camente dal gruppo di lavoro, tenuto conto degli effetti generalizzati che avrebbero sui diritti fondamentali delle persone interessate.

Il sistema CAPPS II solleva in particolare un certo numero di questioni specifiche che richiedono non solo una particolare attenzione da parte del gruppo di lavoro, ma anche clausole di salvaguardia diverse e più efficaci. Qualunque decisione futura sul sistema CAPSS II dovrà essere analizzata specificamente dal gruppo di lavoro e non dovrà derivare da un'estensione automatica del campo di applicazione della prima decisione della Commissione sul livello di protezione adeguato dei trasferimenti di dati passeggeri PNR verso gli Stati Uniti.

Di conseguenza, considerando che il gruppo di lavoro non è stato informato né consultato a proposito del quadro giuridico definitivo del sistema CAPSS II, qualunque utilizzazione di dati a carattere personale da parte della TSA nel quadro del sistema CAPSS II così come è proposta e qualunque prova relativa dovranno essere esclusi ora e in futuro dal campo di applicazione della decisione della Commissione. In altri termini, le riflessioni contenute nel presente parere si basano sul presupposto secondo il quale la decisione della Commissione non sarà estesa in futuro al sistema CAPPS II, né direttamente, né indirettamente attraverso un riferimento alla legislazione interna degli Stati Uniti. In caso contrario, sarebbe opportuno esprimere sin d'ora osservazioni molto più critiche.

Di conseguenza, il gruppo di lavoro raccomanda alla Commissione di precisare, attraverso una clausola specifica nella decisione, che le autorità americane devono astenersi dall'utilizzare i dati passeggeri PNR trasmessi dall'UE non solo per mettere in opera il sistema CAPPS II, ma anche per effettuare le relative prove.

Il gruppo di lavoro ritiene che una simile clausola dovrà inoltre applicarsi a qualunque altra utilizzazione dei dati sui passeggeri europei trasmessi dalle compagnie aeree nel quadro di altri programmi quali "Terrorism Information Awareness" e "US VISIT" o i programmi di trattamento di dati biometrici.

4. Livello degli impegni

Il gruppo di lavoro ricorda che qualunque decisione della Commissione non dovrà basarsi su semplici "impegni" da parte delle autorità amministrative, ma su impegni che siano ufficialmente pubblicati almeno a livello del Registro federale e abbiano forza esecutiva negli Stati Uniti. Più in particolare, non dovrà esserci dubbio in merito all'effetto creativo di diritti a vantaggio di terzi.

Su tale punto, è chiaro che gli impegni presi dagli Stati Uniti non avranno forza esecutiva dal lato degli Stati Uniti. Inoltre, il nuovo paragrafo 47 aggiunto alla fine della dichiarazione d'intenti chiarisce in modo esplicito la forza esecutiva degli impegni presi dagli Stati Uniti, disponendo che "essi non creano diritti o vantaggi a beneficio di persone o parti, private o pubbliche".

Il gruppo di lavoro sottolinea pertanto che il livello degli impegni da parte degli Stati Uniti non può essere considerato come conforme alle esigenze poste nel suo parere 4/2003 e considera che tale questione sia una condizione essenziale che dovrà essere affrontata prima che possa essere formalizzato un accordo.

5. Aspetti specifici

Tenuto conto del contesto globale sopra descritto, le domande americane, così come esse risultano dalla dichiarazione d'intenti (versione aggiornata del 12 gennaio 2004) devono essere valutate alla luce dei pareri emessi in questo settore dal gruppo di lavoro, in particolare il parere 4/2003 del 13 giugno 2003.

A. NATURA TRANSITORIA DEL LIVELLO DI PROTEZIONE ADEGUATO

Un durata di tre anni e mezzo è stata suggerita per l'insieme delle misure, compresi la dichiarazione d'intenti, la constatazione di protezione adeguata e l'accordo internazionale corrispondente.

Il gruppo di lavoro accoglie con favore l'introduzione di una "clausola di caducità" dell'accordo e spera che il periodo di tre anni e mezzo proposto nel suo parere 4/2003 sarà preso in considerazione.

B. LIMITAZIONE AD UNA FINALITÀ SPECIFICA

Il DHS (Ministero americano della sicurezza interna) utilizzerà i dati passeggeri PNR per le esigenze del CBP, al fine di prevenire e combattere:

1) Il terrorismo e i crimini connessi
2) Altri reati gravi, compreso il crimine organizzato, di natura transnazionale;
3) la fuga dall'arresto o custodia per i crimini sopra descritti.

Il gruppo di lavoro rileva che la descrizione delle finalità dell'uso dei dati PNR è più rigorosa e precisa di quanto non fosse in precedenza. Tuttavia, la categoria 2 rimane vaga, in particolare per quanto riguarda il campo di applicazione degli "altri reati gravi" indicati nella dichiarazione americana. Inoltre, la finalità delle misure rimane molto più ampia della lotta contro gli atti di terrorismo, sulla quale il gruppo di lavoro riteneva che fosse opportuno mantenere l'accento (parere 4/2003).

