

IT

IT

IT



COMMISSIONE EUROPEA

Bruxelles, 2.2.2011
COM(2011) 32 definitivo

2011/0023 (COD)

Proposta di

DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

**sull'uso dei dati del codice di prenotazione a fini di prevenzione, accertamento, indagine
e azione penale nei confronti dei reati di terrorismo e dei reati gravi**

{SEC(2011) 132 definitivo}
{SEC(2011) 133 definitivo}

RELAZIONE

1. CONTESTO DELLA PROPOSTA

• Motivazione e obiettivi della proposta

Negli ultimi dieci anni sono andate aumentando nell'UE e nel resto del mondo le forme gravi di criminalità organizzata come la tratta degli esseri umani¹ e il traffico di stupefacenti². Stando al *Sourcebook of Crime and Criminal Justice Statistics*, nel 2007 negli Stati membri (esclusi l'Italia e il Portogallo i cui dati non sono pervenuti) sono stati commessi circa 14 000 reati per 100 000 abitanti, con un'oscillazione compresa tra 14 465 reati in Svezia e 958 a Cipro. La valutazione 2009 di Europol della minaccia rappresentata dalla criminalità organizzata nell'UE (OCTA 2009) evidenzia che la maggior parte dei reati di criminalità organizzata comporta spostamenti internazionali, in genere per far entrare clandestinamente nell'UE persone, stupefacenti o altre merci illecite.

Nel contempo, i terroristi e le loro organizzazioni si trovano sia all'interno che all'esterno dell'UE. Gli attentati terroristici del 2001 negli Stati Uniti, il fallito attentato terroristico dell'agosto 2006 con cui si volevano far esplodere alcuni aerei in volo dal Regno Unito verso gli Stati Uniti e il tentativo di attentato su un volo da Amsterdam verso Detroit nel dicembre 2009 dimostrano che i terroristi sono in grado di preparare attentati contro voli internazionali in qualunque paese. Benché nel 2009 il fenomeno sia diminuito nell'UE, secondo la relazione 2010 di Europol sulla situazione e sulle tendenze del terrorismo nell'UE la minaccia terroristica rimane grave e reale. Poiché la maggior parte delle attività terroristiche ha carattere transnazionale e comporta viaggi internazionali³, anche verso i campi di addestramento al di fuori dell'UE, è necessaria una maggior cooperazione tra le autorità di contrasto.

I reati gravi e i reati di terrorismo danneggiano gravemente le vittime, provocano danni economici su larga scala e minano quel senso di sicurezza indispensabile a chiunque per esercitare efficacemente le proprie libertà e propri diritti.

Uno studio pubblicato nel 2009⁴ per l'Organizzazione internazionale del lavoro stima il costo della coercizione per retribuzioni inferiori al dovuto a seguito della tratta di esseri umani nel 2007 a 2 508 368 218 dollari nelle economie industrializzate e a 19 598 020 343 dollari nell'economia mondiale.

La relazione annuale 2010 sull'evoluzione del fenomeno della droga in Europa elaborata dall'Osservatorio europeo delle droghe e delle tossicodipendenze mette in evidenza la natura globale del fenomeno e i danni gravi e crescenti che ne conseguono. Compromettendo lo sviluppo economico e alimentando la corruzione e la criminalità organizzata, la droga rappresenta una minaccia reale per l'Unione europea. Ogni anno i decessi dovuti al consumo di cocaina nell'UE sono circa 1 000. Secondo stime prudenti, le persone che fanno uso di oppiacei in Europa sono circa 1,35 milioni. Quanto all'impatto economico e sociale della

¹ Valutazione Europol della minaccia rappresentata dalla criminalità organizzata nell'UE, 2009.

² Eurostat 36/2009.

³ Relazione Europol sulla situazione e sulle tendenze del terrorismo nell'Unione europea, 2010.

⁴ *Measuring the costs of coercion to workers in forced labour*- Vinogradova, De Cock, Belsler.

droga, nel 2008 22 Stati membri hanno dichiarato una spesa totale connessa alle droghe illecite pari a 4,2 miliardi di euro.

Un altro studio, realizzato dal ministero dell'Interno del Regno Unito⁵, ha misurato i costi sostenuti per prevenire i reati come le spese di difesa, i costi indotti dalle conseguenze dei reati come l'impatto fisico ed emotivo sulle vittime e il valore dei beni rubati, e i costi sostenuti per rispondere alla criminalità come i costi della giustizia penale: in totale, 36 166 000 000 sterline per il 2003.

Nel contempo, quattro europei su cinque vorrebbero che l'UE prendesse misure più incisive contro la criminalità organizzata e il terrorismo⁶.

In risposta alla minaccia rappresentata dai reati gravi e dal terrorismo, e in considerazione dell'abolizione dei controlli alle frontiere interne ai sensi della convenzione Schengen, l'UE ha disposto la raccolta e lo scambio di dati personali tra autorità di contrasto e altre autorità. Per quanto utili, tali misure si incentrano sui dati riguardanti persone già sospette, ossia già "note" alle autorità di contrasto. Si pensi al sistema d'informazione Schengen (SIS)⁷, al sistema d'informazione Schengen di seconda generazione (SIS II)⁸, al sistema d'informazione visti (VIS)⁹ e al sistema futuro di registrazione ingressi/uscite.

Nella comunicazione "Panorama generale della gestione delle informazioni nello spazio di libertà, sicurezza e giustizia"¹⁰ la Commissione analizza tali misure e sottolinea la necessità di una maggior cooperazione tra le autorità di contrasto in relazione ai passeggeri di voli internazionali da e verso gli Stati membri, e di un uso più sistematico dei dati del codice di prenotazione (Passenger Name Record, PNR) di tali passeggeri per finalità di contrasto. Il "Programma di Stoccolma - Un'Europa aperta e sicura al servizio e a tutela dei cittadini"¹¹ invita inoltre la Commissione a presentare una proposta sull'uso dei dati PNR al fine di prevenire, individuare, indagare e reprimere i reati di terrorismo e altri reati gravi.

I dati PNR sono informazioni non verificate fornite dai passeggeri, che vengono raccolti e conservati nei sistemi di prenotazione e di controllo delle partenze dei vettori aerei a fini commerciali. Contengono vari tipi di informazioni: la data del viaggio, l'itinerario, i dati sull'emissione del biglietto, i recapiti, l'agente di viaggio presso il quale è stato prenotato il volo, le modalità di pagamento, il numero di posto assegnato e le informazioni relative al bagaglio.

Le autorità di contrasto possono usare i dati PNR in vari modi:

reattivamente: 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

⁵ *The economic and social costs of crime against individuals and households 2003/04.*

⁶ Eurobarometro standard 71, pag. 149 dell'allegato.

⁷ Convenzione di applicazione dell'Accordo di Schengen del 14 giugno 1985 tra i governi degli Stati dell'Unione economica Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni (GU L 239 del 22.9.2000, pag. 19). Regolamento (CE) n. 1987/2006, decisione 2007/533/GAI, regolamento (CE) n. 1986/2006.

⁸ Regolamento (CE) n. 1987/2006, decisione 2007/533/GAI, regolamento (CE) n. 1986/2006.

⁹ Decisione 2004/512/CE del Consiglio, regolamento (CE) n. 767/2008, decisione 2008/633/GAI del Consiglio. Si veda anche la dichiarazione sulla lotta al terrorismo adottata dal Consiglio europeo il 25 marzo 2004.

¹⁰ COM(2010) 385.

¹¹ Documento n.17024/09 del Consiglio del 2.12.2009.

indietro nel tempo, è necessario prevedere un periodo di conservazione dei dati a beneficio di queste autorità che sia commisurato;

in tempo reale: prima dell'arrivo o della partenza dei passeggeri 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 criteri di valutazione predeterminati al fine di identificare i sospetti precedentemente "non noti" ed effettuare confronti con varie banche dati di persone e oggetti ricercati;

proattivamente: per analisi e per la definizione di criteri di valutazione che possono poi essere usati per la valutazione prima dell'arrivo e prima della partenza dei passeggeri. Per svolgere tale analisi della pertinenza ai fini della prevenzione, dell'accertamento, dell'indagine e dell'azione penale nei confronti dei reati di terrorismo e dei reati gravi, è necessario prevedere un periodo di conservazione dei dati a beneficio delle autorità di contrasto che sia commisurato.

Raccogliere, analizzare e conservare in modo più sistematico i dati PNR riguardanti i voli internazionali, purché sussistano rigorose garanzie per la protezione dei dati, rafforzerebbe la prevenzione, l'accertamento, l'indagine e l'azione penale nei confronti dei reati di terrorismo e dei reati gravi ed è cosa necessaria, come si va a spiegare, per far fronte a tali minacce alla sicurezza e ridurre i danni connessi.

Attualmente però l'uso dei dati PNR non è disciplinato a livello dell'UE. Ad oggi solo pochi Stati membri hanno messo a punto un sistema PNR e la maggior parte degli Stati membri usa tali dati per la prevenzione, l'accertamento, l'indagine e l'azione penale nei confronti dei reati di terrorismo e dei reati gravi in modo non sistematico o in base a poteri generali conferiti alla polizia o ad altre autorità. All'interno dell'Unione, il Regno Unito ha già introdotto un sistema PNR mentre la Francia, la Danimarca, il Belgio, la Svezia e i Paesi Bassi hanno emanato apposite leggi o stanno testando l'uso dei dati PNR. Molti altri Stati membri stanno valutando l'opportunità di istituire sistemi propri. Le misure nazionali differiscono per vari aspetti: finalità del sistema, periodo di conservazione dei dati, struttura del sistema, ambito geografico e modalità di trasporto considerate. È inoltre molto probabile che una volta che questi Stati membri avranno adottato un quadro normativo completo sull'uso dei dati PNR, le norme sulla protezione dei dati e sulle misure di sicurezza dei trasferimenti dei dati saranno eterogenee. Potrebbero quindi venirsi a creare fino a 27 sistemi notevolmente diversi, con conseguenti disparità nella protezione dei dati personali nell'UE, falle nella sicurezza, aumento dei costi e incertezza giuridica sia per i vettori aerei che per i passeggeri.

La proposta mira pertanto ad armonizzare le disposizioni degli Stati membri relative agli obblighi dei vettori aerei che effettuano voli tra un paese terzo e il territorio di almeno uno Stato membro di trasmettere i dati PNR alle autorità competenti per prevenire, accertare, indagare e perseguire i reati di terrorismo e i reati gravi. Non impone ai vettori aerei di raccogliere informazioni supplementari dai passeggeri o di conservare dati, né fa obbligo ai passeggeri di fornire dati supplementari rispetto a quelli già forniti ai vettori aerei.

È necessario imporre ai vettori aerei tali obblighi giuridici per i motivi che seguono.

