«%ParlID»

Legge federale sul trattamento dei dati dei passeggeri aerei per la lotta ai reati terroristici e ad altri reati gravi (Legge sui dati dei passeggeri aerei, LDPA)

Rapporto esplicativo per la procedura di consultazione

(marzo 2022)

Compendio

Il presente disegno di legge intende consentire alla Svizzera di trattare in modo sistematico i dati dei passeggeri aerei allo scopo di sostenere le autorità federali e cantonali nel prevenire, investigare e perseguire reati terroristici e altri reati gravi.

Situazione iniziale

Al momento dell'acquisto di un biglietto aereo, vengono raccolti diversi dati dei passeggeri. Le imprese di trasporto aereo hanno bisogno di questi dati nell'ambito della prenotazione di voli e del check-in. Questo set di dati dei passeggeri aerei, conosciuto a livello internazionale come Passenger Name Record (PNR), contiene ad esempio il nome e l'indirizzo dei passeggeri così come altre informazioni relative ai loro bagagli e alle modalità di pagamento.

Più di 60 Stati hanno riconosciuto il potenziale del PNR e lo utilizzano da diversi anni per combattere il terrorismo e altre forme gravi di criminalità. Il trattamento dei dati dei passeggeri aerei e le analisi specifiche dei dati permettono di individuare non solo persone già note alle autorità di perseguimento penale, bensì, grazie a nuovi spunti per le indagini, anche persone che sono ancora sconosciute a queste stesse autorità ma che potrebbero presentare un legame con il terrorismo o altre forme gravi di criminalità.

Attualmente l'utilizzo del PNR è promosso in tutto il mondo. Tre risoluzioni del Consiglio di sicurezza dell'ONU vincolanti per la Svizzera impongono alla comunità internazionale di impiegare i dati dei passeggeri aerei ai fini della prevenzione del terrorismo. La Svizzera, in qualità di membro dell'Organizzazione dell'aviazione civile internazionale (OACI), è tenuta ad adottare gli standard previsti da quest'ultima in materia di PNR.

Con la direttiva (UE) 2016/681 l'Unione europea (UE) ha obbligato gli Stati membri a creare un sistema PNR nazionale. La direttiva non costituisce uno sviluppo dell'acquis di Schengen. Tuttavia la Svizzera è interessata dalla sua trasposizione, dato che tutte le imprese di trasporto aereo operanti voli dalla Svizzera verso l'UE e viceversa sono tenute a trasmettere i dati in questione.

Se è vero che i dati PNR dei voli operati dalla Svizzera verso gli Stati membri dell'UE, gli Stati Uniti, il Regno Unito e il Canada sono oggi trasmessi alle rispettive autorità competenti, è altresì vero che la Svizzera non può, dal canto suo, trattare in modo sistematico tali dati fintanto che non disporrà di una base legale e di un sistema PNR nazionale.

In assenza di un sistema PNR la Svizzera dispone di meno dati rispetto agli altri Stati Schengen per effettuare controlli all'entrata sul proprio territorio. Vi è pertanto il rischio che persone che costituiscono un pericolo per la sicurezza pubblica possano fare ingresso indisturbati, attraverso la Svizzera, nello spazio Schengen.

L'utilizzo del PNR rappresenta infine per gli Stati Uniti un requisito per la permanenza della Svizzera nel Visa Waiver Program, un programma che consente ai cittadini svizzeri di recarsi negli USA senza visto, per turismo o affari, per una durata massima di 90 giorni.

Contenuto del progetto

La legge sui dati dei passeggeri aerei (LDPA) intende consentire alla Confederazione di trattare i dati dei passeggeri aerei raccolti in occasione della prenotazione di un volo e del check-in allo scopo di combattere i reati terroristici e altri reati gravi.

La competenza per il trattamento dei dati sarà affidata a un nuovo servizio collocato in seno all'Ufficio federale di polizia (fedpol) denominato «unità d'informazione sui passeggeri» (UIP) e noto a livello internazionale come «Passenger Information Unit». L'UIP riceve i dati dalle imprese di trasporto aereo tra le 24 e le 48 ore prima della partenza di un volo da o verso la Svizzera nonché immediatamente dopo la chiusura dell'imbarco.