C. ELENCO DEI DATI DA TRASFERIRE

Il CBP propone ora che i trasferimenti di dati passeggeri PNR comprenda un elenco di 34 elementi informativi, e ciò è stato approvato dalla Commissione. Questo elenco risulta dall'esclusione di 4 ambiti di dati (identificazione dei biglietti gratuiti, numero dei bagagli, numero di bagagli per ciascun segmento, passaggi alla classe superiore volontari/involontari) dalla lista dei 38 elementi PNR che figura all'Allegato B della dichiarazione d'intenti del 22 maggio 2003 [3].

Il gruppo di lavoro osserva che i progressi realizzati per quanto riguarda l'elenco dei dati da trasmettere sono molto limitati. In effetti, l'elenco americano modificato contiene sempre i 20 elementi di cui il gruppo di lavoro riteneva il trasferimento sproporzionato e problematico nel suo parere 4/2003.

È opportuno inoltre rilevare che le autorità americane hanno fatto passare il numero di elementi da trasmettere da 38 a 34 solo sopprimendo quattro elementi che erano stati accettati dal gruppo di lavoro nel suo parere del 13 giugno. Per quanto riguarda i 20 elementi che continuano ad essere richiesti dalle autorità americane anche se non sono stati accettati dal gruppo di lavoro, non è stata fornita alcuna indicazione o spiegazione per giustificare la necessità del loro trattamento o il loro carattere proporzionale e non eccessivo nella lotta contro il terrorismo in una società democratica.

Il gruppo di lavoro ricorda l'elenco dei 19 elementi accettati nel suo parere del 13 giugno 2003, e il fatto che qualunque aggiunta a questo elenco è soggetta ad una rigorosa verifica dei principi di proporzionalità e di minimizzazione dei dati.

D. DATI SENSIBILI

Il dialogo ha in particolare consentito di fare in modo che alcuni dati PNR non saranno utilizzati, ma soppressi dalle autorità americane, tenendo presente che a tale riguardo l'articolo 8, paragrafo 1, della direttiva fa riferimento ai dati a carattere personale che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento dei dati relativi alla salute e alla vita sessuale.

(3) Anche se l'Allegato B della dichiarazione d'intenti del 22 maggio 2003 enumera 39 elementi, solo 38 possono realmente figurare in un PNR, poiché il vecchio settore OSI ("other service information") dovrebbe essere utilizzato solo se un codice SSR ("special service request") non è disponibile, conformemente al servizio di prenotazione IATA-Manuale, 20a edizione, effettivo 1° giugno 2003 - 31 maggio 2003, punto 10.3, pag. 127.

L'elenco dei codici e degli ambiti dei dati da sopprimere non è ancora disponibile. Il gruppo di lavoro tiene tuttavia a sottolineare che se alcuni codici devono chiaramente essere soppressi (ad esempio quelli che riguardano le preferenze alimentari, lo stato di salute o le condizioni religiose, quali "Tariffa pellegrino", "missionario" o "clero", altri codici richiedono un esame approfondito, in particolare gli ambiti "liberi" del tipo "Notazioni generali" che sono suscettibili di contenere dati sensibili. Nella loro dichiarazione d'intenti (versione 12 gennaio) le autorità americane fanno sapere che questi elementi sarebbero soppressi attraverso l'utilizzazione di un elenco di parole che fanno scattare la procedura di soppressione. Un simile approccio non garantisce l'eliminazione dell'insieme dei dati sensibili che figurano in questi ambiti. Pertanto l' unica soluzione sicura consisterebbe nell'escludere questi campi dal trasferimento, conformemente al parere 4/2003.

A tale proposito, il gruppo di lavoro ricorda il suo parere del 13 giugno 2003 secondo il quale il trasferimento di dati sensibili deve essere escluso. Non si può quindi prevedere di procedere a soppressioni solo dopo aver trasmesso i dati sensibili alle autorità americane. Il gruppo di lavoro invita la Commissione a trovare soluzioni tecniche adeguate (come ad esempio filtri) al fine di evitare qualunque trasmissione di dati sensibili alle autorità americane.

E. Utilizzazione dei dati derivati dalla pratiche passeggeri PNR

In una formula aggiunta alla dichiarazione, le autorità americane descrivono le limitazioni che esistono per quanto riguarda il loro accesso ai dati "derivati" da pratiche PNR i quali sono suscettibili di rivelare alcuni aspetti della vita di un passeggero e rischiano di interferire gravemente con il diritto della persona interessata a una vita privata e familiare, conformemente all'articolo 8 della Convenzione europea dei diritti dell'uomo. La nuova formulazione è la seguente:

"Ulteriori informazioni personali ricercate come risultato diretto dei dati del PNR possono essere ottenute da fonti estranee al governo solo mediante canali legali, e solo a fini legittimi di contrasto del terrorismo o di applicazione delle leggi. Ad esempio, se in un PNR figura un numero di carta di credito, possono essere ricercate informazioni sulle transazioni legate a quel conto mediante procedimenti legali come un ordine di comparizione emesso da un gran giurì o da un giudice, o come altrimenti previsto dalla legge. Inoltre, l'accesso ai dati relativi agli indirizzi di posta elettronica ottenuti da un PNR deve rispettare le norme di legge degli USA per gli ordini di comparizione, i provvedimenti dei giudici, i mandati d'arresto e gli altri procedimenti autorizzati dalla legge, a seconda del tipo delle informazioni ricercate."

