sull'efficacia a fini investigativi di una conservazione di dati eccessivamente lunga e riferita a milioni di persone: « *I dati personali non devono essere conservati oltre il periodo necessario al raggiungimento degli scopi per cui sono stati raccolti. Pertanto, è accettabile soltanto la conservazione dei dati oggetto di trasferimento in conformità con lo scopo dichiarato di controllare l'ingresso nel territorio degli USA onde individuare atti di terrorismo. I dati dovrebbero essere conservati per un breve periodo, non superiore a qualche settimana, o anche a qualche mese, successivamente all'ingresso nel territorio USA. Non è giustificabile un periodo di conservazione dell'ordine di 7-8 anni.* »

²⁶ A. DI MARTINO, *La protezione dei dati personali. Aspetti comparatistici e sviluppo di un modello europeo di tutela*, cit., p. 451.

DHS Privacy Office, che mancano probabilmente dei requisiti di indipendenza ed effettività necessari all'organo superiore²⁷.

A tali fondate ragioni di censura si aggiungono quelle che il Parlamento ha utilizzato per richiedere alla Corte di giustizia delle Comunità europee di annullare la decisione del Consiglio (causa C-317/04) e la decisione sull'adeguatezza (causa C-318/04), sostenendo, in particolare, che quest'ultima è stata adottata *ultra vires*, poiché l'art. 95 del Trattato istitutivo della Comunità europea affida al Consiglio il compito di adottare misure volte all'avvicinamento degli ordinamenti degli Stati membri, in materia di instaurazione e funzionamento del mercato comune; non contempla, invece, la materia oggetto dell'intervenuto accordo (prevenzione del terrorismo).²⁸ Condividendo tale interpretazione, la Corte di Giustizia ha annullato la decisione della Commissione, stabilendo, inoltre, per ragioni di certezza del diritto e al fine di proteggere le persone interessate, di mantenere gli effetti della decisione sull'adeguatezza fino al 30 settembre 2006.

A seguito della sentenza della Corte, accogliendo l'invito del Parlamento²⁹ ad evitare un vuoto giuridico, il 16 ottobre 2006 la Commissione³⁰ ha concluso un accordo provvisorio con l'amministrazione statunitense.

²⁷ A. DI MARTINO, *La protezione dei dati personali. Aspetti comparatistici e sviluppo di un modello europeo di tutela*, cit., p. 451.

²⁸ Il Parlamento, inoltre, ha dedotto la violazione dell'art. 300, comma 3, 2 capoverso, TCE (« In deroga al comma precedente... gli accordi che implicano la modifica di un atto adottato secondo la procedura di cui all'art. 251 sono conclusi previo parere conforme del PE »), dell'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), del 4 novembre 1950 (norma che prevede il diritto al rispetto della vita privata e familiare), dell'obbligo di motivazione, dei principi di proporzionalità e di leale collaborazione. In relazione alla decisione della Commissione 2004/535, il Parlamento rilevava che essa fosse viziata da eccesso di potere e contraria ai principi essenziali della Direttiva 95/46/CE, ai diritti fondamentali ed al principio di proporzionalità.

²⁹ Nella Relazione recante una proposta di raccomandazione del Parlamento europeo destinata al Consiglio sui negoziati in vista di un accordo con gli Stati Uniti d'America sull'impiego dei dati di identificazione delle pratiche passeggeri (PNR) per prevenire e combattere il terrorismo e la criminalità transnazionale, compresa la criminalità organizzata, il Parlamento suggerisce di negoziare un altro accordo tenendo conto delle raccomandazioni del Garante europeo per la protezione dei da-

ti, stabilendo il passaggio al sistema *PUSH* con il quale le autorità USA chiedono dati concreti e necessari caso per caso invece di avere accesso illimitato alle banche dati. Per il medio-lungo termine, invece, il Parlamento sottolinea la necessità di un approccio più coerente a livello dell'Organizzazione internazionale dell'aviazione civile (ICAO) sullo scambio di dati sui passeggeri, per garantire sia la sicurezza del traffico aereo che il rispetto dei diritti umani a livello globale; chiede, inoltre, di fornire all'UE di un quadro giuridico chiaro e coerente, adottando con urgenza il progetto di decisione quadro sulla protezione dei dati. Cfr: *Documento di seduta finale A6-0252/2006 19.7.2006 Commissione per le libertà civili, la giustizia e gli affari interni Relatrice: Sophia in 't Veld*, in http://www.europarl.europa.eu/news/expert/briefing_page/9654-241-08-35-20060706BRI09653-29-08-2006-2006/default_p001c003_it.htm

