

IT

IT

IT



COMMISSIONE EUROPEA

Bruxelles, 21.9.2010
COM(2010) 492 definitivo

COMUNICAZIONE DELLA COMMISSIONE

sull'approccio globale al trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) verso paesi terzi

COMUNICAZIONE DELLA COMMISSIONE

sull'approccio globale al trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) verso paesi terzi

1. INTRODUZIONE

Gli attentati terroristici del 2001 negli Stati Uniti, del 2004 a Madrid e del 2005 a Londra hanno determinato un nuovo approccio alle politiche di sicurezza interna. I falliti attentati terroristici su un aereo nel Natale del 2009 e a Times Square a New York nel 2010 mostrano che il terrorismo è una minaccia reale. Nel contempo, va aumentando la criminalità organizzata, in particolare il traffico di stupefacenti e la tratta di esseri umani¹.

In risposta a queste minacce continue, l'UE e altri paesi terzi hanno adottato nuove misure, fra cui la raccolta e lo scambio di dati personali, che la Commissione ha presentato nel suo documento "Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia"². L'uso dei dati PNR a fini di contrasto è una di queste misure.

Il 16 gennaio 2003 la Commissione ha presentato al Consiglio e al Parlamento europeo la comunicazione "Trasferimento di dati di identificazione delle pratiche (PNR): un approccio globale dell'UE"³ in cui illustrava gli elementi di un approccio europeo globale ai dati PNR. La comunicazione invitava altresì a istituire un valido quadro giuridico per i trasferimenti di dati PNR al Dipartimento per la sicurezza interna degli Stati Uniti e ad adottare una politica interna in materia di dati PNR; esortava inoltre a sviluppare il sistema "push" per il trasferimento dei dati a cura dei vettori aerei⁴ e ad adottare un'iniziativa internazionale per il trasferimento di dati PNR nell'ambito dell'Organizzazione internazionale dell'aviazione civile (ICAO).

Gran parte delle conclusioni della comunicazione sono state attuate e altre sono in fase di attuazione. L'UE ha firmato un accordo con il Dipartimento per la sicurezza interna degli Stati Uniti sul trasferimento dei dati PNR per combattere il terrorismo e altri reati gravi di natura transnazionale, che autorizza il trasferimento dei dati PNR nel rispetto della protezione dei dati personali⁵. La Commissione dal canto suo ha adottato una proposta di decisione quadro sull'uso dei dati del codice di prenotazione nelle attività di contrasto⁶ e sta valutando, sulla base di una valutazione d'impatto, l'opportunità di sostituire tale proposta con una proposta di direttiva sullo stesso argomento. La maggior parte dei vettori aerei ha sviluppato adeguatamente il sistema "push" di trasferimento dei dati, e l'ICAO ha elaborato una serie di orientamenti per il trasferimento dei dati PNR ai governi.

Oltre all'accordo con gli Stati Uniti, l'UE ha firmato accordi analoghi con il Canada⁷ e con l'Australia⁸. Anche la Nuova Zelanda, la Corea del Sud e il Giappone usano i dati del codice di prenotazione ma, alla data del presente documento, non hanno ancora concluso accordi con

¹ Eurostat 36/2009.

² COM(2010) 385.

³ COM(2003) 826.

⁴ Con il sistema "push" è il vettore aereo che trasmette i dati al paese terzo e non già il paese terzo che accede alle banche dati del vettore aereo.

⁵ OJ L 204 del 4.8.2007, pag. 16.

⁶ COM(2007) 654.

⁷ GU L 91 del 29.3.2006, pag. 53; GU L 91 del 29.3.2006, pag. 49; GU L 82 del 21.3.2006, pag. 15.

⁸ OJ L 213 dell'8.8.2008, pag. 49.

l'UE. All'interno dell'Unione, il Regno Unito ha introdotto un sistema PNR altri Stati membri hanno emanato leggi in materia o stanno testando l'uso dei dati PNR.

Questi sviluppi dimostrano che l'uso dei dati PNR è in aumento ed è sempre più spesso considerato un aspetto normale e necessario delle attività di contrasto. Esso tuttavia comporta il trattamento di dati personali e quindi solleva importanti questioni di rispetto della vita privata e della protezione dei dati personali, che sono diritti fondamentali.