Questi chiarimenti sono benvenuti. Tuttavia, non dissipano completamente le preoccupazioni del gruppo di lavoro. In particolare, le finalità per le quali i dati passeggeri PNR possono essere utilizzati non devono comprendere altri imperativi di "applicazione delle leggi" non specificati. Inoltre, l'accesso alle messaggerie elettroniche e ad altre informazioni personali derivate da una pratica PNR deve iscriversi unicamente nel quadro delle esigenze procedurali previste negli strumenti internazionali di cooperazione giudiziaria e di polizia. Inoltre, deve essere chiaro che in caso di abuso un individuo può presentare un ricorso dinanzi a un'autorità indipendente.

F. Periodo di conservazione dei dati

Il CBP conserverà i dati passeggeri PNR ai fini convenuti dal CBP per tre anni e mezzo. I dati che sono consultati manualmente durante questo periodo saranno conservati in uno schedario di dati cancellati per altri 8 anni.

Il gruppo di lavoro rileva che si tratta di un miglioramento rispetto ai 7 anni inizialmente proposti nella dichiarazione del 22 maggio. Una durata di tre anni e mezzo rimane tuttavia molto più lunga del periodo di "alcune settimane o alcuni mesi" auspicato dal gruppo di lavoro nel suo parere 4/2003. Il gruppo di lavoro dubita che l'immagazzinamento generalizzato dell'insieme dei dati PNR per periodi così lunghi possa essere giudicato "proporzionale e necessario in una società democratica".

Inoltre, la conservazione dei dati per altri otto anni, prevista per il semplice caso in cui tali dati siano stati consultati, è sproporzionata nella misura in cui non vi è un collegamento con un'inchiesta concreta o un mandato concernenti la persona i cui dati sono consultati; ciò rende quindi possibile superare de facto il limite di tre anni e mezzo.

Da notare al riguardo che è possibile prevedere soluzioni che sono più rispettose dei principi di protezione dei dati, ma che restano efficaci nella lotta contro la criminalità. L'Australia, ad esempio, ha elaborato un sistema nel quadro del quale le dogane di questo paese conservano o immagazzinano dati su un passeggero solo se quest'ultimo ha commesso un atto illegale o se i dati sono necessari per le esigenze di un'inchiesta riguardante un presunto delitto.

G. Metodo di trasferimento

Per quanto riguarda il metodo di trasferimento, il gruppo di lavoro ricorda il suo parere 4/2003 nel quale considera che il solo meccanismo di trasferimento la cui attuazione non crea problemi gravi è quello del "push" (tramite il quale i dati sono selezionati e trasferiti dalle compagnie aeree alle amministrazioni americane) piuttosto che quello del "pull" (tramite il quale le autorità americane hanno un accesso in linea diretto alle basi di dati delle compagnie aeree ed ai sistemi di prenotazione).

Anche se le autorità americane non pongono più obiezioni da alcuni mesi sul sistema "push", il gruppo di lavoro è estremamente preoccupato per il fatto che i meccanismi tecnici che consentono di applicare un tale sistema gestito direttamente dalle compagnie aeree europee non sono ancora in funzione. Il gruppo di lavoro ritiene che debbano essere attuate misure concrete entro l'aprile del 2004 e incoraggia vivamente la Commissione ad adottare immediatamente le misure necessarie per raggiungere questo obiettivo. Inoltre, il gruppo di lavoro sottolinea che il livello di protezione assicurato dagli Stati Uniti non potrà essere considerato come adeguato senza l'instaurazione di un sistema "push".

H. Momento del trasferimento

Nel suo parere 4/2003, il gruppo di lavoro ritiene che i servizi dell'US CBP dovrebbero ricevere i dati relativi a un volo specifico non prima di 48 ore prima del decollo. Dopo di ciò, i dati dovrebbero essere aggiornati una sola volta.

Su questo punto, l'ultima versione della dichiarazione è rigorosamente fedele alla versione precedente, che prevede un trasferimento dei dati 72 ore prima del decollo e un massimo di tre aggiornamenti.

Il gruppo di lavoro deplora che non sia stato ottenuto alcun miglioramento su questo punto durante i negoziati.

I. Trasferimento di dati passeggeri PNR verso altre autorità amministrative o estere

Nel suo parere 4/2003, il gruppo di lavoro chiede che gli altri organismi pubblici abilitati a ricevere i dati siano identificati con precisione, aggiungendo che qualunque ulteriore trasferimento diretto o indiretto dovrà essere subordinato all'accettazione di impegni specifici almeno altrettanto favorevoli di quelli che sono forniti alla Commissione dalle autorità americane per quanto riguarda la protezione dei dati trasferiti. Inoltre, il numero di autorità suscettibili di ricevere i dati dovrà essere ristretto.

Il gruppo di lavoro nota che non è stato ancora redatto alcun elenco globale delle autorità cui i dati sono suscettibili di essere trasferibili. Inoltre, il gruppo di lavoro rimane preoccupato dalle disposizioni che consentono al CBP di divulgare dati conformemente alle "altre esigenze previste dalla legge", in particolare se queste disposizioni sono previste alla luce delle leggi e dei protocolli di accordo che obbligano gli Stati Uniti a condividere i loro dati con altri paesi.