³⁰ Già due settimane dopo la sentenza della Corte di Giustizia la Commissione ha chiesto al Consiglio di essere autorizzata ad avviare negoziati per un accordo con gli Stati Uniti sull'uso dei dati PNR, sulla base dell'art. 38 del Titolo VI del Trattato dell'Unione europea. Questo titolo (terzo pilastro) è, infatti, il contesto giuridico corretto per concludere un accordo internazionale su questioni attinenti alla pubblica sicurezza ed al diritto penale. <http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/06/800&format=HTML&a->

L'insoddisfazione espressa dal Parlamento, l'annullamento deciso dalla Corte e la persistente situazione di incertezza, fanno eco alle polemiche che seguono l'emanazione dell'*Aviation and Transportation Security Act* e di altre normative più specifiche³¹ che costituiscono il « sistema normativo dello stato d'eccezione, » o « legislazione dell'emergenza ».³²

LA « LEGISLAZIONE DELL'EMERGENZA » ED IL CONFLITTO TRA PRIVACY E SICUREZZA: CENNI AL *PATRIOT ACT*

Una parte considerevole della « normativa dello stato d'eccezione » confluisce in un provvedimento varato dal Congresso il 25 ottobre 2001: « *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, of 2001* » o, più comunemente, *USA Patriot Act*. È un atto normativo volto a disciplinare materie anche molto diverse, con l'intento di combattere e prevenire le organizzazioni terroristiche³³. Dei dieci titoli di cui è composto, i primi due sono volti a fornire maggiore capacità di incisione agli organi inquirenti nel recupero di prove di reato nei settori della comunicazione via cavo e via etere; il terzo emenda le leggi relative al riciclaggio monetario e si occupa della lotta al finanziamento internazionale del terrorismo; il quarto modifica la legislazione relativa alla immigrazione al fine di prevenire che terroristi stranieri possano entrare negli Stati Uniti³⁴.

Si tratta di un intervento incisivo, destinato ad assicurare agli Stati Uniti il privilegio della sicurezza interna, così pesantemente violato dal-

ged=0&language=IT&guiLanguage=en. Il nuovo accordo è *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*, in http://ec.europa.eu/justice_home/fsj/privacy/pnr/2006_10_accord_us_eu.pdf.

³¹ Il riferimento è al *President Issues Military Order* del 13 novembre 2001, intitolato « Detention, Treatment, and Trial of Certain Non-Citizens in the War Against Terrorism », disponibile su <http://www.whitehouse.gov/news/releases/2001/11/20011113-27.html>

³² Il riferimento alla « legislazione dell'emergenza » è di F. LANCHESTER, *Gli Stati Uniti e l'11 settembre*, in www.associazionedeicostituzionalisti.it/dibattiti/vicendeinternazionali/lanchester.html, e di MEGAN ROOS, *Safe on the Ground, Exposed in the Sky: The Battle Between the United States and the European Union Over Passenger Name Information*, cit.

³³ *USA PATRIOT Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272 (2001): « *An act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory*

tools, and for other purposes. » R. BRILLÈ, « *Patriottismo* » costituzionale e libertà di informazione: il caso statunitense, in questa rivista, 2/2006, p. 125 e ss. Si veda: J. SOMA-M. NICHEL-S. RYNERSON-L. MAISH-J. ROGERS, *Balance of Privacy vs. Security: A Historical Perspective of the USA Patriot Act*, 31 Rutgers Computer & Tech. L.J. 285 (2005), p. 294, in cui gli autori affermano che il Patriot Act differisce da altri tipi di legislazione antiterroristica (il confronto proposto è con la legislazione irlandese e canadese) perché focalizza gli aspetti più soft dell'anti-terrorismo come i finanziamenti alle organizzazioni terroristiche, nonché gli aspetti più tecnologici ed operativi.

³⁴ Il quinto ed il settimo provvedono ad indicare i mezzi per facilitare la lotta al terrorismo, mentre il sesto interviene in favore delle vittime degli atti di terrorismo, delle loro famiglie e dei soccorritori; l'ottavo crea nuove fattispecie di reato o aumenta le pene esistenti per quanto riguarda il settore degli atti di terrorismo; il nono è dedicato a rafforzare l'azione di *intelligence* della CIA ed il decimo ad interventi vari. *USA PATRIOT Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272 (2001).

l'attentato terroristico³⁵, anche a costo di sacrificare alcuni diritti fondamentali sanciti dalla Costituzione americana³⁶, tra cui quello alla *privacy*.