Anzitutto i dati PNR consentono alle autorità di contrasto di identificare persone "non note", ossia mai sospettate prima di reati gravi o di terrorismo, ma il cui probabile coinvolgimento è rilevato da un'analisi dei dati per cui è opportuno che le autorità competenti procedano ad ulteriori verifiche. L'identificazione di tali persone aiuta le autorità di contrasto a prevenire ed

individuare reati gravi, tra cui il terrorismo. Per questo le autorità di contrasto devono poter usare i dati PNR sia in tempo reale per esaminarli in base a criteri di valutazione predeterminati che indichino le persone precedentemente "non note" da sottoporre ad ulteriore verifica, sia proattivamente per effettuare analisi e creare criteri di valutazione.

Ad esempio, l'analisi dei dati PNR può dare indicazioni sulle rotte più usate dalla tratta di esseri umani o per il traffico di stupefacenti, che potranno poi essere incluse tra i criteri di valutazione. Verificando in tempo reale i dati PNR in base a questi criteri si possono prevenire o individuare reati. Un esempio concreto: l'analisi dei dati PNR ha permesso di smascherare, in uno Stato membro, un gruppo di trafficanti di esseri umani attivo sempre sulla stessa rotta che si serviva di documenti falsi per il check-in di un volo interno e di documenti autentici per effettuare in contemporanea il check-in su un altro volo a destinazione di un paese terzo; una volta nella sala d'attesa dell'aeroporto, la prassi era imbarcarsi sul volo interno. Senza i dati PNR sarebbe stato impossibile smantellare questa rete della tratta.

L'uso insieme proattivo e in tempo reale dei dati PNR permette così alle autorità di contrasto di far fronte alla minaccia insita nei reati gravi e nel terrorismo in una prospettiva diversa rispetto al trattamento di altre categorie di dati. Come spiegato di seguito, il trattamento dei dati personali accessibili alle autorità di contrasto tramite gli strumenti esistenti e programmati a livello UE, quali la direttiva relativa alle informazioni anticipate sui passeggeri¹², il sistema d'informazione Schengen (SIS) e il sistema d'informazione Schengen di seconda generazione (SIS II), non mette le autorità di contrasto nelle condizioni di identificare sospetti "non noti", come invece è possibile con l'analisi dei dati PNR.

In secondo luogo, i dati PNR aiutano le autorità di contrasto, dopo che è stato commesso un reato, a prevenire, accertare, indagare e perseguire altri reati gravi, tra cui il terrorismo. Per questo le autorità di contrasto devono poter usare i dati PNR in tempo reale per confrontarli con varie banche dati di persone "note" e oggetti ricercati; devono poi poterli usare reattivamente per raccogliere prove e, se pertinente, scoprire complici e smantellare reti criminali.

Ad esempio, grazie alle informazioni sulla carta di credito contenute nei dati PNR le autorità di contrasto possono identificare e provare collegamenti tra una determinata persona e un criminale o un'organizzazione criminale noti. Uno Stato membro ha dato l'esempio di una vasta rete di tratta di esseri umani e traffico di stupefacenti tra uno Stato membro e paesi terzi: dei criminali importavano stupefacenti in varie destinazioni europee facendoli inghiottire a persone a loro volta vittime della tratta. Sono stati identificati perché dai dati PNR è emerso che compravano i biglietti con carte di credito rubate. È stato così possibile procedere ad arresti nello Stato membro in questione. In base a questa esperienza è stato definito un criterio di valutazione che ha permesso di arrestare molte altre persone in altri Stati membri e paesi terzi.

Da ultimo, l'uso dei dati PNR prima dell'arrivo del volo permette alle autorità di contrasto di effettuare valutazioni e sottoporre a controlli approfonditi solo le persone che, in base a criteri di valutazione obiettivi e all'esperienza, è più probabile che costituiscano una minaccia per la sicurezza, agevolando così il viaggio di tutti gli altri passeggeri e riducendo il rischio che, entrando nell'UE, siano sottoposti a controlli basati su criteri illegittimi, quali la cittadinanza

¹² Direttiva 2004/82/CE del 29 agosto 2004.

o il colore della pelle, che le autorità di contrasto, comprese le autorità doganali e le guardie di frontiera, potrebbero erroneamente associare a rischi di sicurezza.

Le misure proposte comportano la raccolta e il trattamento dei dati PNR ad opera delle autorità di contrasto, quindi hanno un impatto sul diritto al rispetto della vita privata e sul diritto alla protezione dei dati. Pertanto, per garantire il rispetto del principio di proporzionalità la proposta, come spiegato di seguito, ha un campo di applicazione scrupolosamente limitato e prevede rigorose garanzie per la protezione dei dati.

La necessità di usare i dati PNR, in misura limitata e in presenza di rigorose garanzie per la protezione dei dati, è suffragata da vari elementi di fatto, come si legge nella valutazione d'impatto che accompagna la presente proposta. Mancando disposizioni armonizzate sulla raccolta e il trattamento dei dati PNR a livello UE, non sono disponibili statistiche dettagliate che indichino in quale misura tali dati contribuiscono a prevenire, accertare, indagare e perseguire i reati gravi e il terrorismo. La necessità di usare i dati PNR trova tuttavia conferma nelle informazioni trasmesse dai paesi terzi e dagli Stati membri che ricorrono già ai dati PNR nelle attività di contrasto.

L'esperienza di tali paesi insegna che l'uso dei dati PNR ha reso possibili progressi decisivi nella lotta soprattutto contro il traffico di stupefacenti, la tratta di esseri umani e il terrorismo, e permette di capire meglio la composizione e il modo di agire di terroristi e altri gruppi criminali. Per quanto riguarda gli stupefacenti, gli Stati membri hanno dichiarato che la maggior parte dei sequestri è stata il risultato dell'uso proattivo e in tempo reale dei dati PNR. Il Belgio ha riferito che il 95% di tutti i sequestri di stupefacenti del 2009 è dipeso esclusivamente o prevalentemente dal trattamento di dati PNR. La Svezia ha dichiarato che il 65-75% di tutti i sequestri di stupefacenti del 2009, pari a 278,9 chili di cocaina e a ulteriori quantità di eroina e altri stupefacenti, è dipeso esclusivamente o prevalentemente dal trattamento di dati PNR. Il Regno Unito segnala che, nel 2010, in sei mesi sono stati sequestrati 212 chili di cocaina e 20 chili di eroina esclusivamente o prevalentemente grazie al trattamento di dati PNR.

• **Contesto generale**

Il 6 novembre 2007 la Commissione ha adottato una proposta di decisione quadro del Consiglio sull'uso dei dati del codice di prenotazione (Passenger Name Record, PNR) nelle attività di contrasto¹³ (di seguito "proposta del 2007"). La proposta è stata discussa a fondo nei gruppi di lavoro del Consiglio e il Consiglio Giustizia e Affari interni ha avallato i progressi conseguiti, in gennaio, luglio e novembre 2008. Grazie a tali discussioni è stato possibile raggiungere un consenso sulla maggior parte delle disposizioni della proposta¹⁴.

Con l'entrata in vigore del trattato sul funzionamento dell'Unione europea (TFUE) il 1° dicembre 2009, la proposta della Commissione, non ancora adottata dal Consiglio, è diventata obsoleta. L'attuale proposta sostituisce la proposta del 2007 e si basa sulle disposizioni del TFUE; tiene largamente conto delle raccomandazioni formulate dal Parlamento europeo nella risoluzione del novembre 2008¹⁵ e rispecchia gli ultimi sviluppi delle discussioni nei gruppi di lavoro del Consiglio nel 2009; tiene altresì conto dei pareri del garante europeo della

¹³ COM(2007) 654.

¹⁴ Documento n. 5618/2/2009 REV 2 del Consiglio del 29.6.2009.

¹⁵ P6_TA (2008)0561.

protezione dei dati¹⁶, del gruppo di lavoro articolo 29 per la protezione dei dati¹⁷ e dell'Agenzia per i diritti fondamentali¹⁸.

- **Disposizioni vigenti nel settore della proposta**

I dati PNR sono diversi e non vanno confusi con i dati API (Advance Passenger Information). Questi sono dati anagrafici raccolti dalla banda a lettura ottica del passaporto (nome, luogo di nascita e cittadinanza dell'interessato, numero e data di scadenza del passaporto) e hanno una portata più limitata rispetto ai dati PNR.

L'uso dei dati API nell'UE è disciplinato dalla direttiva API¹⁹. Ai sensi della direttiva API, tali dati sono messi a disposizione delle autorità di controllo alla frontiera, su richiesta del singolo Stato membro, per i voli diretti verso l'UE al fine di migliorare i controlli alle frontiere e combattere l'immigrazione illegale. Sebbene la direttiva ne consenta l'uso per finalità di contrasto, questa possibilità è subordinata al rispetto di criteri specifici. Pertanto, anche se in alcuni casi le autorità di contrasto usano i dati API per identificare persone sospette e ricercati, tali dati sono usati principalmente come strumento di verifica dell'identità e di gestione delle frontiere. Inoltre, i dati API non permettono alle autorità di contrasto di effettuare valutazioni dei passeggeri, e quindi non contribuiscono a identificare criminali o terroristi "non noti".

Il **sistema d'informazione Schengen (SIS)** intende preservare la sicurezza pubblica, compresa la sicurezza dello Stato, all'interno dello spazio Schengen. Il SIS è un sistema d'informazione centralizzato costituito da una sezione nazionale presso ciascuno Stato partecipante e da un'unità di supporto tecnico in Francia. Gli Stati membri possono segnalare persone ricercate per l'arresto ai fini di estradizione; stranieri ai fini della non ammissione; persone scomparse; testimoni e persone citate a comparire dinanzi all'autorità giudiziaria; persone e veicoli soggetti a controlli supplementari; veicoli, documenti e armi da fuoco persi o rubati; banconote registrate.

Il **sistema d'informazione visti (VIS)** mira ad affrontare entrambi gli aspetti: il suo scopo è migliorare l'attuazione della politica comune in materia di visti agevolando l'esame delle domande di visto e i controlli ai valichi di frontiera esterni, contribuendo nel contempo a prevenire minacce alla sicurezza interna degli Stati membri. Il VIS è un sistema d'informazione centralizzato costituito da una sezione nazionale presso ciascuno Stato partecipante e da un'unità di supporto tecnico in Francia, si avvarrà di un sistema di confronto biometrico per un confronto attendibile delle impronte digitali, che sarà installato alle frontiere esterne dell'UE per verificare l'identità dei titolari del visto, e conterrà dati relativi alle domande di visto, fotografie, impronte digitali, decisioni correlate delle autorità per il visto e collegamenti tra domande connesse.

Pertanto, al pari dei dati API, il SIS e il VIS sono principalmente strumenti di verifica dell'identità e di gestione delle frontiere, e servono solo quando l'identità del sospetto è nota. Questi strumenti non si prestano quindi né per la valutazione dei passeggeri, né per individuare criminali o terroristi "non noti".

¹⁶ GU C 110 dell'1.5.2008.

¹⁷ Parere n. 145 del 5.12.2007.

¹⁸ http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf

¹⁹ Direttiva 2004/82/CE del 29 agosto 2004.