In particolare, il meccanismo di cui ai punti 29 e 35 della dichiarazione differisce sensibilmente dal principio di limitazione ad una specifica finalità così come affermato dal gruppo di lavoro (vale a dire la lotta contro il terrorismo e i reati connessi con il terrorismo) e anche dalle più ampie finalità così come definite ai punti 1 e 3 della dichiarazione.

J. GARANZIE – DIRITTI DELLE PERSONE INTERESSATE

1) INFORMAZIONI CHIARE ALLE PERSONE INTERESSATE

Ai termini del parere 4/2003, e conformemente all'articolo 10 della direttiva, un'informazione chiara e precisa dovrebbe essere fornita alle persone interessate sull'identità del responsabile del trattamento, sulla finalità del trattamento e su qualunque altra informazione, come l'esistenza di un diritto di accesso e di rettifica e le vie di ricorso effettive che sono aperte.

Il gruppo di lavoro rileva che il CBP fornirà informazioni ai viaggiatori. A tal fine, il gruppo di lavoro osserva che sarà possibile redigere rapidamente una nota informativa tipo una volta che il quadro giuridico sarà stato fissato in modo più preciso, tenuto conto anche del progetto sottoposto al gruppo di lavoro. È tuttavia opportuno considerare che una nota informativa globale può servire quale complemento, ma in nessun caso può considerarsi un sostituto ai requisiti giuridici che devono essere rispettati affinché i trasferimenti di dati passeggeri PNR verso gli Stati Uniti siano legittimi.

2) ACCESSO

Nel suo parere del 4/2003, il gruppo di lavoro sottolinea la necessità di garanzie realmente applicabili con riferimento alle regole generali poste dalla Legge sulla libertà d'informazione (FOIA), al fine di garantire che queste ultime non saranno utilizzate da terzi per accedere a dati passeggeri PNR in possesso dell'amministrazione americana e che il diritto di accesso delle persone interessate ai propri dati sarà rispettato in modo generale e non ambiguo.

Per quanto riguarda l'accesso dei terzi, il gruppo di lavoro accoglie favorevolmente i chiarimenti forniti dal CBP nel documento "Exemptions Under the Freedom of Information Act (FOIA) Applicable to Passenger Name Record (PNR) Data".

Tuttavia, per quanto riguarda l'accesso dei passeggeri ai propri dati, il gruppo di lavoro continua ad avere timori sul modo in cui talune esenzioni potrebbero essere utilizzate per opporsi ai diritti di una persona interessata, consentendo in tal modo all'amministrazione di rifiutarle l'accesso ai suoi dati.

Inoltre, il gruppo di lavoro sottolinea che il diritto di accesso delle persone interessate non è stato esplicitamente esteso, come era auspicato nel parere 4/2003, ai nuovi dati suscettibili di essere generati dal trattamento dei dati trasmessi dall'Europa (profilo di rischio, elenchi d'esclusione, ecc.).

3) RETTIFICA

Nel suo parere 4/2003, il gruppo di lavoro insiste sull'importanza di fornire alle persone interessate un meccanismo efficace per ottenere la rettifica dei loro dati. Il gruppo di lavoro rileva che il campo d'applicazione della legge americana sulla vita privata ("US Privacy Act") è limitato ai residenti americani. Pertanto la questione della non discriminazione dei residenti europei rispetto ai cittadini americani non è sempre risolta ed è opportuno determinare se il meccanismo di rettifica esposto nella dichiarazione possa essere considerato uno strumento efficace e giuridicamente vincolante per quanto riguarda il diritto di rettifica che il FOIA concede ai cittadini americani e ai residenti esteri.

4) RICORSI

Il "DHS Privacy Office" (Ufficio responsabile per la protezione della vita privata del Ministero della sicurezza interna) ha concordato di esaminare rapidamente i ricorsi che gli saranno presentati dalle autorità incaricate della protezione dei dati degli Stati membri per conto di un residente dell'Unione europea il quale ritenga che il DHS, compreso il suo "Privacy Office", non ha trattato il suo ricorso in modo soddisfacente.

Il gruppo di lavoro accoglie con favore questa evoluzione. È importante che una persona possa ottenere un aiuto qualificato in alcuni casi; tuttavia, la questione relativa all'indipendenza reale del "Chief Privacy Officer" (direttore responsabile per la privacy del DHS) così come è stata sollevata nel parere 4/2003 del gruppo, non è stata ancora risolta. I membri del gruppo di lavoro ritengono che le disposizioni interne che sono state adottate per quanto riguarda le funzioni del "panel" cui si fa riferimento nell'FAQ 5 dell'Accordo sulla sfera di sicurezza possano essere utili in questo contesto. Essi studieranno le correzioni che sarà eventualmente opportuno effettuare al fine di un'applicazione nel contesto dei PNR.

Il gruppo di lavoro deplora d'altro canto che i passeggeri non abbiano la garanzia di poter ricorrere in tutti casi a un meccanismo di ricorso veramente indipendente in caso di controversie con il DHS. Inoltre, sembra ora che la dichiarazione non avrà effetti giuridici vincolanti né genererà obblighi il cui rispetto possa essere preteso dinanzi a un tribunale (cfr. il precedente punto 9). Ciò costituisce un'importante differenza rispetto ai diritti di cui gode qualunque individuo i cui dati sono trattati nell'UE, indipendentemente dalla sua nazionalità.