Il riferimento più frequente è alla violazione del Quarto Emendamento alla Costituzione americana³⁷, che protegge il cittadino da violazioni governative, permettendo solo « intrusioni » opportunamente regolate³⁸.

Il compito di ridisegnare i confini della *privacy* del singolo³⁹ è affidato alla sezione 215 del *Patriot Act*.⁴⁰ La nuova normativa permette all'*FBI* di ordinare la produzione di « *any tangible thing*, » e, dunque, libri, documenti, giornali e quanto possa servire ad indagini volte alla protezione dal terrorismo o da altre attività clandestine. La normativa prece-

³⁵ « *Gli Stati Uniti in questo senso sono stati i primi a muoversi per dotarsi di un pacchetto anti-terrorismo? organico che, in quanto giustificato dall'emergenza, deroga alla normalità ed è posto a presidio del valore? sicurezza?* » R. BILLÈ, « *Patriotismo? costituzionale e libertà di informazione: il caso statunitense*, cit., p.138.

³⁶ K. RUZENSKI: *Balancing Fundamental Civil Liberties and the Need for Increased Homeland Security: the Attorney-Client Privilege After September 11TH*, 19 St. John's J.L. Comm. 46 (2005), p.437: « *The Patriot Act is regarded as a metaphor for many violations of constitutional rights.* » N. GRAHAM, in *Patriot Act II and Denationalization: an Unconstitutional Attempt to Revive Stripping Americans of Their Citizenship*, 52 Clev. St. L. Rev. 593, (2004-2005) p. 594 e ss., riscontra una violazione costituzionale nell'intento governativo (espresso nella sez. 501 del *Patriot Act*) di privare della cittadinanza, senza il loro consenso, gli americani che procurano supporto materiale alle organizzazioni terroristiche. La sentenza di riferimento è *Afroyim v. Rusk*, 387 U.S. 253 (1967) che riconduce il diritto alla cittadinanza sotto la protezione del XIV emendamento. Un altro intervento legislativo che condivide con il *Patriot Act* il fine della lotta al terrorismo è l'emendamento al *Bureau of Prisons*, del 31 ottobre 2001. Entrambi i provvedimenti sono definiti « nemici della libertà » dalle organizzazioni di tutela dei diritti civili. Si veda: K. RUZENSKI: *Balancing Fundamental Civil Liberties and the Need for Increased Homeland Security: the Attorney-Client Privilege After September 11TH*, cit., p. 485 e ss.

³⁷ U.S. Const. amend. IV: « *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly*

describing the place to be searched, and the persons or things to be seized. »

³⁸ D. HARRISON, in *The USA PATRIOT Act: A New Way of Thinking, an Old Way of Reacting*, Higher Education Responds, 5 N.C. J.L. & Tech. 177, (2004) p. 185: « *In response to the September 11 attacks, the PATRIOT Act thrusts the Fourth Amendment back to the forefront of the national consciousness. Title II fundamentally changes the relationship of a communications provider to those it serves and increases the power of law enforcement to perform surveillance and to retrieve information. These changes are seen by many, on all sides of the political and civil liberties spectrum, as significantly altering the privacy landscape in the United States of America.* »

³⁹ D. HARRISON, in *The USA PATRIOT Act: A New Way of Thinking, an Old Way of Reacting*, Higher Education Responds, op. cit., p. 184, sostiene che l'aspettativa di *privacy*, nell'era digitale, vada comunque modificata poiché, sebbene il *Patriot Act* riguardi la sorveglianza dal governo, dev'essere compreso che nell'età digitale ogni aspettativa di *privacy* va ricostruita con la consapevolezza che la tecnologia lascia chiare e durature tracce delle attività dell'utente. L'uso di internet e l'invio di e-mail sono per loro natura non private e non può esserci un'aspettativa di *privacy* nel loro uso.

⁴⁰ USA PATRIOT Act, sez. 215(a)(1) « *The Director of the Federal Bureau of Investigation . . . may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.* »

dente a riguardo permetteva solo le registrazioni riguardanti i sospettati, sulla base di specifici e ragionevoli indizi, di appartenere a servizi segreti stranieri⁴¹.

La sezione 215 del *Patriot Act* ha cambiato sia l'ambito sia i presupposti in base ai quali l'autorità di polizia può richiedere la produzione di registrazioni e documenti, eliminando precedenti restrizioni sul tipo di informazioni ottenibili e sulla necessità di provare il nesso tra l'obiettivo dell'indagine e le registrazioni richieste⁴².