Mediante il confronto dei dati dei passeggeri aerei con i dati contenuti nei sistemi di informazione di polizia, l'UIP è in grado di identificare, al momento della loro entrata in Svizzera o dell'uscita dal Paese, le persone sospettate o accusate di pianificare o di aver commesso un reato terroristico o un altro reato grave. L'UIP comunicherà in seguito soltanto questi risultati («riscontri positivi») alle competenti autorità della Confederazione e dei Cantoni onde permettere loro di adottare per tempo le misure necessarie. Su incarico di queste autorità, l'UIP deve poter inoltre eseguire analisi mirate dei dati dei passeggeri aerei. Questa procedura consente di individuare persone o legami che suggeriscono la presenza di reti criminali operanti a livello internazionale.

I dati dei passeggeri aerei sono pseudonimizzati automaticamente trascorsi sei mesi dalla loro registrazione presso l'UIP e cancellati dopo cinque anni.

La metà dei collaboratori che presteranno servizio presso l'UIP saranno distaccati dai Cantoni che si faranno carico anche dei relativi costi. Questo assetto tiene conto del fatto che l'UIP opera in larga misura al servizio delle autorità cantonali di perseguimento penale.

Indice

1 Situazione iniziale

Chi prenota un volo comunica alla compagnia di volo o all'agenzia di viaggio una serie di informazioni che sono in seguito conservate nel rispettivo sistema di prenotazione anche dopo la conclusione del viaggio. Tali informazioni, raggruppate in un set di dati dei passeggeri aerei[1] («Passenger Name Record», PNR), forniscono indicazioni non solo sul nome del passeggero e sui suoi dati di contatto (indirizzo di domicilio, telefono e indirizzo di posta elettronica), ma anche sulle modalità di pagamento e su altre persone che viaggiano insieme al passeggero in questione.

In tutto il mondo oltre 60 Paesi hanno già riconosciuto il potenziale del PNR per la sicurezza e utilizzano tali dati quale strumento efficace per combattere il terrorismo e altre forme gravi di criminalità. Ciò consente loro di localizzare tempestivamente gli autori di reati durante i loro spostamenti e di individuarli al momento dell'ingresso o dell'uscita dal Paese nonché di risalire a reti attive a livello internazionale ad esempio nel terrorismo o nella tratta di esseri umani.

Le imprese di trasporto aereo forniscono già oggi i dati PNR relativi ai voli operati dalla Svizzera verso determinati Stati, tra cui gli Stati Uniti d'America. La trasmissione dei dati agli USA si basa sull'Accordo del 23 dicembre 2008[2], che sostituisce un pertinente accordo del 2003 di durata limitata. Nel giugno 2018 gli USA hanno dichiarato che la permanenza della Svizzera nel «Visa Waiver Program» (VWP) è vincolata al suo utilizzo del PNR. Il VWP consente ai cittadini svizzeri di recarsi negli USA senza visto, per turismo o affari, per una durata massima di 90 giorni.

Inoltre, tre risoluzioni del Consiglio di sicurezza dell'ONU[3], vincolanti anche per la Svizzera, sollecitano la comunità internazionale a rafforzare in tutti gli Stati membri le capacità per raccogliere, diffondere e analizzare i dati PNR.

A livello europeo l'Organizzazione per la sicurezza e la Cooperazione in Europa (OSCE), di cui fa parte anche la Svizzera, esorta a utilizzare i dati PNR. L'OSCE definisce il trattamento di dati PNR una misura importante ai fini della prevenzione, dell'accertamento e del perseguimento di reati di terrorismo e sostiene gli Stati nella creazione di un sistema PNR nazionale.

In una prima fase, l'Unione europea ha definito il trattamento dei dati dell'«Advance Passenger Information» (dati API), che rappresentano una parte dei dati PNR, all'interno della direttiva (UE) 2004/82/CE (direttiva API)[4]. La direttiva API è parte dell'acquis di Schengen ed è pertanto vincolante per la Svizzera.