Di conseguenza l'UE è confrontata a nuove sfide per quanto riguarda il trasferimento internazionale dei dati PNR. È assai probabile che nei prossimi anni aumenteranno nel mondo i paesi che sviluppano sistemi PNR. Inoltre l'UE ha acquisito una conoscenza approfondita della struttura e del valore dei sistemi PNR grazie all'esperienza delle verifiche congiunte degli accordi con gli USA e il Canada.

La Commissione ritiene pertanto necessario riconsiderare il suo approccio globale al trasferimento dei dati PNR verso i paesi terzi. Tale revisione dovrebbe apportare maggiori salvaguardie sul fronte della protezione dei dati e il pieno rispetto dei diritti fondamentali, ed essere in linea con i principi di elaborazione delle politiche esposti nel documento "Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia"⁹. Particolarmente importanti ai fini del nuovo approccio ai dati PNR sono le posizioni sulle problematiche generali PNR delle principali parti interessate, quali gli Stati membri, il Parlamento europeo, il Garante europeo della protezione dei dati e il Gruppo di lavoro articolo 29 per la protezione dei dati.

L'obiettivo principale della presente comunicazione è istituire, per la prima volta, un insieme di criteri generali su cui basare i futuri negoziati per la conclusione di accordi PNR con i paesi terzi. L'UE potrà così far fronte alle attuali tendenze e la Commissione disporrà di un metodo per comunicare ai paesi terzi, agli Stati membri e ai cittadini il modo in cui intende definire la sua politica esterna in materia di dati PNR. In futuro, le raccomandazioni della Commissione relative ai negoziati per gli accordi PNR con i paesi terzi dovranno quanto meno rispettare i criteri generali stabiliti nella comunicazione, fermo restando che ogni raccomandazione potrà fissare criteri aggiuntivi.

2. TENDENZE INTERNAZIONALI IN MATERIA DI DATI PNR

2.1. Dati PNR e loro uso

I dati del codice di prenotazione (PNR) sono informazioni non verificate fornite dai passeggeri e raccolte dai vettori aerei ai fini della prenotazione e delle operazioni di check-in; riguardano il viaggio di ciascun passeggero e sono conservati nei sistemi di prenotazione e di controllo delle partenze dei vettori aerei; contengono vari tipi di informazioni, come la data del viaggio, l'itinerario, i dati sull'emissione del biglietto, i recapiti quali l'indirizzo e i numeri di telefono, l'agente di viaggio, le modalità di pagamento, il numero di posto assegnato e le informazioni relative al bagaglio.

I dati PNR sono diversi dai dati API (Advance Passenger Information) che sono dati anagrafici raccolti dalla banda a lettura ottica del passaporto comprendenti il nome, il luogo di residenza, il luogo di nascita e la cittadinanza dell'interessato. Ai sensi della direttiva API¹⁰, tali dati sono messi a disposizione delle autorità di controllo alla frontiera solo per i voli diretti verso l'UE al fine di migliorare i controlli alle frontiere e combattere l'immigrazione

⁹ COM(2010) 385.

¹⁰ Direttiva 2004/82/CE del Consiglio, del 29 aprile 2004, concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate.

illegale. Sebbene la direttiva permetta di utilizzare i dati API per altre finalità di applicazione normativa, tale uso costituisce l'eccezione e non la regola. I dati API sono conservati dagli Stati membri per 24 ore.

I dati API sono usati principalmente per i controlli di identità nell'ambito dei controlli alle frontiere e della gestione delle frontiere, anche se in alcuni casi li usano anche le autorità di contrasto per identificare persone sospette e ricercati. Sono quindi impiegati soprattutto come strumento di gestione delle identità. Il loro uso sta diventando sempre più comune a livello mondiale: sono oltre 30 i paesi che li usano sistematicamente e oltre 40 quelli che stanno istituendo un sistema API.

Oltre ai dati API, alcuni paesi impongono ai vettori aerei di trasmettere anche i dati PNR. Questi sono usati per combattere il terrorismo e altri reati gravi, quali la tratta di esseri umani e il traffico di stupefacenti. I dati PNR sono stati usati per quasi 60 anni, perlopiù dalle autorità doganali ma anche dalle autorità di contrasto in tutto il mondo. Tuttavia fino a poco tempo fa non era tecnologicamente possibile accedere in anticipo e elettronicamente a tali dati, pertanto se ne limitava l'uso al trattamento manuale e solo per alcuni voli. Le tecnologie odierne permettono ormai la trasmissione elettronica anticipata di tali dati.