L'Unione europea ha concluso con gli Stati Uniti, il Canada e l'Australia accordi per il trasferimento dei dati PNR nell'ambito della lotta ai reati gravi di natura transnazionale e al terrorismo, applicabili esclusivamente al traffico aereo, che fanno obbligo ai vettori aerei che raccolgono i dati PNR dei passeggeri a fini commerciali di trasmetterli alle autorità competenti degli Stati Uniti, del Canada e dell'Australia. Tali accordi dovranno essere rinegoziati nel 2011. Anche altri paesi, segnatamente la Corea del Sud e il Giappone, hanno chiesto di negoziare accordi di questo tipo. La Commissione ha esposto gli elementi essenziali di una politica dell'UE in questo ambito nella comunicazione del 21 settembre 2010 sull'approccio globale al trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) verso paesi terzi²⁰. L'attuale proposta è pienamente coerente con la politica definita in tale comunicazione.

- **Coerenza con gli altri obiettivi e politiche dell'Unione**

Il sistema d'informazione Schengen (SIS)²¹, il sistema d'informazione Schengen di seconda generazione (SIS II)²², il sistema d'informazione visti (VIS)²³, il futuro sistema di registrazione ingressi/uscite e il programma per viaggiatori registrati sono misure dell'Unione che riguardano direttamente operazioni effettuate fisicamente alla frontiera.

Sebbene i dati PNR siano dati dei passeggeri relativi al viaggio, essi servono principalmente come strumento di intelligence criminale e non come strumento di controllo alla frontiera. Sono usati prima dell'attraversamento della frontiera e non al valico di frontiera. Obiettivo principale dell'uso dei dati PNR è lottare contro il terrorismo e i reati gravi piuttosto che combattere l'immigrazione illegale e agevolare dei controlli di frontiera.

La proposta non modifica né interferisce con le attuali norme dell'UE sulle modalità dei controlli alle frontiere o sull'ingresso e l'uscita dal territorio dell'Unione. La proposta coesisterà con tali disposizioni, lasciandole invariate.

- **Impatto sui diritti fondamentali**

La proposta è pienamente in linea con l'obiettivo generale di creare uno spazio di libertà, sicurezza e giustizia. In considerazione della natura delle disposizioni proposte, la presente proposta è stata oggetto di un esame approfondito per garantirne la compatibilità con i diritti fondamentali, in particolare il diritto alla protezione dei dati di carattere personale sancito all'articolo 8 della Carta dei diritti fondamentali dell'Unione europea, come risulta dalla valutazione d'impatto che accompagna la proposta. Essa è inoltre in linea con l'articolo 16 del TFUE, che riconosce ad ogni persona il diritto alla protezione dei dati di carattere personale che la riguardano.

La proposta è compatibile con i principi in materia di protezione dei dati e le sue disposizioni sono in linea con la decisione quadro 2008/977/GAI del Consiglio sulla protezione dei dati

²⁰ COM(2010) 492.

²¹ Convenzione di applicazione dell'Accordo di Schengen del 14 giugno 1985 tra i governi degli Stati dell'Unione economica Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni (GU L 239 del 22.9.2000, pag. 19).

²² Regolamento (CE) n. 1987/2006, decisione 2007/533/GAI, regolamento (CE) n. 1986/2006.

²³ Decisione 2004/512/CE del Consiglio, regolamento (CE) n. 767/2008, decisione 2008/633/GAI del Consiglio. Si veda anche la dichiarazione sulla lotta al terrorismo adottata dal Consiglio europeo il 25 marzo 2004.

personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale²⁴ (di seguito "decisione quadro 2008/977/GAI"). Agli interessati è quindi riconosciuto il diritto di accesso, il diritto di rettifica, cancellazione o blocco, così come il diritto a compensazione e il diritto di proporre un ricorso giurisdizionale. Inoltre, e al fine di rispettare il principio di proporzionalità, in alcuni ambiti la proposta prevede norme di protezione dei dati più severe rispetto alla richiamata decisione quadro.

In particolare, il campo di applicazione della proposta è rigorosamente limitato e le autorità di contrasto sono autorizzate ad usare i dati PNR solo per combattere una serie di reati gravi specifici, elencati esaustivamente, che lo Stato membro punisce con la reclusione non inferiore a tre anni. Inoltre, affinché il trattamento dei dati di persone innocenti e non sospette rimanga quanto più limitato, alcuni aspetti del campo di applicazione della proposta relativi alla definizione e applicazione di criteri di valutazione sono stati anch'essi limitati ai reati gravi di natura transnazionale, ossia intrinsecamente connessi al viaggio e quindi al tipo di dati trattati. La proposta consente la conservazione dei dati PNR per un periodo massimo di cinque anni, dopodiché i dati devono essere cancellati. Inoltre, i dati devono essere resi anonimi dopo appena 30 giorni perché è allo scadere di questo termine che è permesso l'uso proattivo dei dati PNR a condizione che i dati siano anonimi. Sono vietati la raccolta e l'uso dei dati sensibili che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, lo stato di salute o l'orientamento sessuale dell'interessato. La proposta dispone altresì che uno Stato membro non possa prendere decisioni che comportino conseguenze giuridiche negative per l'interessato o lo danneggino in modo significativo, soltanto sulla base del trattamento automatico dei dati PNR. Per giunta, decisioni di questo tipo non potranno in nessun caso fondarsi neanche sull'origine razziale o etnica, sulle convinzioni religiose o filosofiche, sulle opinioni politiche, sull'appartenenza sindacale, sullo stato di salute o sull'orientamento sessuale dell'interessato. Inoltre, i vettori dovranno trasmettere i dati PNR esclusivamente mediante il cosiddetto metodo "push", il che significa che gli Stati membri non avranno accesso diretto ai sistemi informatici dei vettori. Gli Stati membri potranno trasmettere i dati PNR a paesi terzi solo in circostanze molto limitate e solo caso per caso. Per assicurare una protezione dei dati effettiva e di livello elevato, è chiesto agli Stati membri di provvedere affinché un'autorità nazionale di controllo indipendente (autorità per la protezione dei dati) sia incaricata di dare consulenza e sorvegliare le modalità di trattamento dei dati PNR. Agli Stati membri è altresì chiesto di istituire un'unica unità designata (Unità d'informazione sui passeggeri) per gestire e proteggere i dati. Tutti i trattamenti di dati PNR dovranno essere registrati o documentati a cura di questa Unità d'informazione sui passeggeri ai fini della verifica della legittimità del trattamento, dell'autocontrollo e per garantire l'integrità dei dati e la sicurezza del loro trattamento. Gli Stati membri dovranno altresì provvedere affinché i passeggeri siano informati in modo chiaro e preciso della raccolta dei dati PNR e dei loro diritti.

Pertanto, oltre ad essere in linea con le norme e i principi vigenti in materia di protezione dei dati, la proposta contiene una serie di garanzie che assicurano il pieno rispetto del principio di proporzionalità e un livello elevato di protezione dei diritti fondamentali.

2. CONSULTAZIONE DELLE PARTI INTERESSATE E VALUTAZIONE DELL'IMPATTO

• Consultazione delle parti interessate

²⁴ GUL 350 del 30.12.2008, pag. 60.

Metodi di consultazione, principali settori interessati e profilo generale dei partecipanti

Per elaborare la proposta del 2007 la Commissione ha consultato tutte le parti interessate attraverso un questionario inviato nel dicembre 2006 a tutti gli Stati membri, alle autorità nazionali per la protezione dei dati degli Stati membri, al garante europeo della protezione dei dati, all'*Association of European Airlines* (AEA), all'*Air Transport Association of America*, all'*International Air Carrier Association* (IACA), alla *European Regions Airline Association* (ERA) e all'*International Air Transport Association* (IATA). Le risposte sono state sintetizzate nella valutazione d'impatto che accompagna la proposta del 2007. Successivamente, la Commissione ha invitato i rappresentanti degli Stati membri a una riunione per uno scambio di opinioni.

A seguito dell'adozione della proposta del 2007, tutte le parti interessate hanno pubblicato la loro posizione al riguardo. Il 20 novembre 2008 il Parlamento europeo ha adottato una risoluzione sulla proposta²⁵. Gli Stati membri hanno espresso le rispettive posizioni durante le discussioni nei gruppi di lavoro del Consiglio²⁶, al pari del garante europeo della protezione dei dati²⁷, del gruppo di lavoro articolo 29 per la protezione dei dati²⁸ e dell'Agazia per i diritti fondamentali²⁹.

Sintesi delle risposte

La principale critica mossa dal Parlamento europeo nella sua risoluzione riguarda l'assenza di una dimostrazione sufficiente della necessità dell'azione proposta. Il Parlamento europeo mette in discussione il fatto che la proposta rispetti i requisiti richiesti per giustificare un'ingerenza nel diritto alla protezione dei dati personali; esprime preoccupazione in ordine al fatto che non sia stato valutato il valore aggiunto della proposta alla luce delle altre iniziative sulle frontiere; quanto alla protezione dei dati, chiede una precisa limitazione delle finalità e sottolinea che solo specifiche autorità possono accedere ai dati PNR; teme da ultimo che il metodo proposto di analisi automatizzata dei dati PNR sulla base di criteri predeterminati basati sui fatti possa comportare un uso molto ampio dei dati, e sottolinea che tale valutazione non dovrebbe mai portare all'elaborazione di profili sulla base di dati sensibili.

Il gruppo di lavoro articolo 29 per la protezione dei dati giudica la proposta sproporzionata e suscettibile di violare il diritto alla protezione dei dati; mette in discussione il regime di protezione dei dati, in quanto la decisione quadro 2008/977/GAI non si applica ai dati trattati a livello nazionale; considera la dimostrazione della necessità della proposta inadeguata, il periodo di conservazione dei dati sproporzionato (13 anni) e ritiene che il trasferimento dei dati debba effettuarsi solo con metodo "push".

Il garante europeo della protezione dei dati dubita che siano state dimostrate la necessità e la proporzionalità della proposta, poiché questa concerne la raccolta di dati di persone innocenti; critica la proposta che porterebbe a una società della sorveglianza e contesta il regime di protezione dei dati in quanto i dati trattati a livello nazionale non rientrano nel campo di

²⁵ P6_TA (2008)0561.

²⁶ Documento n.17024/09 del Consiglio del 2.12.2009.

²⁷ GU C 110 dell'1.5.2008.

²⁸ Parere comune relativo alla proposta di decisione quadro del Consiglio sull'uso dei dati del codice di prenotazione (Passenger Name Record, PNR) nelle attività di contrasto, presentata dalla Commissione il 6 novembre 2007 (WP 145 del 5.12.2007), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp145_it.pdf.

²⁹ http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf.

applicazione della decisione quadro 2008/977/GAI; suggerisce specificamente di definire meglio le autorità che potranno accedere ai dati e le condizioni di trasferimento dei dati verso paesi terzi.

Anche l'Agenzia per i diritti fondamentali ritiene che non siano state dimostrate la necessità e proporzionalità della proposta e aggiunge che questa dovrebbe prevedere più garanzie per evitare la profilazione in base a dati sensibili.