Un altro aspetto del diritto alla privacy che può dirsi ridefinito dalla normativa anti-terrorismo è il diritto alla segretezza delle comunicazioni tra avvocato e cliente.

Il 31 ottobre 2001, dopo soli cinque giorni dall'introduzione del *Patriot Act*, il procuratore Generale *Ashcroft* ha emanato un provvisorio emendamento al *Bureau of Prisons*⁴³, riducendo pesantemente le garanzie di segretezza riconosciute alle comunicazioni tra i detenuti ed i loro avvocati⁴⁴.

L'intento della norma è di evitare che il detenuto, comunicando con l'esterno tramite il proprio avvocato, possa organizzare azioni terroristiche

⁴¹ La legge emendata dal *Patriot Act* è la 50 U.S.C. 1862(a) (2000). D. HARRISON in *The USA PATRIOT Act: A New Way of Thinking, an Old Way of Reacting, Higher Education Responds*, cit., p. 197, propone un confronto tra le due normative, giungendo alla conclusione che i poteri delle corti di obbligare alla produzione di documenti e libri non sono molto più ampi dei poteri attribuiti ai giudici durante investigazioni di carattere ordinario. Non vanno, dunque, assecondate le crescenti paure seguite all'approvazione del *Patriot Act*. Di parere opposto l'*American Civil Liberties Union (ACLU)* che ha citato il governo sostenendo che la formulazione della sezione 215 fomenta una infondata paura verso le attività e le organizzazioni musulmane. Tra le violazioni della *privacy* paventate vi è anche quella inerente le letture abituali. Secondo la sezione 215 i gestori di biblioteche devono rivelare agli organi investigativi le preferenze di lettura dei loro clienti, se ciò è ritenuto utile alle indagini sulla commissione di un crimine. A tale riguardo, già la sentenza *Brown v. Johnston*, 328 N.W.2d 510, 511 (Iowa 1983), pur riconoscendo un diritto alla segretezza delle letture, aveva però escluso la prevalenza di tale diritto sull'interesse pubblico ad investigazioni criminali. Si veda: J. PERRINE, *The USA PATRIOT Act: Big Brother or Business as Usual?* 19 ND J. L. Ethics & Pub. Pol'y 163, (2005)p. 192; V. DINH: *How the USA Patriot Act Defends Democracy*, 2 Geo. J.L. & Pub. Pol'y 393 (2004), p. 395.

⁴² D. HARRISON, *The USA PATRIOT*

Act: A New Way of Thinking, an Old Way of Reacting, Higher Education Responds, op. cit., p. 197 e ss. R. BILLÈ «Patriottismo» costituzionale e libertà di informazione: il caso statunitense, cit., p. 143 «risulta sufficiente per la polizia federale certificare la rilevanza delle informazioni ai fini delle indagini senza doverne comunque dare dimostrazione. Rispettati questi vincoli al giudice non rimane altro che emanare l'ordine di sequestro, non avendo alcuna discrezionalità in merito». La nuova normativa prevede, tuttavia, un limite: le investigazioni condotte secondo quanto stabilito dalla sez. 215, se coinvolgono la sfera intima di un cittadino americano non possono riguardare esclusivamente attività protette dal Primo Emendamento alla costituzione e, dunque, libertà di religione, parola, stampa, associazione. *USA PATRIOT Act*, sez. 215(a)(2).

⁴³ *Dep't. of Justice, Bureau of Prisons*, 66 Fed. Reg. 55062 (Oct. 31, 2001)

⁴⁴ Le comunicazioni confidenziali tra avvocato e cliente, finalizzate a dare ed ottenere consigli legali, sono sempre state protette dall'ordinamento americano. In questo senso, con la sentenza *Upjohn v. United States*, 449 U.S. 383, 389 (1981), la corte sottolinea che il diritto alla comunicazione tra avvocato e cliente è la più antica delle comunicazioni confidenziali conosciute dal *common law*. Il sesto emendamento alla Costituzione americana prevede, inoltre: «in all criminal prosecutions, the accused shall enjoy the right ... to have the Assistance of Counsel for his defense.»

o atti di violenza. Se, dunque, il Procuratore Generale ha il ragionevole sospetto che le comunicazioni tra avvocato e cliente possano essere usate per facilitare atti di violenza o terrorismo, può decidere di ascoltare le relative conversazioni⁴⁵.