L'uso dei dati PNR varia molto da quello dei dati API, soprattutto perché i primi contengono informazioni assai varie. I dati PNR servono principalmente come strumento di intelligence criminale e non come strumento di verifica dell'identità e sono usati essenzialmente: i) per valutare i rischi posti dai passeggeri e identificare le persone "non note", ossia quelle ancora non considerate sospette ma che potrebbero interessare le autorità di contrasto; ii) perché sono disponibili prima dei dati API e lasciano quindi più tempo per le autorità di contrasto per trattarli, analizzarli e provvedere al follow-up; iii) per individuare le persone cui appartengono specifici indirizzi, carte di credito, ecc. connessi a reati; iv) per confrontare dati PNR allo scopo di individuare complici, ad esempio scoprendo chi viaggia insieme.

I dati PNR sono unici per natura e uso. L'uso può essere:

reattivo (dati storici): nel quadro di indagini, azioni penali, per lo smantellamento di reti dopo la commissione di un reato. Perché le autorità di contrasto possano risalire sufficientemente indietro nel tempo, è necessario prevedere un periodo di conservazione dei dati a beneficio di queste autorità che sia commisurato;

in tempo reale (dati attuali): per prevenire reati, svolgere indagini o arrestare persone prima o dopo che sia commesso un reato o in flagranza di reato. In tali casi i dati PNR sono necessari per effettuare confronti con indicatori di rischio fattuali predeterminati al fine di individuare i sospetti precedentemente "non noti" e per effettuare confronti con varie banche dati di persone e oggetti ricercati;

proattivo (modelli): per analizzare tendenze e creare modelli di spostamento e comportamento generale basati su fatti, utilizzabili in tempo reale. Per creare modelli di spostamento e comportamento gli analisti delle tendenze devono poter usare i dati per un periodo sufficientemente lungo. È pertanto necessario prevedere un periodo di conservazione dei dati a beneficio delle autorità di contrasto che sia commisurato.

2.2. Tendenze attuali

Alcuni paesi terzi (Stati Uniti, Canada, Australia, Nuova Zelanda e Corea del Sud) usano già i dati PNR a fini di contrasto. Altri (Giappone, Arabia Saudita, Sudafrica e Singapore) hanno emanato leggi in materia e/o stanno testando l'uso dei dati PNR. Molti altri paesi terzi hanno iniziato a valutare l'opportunità di usare i dati PNR ma non hanno ancora emanato leggi al riguardo. All'interno dell'Unione, il Regno Unito ha già introdotto un sistema PNR. La Francia, la Danimarca, il Belgio, la Svezia e i Paesi Bassi dispongono della pertinente

legislazione e/o stanno testando l'uso dei dati PNR. Molti altri Stati membri stanno valutando l'opportunità di istituire sistemi PNR.

La Commissione europea, riconoscendo la necessità dei dati PNR ai fini della prevenzione e della lotta al terrorismo e altri reati gravi, in linea con la comunicazione del 2003 ha presentato una proposta di decisione quadro sull'uso dei dati del codice di prenotazione nelle attività di contrasto. A seguito dell'entrata in vigore del trattato di Lisbona, la Commissione sta valutando l'opportunità di sostituire tale proposta con una proposta di direttiva sullo stesso argomento. L'obiettivo della proposta sarà imporre ai vettori aerei l'obbligo di trasmettere i dati PNR agli Stati membri a fini di lotta contro il terrorismo e altri reati gravi.

È opinione sempre più diffusa a livello internazionale che i dati PNR siano uno strumento necessario nella lotta contro il terrorismo e altri reati gravi. Questa tendenza risulta da tre fattori. Primo, il terrorismo e la criminalità internazionale sono una grave minaccia per la società che occorre affrontare con adeguate misure. L'accesso ai dati PNR e la loro analisi è una delle misure ritenute necessarie sotto il profilo del contrasto. Secondo, recenti progressi tecnologici hanno reso possibile tali accesso e analisi che solo pochi anni fa erano inconcepibili. Di tali progressi tecnologici si avvalgono però ampiamente anche i criminali per pianificare, preparare e commettere i reati. Terzo, considerato il rapido aumento dei viaggi internazionali e del volume dei passeggeri, il trattamento elettronico dei dati prima dell'arrivo dei passeggeri facilita di molto e accelera i controlli di sicurezza e alle frontiere in quanto il rischio è valutato prima dell'arrivo. In tal modo le autorità di contrasto possono concentrarsi solo sui passeggeri per i quali sussistono motivi fattuali di ritenere che possano costituire un effettivo rischio per la sicurezza, anziché fare valutazioni basate sull'istinto, su stereotipi o su profili.