K. Audit

La nuova formulazione seguente è stata inserita nella dichiarazione d'intenti (paragrafo 43) "Il CBP, in collaborazione col DHS, s'impegna a partecipare, una volta all'anno o anche più spesso se così deciso dalle parti, a un'analisi congiunta con la Commissione, assistita come del caso da esperti degli Stati membri dell'Unione europea (4), sull'attuazione della presente dichiarazione d'intenti, al fine di contribuire da entrambe le parti all'effettivo funzionamento dei procedimenti descritti nella dichiarazione stessa. Detta analisi congiunta può riguardare i risultati della relazione annuale presentata al Congresso dal direttore per la privacy del DHS (come previsto al paragrafo 42 della presente dichiarazione d'intenti) e, nella misura in cui ciò è autorizzato dal direttore per la privacy, tutti gli audit effettuati nel periodo cui si riferisce la relazione, o altri risultati riguardanti in particolare la sicurezza dei dati, la condivisione del PNR con le autorità designate e l'accesso personale al PNR nelle banche dati rilevanti, nonché il trattamento dei reclami. Nella misura in cui ciò è autorizzato dal direttore per la privacy del DHS, l'analisi congiunta può comprendere un esame dell'applicazione della dichiarazione d'intenti e può anche riguardare questioni che possono aiutare a migliorare i risultati dell'uso dei dati del PNR ai fini di cui al paragrafo 3 della presente dichiarazione d'intenti."

Si tratta di un'altra evoluzione favorevole e il gruppo di lavoro si aspetta che tali revisioni siano realizzate con l'apertura e la trasparenza necessarie a garantirne l'efficacia. In ogni caso, i membri del gruppo di lavoro s'impegnano a partecipare eventualmente a qualunque revisione di questo tipo e ad osservare le regole di confidenzialità concordate tra le due parti. Il gruppo di lavoro si riserva evidentemente il diritto di rianalizzare la questione, se lo ritiene necessario, qualunque sia il calendario di tali revisioni.

L. Analisi incrociata di schede

I recenti avvenimenti dimostrano che un nuovo elemento deve essere preso in considerazione oltre a quelli che sono stati ricordati sino ad ora. I dati passeggeri PNR raccolti dal CBP sono confrontati negli Stati Uniti con elenchi di persone ricercate.

Queste operazioni di analisi incrociata di schede sono all'origine dell'annullamento all'ultimo minuto di molti voli provenienti dall'UE. Le informazioni fornite successivamente al pubblico mostrano che tali annullamenti erano dovuti ad errori o a casi di confusione d'identità o di omonimia con persone sospettate di terrorismo.

Queste circostanze si iscrivono nel quadro della qualità dei dati e del principio di protezione dei dati. Il gruppo di lavoro ritiene che altre iniziative debbano essere adottate per evitare di esporre i passeggeri, i membri dell'equipaggio e le compagnie aeree a questo tipo di problemi.

(4) La composizione delle équipe delle due parti sarà comunicata in anticipo e può comprendere le autorità competenti per la privacy/la protezione dei dati, i controlli doganali e altre forme di applicazione delle norme, sicurezza dei confini e/o dell'aviazione. Le autorità partecipanti dovranno rispettare la riservatezza delle discussioni e saranno sottoposte ai nulla osta di sicurezza eventualmente necessari. La riservatezza però non sarà un ostacolo a che entrambe le parti possano riferire in modo appropriato dei risultati dell'analisi congiunta alle rispettive autorità competenti, compresi il Congresso degli USA e il Parlamento europeo. Le due parti determinano insieme le modalità dettagliate per l'analisi congiunta.

CONCLUSIONI

Il gruppo di lavoro ricorda che l'obiettivo globale, conformemente a quanto indicato nel suo parere 4/2003, è la messa a punto di un quadro giuridico chiaro affinché qualunque trasferimento di dati delle compagnie aeree verso gli Stati Uniti sia compatibile con i principi di protezione dei dati personali. Il gruppo di lavoro ha preso nota dei progressi realizzati nel dialogo USA-UE per quanto riguarda i dati passeggeri PNR, in particolare l'ultima dichiarazione del 12 gennaio 2004 recentemente presentata dall'amministrazione americana, ed esprime soddisfazione per i miglioramenti rispetto alla versione precedente.

Secondo il gruppo di lavoro, tuttavia, i limitati progressi che sono stati registrati non consentono di giudicare che sia stato raggiunto un livello adeguato di protezione dei dati. Il gruppo di lavoro ritiene che qualunque soluzione dovrà rispettare almeno i seguenti principi di protezione dei dati:

Qualità dei dati:
- il trasferimento di dati deve unicamente avere come finalità la lotta contro gli atti di terrorismo e taluni reati collegati al terrorismo (da definire);
- l'elenco dei dati da trasferire deve essere proporzionale e non deve essere eccessivo;
- le analisi incrociate di dati relativi a individui sospetti devono rispettare norme di qualità elevate in grado di garantire la certezza dei risultati;
- i periodi di conservazione dei dati devono essere brevi e proporzionali;
- i dati dei passeggeri non devono essere utilizzati per realizzare e/o sperimentare il sistema CAPPS II o sistemi analoghi.