Tra le conseguenze del *Patriot Act* non vi è solo una ridefinizione dei diritti costituzionalmente tutelati, ma — come spesso è accaduto nella storia delle istituzioni statunitensi — una restrizione delle garanzie processuali⁴⁶.

Il *Patriot Act*, infatti, riconsidera anche le norme sulle notificazioni di garanzia, prevedendo che, pur nel pieno rispetto di quanto stabilito da provvedimenti, ordini dei giudici ed ogni regola di legge per cercare e acquisire le prove di un crimine, ogni notizia richiesta dall'indagato può essere fornita con un certo ritardo, se il giudice ha ragionevoli elementi per ritenere che provvedere immediatamente alla notifica possa avere conseguenze sfavorevoli per le indagini⁴⁷. Tra le conseguenze sfavorevoli previste vi sono il pericolo di sicurezza fisica di un individuo, il pericolo di fuga dell'indagato, l'intimidazione dei testimoni, la falsificazione di prove o grave inquinamento delle indagini⁴⁸.

Con l'intento di combattere il terrorismo, il *Patriot Act* ha reso più penetranti anche le norme riguardanti le intercettazioni telefoniche.

La sezione 214 permette agli investigatori di ottenere dalla *FISA Court*⁴⁹ l'utilizzo di un dispositivo capace di registrare i numeri delle

⁴⁵ *Bureau of Prisons, U.S. Dep't of Justice*, 28 C.F.R. 500, 501.3 d) (2002). Si veda: K. RUZENSKI, *Balancing Fundamental Civil Liberties and the Need for Increased Homeland Security: the Attorney-Client Privilege After September 11th*, cit., p.467; L'American Bar Association e la National Association of Criminal Defense Lawyers concordano nell'affermare che ascoltare le comunicazioni tra avvocato e cliente, così come stabilito dalla normativa, costituisce una violazione del sesto emendamento. La Costituzione riconosce il diritto dell'accusato a parlare in via confidenziale con un avvocato. Secondo la nuova normativa, un accusato, temendo di essere ascoltato, potrebbe sentirsi inibito nel parlare liberamente. Secondo la normativa, come emendata dal *Patriot Act*, il Procuratore Generale deve innanzi tutto valutare che il soggetto possa considerarsi sospettato di « terrorism » o di « acts of violence », ed eventualmente sarà poi un gruppo separato di avvocati a valutare le comunicazioni e ad eliminare ogni informazione confidenziale che non possa essere ricondotta al progetto di un nuovo crimine o ad operazioni di terrorismo.

⁴⁶ Si veda: J. SOMA-M. NICHEL-S. RYNERSON-L. MAISH-J. ROGERS, *Balance of Privacy vs. Security: A Historical Perspective of the USA Patriot Act*, cit., p.311 e ss. Gli autori sottolineano che già in preceden-

za il governo degli Stati Uniti, sulla scorta di eventi significativi, si è trovato a bilanciare l'equilibrio tra *privacy* e sicurezza in favore di quest'ultima. Nel 1798 con l'*Alien and Sedition Act* propose misure restrittive volte a scongiurare le infiltrazioni di giacobini francesi sovversivi; durante la guerra civile americana, il presidente Lincoln dichiarò lo stato di emergenza e la « sospensione » dei diritti civili in alcuni Stati; un altro esempio di restrizioni al godimento di diritti civili è ancora l'internamento di nippo-americani durante la seconda guerra mondiale, considerato sostanzialmente legittimo dalla Corte Suprema statunitense sulla base del principio generale del « *salus rei publicae suprema lex esto* » (v. *Korematsu vs. United States*, 323 U.S.214 (1944); il *Foreign Intelligence Surveillance Act* del 1978. Si veda D. HARRISON, *The USA PATRIOT Act: A New Way of Thinking, an Old Way of Reacting, Higher Education Responds*, cit., p. 178.

⁴⁷ Sez. 213, (2)(b)USA PATRIOT Act.

⁴⁸ V. DINH, *How the USA Patriot Act Defends Democracy*, cit., p. 393. J. PERRINE, *The USA PATRIOT Act: Big Brother or Business as Usual?*cit., p.167 e ss.

⁴⁹ La *FISA Court* è un organo segreto composto da giudici nominati dal Presidente della Corte Suprema, con il compito di autorizzare le indagini investigative con-

chiamate effettuate e ricevute da un telefono, solo certificando che le informazioni risultanti potrebbero essere rilevanti per un'indagine contro il terrorismo internazionale o le attività di spionaggio clandestine⁵⁰.