2.3. Effetti delle tendenze attuali sull'Unione europea

Le norme di protezione dei dati vigenti nell'UE vietano ai vettori aerei che effettuano voli in partenza dall'UE di trasmettere i dati PNR dei loro passeggeri a paesi terzi che non garantiscono un adeguato livello di protezione dei dati personali senza che siano adottate garanzie appropriate. Di conseguenza, quando gli Stati Uniti, il Canada e l'Australia hanno richiesto ai vettori aerei di trasmettere i dati PNR per i voli diretti in quei paesi, i vettori aerei si sono trovati in una situazione alquanto delicata. L'UE è quindi intervenuta e ha negoziato e firmato accordi internazionali distinti con questi tre paesi¹¹ rendendo possibile il trasferimento dei dati PNR al di fuori dell'UE alle autorità di contrasto di tali paesi. L'intervento dell'UE mirava a venire in aiuto ai vettori aerei, a garantire un livello di protezione adeguato dei dati dei passeggeri e a riconoscere la necessità e l'importanza dell'uso dei dati PNR nella lotta al terrorismo e altri reati gravi.

Essendo sempre più numerosi i paesi che attuano sistemi PNR, la stessa questione si riproporrà in futuro. Inoltre, se la Commissione decide di presentare una proposta di direttiva PNR dell'UE, la frequenza di tali richieste potrebbe aumentare in quanto i paesi terzi potrebbero chiedere che l'UE rispetti il principio di reciprocità.

Finora gli accordi internazionali PNR con paesi terzi sono stati conclusi “su richiesta”, caso per caso. Benché tutti gli accordi trattino questioni comuni e disciplinino la stessa materia, le

¹¹ Accordo PNR CE-USA del 2004 (GU L 183 del 20.5.2004, pag. 84) e decisione della Commissione del 14 maggio 2004 (GU 235 del 6.7.2004, pag. 11); Accordo PNR UE-USA del 2006 (GU L 298 del 27.10.2006, pag. 29) e lettere di accompagnamento (GU C 259 del 27.10.2006, pag. 1), accordo PNR UE-USA del 2007 (GU L 204 del 4.8.2007, pag. 18), accordo PNR UE-Canada (GU L 82 del 21.3.2006, pag. 15 e GU L 91 del 29.3.2006, pag. 49) e accordo PNR UE-Australia (GU L 213 dell'8.8.2008, pag. 47).

loro disposizioni non sono identiche. Ne consegue che talvolta le norme per i vettori aerei e la protezione dei dati sono difformi. Poiché è probabile che le richieste aumentino nei prossimi anni, una strategia potrebbe aiutare l'UE a trattare le richieste in modo più strutturato, riducendo le differenze tra i vari accordi.

3. UN APPROCCIO GLOBALE RIVISTO DELL'UE AI DATI PNR

3.1. Motivi alla base della revisione dell'approccio globale ai dati PNR

Proprio ora che vanno attuandosi le conclusioni della comunicazione del 2003 e che l'UE deve far fronte a nuove tendenze e sfide, è importante che l'Unione tenga debito conto di queste ultime sviluppando il suo approccio globale al trasferimento dei dati PNR verso paesi terzi, per i motivi che seguono.

Lotta al terrorismo e altri reati gravi di natura transnazionale: l'UE ha l'obbligo verso se stessa e i paesi terzi di cooperare con questi ultimi nella lotta contro tali minacce. Un metodo di cooperazione consiste nello scambio di dati con i paesi terzi. Mettere a disposizione i dati PNR a fini di contrasto è cosa necessaria per combattere il terrorismo e altri reati gravi di natura transnazionale. Sia la strategia sulla dimensione esterna nel settore della giustizia e degli affari interni¹² che la strategia antiterrorismo dell'Unione europea¹³ e il programma di Stoccolma¹⁴ evidenziano la necessità di cooperare strettamente con i paesi terzi.

Garantire la protezione dei dati personali e il rispetto della vita privata: l'UE si impegna ad assicurare una protezione effettiva e di livello elevato dei dati personali, e quindi a garantire che le trasmissioni di dati PNR verso paesi terzi avvengano in modo sicuro in linea con le norme UE vigenti, e che i passeggeri possano far valere i loro diritti in relazione al trattamento dei dati che li riguardano.