Alcune associazioni di compagnie aeree, segnatamente l'*International Air Transport Association* (IATA) e l'*Association of European Airlines* (AEA), hanno formulato anch'esse pareri sulla proposta criticandone soprattutto la struttura decentrata e sottolineando che la raccolta centralizzata dei dati consentirebbe vantaggi finanziari per i vettori aerei. Hanno inoltre criticato la scelta del metodo "push" e chiesto che la scelta del metodo di trasferimento fosse lasciata ai vettori.

Il processo di consultazione ha ampiamente influenzato l'elaborazione della proposta legislativa. Sebbene molte parti interessate non fossero convinte della necessità di usare i dati PNR, tutte hanno concordato sulla preferibilità di una normativa UE rispetto allo sviluppo di sistemi PNR nazionali eterogenei. Uno degli effetti delle consultazioni è stata la limitazione della finalità dei dati alla lotta contro il terrorismo e i reati gravi, e del campo di applicazione della proposta al trasporto aereo. È stato scelto un solido regime di protezione dei dati, che prevede uno specifico periodo di conservazione e il divieto di usare dati sensibili, quelli cioè che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la salute o l'orientamento sessuale. È stato preferito il metodo "push" e sono state introdotte rigorose restrizioni dei trasferimenti successivi verso paesi terzi.

- **Ricorso al parere di esperti**

Non è stato necessario consultare esperti esterni.

- **Valutazione dell'impatto**

La Commissione ha effettuato la valutazione d'impatto prevista nel programma di lavoro³⁰.

La valutazione d'impatto esamina quattro opzioni principali, ciascuna con due varianti:

opzione A: nessun intervento dell'UE in questo ambito e mantenimento dello status quo;

opzione B: definizione della struttura di un sistema di raccolta e trattamento dei dati PNR; opzione B.1: raccolta e trattamento decentrati dei dati a cura degli Stati membri, e opzione B.2: raccolta e trattamento centralizzati dei dati a livello UE;

opzione C: limitazione della finalità delle misure proposte; opzione C.1: accesso solo a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, e opzione C.2: accesso a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi e per altri obiettivi strategici;

³⁰ SEC(2011) 132

opzione D: definizione dei modi di trasporto rientranti nel campo di applicazione della proposta; opzione D.1: solo i vettori aerei, e opzione D.2: vettori aerei, marittimi e ferroviari.

Le opzioni sono state valutate in base ai seguenti criteri: sicurezza nell'UE, protezione dei dati personali, costi per le autorità pubbliche, costi per i vettori/concorrenza nel mercato interno e stimolo a un approccio globale.

La valutazione d'impatto giunge alla conclusione che l'opzione preferibile è una proposta legislativa applicabile al traffico aereo, con raccolta decentrata dei dati PNR a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e altri reati gravi (combinazione delle opzioni B.1, C.1 e D.1). Questa opzione rafforzerebbe la sicurezza nell'UE minimizzando nel contempo l'impatto sulla protezione dei dati personali e mantenendo i costi a un livello accettabile.

3. ELEMENTI GIURIDICI DELLA PROPOSTA

- **Sintesi delle misure proposte**

Obiettivo della proposta è armonizzare le disposizioni degli Stati membri relative all'obbligo dei vettori aerei che effettuano voli tra un paese terzo e il territorio di almeno uno Stato membro di trasmettere i dati PNR alle autorità competenti per prevenire, accertare, indagare e perseguire i reati di terrorismo e i reati gravi. Tutti i trattamenti di dati PNR effettuati in base alla presente proposta saranno conformi alle norme di protezione dei dati fissate con decisione quadro 2008/977/GAI.

- **Base giuridica**

TFUE, in particolare l'articolo 82, paragrafo 1, lettera d), e l'articolo 87, paragrafo 2, lettera a).

- **Principio di sussidiarietà**

Le autorità di contrasto devono disporre di strumenti efficaci con cui combattere il terrorismo e i reati gravi. Poiché la maggior parte dei reati gravi e degli atti terroristici comporta viaggi internazionali, le autorità devono poter usare i dati PNR per proteggere la sicurezza interna dell'UE. Inoltre, le indagini svolte dalle autorità competenti degli Stati membri per prevenire, accertare, indagare e perseguire i reati di terrorismo e i reati gravi dipendono in larga misura dalla cooperazione internazionale e transfrontaliera.

Poiché nello spazio Schengen le persone possono circolare liberamente, è necessario che tutti gli Stati membri raccolgano, trattino e scambino i dati PNR in modo da evitare falle nella sicurezza. Promuovendo un'azione collettiva e coerente, tale misura contribuirà a rafforzare la sicurezza dell'UE.

L'intervento dell'UE contribuirà a garantire l'applicazione di norme di protezione dei dati armonizzate negli Stati membri. I diversi sistemi degli Stati membri che hanno già istituito meccanismi di questo tipo, o che prevedono di farlo, rischiano di avere un impatto negativo sui vettori aerei che possono vedersi costretti a osservare molteplici requisiti nazionali potenzialmente divergenti, per esempio in ordine al tipo di informazioni da trasmettere e alle condizioni in cui tali informazioni vanno trasmesse agli Stati membri. Tanta divergenza

rischia poi di compromettere l'efficace cooperazione tra gli Stati membri finalizzata a prevenire, accertare, indagare e perseguire i reati di terrorismo e i reati gravi.

Poiché gli obiettivi della presente proposta non possono essere conseguiti in misura sufficiente dagli Stati membri e possono dunque essere conseguiti meglio a livello di Unione, si può concludere che l'UE è nel contempo autorizzata ad intervenire e nella posizione migliore per farlo rispetto ai singoli Stati membri. La proposta è quindi conforme al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea.

- **Principio di proporzionalità**

Raccogliere, analizzare e conservare in modo sistematico i dati PNR riguardanti i voli diretti nell'UE da paesi terzi, purché sussistano rigorose garanzie per la protezione dei dati, rafforzerebbe la prevenzione, l'accertamento, l'indagine e l'azione penale nei confronti dei reati di terrorismo e dei reati gravi ed è cosa necessaria per far fronte a tali minacce alla sicurezza.

Il campo di applicazione della proposta è limitato agli elementi che richiedono un approccio UE armonizzato: definizione dei modi in cui gli Stati membri possono usare i dati PNR, dati da raccogliere, finalità per le quali possono essere usate le informazioni, comunicazione dei dati tra le unità PNR degli Stati membri e condizioni tecniche di tale comunicazione.

L'azione proposta è una direttiva. La scelta di un sistema decentrato implica che gli Stati membri possano decidere come installare il rispettivo sistema PNR e definirne gli aspetti tecnici.

In ossequio al principio di proporzionalità enunciato nell'articolo 5 del trattato sull'Unione europea, la presente proposta si limita a quanto è necessario e proporzionato per conseguire i suoi obiettivi.

- **Scelta dello strumento**

Strumento proposto: la direttiva.

Altri mezzi non risulterebbero adeguati per il seguente motivo.

Dato che l'obiettivo della misura è il ravvicinamento delle normative degli Stati membri, l'unico strumento adeguato è la direttiva.

4. INCIDENZA SUL BILANCIO

Nessuna.

5. INFORMAZIONI SUPPLEMENTARI

- **Simulazione, fase pilota e periodo transitorio**

La proposta contempla un periodo transitorio di attuazione di due anni. Sarà inoltre prevista una fase transitoria per la raccolta dei dati PNR, al fine di giungere alla raccolta dei dati di tutti i voli entro 6 anni dall'entrata in vigore della direttiva.

- **Applicazione territoriale**

Gli Stati membri sono destinatari della direttiva proposta. La sua applicazione al Regno Unito, all'Irlanda e alla Danimarca sarà decisa conformemente alle disposizioni dei protocolli n. 21 e n. 22 allegati al trattato sul funzionamento dell'Unione europea.

- **Riesame/revisione/clausola di caducità**

La proposta contiene una disposizione che prevede il riesame del funzionamento della direttiva quattro anni dopo il suo recepimento e un riesame speciale dell'eventuale estensione del suo campo di applicazione ai dati PNR dei passeggeri in viaggio su voli interni all'UE.

Proposta di

DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

sull'uso dei dati del codice di prenotazione a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 82, paragrafo 1, lettera d), e l'articolo 87, paragrafo 2, lettera a),

vista la proposta della Commissione,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo³¹,

visto il parere del Comitato delle regioni³²,

sentito il garante europeo della protezione dei dati,

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

- (1) Il 6 novembre 2007 la Commissione ha adottato una proposta di decisione quadro del Consiglio sull'uso dei dati del codice di prenotazione (Passenger Name Record, PNR) nelle attività di contrasto³³. Tuttavia, con l'entrata in vigore del trattato di Lisbona il 1° dicembre 2009, la proposta della Commissione, all'epoca non ancora adottata dal Consiglio, è diventata obsoleta.
- (2) Il "Programma di Stoccolma - Un'Europa aperta e sicura al servizio e a tutela dei cittadini"³⁴ invita la Commissione a presentare una proposta sull'uso dei dati PNR al fine di prevenire, individuare, indagare e reprimere i reati di terrorismo e altri reati gravi.
- (3) Nella comunicazione del 21 settembre 2010 "sull'approccio globale al trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) verso paesi terzi"³⁵ la Commissione espone alcuni elementi essenziali di una politica dell'UE in questo ambito.

³¹ GU C , , pag. .

³² GU C , , pag. .

³³ COM(2007) 654.

³⁴ Documento n.17024/09 del Consiglio del 2.12.2009.

³⁵ COM(2010) 492.

- (4) La direttiva 2004/82/CE del Consiglio, del 29 aprile 2004, concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate³⁶ disciplina la trasmissione anticipata, da parte dei vettori, dei dati relativi alle persone trasportate alle competenti autorità nazionali al fine di migliorare i controlli alle frontiere e combattere l'immigrazione illegale.
- (5) I dati PNR sono necessari per prevenire, accertare, indagare e perseguire efficacemente i reati di terrorismo e i reati gravi, e rafforzare così la sicurezza interna.
- (6) I dati PNR aiutano le autorità di contrasto a prevenire, accertare, indagare e perseguire i reati gravi, tra cui il terrorismo, poiché queste li confrontano con varie banche dati di persone e oggetti ricercati per raccogliere prove e, se pertinente, scoprire complici e smantellare reti criminali.
- (7) I dati PNR consentono alle autorità di contrasto di identificare persone “non note”, ossia mai sospettate prima di reati gravi o di terrorismo, ma il cui probabile coinvolgimento è rilevato da un’analisi dei dati per cui è opportuno che le autorità competenti procedano ad ulteriori verifiche. Usando i dati PNR le autorità di contrasto possono far fronte alla minaccia insita nei reati gravi e nel terrorismo in una prospettiva diversa rispetto al trattamento di altre categorie di dati. Tuttavia, affinché il trattamento dei dati di persone innocenti e non sospette rimanga quanto più limitato, è opportuno che gli aspetti dell’uso dei dati PNR relativi alla definizione e applicazione di criteri di valutazione siano anch’essi limitati ai reati gravi di natura transnazionale, ossia intrinsecamente connessi al viaggio e quindi al tipo di dati trattati.
- (8) Il trattamento dei dati personali deve essere proporzionato all’obiettivo specifico di sicurezza perseguito dalla presente direttiva.
- (9) L’uso dei dati PNR e delle informazioni anticipate sui passeggeri ha costituito, in alcuni casi, un valore aggiunto in termini di assistenza apportata agli Stati membri nel verificare l’identità delle persone, e di maggior valore delle attività di contrasto.
- (10) Per prevenire, accertare, indagare e perseguire i reati di terrorismo e i reati gravi è pertanto essenziale che tutti gli Stati membri introducano disposizioni che stabiliscano obblighi a carico dei vettori aerei che effettuano voli internazionali da o per il territorio degli Stati membri dell’Unione europea.
- (11) I vettori aerei già raccolgono e trattano i dati PNR dei loro passeggeri a fini commerciali. La presente direttiva non deve imporre ai vettori aerei di raccogliere dati supplementari dai passeggeri o di conservarli, né fare obbligo ai passeggeri di fornire altri dati rispetto a quelli già forniti ai vettori aerei.
- (12) È opportuno che la definizione di reati di terrorismo sia mutuata dagli articoli da 1 a 4 della decisione quadro 2002/475/GAI del Consiglio sulla lotta contro il terrorismo³⁷, e che la definizione di reati gravi sia mutuata dall’articolo 2 della decisione quadro 2002/584/GAI del Consiglio, del 13 giugno 2002, relativa al mandato d’arresto

³⁶ GU L 261 del 6.8.2004, pag. 24.