Mentre la normativa precedente in materia autorizzava solo l'intercettazione di un determinato apparecchio telefonico⁵¹, la sezione 206 del *Patriot Act* permette alla *FISA* di autorizzare, in alcune circostanze, anche le « *roving wiretaps* », una forma di « intercettazione itinerante » che riguarda tutte le telefonate che coinvolgono l'indagato⁵². I vantaggi per le forze di polizia nell'uso delle « intercettazioni mobili », rispetto a quelle « statiche » stanno nel non dover ritornare dalla corte per un nuovo ordine di sorveglianza ogni volta che l'obiettivo dell'indagine cambia posizione, potendo invece presentare un generico ordine con l'avvertimento che la sorveglianza avrà inizio non appena tecnicamente attuabile⁵³.

Le norme del *Patriot Act* limitano le garanzie connesse alle libertà civili, e pertanto il Congresso, nel 2001, aveva acconsentito all'approvazione del *Patriot Act* solo laddove fosse stato predisposto un meccanismo di decadenza automatica delle sue disposizioni più limitative, che tuttavia sarebbero rimaste in vigore anche oltre la data di scadenza naturale solo in caso di un voto di rinnovo delle stesse ad opera del Congresso. Nel dicembre 2005 il Senato ha bocciato la proposta di rinnovo del *Patriot Act*, che ha, così, ottenuto solo una proroga di un mese, poi rinnovata per un altro mese. Il 2 marzo 2006, dopo l'approvazione da parte del senato del *Usa Patriot and Terrorism Preventive Reauthorization Act of 2005* e del *Usa Patriot Act Additional Reauthorizing Amendments Act of 2006* da parte della *House of Representatives*, tali proroghe sono state rese permanenti⁵⁴.

La normativa *Atsa*, ed il *Patriot Act* ben riproducono i caratteri della legislazione dello stato d'eccezione, in cui il bisogno di sicurezza può introdurre limitazioni nel godimento di diritti fondamentali⁵⁵.

dotte dalle agenzie governative in indagini relative ad intelligence straniera e terrorismo. Si veda R. BRILLÈ, « *Patriottismo* » costituzionale e libertà di informazione: il caso statunitense, cit., p. 143.

⁵⁰ Sez. 214, *USA PATRIOT Act*. Si veda J. POKULA, *Perspectives on the Usa Patriot Act: the Patriot Act: Indispensable Tool Against Terror*, 76 PA Bar Assn. Quarterly, 33, (2005) p. 36.

⁵¹ La normativa precedente, emendata dal *Patriot Act* è il *Foreign Intelligence Surveillance Act* del 1978, 50 U.S.C. 1801-11 (2000) e 18 U.S.C. 2511, 2518-19 (2000).

⁵² Questo tipo di intercettazione è impiegata quando l'indagato può ostacolare l'identificazione di uno specifico mezzo di comunicazione da intercettare. Sez. 206, *USA Patriot Act*.

⁵³ J. PERRINE, *The USA Patriot Act: Big Brother or Business as Usual?*, 19

ND J. L. Ethics & Pub Pol'y 163, (2005), p. 176 e ss.; D. HARRISON, *The USA PATRIOT Act: A New Way of Thinking, an Old Way of Reacting*, *Higher Education Responds*, cit., p. 194 e ss.

⁵⁴ R. BRILLÈ, « *Patriottismo* » costituzionale e libertà di informazione: il caso statunitense, cit., 150-151.

⁵⁵ D. HARRISON, *The USA PATRIOT Act: A New Way of Thinking, an Old Way of Reacting*, *Higher Education Responds*, cit., p. 178: « *The tensions that are inherent in the debate between surveillance needs and the preservation of civil liberties have their roots in the fundamental struggle of community interests versus individual interests — a struggle that has defined much of the history of the United States, from the Declaration of Independence through the Constitution, Bill of Rights, and the statutes and judicial interpretations that have followed.* ».

La conferma di validità del *Patriot Act* e le persistenti difficoltà nel negoziare un accordo sul trasferimento dei dati personali dei passeggeri — l'annullamento della Corte di Giustizia, ha, infatti, riguardato la base giuridica della decisione, lasciando insolute molte questioni inerenti al contenuto dell'accordo — sembrano assegnare alle istanze di protezione tipiche dello stato d'eccezione il carattere della permanenza, privando della necessaria tutela i diritti e le libertà civili.

DANIELA MAFFEI