I dati sensibili non devono essere trasmessi.

Diritti delle persone interessate:
- È opportuno trasmettere informazioni chiare, attuali e comprensibili ai passeggeri;
- Un diritto d'accesso e di rettifica deve essere concesso senza discriminazioni;
- È opportuno prevedere disposizioni sufficienti in grado di garantire ai passeggeri il diritto di rivolgersi a un organo di ricorso veramente indipendente.

Livello d'impegno delle autorità americane:
- Gli impegni presi dalla parte americana devono avere un carattere giuridico chiaramente vincolante per gli USA;
- È opportuno chiarire il campo di applicazione, la base giuridica e il valore di un eventuale "accordo internazionale leggero".

Gli ulteriori trasferimenti di dati passeggeri PNR ad altri governi o organismi esteri devono essere strettamente limitati.

Metodo di trasferimento: è opportuno utilizzare un metodo di trasferimento "push", attraverso il quale i dati sono selezionati e trasferiti dalle compagnie aeree alle amministrazioni americane.

Fatto a Bruxelles, il 29 gennaio 2004

Dal gruppo di lavoro
Il Presidente
Stefano RODOTÀ

92 Opinion 3/2004 on the level of protection ensured in Canada for the transmission of Passenger Name Records and Advanced Passenger Information from airlines (*)

ARTICLE 29 Data Protection Working Party

10037/04/EN
WP 88

Opinion 3/2004 on the level of protection ensured in Canada for the transmission of Passenger Name Records and Advanced Passenger Information from airlines

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/internal_market /privacy/docs/wpdocs /2004/wp88_en.pdf

Adopted on 11th February 2004

Nuove Tecnologie

93 Documento di lavoro sull'amministrazione elettronica

ARTICOLO 29 – Gruppo di lavoro per la tutela dei dati personali

10593/02/IT
WP 73

Documento di lavoro sull'amministrazione elettronica

Adottato l'8.5.2003

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/internal_market /privacy/docs/wpdocs /2003/e-government_it.pdf

94 Parere 2/2003 sull'applicazione dei principi di tutela dei dati agli elenchi Whois (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

10972/03/IT
def. WP 76

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito a seguito della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995 [1],

visti gli articoli 29 e 30, paragrafi 1, lettera a), e 3, di tale direttiva, e l'articolo 14, paragrafo 3, della direttiva 97/66/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997,

visto il regolamento interno, in particolare gli articoli 12 e 14,

ha adottato il presente parere:

1. Introduzione:

Gli elenchi Whois pongono vari problemi dal punto di vista della tutela dei dati. I *dati Whois* si riferiscono alle persone che hanno registrato un nome di dominio e contengono in particolare informazioni sul nome del punto di contatto del nome del dominio, inclusi numero di telefono, indirizzo e E-mail e altri dati personali. Inizialmente tali dati sono stati pubblicati per consentire alle persone che effettuano attività in rete di contattare la persona tecnicamente responsabile di un'altra rete o di un altro dominio, in caso di problema. Di per se stesso, tale obiettivo è legittimo.

Il gruppo è consapevole dell'importanza crescente assunta dal dibattito su Whois a mano che un numero sempre maggiore di individui (privati) registrano i loro nomi di dominio e che sono state sporte denunce per l'uso improprio dei dati Whois in vari paesi. La registrazione di nomi di dominio da parte di singoli pone considerazioni giuridiche diverse da quelle di società o di altre persone giuridiche che registrano nomi di dominio, come verrà chiarito nel presente parere.

Il gruppo ha quindi seguito con interesse i lavori della Task Force ICANN Whois riguardanti tali elenchi Whois nonché i lavori svolti in questo campo dal gruppo internazionale per la protezione dei dati nelle telecomunicazioni [2].

Il gruppo è consapevole del fatto che gli elenchi Whois saranno discussi nel quadro della conferenza ICANN/GAC che si terrà a Montreal alla fine del mese di giugno. Il gruppo gradirebbe contribuire alla discussione presentando il suo parere, mirante a sottolineare un certo numero di questioni fondamentali che sorgono con l'applicazione dei principi di protezione dei dati agli elenchi Whois. Il parere riguarda gli elenchi Whois ma, nella misura in cui le stesse circostanze o circostanze simili vi si riferiscano, le stesse considerazioni si applicano anche ad altri registri di nomi di dominio e di indirizzi IP a livello regionale, ad esempio RIPE in Europa, AP-NIC in Asia, ecc.