1 Per la definizione v. glossario in allegato.
2 RS **0.748.710.933.6**
3 Risoluzione 2178 (2014) adottata dal Consiglio di sicurezza nella 7272ª sessione del 24 settembre 2014, risoluzione 2396 (2017) adottata dal Consiglio di sicurezza nella 8148ª sessione del 21 dicembre 2017, risoluzione 2482 (2019) adottata dal Consiglio di sicurezza nella 8582ª sessione del 19 luglio 2019.
4 Direttiva 2004/82/CE del Consiglio, del 29 aprile 2004, concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate, GU L 261 del 6.8.2004, pag. 24.

Non è invece vincolante per la Svizzera la direttiva (UE) 2016/681 del 27 aprile 2016 (direttiva PNR)[5], con cui l'UE obbliga gli Stati membri a creare sistemi PNR nazionali. La direttiva non costituisce uno sviluppo dell'acquis di Schengen e la Svizzera non è pertanto obbligata a trasporla. Tuttavia la Svizzera è interessata dalla sua trasposizione dato che le imprese di trasporto aereo vengono obbligate a trasmettere dati anche per i voli operati dalla Svizzera verso l'UE.

Con l'introduzione il 1° ottobre 2015 degli articoli 104*a* e 104*b* all'interno della legge federale del 16 dicembre 2005[6] sugli stranieri e la loro integrazione (LStrI), la Svizzera dispone della base giuridica necessaria a trattare automaticamente i dati API. Tuttavia, al pari dell'UE, la Svizzera non rileva attualmente questi dati in modo sistematico, bensì soltanto per determinati voli considerati a rischio provenienti da Paesi terzi. Il trattamento di questi dati ha lo scopo non solo di migliorare il controllo alla frontiera e di lottare efficacemente contro l'entrata illegale nello spazio Schengen e il transito illegale nelle zone di transito internazionali degli aeroporti, ma anche di contrastare la criminalità organizzata internazionale e il terrorismo (art. 104*a* cpv. 1 lett. c LStrI).

Dati API	
Generalità	Cognome, nome, sesso, data di nascita, cittadinanza
Documento di viaggio	Numero, Stato di rilascio, tipo e data di scadenza
Visto o titolo di soggiorno, ove disponibile	Numero, Stato di rilascio, tipo e data di scadenza
Itinerario di volo prenotato, ove noto	Aeroporto di partenza, aeroporti di scalo in Svizzera o aeroporto di destinazione in Svizzera
Numero del trasporto	
Numero complessivo delle persone trasportate sul volo in questione	
Data e ora previste del decollo e dell'atterraggio	

Dal 1° gennaio 2018 le autorità svizzere di perseguimento penale hanno la possibilità di chiedere sulla base dell'articolo 21*f* della legge federale del 21 dicembre 1948[7] sulla navigazione aerea (LNA) i dati dei passeggeri, laddove questi ultimi siano stati rilevati dalle imprese di trasporto aereo «nell'ambito della loro normale attività». Le

5 Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, GU L 119 del 4.5.2016, pag. 132.
6 RS **142.20**
7 RS **748.0**

autorità di perseguimento penale, oltre ai dati API, entrano pertanto in possesso anche dei seguenti dati sui passeggeri:

- eventuali compagni di viaggio;
- informazioni relative al pagamento, in particolare il metodo di pagamento e il mezzo di pagamento impiegato;
- dati concernenti il servizio presso il quale è stato prenotato il trasporto.

1.1 Necessità di agire e obiettivi

La Svizzera non dispone attualmente né di una base giuridica né di un sistema d'informazione per il trattamento di dati PNR. Per trattamento s'intende qualsiasi operazione relativa a dati personali[8], indipendentemente dai mezzi e dalle procedure impiegati, segnatamente la raccolta, la registrazione, la conservazione, l'utilizzazione, la modificazione, la comunicazione, l'archiviazione, la cancellazione o la distruzione di dati (art. 5 della legge federale del 25 settembre 2020[9] sulla protezione dei dati [nLPD]).