Necessità di garantire la certezza del diritto e di semplificare gli obblighi imposti ai vettori aerei: è importante che l'UE fornisca un quadro normativo coerente per la trasmissione dei dati PNR verso paesi terzi a cura dei vettori aerei, in modo da tutelare questi ultimi da sanzioni e garantire che le condizioni e le modalità di trasmissione dei dati a livello mondiale siano il più uniformi e armonizzate possibili, così da ridurre l'onere di costo per l'industria e garantire la parità delle condizioni di concorrenza nel settore.

Stabilire condizioni generali che garantiscano la coerenza e sviluppino un approccio internazionale: gli accordi PNR firmati dall'UE con alcuni paesi terzi sono simili per quanto riguarda l'oggetto ma variano in ordine alle modalità di trasmissione dei dati e alla natura degli impegni dei paesi terzi. Tale diversità di impegni è in parte accettabile, dato che ogni paese ha normative e ordinamenti giuridici diversi, ma tutti dovrebbero rispettare determinati criteri generali (v. oltre sezioni 3.2 e 3.3). Al fine di garantire un trattamento dei passeggeri quanto più uniforme e ridurre il costo per l'industria, è importante che il contenuto e le norme dei futuri accordi con i paesi terzi siano il più simili possibile. Ciò potrebbe costituire la base per il passo successivo: un approccio multilaterale più armonizzato allo scambio dei dati PNR.

Diminuire i disagi per i passeggeri: per contrastare le minacce alla sicurezza che incombono sulle nostre società, i controlli dei passeggeri ai valichi di frontiera sono sempre più scrupolosi e lunghi. Nel contempo, il volume dei viaggi internazionali è in continuo aumento e i tempi di attesa alle frontiere si allungano. La trasmissione elettronica anticipata dei dati PNR prima

¹² COM(2005) 491.

¹³ Documento del Consiglio 14469/4/05 del 30.11.2005.

¹⁴ Documento del Consiglio 17024/09 del 2.12.2009.

dell'attraversamento delle frontiere permette di controllare i passeggeri in anticipo, consentendo così a questi ultimi di attraversare le frontiere più rapidamente e più facilmente e alle autorità di contrasto di concentrarsi solo su persone già individuate che presentano un interesse.

3.2. Considerazioni generali

L'approccio globale rivisto ai dati PNR servirà all'UE da base per stabilire il modo migliore per trattare le future richieste dei paesi terzi di trasmettere dati PNR. Oltre ai principi di elaborazione delle politiche esposti nel documento "Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia", valgono le considerazioni che seguono.

Interesse comune per la sicurezza: terrorismo e altri reati gravi sono per natura internazionali. Alcuni paesi sono più esposti di altri alle crescenti minacce legate al terrorismo e altri reati gravi. L'UE si impegna a cooperare con loro e a prestare assistenza nella lotta contro tali minacce alla sicurezza.

Protezione dei dati personali: poiché la trasmissione, l'uso e il trattamento dei dati PNR incidono sul diritto fondamentale della persona alla protezione dei dati personali, è essenziale che l'UE cooperi solo con i paesi terzi che possono fornire un livello di protezione adeguato dei dati PNR provenienti dall'UE.

Relazioni esterne: occorre considerare anche le relazioni esterne globali dell'UE con il paese terzo. Il funzionamento e la cooperazione con il sistema giudiziario e le forze di polizia, lo Stato di diritto e il rispetto generale dei diritti fondamentali sono tutti importanti fattori di cui tenere conto.

3.3. Norme, contenuto e criteri

L'approccio globale ai dati PNR dovrebbe enunciare le norme generali che gli accordi internazionali tra l'UE e i paesi terzi dovrebbero rispettare per garantire la maggiore coerenza possibile per quanto riguarda le garanzie di protezione dei dati che tali paesi dovranno applicare e le modalità di trasmissione dei dati da parte dei vettori aerei.

È inoltre fondamentale che l'UE disponga di meccanismi per controllare la corretta attuazione degli accordi, ad esempio le verifiche periodiche congiunte, e di efficaci meccanismi di composizione delle controversie.

3.3.1. Protezione dei dati personali

La raccolta e il trasferimento dei dati PNR verso paesi terzi concerne un numero molto elevato di persone e i loro dati personali. La protezione efficace dei dati personali merita pertanto particolare attenzione.