2. L'applicazione dei principi della protezione dei dati agli elenchi Whois:

- Dal punto di vista della tutela dei dati, è indispensabile determinare in termini estr mamente chiari quale sia l'obiettivo degli elenchi Whois e quali obiettivi possano

(*) Il gruppo di lavoro è stato istituito ai sensi dell'articolo 29 della direttiva 95/46/CE. È un organo europeo indipendente a carattere consultivo in materia di tutela dei dati e della vita e della vita privata. I suoi compiti sono illustrati all'articolo 30 della direttiva 95/46/CE e all'articolo 14 della direttiva 97/66/CE. Le funzioni di segretariato sono espletate dalla Direzione E (Servizi, Proprietà intellettuale e industriale, Media e Protezione dei dati) della Commissione europea, Direzione generale mercato interno, B-1049 Bruxelles, Belgio, Ufficio n. C100-6/136. Website: www.europa.eu.int /comm/privacy

(1) Gazzetta ufficiale L 281 del 23/11/1995, pag. 31, disponibile su: http://europa.eu.int /comm/internal_market/en /media/dataprot/index.htm

(2) Posizione comune sugli aspetti della vita privata e della tutela dei dati della registrazione dei nomi di dominio su Internet, adottata in occasione della 27ª riunione del gruppo di lavoro il 4/5 maggio 2000 a Rethymnon/Creta, disponibile su: www.datenschutz-berlin.de /doc/int/iwgdpt /dns_en.htm

considerarsi legittimi e compatibili con l'obiettivo originale. Le relazioni della Task Force Whois non hanno trattato questi aspetti. Si tratta di una questione estremamente delicata, dato che l'obiettivo degli elenchi Whois non può essere esteso ad altri obiettivi per il semplice fatto che possano essere ritenuti convenienti da certi potenziali utilizzatori degli elenchi. Alcuni obiettivi che potrebbero sollevare problemi connessi con la tutela di dati (compatibilità) sono ad esempio l'utilizzazione di dati da parte di operatori del settore privato nell'ambito di attività di polizia private connesse con presunte violazioni dei loro diritti, ad esempio nel campo della gestione dei diritti digitali.

- L'articolo 6, lettera c) della direttiva impone chiari limiti quanto alla raccolta e all'elaborazione di dati personali nel senso che essi debbono essere pertinenti e non eccessivi per i fini cui sono destinati. In questa prospettiva è indispensabile limitare la quantità di dati personali da raccogliere e elaborare. Di ciò si dovrebbe tener particolarmente conto al momento di discutere il desiderio di alcune parti interessate di aumentare l'uniformità dei vari elenchi Whois.
  La registrazione di nomi di dominio da parte di singoli pone considerazioni giuridiche diverse da quelle di società o di altre persone giuridiche che registrano nomi di dominio.
  - Nel primo caso, la pubblicazione di determinate informazioni circa la società o l'organizzazione (ad esempio, identificazione e indirizzo fisico) è frequentemente un requisito legale nell'ambito delle attività commerciali o professionali svolte. Occorre peraltro osservare che, anche nel caso di società o di organizzazioni che registrano nomi di dominio, i singoli non possono essere obbligati a fornire il loro nome da pubblicare come punto di contatto, dato che possono esercitare il loro diritto di opposizione.
  - Nel secondo caso, ove un singolo registri un nome di dominio, la situazione è diversa e, quantunque sia chiaro che l'identità e il contatto debbano essere conosciuti dal fornitore del servizio, non esiste giustificazione giuridica alla pubblicazione obbligatoria dei dati personali di tale persona. Una tale pubblicazione di dati personali di persone, ad esempio i loro indirizzi e numeri di telefono, verrebbe a scontrarsi con il diritto di tali persone di decidere se i dati di carattere personale loro relativi, e quali di tali dati, debbano figurare in un elenco pubblico [3]. Peraltro l'obiettivo originale di tali elenchi Whois può essere ugualmente raggiunto, in quanto i particolari della persona sono noti al fornitore di servizi Internet che può, in caso di problemi connessi con il sito, contattare la persona [4].

• Alla luce del principio della proporzionalità, è necessario cercare metodi meno invasivi in grado di raggiungere gli obiettivi degli elenchi Whois senza rendere tutti i dati direttamente disponibili on-line per chiunque. Come già menzionato nell'introduzione, i fornitori di servizi Internet possono svolgere, e di fatto lo fanno in alcuni paesi, un ruolo importante in questo campo. In ogni caso dovrebbero essere elaborati meccanismi di filtraggio per garantire una limitazione degli obiettivi nelle interfacce per accedere agli elenchi.

• Il fatto che dati personali sono resi pubblici non significa che i requisiti della direttiva sulla tutela dei dati non si applicano a tali dati. Al contrario, come si è già affermato nei precedenti pareri del gruppo [5], è perfettamente chiaro, dalla formulazione della legislazione in merito alla tutela dei dati, che le disposizioni si applicano anche ai dati resi pubblici: anche dopo essere stati resi pubblici, i dati restano tuttora personali e, di conseguenza, le persone interessate non possono essere private della protezione cui hanno diritto per quanto riguarda il trattamento dei loro dati.

• Il gruppo è particolarmente preoccupato delle proposte relative a dispositivi Whois dotati di maggiori possibilità di ricerca. In questo contesto esso gradirebbe menzionare le conclusioni del suo parere 5/2000 sull'utilizzazione degli elenchi telefonici pubblici per servizi di ricerca inversa o multicriterio (elenchi invertiti) [6]: l'elaborazione di dati personali in elenchi invertiti e in servizi di ricerca multicriterio senza il consenso chiaro e informato della persona interessata è sleale e illecita.