Diversi Stati, tra cui importanti partner economici della Svizzera, chiedono già da tempo i dati PNR alle imprese di trasporto aereo i cui voli atterrano sui loro territori.

I dati sono utilizzati per la lotta al terrorismo e ad altri reati gravi. Il trattamento sistematico dei dati relativi ai passeggeri aerei permette di localizzare le persone ricercate a livello nazionale o internazionale. Le autorità di perseguimento penale possono inoltre ricevere informazioni su persone finora sconosciute alla polizia che hanno legami con il terrorismo o con altre forme gravi di criminalità. Il PNR può pertanto fornire un contributo importante nell'individuare e perseguire reti criminali operanti a livello internazionale. Le imprese di trasporto aereo sono soggette all'obbligo di trasmettere i dati PNR anche per i voli operati dalla Svizzera.

La Svizzera ha concluso un primo accordo con gli USA nel 2003, che prevede la comunicazione dei dati. La trasmissione di dati per i voli operati dalla Svizzera verso il Canada si fonda invece su un memorandum d'intesa concluso tra i due Paesi nel 2006[10].

Lo scambio di dati tra UE e Svizzera va sancito di comune intesa sulla base di un trattato internazionale. Fino alla sua conclusione, la trasmissione di dati agli Stati membri dell'UE dovrà basarsi su una soluzione transitoria elaborata con la partecipazione dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT). Nel maggio 2018 l'Ufficio federale dell'aviazione civile (UFAC) ha comunicato alle imprese di trasporto aereo interessate che, fino alla creazione di una base legale, la trasmissione dei dati dei passeggeri aerei agli Stati membri dell'UE richiedenti sarà possibile se i passeggeri aerei vengono informati nelle condizioni di trasporto in merito alla trasmissione dei loro dati e vi danno il loro consenso. L'IFPDT

8 Per la definizione v. glossario in allegato.
9 FF **2020** 6695 (nel presente rapporto si rinvia alla nuova legge sulla protezione dei dati che sarà applicabile al momento dell'entrata in vigore della legge sui dati dei passeggeri aerei).
10 Consultabile al seguente indirizzo: https://www.newsd.admin.ch/newsd/message/attachments/2242.pdf

ha ribadito da allora a più riprese la necessità di creare rapidamente le basi giuridiche necessarie.

L'assenza di una base legale non consente alla Svizzera di trattare autonomamente i dati PNR. Questa situazione potrebbe avere come conseguenza che persone sospettate di aver commesso o pianificato reati terroristici o un altro reato grave, una volta atterrate in Svizzera, possano proseguire il proprio viaggio nello spazio Schengen per via terrestre aggirando così i sistemi PNR impiegati nei singoli Stati.

Affinché la Svizzera possa in futuro trattare dati PNR per la lotta al terrorismo e ad altri reati gravi, necessita sia di una base giuridica formale, come quella che s'intende creare con il presente progetto di legge, sia di un sistema di informazione PNR.

Il 12 febbraio 2020 il Consiglio federale ha incaricato il Dipartimento federale di giustizia e polizia (DFGP) di elaborare, in collaborazione con il Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni (DATEC), e di sottoporgli un avamprogetto di legge sulla raccolta e l'utilizzo di dati PNR nonché sulla loro trasmissione a Stati che garantiscono una protezione e un trattamento dei dati conforme agli standard della direttiva PNR. Inoltre occorre mettere a punto in collaborazione con il Dipartimento federale degli affari esteri (DFAE) un mandato per l'avvio dei negoziati con l'UE in merito a un accordo relativo al PNR.