In Europa, i diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale sono sanciti dall'articolo 8 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea¹⁵. Tali diritti fondamentali spettano a ogni persona, indipendentemente

¹⁵ Va rilevato che principi analoghi in materia di protezione dei dati sono contemplati da strumenti internazionali sulla protezione della vita privata e dei dati personali quali: l'articolo 17 del Patto internazionale relativo ai diritti civili e politici sul diritto alla vita privata del 16 dicembre 1966, gli Orientamenti delle Nazioni Unite per la gestione degli schedari computerizzati di dati personali (risoluzione 45/95 dell'Assemblea generale delle Nazioni Unite del 14 dicembre 1990), la raccomandazione del Consiglio dell'OCSE sugli orientamenti per la tutela della vita privata e i flussi transfrontalieri di dati personali e la Convenzione del Consiglio d'Europa sulla protezione delle persone

dalla cittadinanza e dal luogo di residenza. Altre norme sulla protezione dei dati sono contenute nella Convenzione n. 108 del 1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale e relativo protocollo addizionale n. 181 del 2001.

Eventuali limitazioni dell'esercizio dei diritti e delle libertà riconosciuti dalla Carta devono essere previste per legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere decise limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione, ovvero all'esigenza di proteggere i diritti e le libertà altrui.

Poiché i sistemi di protezione dei dati dei paesi terzi possono differire dalla protezione dei dati garantita nell'UE, è importante che per i trasferimenti di dati PNR da Stati membri dell'UE verso paesi terzi lo Stato terzo garantisca un livello adeguato di protezione dei dati in forza di una solida base giuridica. Tale livello adeguato può essere previsto dalla legislazione del paese terzo o da impegni giuridicamente vincolanti inseriti nell'accordo internazionale che disciplina il trattamento dei dati personali.

L'adeguatezza del livello di protezione garantito da un paese terzo deve essere valutata con riguardo a tutte le circostanze relative a un trasferimento di dati. In tale contesto, l'UE terrà conto anche del rispetto da parte del paese terzo delle norme internazionali, segnatamente la ratifica degli strumenti internazionali in materia di protezione dei dati e di diritti fondamentali in generale. Le decisioni di adeguatezza già adottate dalla Commissione europea in quest'ambito dovrebbero servire da orientamenti per stabilire cosa può considerarsi adeguato.

I principi di base cui i paesi terzi richiedenti dovrebbero attenersi in materia di protezione dei dati personali sono i seguenti.

- **Limitazione delle finalità – uso dei dati:** l'uso che un paese terzo può fare dei dati deve essere determinato con chiarezza e precisione nell'accordo e non deve essere più ampio di quanto necessario in vista degli obiettivi da conseguire. L'esperienza degli attuali accordi PNR insegna che i dati PNR dovrebbero essere usati solo a fini di contrasto e sicurezza per combattere il terrorismo e altri reati gravi di natura transnazionale. Le nozioni chiave di terrorismo e altri reati gravi di natura transnazionale dovrebbero essere definite in base al metodo di definizione seguito nei pertinenti strumenti giuridici dell'UE.
- **Limitazione delle finalità – scambio dei dati:** lo scambio dei dati dovrebbe essere limitato allo stretto necessario ed essere proporzionato. Ogni accordo dovrebbe elencare in modo tassativo le categorie di dati PNR da trasferire.
- **Categorie particolari di dati personali (dati sensibili):** i dati PNR che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la salute o l'orientamento sessuale possono essere usati solo in circostanze eccezionali di rischio imminente di perdite umane e purché il paese terzo offra garanzie appropriate (ad esempio, l'uso dei dati sensibili sarà possibile solo caso per caso, previa autorizzazione di un alto funzionario, e rigorosamente limitato alle finalità del trasferimento originario).
- **Sicurezza dei dati:** i dati PNR devono essere protetti contro l'utilizzo improprio e l'accesso non autorizzato, avvalendosi di tutte le procedure e misure tecniche e di sicurezza appropriate per prevenire rischi per la sicurezza, la riservatezza o l'integrità dei dati.

rispetto al trattamento automatizzato di dati a carattere personale (STCE n. 108) e relativo protocollo addizionale (STCE n. 181), cui possono aderire anche Stati non europei.