³⁷ GU L 164 del 22.6.2002, pag. 3. Decisione modificata dalla decisione quadro 2008/919/GAI del Consiglio del 28 novembre 2008 (GU L 330 del 9.12.2008, pag. 21).

europeo e alle procedure di consegna tra Stati membri³⁸. Gli Stati membri possono tuttavia escludere i reati minori per i quali, tenuto conto dei rispettivi ordinamenti giuridici penali, il trattamento dei dati PNR ai sensi della presente direttiva non sia conforme al principio di proporzionalità. È altresì opportuno che la definizione di reati gravi di natura transnazionale sia mutuata dall'articolo 2 della decisione quadro 2002/584/GAI del Consiglio e dalla convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale.

- (13) È auspicabile che i dati PNR siano trasferiti ad un'unica unità designata (unità informazioni sui passeggeri) dello Stato membro interessato, in modo da garantire la trasparenza e ridurre i costi per i vettori aerei.
- (14) Gli elenchi di dati PNR richiesti, da trasmettere all'Unità d'informazione sui passeggeri, devono essere compilati con l'obiettivo di riflettere l'esigenza legittima delle autorità pubbliche di prevenire, accertare, indagare e perseguire i reati di terrorismo o i reati gravi, migliorando così la sicurezza interna nell'UE e la protezione dei diritti fondamentali dei cittadini, in particolare il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali. In tali elenchi non devono figurare dati personali che possano rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale dell'interessato, né dati relativi al suo stato di salute o alla sua vita sessuale. I dati PNR devono contenere i dati della prenotazione e dell'itinerario di viaggio dei passeggeri, sulla cui base le autorità competenti possano identificare i passeggeri che rappresentano una minaccia per la sicurezza interna.
- (15) Attualmente esistono due metodi di trasferimento dei dati: il metodo "pull", per cui le autorità competenti dello Stato membro che chiede i dati possono accedere al sistema di prenotazione del vettore aereo ed estrarre ("pull") una copia dei dati richiesti; il metodo "push", per cui i vettori aerei trasferiscono ("push") i dati richiesti all'autorità richiedente, mantenendo il controllo dei dati forniti. È opinione condivisa che il metodo "push" offra un livello più elevato di protezione dei dati e debba essere obbligatorio per tutti i vettori aerei.
- (16) La Commissione sostiene gli orientamenti sui PNR dell'Organizzazione per l'aviazione civile internazionale (ICAO). È pertanto necessario basarsi su questi orientamenti per adottare i formati di dati supportati dai vettori aerei per il trasferimento dei dati PNR agli Stati membri. Ne consegue che i formati di dati supportati e i pertinenti protocolli applicabili al trasferimento di dati a cura dei vettori aerei debbano essere adottati in conformità della procedura consultiva di cui al regolamento (UE) n. ... del Parlamento europeo e del Consiglio [.....].
- (17) Gli Stati membri devono prendere tutte le misure necessarie per permettere ai vettori aerei di rispettare gli obblighi previsti nella presente direttiva. È poi opportuno che prevedano sanzioni dissuasive, efficaci e proporzionate, anche pecuniarie, a carico dei vettori aerei che non si conformino agli obblighi in materia di trasferimento dei dati PNR. In caso di violazioni gravi ripetute, che potrebbero compromettere la realizzazione degli obiettivi di base della presente direttiva, queste sanzioni potrebbero

³⁸ GUL 190 del 18.7.2002, pag. 1.

includere, in casi eccezionali, provvedimenti quali il fermo, il sequestro e la confisca del mezzo di trasporto, o la sospensione o il ritiro temporaneo della licenza d'esercizio.

- (18) Ciascuno Stato membro dovrebbe impegnarsi a valutare le minacce potenziali connesse ai reati di terrorismo e ai reati gravi.
- (19) Nel pieno rispetto del diritto alla protezione dei dati personali e del diritto alla non discriminazione, non possono essere prese decisioni che comportino conseguenze giuridiche negative per l'interessato o lo danneggino gravemente, soltanto sulla base del trattamento automatico dei dati PNR. Decisioni di questo tipo non possono fondarsi neanche sull'origine razziale o etnica, sulle opinioni politiche, sulle convinzioni religiose o filosofiche, sull'appartenenza sindacale dell'interessato, sul suo stato di salute o sul suo orientamento sessuale.
- (20) Gli Stati membri dovrebbero condividere i dati PNR che ricevono, quando il trasferimento è necessario a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi. Le disposizioni della presente direttiva non devono incidere sugli altri strumenti dell'Unione in materia di scambio di informazioni tra forze di polizia e autorità giudiziarie, in particolare la decisione 2009/371/GAI del Consiglio, del 6 aprile 2009, che istituisce l'Ufficio europeo di polizia (Europol)³⁹ e la decisione quadro 2006/960/GAI del Consiglio, del 18 dicembre 2006, relativa alla semplificazione dello scambio di informazioni e intelligence tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge⁴⁰. Tale scambio di dati PNR tra autorità di polizia e giudiziarie dovrebbe rispondere alle norme in materia di cooperazione di polizia e giudiziaria.
- (21) Il periodo di conservazione dei dati PNR deve essere proporzionato agli obiettivi di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi. Tenuto conto della loro natura e uso, è necessario che i dati PNR siano conservati per un periodo abbastanza lungo per poter effettuare analisi e utilizzarli nelle indagini. Per evitare un uso sproporzionato, è necessario che dopo un periodo iniziale i dati siano resi anonimi e accessibili soltanto a condizioni molto rigorose e limitate.
- (22) Qualora dei dati PNR siano stati trasferiti a un'autorità competente e siano usati nell'ambito di specifiche indagini o azioni penali, la loro conservazione presso quell'autorità deve rispondere alle norme di diritto interno dello Stato membro interessato, indipendentemente dai periodi di conservazione stabiliti dalla presente direttiva.
- (23) Il trattamento a livello nazionale dei dati PNR effettuato in ciascuno Stato membro dall'Unità d'informazione sui passeggeri e dalle autorità competenti deve rispondere a una norma di protezione dei dati personali ai sensi della legislazione nazionale che sia in linea con la decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale⁴¹ (di seguito "decisione quadro 2008/977/GAI").

³⁹ GU L 121 del 15.5.2009, pag. 37.

⁴⁰ GU L 386 del 29.12.2006, pag. 89.

⁴¹ GU L 350 del 30.12.2008, pag. 60.

- (24) In considerazione del diritto alla protezione dei dati personali, è necessario che i diritti degli interessati in relazione al trattamento dei dati PNR che li riguardano, cioè il diritto di accesso, il diritto di rettifica, cancellazione o blocco, così come il diritto a compensazione e il diritto di proporre un ricorso giurisdizionale, siano conformi alla decisione quadro 2008/977/GAI.
- (25) In ordine al diritto del passeggero di essere informato del trattamento dei propri dati personali, gli Stati membri devono fare in modo che i passeggeri ricevano informazioni accurate sulla raccolta dei dati PNR e sul loro trasferimento all'Unità d'informazione sui passeggeri.
- (26) Il trasferimento di dati PNR dagli Stati membri ai paesi terzi deve essere consentito solo caso per caso e conformemente alla decisione quadro 2008/977/GAI. Per garantire la protezione dei dati personali, tali trasferimenti devono essere subordinati a requisiti supplementari in materia di finalità del trasferimento, qualità dell'autorità ricevente e garanzie applicabili ai dati personali trasferiti nel paese terzo.
- (27) L'autorità nazionale di controllo istituita in virtù della decisione quadro 2008/977/GAI dovrebbe essere altresì incaricata di dare consulenza in merito alle disposizioni della presente direttiva e di sorvegliarne l'applicazione e l'attuazione.
- (28) La presente direttiva non pregiudica la possibilità che gli Stati membri istituiscano, ai sensi della legislazione nazionale, un sistema di raccolta e trattamento dei dati PNR per finalità diverse da quelle previste nella presente direttiva ovvero presso vettori diversi da quelli precisati nella presente direttiva, riguardante i voli nazionali e nel rispetto delle pertinenti norme di protezione dei dati, purché la legislazione nazionale sia conforme all'acquis dell'Unione. È opportuno che la raccolta dei dati PNR nei voli interni sia oggetto di una futura riflessione specifica.
- (29) Poiché le disposizioni nazionali relative al trattamento dei dati personali, compresi i dati PNR, divergono sul piano giuridico e tecnico, i vettori aerei fanno e dovranno far fronte a una molteplicità di requisiti riguardo al tipo di informazioni da trasmettere e alle condizioni in cui tali informazioni vanno trasmesse alle autorità nazionali competenti. Tale divergenza rischia di compromettere l'efficace cooperazione, tra queste autorità, in materia di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.
- (30) Poiché gli obiettivi della presente direttiva non possono essere conseguiti in misura sufficiente dagli Stati membri e possono dunque essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. La presente direttiva si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.
- (31) La presente direttiva rispetta i diritti fondamentali e i principi della Carta dei diritti fondamentali dell'Unione europea, in particolare il diritto alla protezione dei dati personali, il diritto al rispetto della vita privata e il diritto alla non discriminazione, tutelati dagli articoli 8, 7 e 21 della Carta, e deve essere attuata di conseguenza. La direttiva è compatibile con i principi di protezione dei dati e le sue disposizioni sono in linea con la decisione quadro 2008/977/GAI. Inoltre, e al fine di rispettare il principio

di proporzionalità, in specifici ambiti essa prevede norme di protezione dei dati più severe rispetto alla decisione quadro 2008/977/GAI.