1.2 Alternative esaminate e soluzione scelta

Considerazioni di natura legislativa

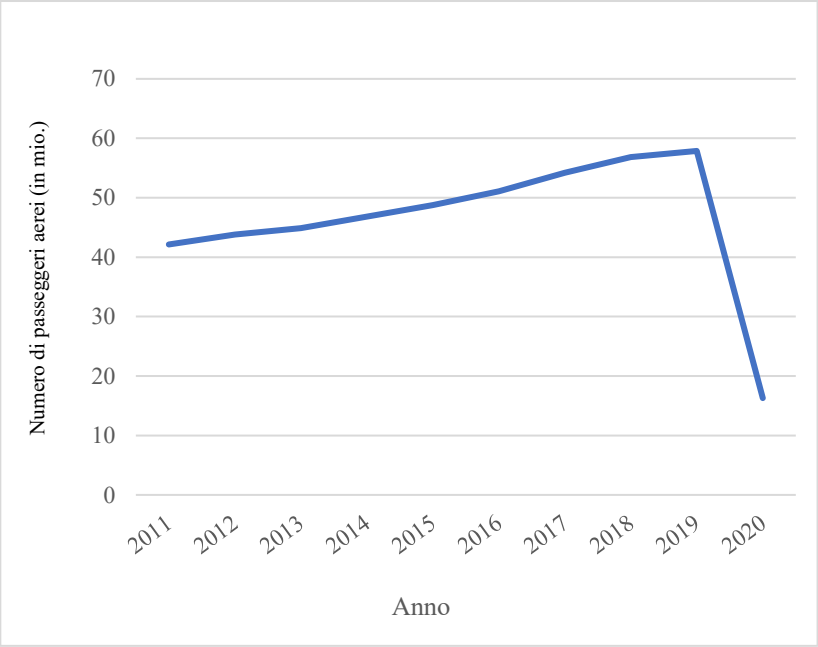
È stata esaminata la possibilità di creare le basi giuridiche necessarie non all'interno di una nuova legge, bensì di leggi federali già vigenti quali la legge federale sulla navigazione aerea (LNA)[11], la legge federale sugli stranieri e la loro integrazione (LStrI)[12] o la legge federale sulle attività informative (LAIn)[13]. Ne sarebbe risultata una base giuridica sconnessa e pertanto caotica, il che non sarebbe né nell'interesse delle imprese di trasporto aereo né in quello dei passeggeri. Questa possibilità è quindi stata scarta.

Una nuova legge che disciplini il trattamento dei dati dei passeggeri aerei offre per contro la massima trasparenza e coerenza. Tale scelta appare giustificata anche per quanto riguarda i dettagli da definire. Infatti, oltre alla trasmissione dei dati dei passeggeri da parte delle imprese di trasporto aereo e all'applicazione di sanzioni in caso di violazione di tale obbligo, occorre disciplinare anche l'organizzazione e i compiti dell'unità d'informazione sui passeggeri (UIP) di cui è prevista la creazione. I compiti dell'UIP consistono nel trattare i dati dei passeggeri e nel comunicarli alle competenti autorità in Svizzera e all'estero. A tal fine l'UIP ha accesso ai diversi sistemi di informazione della Confederazione.

Dal presente progetto discendono in parte nuovi obblighi per le imprese di trasporto aereo operanti in Svizzera. Nel 2019 tali obblighi avrebbero potuto riguardare fino a 217 e nel 2020 fino a 198 imprese di trasporto aereo che offrono voli charter e di linea. Nell'anno precedente alla pandemia queste imprese hanno trasportato circa 60 milioni di passeggeri dalla Svizzera all'estero e viceversa.

11 RS **748.0**
12 RS **142.20**
13 RS **121**

Grafico: numero di passeggeri aerei partiti dalla Svizzera o giunti in Svizzera a bordo di voli charter o di linea (fonte: UFAC).



Una legge sui dati dei passeggeri aerei che comprenda tutte le disposizioni rilevanti concernenti il PNR permette di rendere il quadro giuridico chiaramente riconoscibile per le imprese di trasporto aereo interessate.

Anche sul piano della protezione dei dati va considerato positivamente il fatto di disporre di un'unica legge federale. I passeggeri aerei devono infatti poter facilmente riconoscere perché e a quali condizioni i loro dati sono trattati dallo Stato e sapere di quali diritti godono in qualità di passeggeri.

Utilizzo di dati PNR in materia di salute pubblica

fedpol ha esaminato anche la possibilità di utilizzare i dati dei passeggeri aerei per ragioni di protezione della salute pubblica. D'intesa con l'Ufficio federale della sanità pubblica (UFSP) è stato deciso di rinunciare a questa possibilità. I dati relativi agli spostamenti e al soggiorno per ragioni di salute vanno rilevati all'occorrenza direttamente presso il singolo passeggero.