- **Supervisione e responsabilità:** deve essere disposto un sistema di supervisione in base al quale un'autorità pubblica indipendente incaricata della protezione dei dati e dotata di effettivi poteri d'intervento e contrasto potrà esercitare il controllo delle autorità pubbliche che usano i dati PNR. Queste ultime risponderanno del rispetto delle regole stabilite in materia di protezione dei dati personali; l'autorità indipendente dovrà essere competente a trattare i reclami di singoli individui in relazione al trattamento dei dati PNR.
- **Trasparenza e segnalazione:** ogni persona deve essere informata quanto meno delle finalità del trattamento dei dati personali, dell'identità del responsabile del trattamento, delle norme o leggi che lo giustificano, della tipologia dei terzi a cui i dati sono comunicati e delle modalità e autorità di ricorso.
- **Accesso, rettifica e cancellazione:** chiunque ha il diritto di accedere ai propri dati PNR e, se del caso, di farli rettificare o cancellare.
- **Ricorso:** chiunque ha il diritto a un ricorso effettivo, in sede amministrativa e giudiziaria, su base non discriminatoria indipendentemente dalla cittadinanza o dal luogo di residenza, qualora ne sia stato violato il diritto al rispetto della vita privata o alla protezione dei dati personali. Ogni violazione deve essere soggetta a sanzione e/o riparazione appropriata e efficace.
- **Decisioni individuali automatizzate:** le decisioni che comportano azioni o effetti negativi nei confronti di una persona non possono fondarsi esclusivamente su un trattamento automatizzato di dati personali senza partecipazione umana.
- **Conservazione dei dati:** il periodo di conservazione dei dati PNR non dovrebbe essere più lungo del tempo necessario per eseguire i compiti definiti. Tale periodo dovrebbe tenere conto dei vari modi in cui i dati PNR sono usati (v. sopra sezione 2.1) e le possibilità di limitare i diritti di accesso durante la sua durata, ad esempio rendendo gradualmente anonimi i dati.
- **Restrizioni dei trasferimenti successivi ad altre autorità governative:** i dati PNR possono essere comunicati ad altre autorità governative con poteri nella lotta al terrorismo e altri reati gravi di natura transnazionale solo se tali autorità garantiscono la stessa protezione offerta dal destinatario ai sensi dell'accordo, con un impegno nei confronti di quest'ultimo. I dati PNR non dovrebbero essere mai comunicati in blocco ma solo caso per caso.
- **Restrizioni dei trasferimenti successivi verso paesi terzi:** questa restrizione riguarda principalmente l'uso e l'ulteriore diffusione per evitare che le disposizioni dell'accordo vengano eluse quando i dati PNR sono messi a disposizione di un altro paese terzo. Tali trasferimenti successivi devono essere oggetto di garanzie appropriate. In particolare, il paese terzo ricevente può trasferire tali informazioni alle autorità competenti di un altro paese terzo solo se quest'ultimo s'impegna a trattare i dati allo stesso livello di protezione stabilito dall'accordo e il trasferimento è rigorosamente limitato alle finalità del trasferimento originario. I dati PNR non dovrebbero essere mai trasferiti in blocco ma solo caso per caso.

3.3.2. *Modalità di trasmissione*

Al fine di garantire la certezza del diritto e ridurre al minimo l'onere finanziario a carico dei vettori aerei, è importante semplificare le norme che disciplinano la trasmissione dei dati da parte dei vettori aerei verso paesi terzi. Obblighi uniformi consentirebbero di ridurre notevolmente l'onere finanziario a carico dei vettori aerei, che dovrebbero sostenere meno

investimenti per adempiere ai loro obblighi. A tal fine, sarebbe auspicabile che venissero uniformate almeno le seguenti modalità di trasmissione.

- **Metodo di trasmissione:** per proteggere i dati contenuti nelle banche dati dei vettori aerei e mantenerne il controllo, bisognerebbe procedere al trasferimento esclusivamente in base al sistema "push".
- **Frequenza di trasmissione:** dovrebbe essere fissato un limite ragionevole al numero di volte in cui un paese terzo può chiedere la trasmissione dei dati, in modo da garantire un adeguato vantaggio in termini di sicurezza e nel contempo ridurre al minimo i costi per i vettori aerei.
- **Nessun obbligo per i vettori aerei di raccogliere dati supplementari:** i vettori aerei non dovrebbero essere tenuti a raccogliere altri dati in aggiunta a quelli che già raccolgono, né a raccogliere determinati tipi di dati; ai vettori può essere richiesto soltanto di trasmettere le informazioni che di norma raccolgono nello svolgimento delle loro attività.