- (32) In particolare, il campo di applicazione della presente direttiva è quanto più limitato; è ammessa la conservazione dei dati PNR per un periodo massimo di cinque anni, scaduto il quale i dati devono essere cancellati; i dati devono essere resi anonimi dopo un periodo brevissimo; sono vietati la raccolta e l'uso di dati sensibili. Per assicurare una protezione dei dati effettiva e di livello elevato, gli Stati membri sono tenuti a provvedere affinché un'autorità nazionale di controllo indipendente sia incaricata di dare consulenza e sorvegliare le modalità di trattamento dei dati PNR. Tutti i trattamenti di dati PNR devono essere registrati o documentati ai fini della verifica della legittimità del trattamento, dell'autocontrollo e per garantire l'integrità dei dati e la sicurezza del loro trattamento. Gli Stati membri devono altresì provvedere affinché i passeggeri siano informati in modo chiaro e preciso della raccolta dei dati PNR e dei loro diritti.
- (33) [A norma dell'articolo 3 del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, detti Stati membri hanno notificato che desiderano partecipare all'adozione e all'applicazione della presente direttiva] OPPURE [Fatto salvo l'articolo 4 del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, detti Stati membri non partecipano all'adozione della presente direttiva, non sono da essa vincolati, né sono soggetti alla sua applicazione].
- (34) A norma degli articoli 1 e 2 del protocollo n. 22 sulla posizione della Danimarca, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, la Danimarca non partecipa all'adozione della presente direttiva, non è da essa vincolata, né è soggetta alla sua applicazione,

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto e campo di applicazione

1. La presente direttiva dispone il trasferimento a cura dei vettori aerei dei dati del codice di prenotazione dei passeggeri dei voli internazionali da e verso gli Stati membri, così come il trattamento di quei dati, comprese le operazioni di raccolta, uso e conservazione a cura degli Stati membri e il loro scambio reciproco.
2. I dati PNR raccolti conformemente alla presente direttiva possono essere trattati solo per le seguenti finalità:

- (a) prevenire, accertare, indagare e perseguire i reati di terrorismo e i reati gravi conformemente all'articolo 4, paragrafo 2, lettere b) e c), e
- (b) prevenire, accertare, indagare e perseguire i reati di terrorismo e i reati gravi di natura transnazionale conformemente all'articolo 4, paragrafo 2, lettere a) e d).

Articolo 2

Definizioni

Ai fini della presente direttiva si intende per:

- a) "veicolo aereo", un'impresa di trasporto aereo titolare di una licenza di esercizio in corso di validità o equivalente che le consente di effettuare trasporti aerei di passeggeri;
- b) "volo internazionale", un volo di linea o non di linea effettuato da un veicolo aereo che deve atterrare nel territorio di uno Stato membro in provenienza da un paese terzo oppure deve partire dal territorio di uno Stato membro con destinazione finale in un paese terzo, compresi in entrambi i casi i voli di trasferimento o di transito;
- c) "dati del codice di prenotazione" o "dati PNR", le informazioni relative al viaggio di ciascun passeggero comprendenti i dati necessari per il trattamento e il controllo delle prenotazioni a cura delle compagnie aeree e di prenotazione interessate per ogni volo prenotato da qualunque persona o per suo conto, siano esse registrate in sistemi di prenotazione, in sistemi di controllo delle partenze (Departure Control Systems, DCS) o in altri sistemi equivalenti con le stesse funzionalità;
- d) "passeggero", chiunque, salvo i membri dell'equipaggio, sia trasportato o da trasportare in un aeromobile con il consenso del veicolo;
- e) "sistema di prenotazione", il sistema d'inventario interno del veicolo aereo in cui sono raccolti i dati PNR ai fini della gestione delle prenotazioni;
- f) "metodo push", il metodo in base al quale i vettori aerei trasferiscono i dati PNR richiesti alla banca dati dell'autorità richiedente;
- g) "reati di terrorismo", i reati ai sensi del diritto nazionale di cui agli articoli da 1 a 4 della decisione quadro 2002/475/GAI del Consiglio;
- h) "reati gravi", i reati ai sensi del diritto nazionale di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio, se punibili con una pena detentiva o una misura di sicurezza privativa della libertà personale non inferiore a tre anni conformemente al diritto nazionale di uno Stato membro. Gli Stati membri possono tuttavia escludere i reati minori per i quali, tenuto conto dei rispettivi ordinamenti giuridici penali, il trattamento dei dati PNR ai sensi della presente direttiva non sia conforme al principio di proporzionalità.;
- i) "reati gravi di natura transnazionale", i reati ai sensi del diritto nazionale di cui all'articolo 2, paragrafo 2, della decisione quadro 2002/584/GAI del Consiglio, se punibili con una pena detentiva o una misura di sicurezza privativa della libertà

personale non inferiore a tre anni conformemente al diritto nazionale di uno Stato membro, e se:

- i) sono commessi in più di uno Stato;
- ii) sono commessi in uno Stato ma preparati, pianificati, diretti o controllati in misura sostanziale in un altro Stato;
- iii) sono commessi in uno Stato ma vi è implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato;
- iv) sono commessi in uno Stato ma hanno effetti sostanziali in un altro Stato.

CAPO II

COMPETENZE DEGLI STATI MEMBRI

Articolo 3

Unità d'informazione sui passeggeri

1. Ciascuno Stato membro istituisce o designa un'autorità competente in materia di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, o una sua sezione che agisca in qualità di "Unità d'informazione sui passeggeri" incaricata di raccogliere i dati PNR presso i vettori aerei, di conservarli e analizzarli e di trasmettere i risultati di tale analisi alle autorità competenti di cui all'articolo 5. I membri del suo personale possono essere funzionari distaccati delle autorità pubbliche competenti.
2. Due o più Stati membri possono istituire o designare una stessa autorità che agisca in qualità di Unità d'informazione sui passeggeri. Tale unità è stabilita in uno degli Stati membri partecipanti ed è considerata l'Unità nazionale d'informazione sui passeggeri di tutti gli Stati membri partecipanti. Gli Stati membri partecipanti ne concordano le precise modalità di funzionamento e rispettano le prescrizioni di cui alla presente direttiva.
3. Ciascuno Stato membro informa la Commissione entro un mese dall'istituzione dell'Unità d'informazione sui passeggeri, e può aggiornare in qualsiasi momento la sua dichiarazione. La Commissione pubblica questa informazione e gli eventuali aggiornamenti nella *Gazzetta ufficiale dell'Unione europea*.

Articolo 4

Trattamento dei dati PNR

1. I dati PNR trasferiti dai vettori aerei conformemente all'articolo 6 che riguardano i voli internazionali in arrivo nel territorio o in partenza dal territorio di ogni Stato membro sono raccolti dall'Unità d'informazione sui passeggeri dello Stato membro interessato. Qualora nei dati PNR trasferiti dai vettori aerei siano compresi altri dati

rispetto a quelli elencati nell'allegato, l'Unità d'informazione sui passeggeri li cancella non appena li riceve.

2. L'Unità d'informazione sui passeggeri provvede al trattamento dei dati PNR unicamente per le seguenti finalità:
 - (a) valutare i passeggeri prima dell'arrivo o della partenza prevista per identificare quelli che potrebbero essere implicati in reati di terrorismo o in reati gravi di natura transnazionale, da sottoporre all'ulteriore verifica delle autorità competenti di cui all'articolo 5. Nell'effettuare tale valutazione l'Unità d'informazione sui passeggeri può analizzare i dati PNR sulla base di criteri di rischio prestabiliti. Gli Stati membri provvedono affinché i riscontri positivi a seguito di tale trattamento automatizzato siano singolarmente sottoposti a un esame non automatizzato per verificare se sia necessario l'intervento dell'autorità competente di cui all'articolo 5;
 - (b) valutare i passeggeri prima dell'arrivo o della partenza prevista per identificare quelli che potrebbero essere implicati in reati di terrorismo o in reati gravi, da sottoporre all'ulteriore verifica delle autorità competenti di cui all'articolo 5. Nell'effettuare tale valutazione l'Unità d'informazione sui passeggeri può confrontare i dati PNR con le banche dati pertinenti, anche internazionali o nazionali e compresi i duplicati nazionali di banche dati dell'Unione, che siano state istituite in base alla normativa dell'Unione e riguardino persone o oggetti ricercati o segnalati, conformemente alle norme europee, internazionali e nazionali applicabili a tali schedari. Gli Stati membri provvedono affinché i riscontri positivi a seguito di tale trattamento automatizzato siano singolarmente sottoposti a un esame non automatizzato per verificare se sia necessario l'intervento dell'autorità competente di cui all'articolo 5;
 - (c) rispondere, caso per caso, alle richieste debitamente motivate delle autorità competenti di trasmettere e trattare dati PNR in casi specifici a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, e di comunicare i risultati di tale trattamento alle autorità stesse, e
 - (d) analizzare i dati PNR per aggiornare i criteri o definirne di nuovi al fine di effettuare valutazioni per identificare le persone che potrebbero essere implicate in reati di terrorismo o in reati gravi di natura transnazionale conformemente alla lettera a).
3. La valutazione dei passeggeri prima dell'arrivo previsto nello Stato membro o della partenza prevista dallo Stato membro ai sensi del paragrafo 2, lettera a), è effettuata in modo non discriminatorio in base a criteri di valutazione stabiliti dall'Unità d'informazione sui passeggeri. Gli Stati membri assicurano che i criteri di valutazione siano stabiliti dall'Unità d'informazione sui passeggeri in cooperazione con le autorità competenti di cui all'articolo 5. I criteri di valutazione non sono in alcun caso basati sull'origine razziale o etnica, sulle convinzioni religiose o filosofiche, sulle opinioni politiche, sull'appartenenza sindacale, sullo stato di salute o sull'orientamento sessuale dell'interessato.

4. L'Unità d'informazione sui passeggeri di uno Stato membro trasferisce i dati PNR o i risultati del trattamento dei dati PNR dei passeggeri identificati conformemente al paragrafo 2, lettere a) e b), per ulteriore verifica, alle autorità competenti dello stesso Stato membro. Tali trasferimenti sono effettuati solo caso per caso.

Articolo 5

Autorità competenti

1. Ciascuno Stato membro adotta l'elenco delle autorità competenti autorizzate a chiedere o ricevere dalle Unità d'informazione sui passeggeri i dati PNR o i risultati del loro trattamento ai fini di un'ulteriore verifica delle informazioni o di interventi appropriati per prevenire, accertare, indagare e perseguire i reati di terrorismo e i reati gravi.
2. Sono autorità competenti le autorità preposte alla prevenzione, all'accertamento, all'indagine o all'azione penale nei confronti dei reati di terrorismo e dei reati gravi.
3. Entro dodici mesi dall'entrata in vigore della presente direttiva, ciascuno Stato membro notifica alla Commissione l'elenco delle proprie autorità competenti e può aggiornare in qualsiasi momento la sua dichiarazione. La Commissione pubblica questa informazione e gli eventuali aggiornamenti nella *Gazzetta ufficiale dell'Unione europea*.
4. Le autorità competenti degli Stati membri possono sottoporre a ulteriore trattamento i dati PNR dei passeggeri e i risultati del loro trattamento ricevuti dall'Unità d'informazione sui passeggeri unicamente per prevenire, accertare, indagare o perseguire i reati di terrorismo o altri reati gravi.
5. Il paragrafo 4 non pregiudica le competenze delle autorità di polizia e giudiziarie nazionali qualora siano individuati altri reati o indizi di reato durante l'azione di contrasto determinata da tale trattamento.
6. Le autorità competenti non possono prendere decisioni che comportino conseguenze giuridiche negative per l'interessato o lo danneggino in modo significativo, soltanto sulla base del trattamento automatico dei dati PNR. Decisioni di questo tipo non possono fondarsi neanche sull'origine razziale o etnica, sulle opinioni politiche, sulle convinzioni religiose o filosofiche, sull'appartenenza sindacale dell'interessato, sul suo stato di salute o sul suo orientamento sessuale.