(3) Articolo 12, paragrafo 2, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

(4) Un sistema del genere è stato istituito in vari paesi europei, ad esempio in Francia (attraverso l'AFNIC) e nel Regno Unito. Nel Regno Unito, ad esempio, le persone singole che registrano nomi di dominio ('tag-holders') possono registrarsi negli elenchi Whois a cura del loro FSI, il che significa che, in caso di problema con un sito web, si può contattare il proprietario attraverso l'FSI senza che l'indirizzo della persona in questione figuri in una base dati aperta.

(5) Parere n. 3/99 relativo alle informazioni del settore pubblico e alla protezione di dati personali, WP 20.

(6) http://europa.eu.int /comm/internal_market /en/dataprot/wpdocs /wpdocs_2k.htm

• Il gruppo desidera esprimere il suo sostegno alle proposte relative alla precisione dei dati (che è altresì uno dei principi della direttiva europea sulla tutela dei dati [7]) e alla limitazione dell'accesso massiccio a fini di marketing diretto.

L'utilizzazione intensiva dei dati Whois per il marketing diretto è totalmente in contraddizione con i fini per i quali sono stati allestiti e vengono gestiti gli elenchi. Alla luce delle disposizioni della direttiva sulle comunicazioni elettroniche [8] qualsiasi utilizzazione di indirizzi E-mail per il marketing diretto deve basarsi unicamente sul consenso della persona interessata.

Il gruppo invita l'ICANN e la comunità Whois ad esaminare modalità per aumentare la protezione della vita privata nella gestione degli elenchi Whois, in modo sia da raggiungere l'obiettivo originale sia da proteggere i diritti delle persone. Dovrebbe essere comunque possibile, per persone singole, registrare nomi di dominio senza che sia necessario che i loro dati personali figurino in un registro pubblico.

Per il gruppo
Il presidente
Stefano RODOTA

(7) Cfr. articolo 6, lettera d) della direttiva.
(8) Direttive 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

95 Documento di lavoro sulle piattaforme informatiche fidate, in particolare per quanto riguarda il lavoro effettuato da Trusted Computing Group (Gruppo TCG) (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

11816/03/FR
WP 86

Documento di lavoro sulle piattaforme informatiche fidate, in particolare per quanto riguarda il lavoro effettuato da Trusted Computing Group (Gruppo TCG)

Adottato il 23 gennaio 2004

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/internal_market /privacy/docs/wpdocs /2004/wp86_it.pdf

Codici di Condotta comunitari

96 Parere 3/2003 sul codice di condotta europeo della FEDMA per l'utilizzazione dei dati personali nel marketing diretto (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

10066/03/EN def
GL 77

Parere 3/2003 sul codice di condotta europeo della FEDMA per l'utilizzazione dei dati personali nel marketing diretto

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/internal_market /privacy/docs/wpdocs /2003/wp77_it.pdf

Adottato in data 13 giugno 2003

97 Sixth annual report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries covering the year 2001 (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

Sixth annual report
on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries
covering the year 2001

adopted on 16th December 2003

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/internal_market /privacy/docs/wpdocs/2003 /2003-6th-annualreport_en.pdf

25ª Conferenza internazionale delle Autorità di protezione dei dati. Sydney 10-12 settembre 2003

98 Risoluzione relativa al miglioramento della comunicazione di informazioni sulle politiche seguite in materia di protezione dei dati e privacy (*)

Proponente: Autorità per la privacy, Australia; co-sponsors:
- Autorità per la protezione dei dati e l'accesso agli atti, Brandeburgo, Germania
- Commissione nazionale informatica e libertà, Francia
- Autorità per la protezione dei dati, Repubblica Ceca
- Autorità ellenica per la protezione dei dati
- Centro indipendente per la tutela della privacy, Schleswig-Holstein, Germania
- Ispettorato statale per la protezione dei dati, Repubblica di Lituania
- Autorità olandese per la protezione dei dati

RISOLUZIONE

La 25ma Conferenza internazionale delle Autorità di protezione dati e della privacy adotta la seguente risoluzione:

1. La Conferenza richiama l'attenzione di soggetti pubblici e privati sull'importanza
   - di migliorare significativamente la comunicazione delle informazioni da essi fornite sulle modalità di gestione e trattamento di dati personali,
   - di raggiungere una coerenza complessiva nelle modalità di comunicazione di tali informazioni,

e, così facendo,

   - di migliorare la comprensione e la sensibilizzazione dei singoli rispetto ai diritti ed alle opzioni disponibili e la rispettiva capacità di incidere su tali diritti e opzioni, e
   - di incentivare i vari soggetti, in seguito a tale sensibilizzazione, a migliorare le politiche seguite nella gestione e nel trattamento dei dati e ad accrescerne la lealtà e correttezza.

2. La Conferenza si fa promotrice dei seguenti strumenti ai fini del raggiungimento degli obiettivi prima citati:
   - messa a punto e utilizzazione di un formato sintetico per la presentazione di un quadro complessivo delle informazioni in materia di privacy che sia standardizzato a livello mondiale per tutti i soggetti e stabilisca
     - le informazioni più importanti da rendere note ai singoli, le informazioni che con maggiore probabilità i singoli desiderano conoscere, e l'impiego di un linguaggio semplice, inequivocabile e diretto;
     - l'impiego della lingua del sito web o del modulo utilizzati per la raccolta delle informazioni;
   - previsione della limitazione del formato ad un numero ristretto di elementi che, coe-