3.3.3. *Concetti generali*

- **Durata e riesame:** i termini della cooperazione con i paesi terzi dovrebbero essere validi per un periodo determinato e prevedere la possibilità per le parti di denunciare l'accordo. Dovrebbe essere possibile rivedere i termini della cooperazione ove ritenuto opportuno.
- **Monitoraggio:** è fondamentale che l'UE disponga di meccanismi di controllo della corretta attuazione degli accordi, ad esempio le verifiche periodiche congiunte dell'attuazione di tutti gli aspetti degli accordi, tra cui la limitazione delle finalità, i diritti dei passeggeri e i trasferimenti successivi dei dati PNR, comprendenti una valutazione di proporzionalità dei dati conservati in base al loro valore in vista del conseguimento degli obiettivi per i quali i dati sono stati trasferiti. I risultati di tali verifiche congiunte dovrebbero essere presentati al Consiglio e al Parlamento europeo.
- **Composizione delle controversie:** dovrebbero essere previsti efficaci meccanismi di composizione delle controversie in ordine all'interpretazione, all'applicazione e all'attuazione degli accordi.
- **Reciprocità:** dovrebbe essere garantita la reciprocità, soprattutto tramite il trasferimento di informazioni analitiche provenienti dai dati PNR da parte delle autorità competenti del paese terzo ricevente alle autorità di polizia e giudiziarie degli Stati membri, a Europol e Eurojust.

4. **PROSPETTIVA A LUNGO TERMINE**

Poiché a livello mondiale il numero di paesi che usano i dati PNR è in continuo aumento, le problematiche connesse a tale uso interessano la comunità internazionale. L'approccio bilaterale adottato sino ad oggi dall'UE era il più appropriato alle circostanze ed è probabile che rimarrà tale anche nei prossimi anni, tuttavia vi è il rischio che diventi inadeguato se molti altri paesi faranno ricorso ai dati PNR. L'UE dovrebbe pertanto valutare l'opportunità di fissare norme per la trasmissione e l'uso dei dati PNR a livello internazionale. Gli orientamenti sull'accesso ai dati PNR elaborati dall'ICAO nel 2004 offrono una solida base per armonizzare le modalità di trasmissione dei dati PNR. Gli orientamenti però non sono vincolanti né trattano in modo sufficiente le questioni di protezione dei dati, quindi non sono di per sé sufficienti e valgono piuttosto come linee guida, soprattutto per quanto riguarda gli aspetti attinenti ai vettori aerei.

Su queste basi, l'UE dovrebbe valutare l'opportunità di avviare dibattiti con i partner internazionali che usano i dati PNR o che prevedono di farlo, in modo da trovare un eventuale terreno comune per trattare i trasferimenti di dati PNR a livello multilaterale. Se tali discussioni saranno fruttuose, l'UE dovrà avviare negoziati formali con i partner internazionali interessati che conducano a una soluzione multilaterale.

5. CONCLUSIONI

La presente comunicazione fornisce una panoramica delle attuali tendenze nell'uso dei dati PNR all'interno dell'UE e nel mondo. Per rispondere a tali tendenze e alle minacce che continuano a incombere sull'UE e sulla comunità internazionale, la Commissione ritiene necessario che l'UE riveda il suo approccio globale ai dati PNR. La Commissione è giunta a questa conclusione anche considerando le posizioni sulle problematiche generali dei PNR delle principali parti interessate e i principi di elaborazione delle politiche esposti nel documento "Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia".

La presente comunicazione formula, per la prima volta, una serie di considerazioni generali che dovrebbero guidare l'UE nel negoziare accordi PNR con i paesi terzi. L'adesione a tali principi dovrebbe aumentare la coerenza tra i vari accordi PNR e garantire l'osservanza dei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali. Nel contempo, la comunicazione rimane sufficientemente flessibile e adattabile alle particolari problematiche di sicurezza e agli specifici ordinamenti giuridici dei singoli paesi terzi.

Infine, per quanto riguarda la prospettiva a lungo termine di sviluppare politiche PNR a livello mondiale, la presente comunicazione giunge alla conclusione che l'UE dovrebbe valutare l'opportunità di sostituire, a medio termine, gli accordi bilaterali con un accordo multilaterale tra tutti i paesi che usano i dati PNR.