Articolo 6

Obblighi dei vettori aerei

1. Gli Stati membri prendono i necessari provvedimenti affinché i vettori aerei trasferiscano ("push") i dati PNR definiti all'articolo 2, lettera c) e elencati nell'allegato, a condizione che già li raccolgano, alla banca dati dell'Unità nazionale d'informazione sui passeggeri dello Stato membro nel cui territorio atterra o dal cui territorio parte il volo internazionale. Qualora il volo sia operato in code-sharing da uno o più vettori aerei, l'obbligo di trasferire i dati PNR di tutti i passeggeri del volo

spetta al vettore aereo che opera il volo. Qualora il volo faccia uno o più scali negli aeroporti degli Stati membri, i vettori aerei trasferiscono i dati PNR alle Unità d'informazione sui passeggeri di tutti gli Stati membri interessati.

2. I vettori aerei trasferiscono i dati PNR elettronicamente utilizzando i protocolli comuni e i formati di dati supportati da adottare secondo la procedura di cui agli articoli 13 e 14 o, in caso di guasto tecnico, con altro mezzo appropriato assicurando un adeguato livello di sicurezza dei dati:
 - a) da 24 a 48 ore prima dell'ora prevista di partenza del volo,
e
 - b) immediatamente dopo la chiusura del volo, ossia una volta che i passeggeri sono saliti a bordo dell'aeromobile pronto per il decollo e non è più possibile l'imbarco di altri passeggeri.
3. Gli Stati membri possono consentire ai vettori aerei di limitare il trasferimento di cui al paragrafo 2, lettera b), agli aggiornamenti del trasferimento di cui al paragrafo 2, lettera a).
4. Caso per caso, su richiesta di un'Unità d'informazione sui passeggeri conformemente alla legislazione nazionale, i vettori aerei trasferiscono i dati PNR quando è necessario accedervi prima del momento indicato al paragrafo 2, lettera a), per rispondere a una minaccia specifica e reale connessa a reati di terrorismo o a reati gravi.

Articolo 7

Scambio di informazioni tra Stati membri

1. Gli Stati membri provvedono affinché, per quanto riguarda i soggetti identificati da un'Unità d'informazione sui passeggeri a norma dell'articolo 4, paragrafo 2, lettere a) e b), questa trasmetta i risultati del trattamento dei dati PNR alle Unità d'informazione sui passeggeri di altri Stati membri qualora giudichi tale trasferimento necessario per prevenire, accertare, indagare o perseguire reati di terrorismo o i reati gravi. Le Unità d'informazione sui passeggeri degli Stati membri riceventi trasmettono i dati PNR o i risultati del loro trattamento alle rispettive autorità competenti.
2. L'Unità d'informazione sui passeggeri di uno Stato membro è autorizzata a chiedere, se necessario, all'Unità d'informazione sui passeggeri di qualsiasi altro Stato membro di trasmetterle dati PNR conservati nella sua banca dati in virtù dell'articolo 9, paragrafo 1, e, se necessario, i risultati del trattamento di dati PNR. La richiesta di tali dati può riguardare uno o più elementi di dati combinati fra loro, secondo quanto ritenga necessario l'Unità d'informazione sui passeggeri richiedente in relazione a un caso specifico di prevenzione, accertamento, indagine o azione penale nei confronti di reati di terrorismo o di reati gravi. Le Unità d'informazione sui passeggeri comunicano i dati richiesti appena possibile e trasmettono anche i risultati del trattamento dei dati PNR, se già predisposti ai sensi dell'articolo 4, paragrafo 2, lettere a) e b).

3. L'Unità d'informazione sui passeggeri di uno Stato membro è autorizzata a chiedere, se necessario, all'Unità d'informazione sui passeggeri di qualsiasi altro Stato membro di trasmetterle dati PNR conservati nella sua banca dati in virtù dell'articolo 9, paragrafo 2, e, se necessario, i risultati del trattamento di dati PNR. L'Unità d'informazione sui passeggeri può chiedere di accedere integralmente e senza mascheratura a dati PNR specifici conservati dall'Unità d'informazione sui passeggeri di un altro Stato membro solo in casi eccezionali per rispondere a una minaccia specifica o nell'ambito di un'indagine o di un'azione penale specifica connessa a reati di terrorismo o a reati gravi.
4. Nella sola ipotesi che ciò sia necessario per prevenire una minaccia grave e immediata alla sicurezza pubblica, le autorità competenti di uno Stato membro hanno facoltà di chiedere direttamente all'Unità d'informazione sui passeggeri di qualsiasi altro Stato membro di trasmettere loro dati PNR conservati nella sua banca dati in virtù dell'articolo 9, paragrafi 1 e 2. Tali richieste rientrano nell'ambito di un'indagine o di un'azione penale specifica nei confronti di reati di terrorismo o di reati gravi e sono motivate. Le Unità d'informazione sui passeggeri rispondono a tali richieste in via prioritaria. In tutti gli altri casi, le autorità competenti inoltrano le richieste tramite l'Unità d'informazione sui passeggeri del proprio Stato membro.
5. In circostanze eccezionali, se è necessario accedere tempestivamente a dati PNR per rispondere a una minaccia specifica e reale connessa a reati di terrorismo o reati gravi, l'Unità d'informazione sui passeggeri di uno Stato membro è autorizzata a chiedere all'Unità d'informazione sui passeggeri di un altro Stato membro di trasmetterle in qualsiasi momento i dati PNR relativi ai voli in arrivo nel suo territorio o in partenza dal suo territorio.
6. Lo scambio di informazioni ai sensi del presente articolo può avvenire tramite qualsiasi canale esistente di cooperazione giudiziaria internazionale. La lingua utilizzata per la richiesta e lo scambio di informazioni è quella applicabile al canale utilizzato. Nell'effettuare le notifiche a norma dell'articolo 3, paragrafo 3, gli Stati membri comunicano alla Commissione anche gli estremi dei punti di contatto cui possono essere trasmesse le richieste in casi di urgenza. La Commissione comunica agli Stati membri le notifiche ricevute.

Articolo 8

Trasferimento dei dati ai paesi terzi

Uno Stato membro può trasferire i dati PNR e i risultati del loro trattamento a un paese terzo soltanto caso per caso e se:

- a) ricorrono le condizioni di cui all'articolo 13 della decisione quadro 2008/977/GAI del Consiglio,
- b) il trasferimento è necessario per le finalità specificate all'articolo 1, paragrafo 2, della presente direttiva, e
- c) il paese terzo accetta di trasferire i dati ad un altro paese terzo soltanto se il trasferimento è necessario per le finalità specificate all'articolo 1, paragrafo 2,

della presente direttiva e soltanto previa autorizzazione esplicita dello Stato membro.

Articolo 9

Periodo di conservazione dei dati

1. Gli Stati membri provvedono affinché i dati PNR trasmessi dai vettori aerei all'Unità d'informazione sui passeggeri siano da questa conservati in una banca dati per un periodo di 30 giorni dal trasferimento all'Unità d'informazione sui passeggeri del primo Stato membro dal cui territorio parte o nel cui territorio atterra il volo internazionale.
2. Allo scadere del periodo di 30 giorni dal trasferimento dei dati PNR all'Unità d'informazione sui passeggeri di cui al paragrafo 1, i dati sono conservati presso l'Unità d'informazione sui passeggeri per altri cinque anni. Durante questo periodo, tutti gli elementi d'informazione che potrebbero servire ad identificare il passeggero cui si riferiscono i dati PNR sono mascherati. I dati PNR resi così anonimi sono accessibili solo a un numero limitato di membri del personale dell'Unità d'informazione sui passeggeri specificamente autorizzati a analizzare i dati PNR e a sviluppare criteri di valutazione in conformità dell'articolo 4, paragrafo 2, lettera d). L'accesso integrale ai dati PNR è consentito solo al capo dell'Unità d'informazione sui passeggeri per le finalità dell'articolo 4, paragrafo 2, lettera c), e quando si può ragionevolmente ritenere che l'accesso sia necessario per un'indagine e in risposta a una minaccia o un rischio specifico e reale o nell'ambito di un'indagine o di un'azione penale specifica.

Ai fini della presente direttiva, gli elementi d'informazione che potrebbero servire a identificare il passeggero cui si riferiscono i dati PNR e che vanno filtrati e mascherati sono i seguenti:

 - il nome o i nomi, compresi i nomi di altri passeggeri figuranti nel PNR e il numero di viaggiatori che viaggiano insieme figurante nel PNR;
 - l'indirizzo e gli estremi;
 - le osservazioni generali contenenti informazioni che potrebbero servire ad identificare il passeggero cui si riferiscono i dati PNR, e
 - informazioni anticipate sui passeggeri eventualmente assunte.
3. Gli Stati membri provvedono affinché i dati PNR siano cancellati allo scadere del periodo di cui al paragrafo 2. Questo obbligo non incide sui casi in cui dati PNR specifici sono stati trasferiti a un'autorità competente e sono usati nell'ambito di specifiche indagini o azioni penali, nel qual caso la loro conservazione presso l'autorità competente è disciplinata dalla legislazione nazionale dello Stato membro.
4. Gli esiti dell'operazione di riscontro di cui all'articolo 4, paragrafo 2, lettere a) e b), sono conservati presso l'Unità d'informazione sui passeggeri soltanto per il tempo necessario a informare le autorità competenti di un riscontro positivo. L'esito di un'operazione automatizzata di riscontro, anche qualora risulti negativo a seguito

dell'esame individuale non automatizzato, è comunque memorizzato per un periodo massimo di tre anni in modo da evitare futuri "falsi" riscontri positivi, a meno che i dati di riferimento non siano stati ancora cancellati in conformità del paragrafo 3 allo scadere dei cinque anni, nel qual caso il registro è conservato fino a cancellazione dei dati di riferimento.

Articolo 10

Sanzioni nei confronti dei vettori aerei

Gli Stati membri prevedono, conformemente al diritto nazionale, sanzioni dissuasive, effettive e proporzionate, anche pecuniarie, a carico dei vettori aerei che non trasmettono i dati richiesti in forza della presente direttiva, nella misura in cui li hanno già raccolti, o non li trasmettono nel formato richiesto o altrimenti violano le disposizioni nazionali adottate in conformità della presente direttiva.