Revisione della direttiva API

I dati API rappresentano una parte dei dati PNR e vengono trattati anch'essi a livello globale.

In Svizzera l'obbligo di comunicazione dei dati API da parte delle imprese di trasporto aereo è disciplinato dall'articolo 104 LStrI. Tale obbligo si limita attualmente ai voli in arrivo in Svizzera giudicati a rischio.

L'UE sta sottoponendo a revisione la direttiva API. La revisione sarà presumibilmente conclusa nel corso del 2022.

Tale revisione dovrebbe comportare per la Svizzera una sostituzione dell'attuale sistema API (art. 104*a* LStrI) e probabilmente anche un adeguamento di altre disposizioni pertinenti della LStrI.

Sulla base dei parallelismi presenti nei dati API e PNR, è stato esaminato se e in quale misura la revisione della direttiva API debba essere considerata nel presente progetto legislativo.

Un valido motivo che depone a sfavore di un'inclusione della direttiva API nel progetto è rappresentato dal diverso scopo del trattamento dei dati. Infatti, a differenza dei dati PNR che possono essere trattati soltanto ai fini della prevenzione e dell'accertamento di reati di terrorismo o di altri reati gravi, i dati API possono essere utilizzati per migliorare il controllo alla frontiera e lottare contro l'immigrazione illegale nonché, a determinate condizioni, anche per scopi di perseguimento penale. Lo scopo del loro trattamento risulta pertanto notevolmente più ampio rispetto a quello previsto per i dati PNR.

I differenti scopi di trattamento determinano anche diverse autorizzazioni di accesso e diversi termini entro i quali i dati possono essere trattati.

Il contenuto della revisione della direttiva API al momento non è ancora stato stabilito in modo definitivo. Non è neanche chiara la data in cui dovrebbe entrare in vigore. Per tale regione, l'avamprogetto di legge sui dati dei passeggeri aerei non terrà conto della revisione della direttiva API. Le pertinenti disposizioni della LStrI inerenti all'obbligo di raccolta e di comunicazione dei dati API andranno pertanto adeguate al momento opportuno.

1.3 Rapporto con il programma di legislatura e il piano finanziario, nonché con le strategie del Consiglio federale

Il messaggio concernente un sistema d'informazione nazionale PNR e il relativo credito d'impegno sono annunciati nel Programma di legislatura 2019–2023, sotto forma di altri oggetti di attuazione dell'obiettivo 14 «La Svizzera previene la violenza, la criminalità e il terrorismo e li combatte efficacemente»[14].

Il PNR contribuisce inoltre anche all'attuazione dell'obiettivo 12 «La Svizzera ha relazioni regolamentate con l'UE» come pure dell'obiettivo 15 «La Svizzera è al corrente delle minacce alla propria sicurezza e dispone degli strumenti necessari per fronteggiarle in modo efficace».

La legge sui dati dei passeggeri aerei fornisce la base giuridica necessaria ai fini della creazione di un servizio nazionale presso fedpol (unità d'informazione sui passeggeri, UIP) che si occupi del trattamento dei dati dei passeggeri aerei per combattere il

14 Messaggio del 29 gennaio 2020 sul programma di legislatura 2019–2023, FF **2020** 1565

terrorismo e altre forme gravi di criminalità. A tal fine l'UIP gestisce un sistema di informazione PNR.

I mezzi finanziari per la creazione del sistema di informazione PNR sono iscritti nella pianificazione finanziaria della Confederazione[15].

Nella Strategia della Svizzera del 18 settembre 2015[16] per la lotta al terrorismo, il Consiglio federale aveva già indicato l'uso del PNR quale misura possibile per impedire ingressi, partenze e transiti indesiderati di persone sospettate di terrorismo.