Articolo 11

Protezione dei dati personali

1. Ciascuno Stato membro dispone che, in relazione a qualsiasi trattamento di dati personali a norma della presente direttiva, ogni passeggero goda di un diritto di accesso, di un diritto di rettifica, cancellazione o blocco, di un diritto a compensazione e di un diritto di proporre un ricorso giurisdizionale identici a quelli previsti dalle norme nazionali di attuazione degli articoli 17, 18, 19 e 20 della decisione quadro 2008/977/GAI del Consiglio. Si applicano pertanto le disposizioni degli articoli 17, 18, 19 e 20 della decisione quadro 2008/977/GAI del Consiglio.
2. Ciascuno Stato membro dispone che le norme nazionali di attuazione degli articoli 21 e 22 della decisione quadro 2008/977/GAI del Consiglio riguardanti la riservatezza del trattamento e la sicurezza dei dati si applichino anche a qualsiasi trattamento di dati personali effettuato in conformità della presente direttiva.
3. È vietato qualsiasi trattamento di dati PNR che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, lo stato di salute o l'orientamento sessuale dell'interessato. Qualora l'Unità d'informazione sui passeggeri riceva dati PNR che rivelano tali informazioni, questi sono cancellati immediatamente.
4. Tutti i trattamenti di dati PNR effettuati dai vettori aerei, tutti i trasferimenti di dati PNR a opera delle Unità d'informazione sui passeggeri e tutte le richieste delle autorità competenti o delle Unità d'informazione sui passeggeri di altri Stati membri e di paesi terzi, anche se rifiutate, sono registrati o documentati presso l'Unità d'informazione sui passeggeri e le autorità competenti ai fini della verifica della correttezza del trattamento, dell'autocontrollo e per garantire l'integrità dei dati e la sicurezza del loro trattamento, in particolare da parte delle autorità nazionali di controllo per la protezione dei dati. I registri sono conservati per cinque anni, a meno che i dati di riferimento non siano stati ancora cancellati in conformità dell'articolo 9, paragrafo 3, allo scadere dei cinque anni, nel qual caso i registri sono conservati fino a cancellazione dei dati di riferimento.

5. Gli Stati membri dispongono che i vettori aerei, i loro agenti o altri venditori di biglietti per il trasporto di passeggeri sui servizi aerei informino in modo chiaro e preciso i passeggeri dei voli internazionali, al momento in cui prenotano il volo e acquistano il biglietto, della trasmissione dei dati PNR all'Unità d'informazione sui passeggeri, delle finalità del trattamento, del periodo di conservazione dei dati e del loro possibile uso per prevenire, accertare, indagare e perseguire i reati di terrorismo e i reati gravi, della possibilità di scambiare e condividere tali dati e dei loro diritti alla protezione dei dati, in particolare il diritto di sporgere reclamo presso un'autorità nazionale di controllo per la protezione dei dati di loro scelta. Gli Stati membri mettono queste stesse informazioni a disposizione del pubblico.
6. È vietato qualsiasi trasferimento di dati PNR dalle Unità d'informazione sui passeggeri e dalle autorità competenti a privati negli Stati membri o in paesi terzi.
7. Fatto salvo l'articolo 10, gli Stati membri adottano opportune misure per garantire la piena attuazione delle disposizioni della presente direttiva e stabiliscono in particolare sanzioni efficaci, proporzionate e dissuasive da applicarsi in caso di violazione delle disposizioni adottate in conformità della presente direttiva.

Articolo 12

Autorità nazionale di controllo

Ciascuno Stato membro dispone che l'autorità nazionale di controllo istituita in virtù dell'articolo 25 della decisione quadro 2008/977/GAI sia altresì incaricata di dare consulenza e sorvegliare l'applicazione, nel suo territorio, delle disposizioni da quello adottate in conformità della presente direttiva. Le altre disposizioni dell'articolo 25 della decisione quadro 2008/977/GAI sono ugualmente applicabili.

CAPO IV

MISURE DI ESECUZIONE

Articolo 13

Protocolli comuni e formati di dati supportati

1. Per un periodo di un anno dall'adozione dei protocolli comuni e dei formati di dati supportati conformemente all'articolo 14, tutti i trasferimenti di dati PNR dai vettori aerei alle Unità d'informazione sui passeggeri ai fini della presente direttiva sono effettuati elettronicamente o, in caso di guasto tecnico, con altro mezzo appropriato.
2. Allo scadere del termine di un anno dalla data di adozione dei protocolli comuni e dei formati di dati supportati, tutti i trasferimenti di dati PNR dai vettori aerei alle Unità d'informazione sui passeggeri ai fini della presente direttiva sono effettuati elettronicamente e con metodi sicuri utilizzando protocolli comuni accettati, identici per tutti i trasferimenti, che garantiscano la sicurezza dei dati durante il trasferimento, e un formato di dati supportato che ne garantisca la leggibilità a tutti

gli interessati. Tutti i vettori aerei hanno l'obbligo di scegliere e notificare all'Unità d'informazione sui passeggeri il protocollo comune e il formato di dati che intendono usare per i loro trasferimenti.

3. La Commissione stabilisce l'elenco dei protocolli comuni accettati e dei formati di dati supportati, e se necessario l'adeguata conformemente alla procedura di cui all'articolo 14, paragrafo 2.
4. Finché non sono disponibili i protocolli comuni accettati e i formati di dati supportati di cui ai paragrafi 2 e 3, resta d'applicazione il paragrafo 1.
5. Ciascuno Stato membro provvede affinché siano prese le necessarie misure tecniche per usare i protocolli comuni e i formati di dati entro un anno dalla data di adozione dei protocolli comuni e dei formati di dati supportati.

Articolo 14

Procedura di comitato

1. La Commissione è assistita da un comitato (di seguito "comitato") ai sensi del regolamento [.../2011/UE] del 16 febbraio 2011.
2. Quando è fatto riferimento al presente paragrafo, si applica l'articolo 4 del regolamento [.../2011/UE] del 16 febbraio 2011.

CAPO V

DISPOSIZIONI FINALI

Articolo 15

Recepimento

1. Gli Stati membri mettono in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva entro due anni dalla sua entrata in vigore. Essi comunicano immediatamente alla Commissione il testo di tali disposizioni nonché una tavola di concordanza tra queste ultime e la presente direttiva.

Quando gli Stati membri adottano tali disposizioni, queste contengono un riferimento alla presente direttiva o sono corredate di un siffatto riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono decise dagli Stati membri.

2. Gli Stati membri comunicano alla Commissione il testo delle disposizioni essenziali di diritto interno adottate nella materia disciplinata dalla presente direttiva.

Articolo 16

Disposizioni transitorie

Alla data di cui all'articolo 15, paragrafo 1, ossia due anni dopo l'entrata in vigore della presente direttiva, gli Stati membri garantiscono che siano raccolti i dati PNR di almeno il 30% di tutti i voli di cui all'articolo 6, paragrafo 1. Per due anni dalla data di cui all'articolo 15 gli Stati membri garantiscono che siano raccolti i dati PNR di almeno il 60 % di tutti i voli di cui all'articolo 6, paragrafo 1. Dopo quattro anni dalla data di cui all'articolo 15 gli Stati membri garantiscono che siano raccolti i dati PNR di tutti i voli di cui all'articolo 6, paragrafo 1.

Articolo 17

Riesame

Sulla scorta delle informazioni comunicate dagli Stati membri, la Commissione:

- a) esamina la fattibilità e la necessità di includere i voli interni nel campo di applicazione della presente direttiva, alla luce dell'esperienza maturata dagli Stati membri che raccolgono i dati PNR in relazione ai voli interni. La Commissione presenta una relazione al Parlamento europeo e al Consiglio entro due anni dalla data di cui all'articolo 15, paragrafo 1;
- b) procede a un riesame dell'applicazione della presente direttiva e riferisce al Parlamento europeo e al Consiglio entro quattro anni dalla data di cui all'articolo 15, paragrafo 1. Il riesame verte su tutti gli elementi della presente direttiva, con particolare riguardo al rispetto del livello di protezione dei dati personali, alla durata della conservazione dei dati e alla qualità delle valutazioni. Esso ricomprende anche le statistiche raccolte in conformità dell'articolo 18.

Articolo 18

Statistiche

1. Gli Stati membri predispongono una serie di statistiche sui dati PNR trasmessi alle Unità d'informazione sui passeggeri. Queste statistiche indicano quanto meno, per vettore aereo e per destinazione, il numero di identificazioni di persone che potrebbero essere implicate in un reato di terrorismo o in un reato grave ai sensi dell'articolo 4, paragrafo 2, e il numero delle successive azioni di contrasto intraprese che hanno comportato l'uso di dati PNR.
2. Tali statistiche non contengono dati personali e sono trasmesse ogni anno alla Commissione.

Articolo 19

Relazione con altri strumenti

1. Gli Stati membri possono continuare ad applicare tra loro gli accordi o le intese bilaterali o multilaterali sullo scambio di informazioni tra autorità competenti in vigore al momento dell'adozione della presente direttiva, purché compatibili con quest'ultima.
2. La presente direttiva non pregiudica gli obblighi e impegni dell'Unione europea derivanti da accordi bilaterali e/o multilaterali conclusi con paesi terzi.

Articolo 20

Entrata in vigore

La presente direttiva entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Gli Stati membri sono destinatari della presente direttiva conformemente ai trattati.

Fatto a Bruxelles, il [...]

Per il Parlamento europeo
Il presidente

Per il Consiglio
Il presidente

ALLEGATO

Dati PNR raccolti dai vettori aerei

- (1) Codice PNR di identificazione della pratica
- (2) Data di prenotazione/emissione del biglietto
- (3) Data o date previste di viaggio
- (4) Nome o nomi
- (5) Indirizzo, recapito telefonico e indirizzo di posta elettronica
- (6) Informazioni su tutte le modalità di pagamento, compreso l'indirizzo di fatturazione
- (7) Itinerario completo per specifico PNR
- (8) Informazioni sui viaggiatori abituali "Frequent flyer"
- (9) Agenzia/agente di viaggio
- (10) Status di viaggio del passeggero, incluse conferme, check-in, precedenti assenze all'imbarco o passeggero senza prenotazione
- (11) PNR scissi/divisi
- (12) Osservazioni generali (comprese tutte le informazioni disponibili sui minori non accompagnati di età inferiore a 18 anni, quali nome e sesso del minore, età, lingua o lingue parlate, nome e recapito dell'accompagnatore alla partenza e relazione con il minore, nome e recapito dell'accompagnatore all'arrivo e relazione con il minore, agente alla partenza e all'arrivo)
- (13) Dati sull'emissione del biglietto, compresi il numero del biglietto, la data di emissione del biglietto, i biglietti di sola andata, i campi ATFQ
- (14) Informazioni sul posto, compreso il numero di posto assegnato
- (15) Informazioni sul code share (codici comuni)
- (16) Tutte le informazioni relative al bagaglio
- (17) Numero di viaggiatori e altri nomi figuranti nel PNR
- (18) Informazioni anticipate sui passeggeri (API) eventualmente assunte
- (19) Cronistoria delle modifiche del PNR di cui ai numeri da 1 a 18