2 Diritto comparato, in particolare rapporto con il diritto europeo

UE

Diversi Stati membri dell'UE hanno iniziato a trattare dati PNR in virtù della loro legislazione nazionale già prima del 2016. Il 27 aprile 2016 il Parlamento europeo e il Consiglio hanno adottato la direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine, e azione penale nei confronti dei reati di terrorismo e dei reati gravi (direttiva PNR). La direttiva, entrata in vigore il 24 maggio 2016, ha come scopo di armonizzare le disposizioni legislative degli Stati membri, di evitare l'incertezza giuridica e le lacune in materia di sicurezza e di salvaguardare la protezione dei dati. La Danimarca è l'unico Stato membro non vincolato a tale direttiva[17]. Tuttavia, nel frattempo ha sviluppato ugualmente un ampio sistema PNR sulla base della propria legislazione nazionale e ha aderito allo scambio d'informazioni PNR tra gli Stati membri dell'UE.

La direttiva disciplina oltre alle competenze delle cosiddette unità d'informazione sui passeggeri che sono responsabili per la gestione operativa all'interno dei singoli Stati membri (art. 4), anche il trattamento dei dati (in particolare art. 6) nonché gli obblighi dei vettori aerei riguardanti i trasferimenti di dati (art. 8). I dati sono anonimizzati[18] trascorsi sei mesi dalla loro registrazione e cancellati dopo cinque anni (art. 12). L'articolo 13 concerne la protezione dei dati personali e contiene importanti garanzie per la protezione dei diritti fondamentali.

La Commissione europea ha riesaminato tutti gli elementi della direttiva conformemente all'articolo 19 e ne ha illustrato i risultati in una relazione del 24 luglio 2020[19] al Parlamento europeo e al Consiglio. La Commissione ritiene che non sia necessario apportare modifiche concrete. Tuttavia dinanzi alla Corte di giustizia dell'Unione europea (CGUE) sono pendenti due cause, una avviata in Germania e una in Belgio, concernenti questioni di protezione dei dati e di

15 Preventivo 2022 con piano integrato dei compiti e delle finanze 2023 – 2025, volume 2A, pag. 221
16 FF **2015** 6148
17 Direttiva PNR, consid. 40
18 Per la definizione v. glossario in allegato.
19 Relazione della Commissione al Parlamento europeo e al Consiglio sul riesame della direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, COM/2020/305 final

proporzionalità della direttiva PNR[20]. Nella propria relazione, la Commissione europea non esclude che le sentenze della CGUE possano portare a una modifica della direttiva PNR. Ritiene comunque che il sistema PNR risulti uno strumento efficace nella lotta al terrorismo e alle forme gravi di criminalità. Senza l'uso dei dati PNR, non sarebbe stato possibile procedere a indagini approfondite o ad arresti. Infine, le rigorose prescrizioni in materia di protezione dei dati fanno sì che soltanto un numero esiguo di dati personali venga trasmesso alle competenti autorità.

Gli Stati membri dell'UE hanno confermato che la durata di conservazione prevista dalla direttiva PNR è necessaria sul piano operativo. Sostengono inoltre che le norme relative all'accesso da parte delle autorità ai dati conservati dalla UIP e all'anonimizzazione dei dati si siano dimostrate sufficienti a prevenire abusi, ma anche che il miglioramento della qualità dei dati rappresenti una sfida.

Nella comunicazione del 21 settembre 2010[21] sull'approccio globale al trasferimento dei dati del codice di prenotazione (PNR) verso paesi terzi, la Commissione europea ha stabilito criteri di cui occorrerà tener conto nell'iter decisionale relativo a futuri accordi con Paesi terzi. L'UE dovrà quindi cooperare solo con i Paesi terzi in grado di garantire un livello di protezione adeguato dei dati PNR provenienti dall'UE. Vanno anche considerate nel loro insieme le relazioni esterne tra l'UE e il Paese terzo, tenendo conto in particolare di fattori quali il funzionamento delle autorità di polizia e giudiziarie e la collaborazione con queste ultime, lo Stato di diritto e il rispetto generale dei diritti fondamentali. Nella strategia dell'UE per l'Unione della sicurezza[22] per il periodo 2020-2025 è prevista, come azione a medio termine, una revisione dell'attuale approccio relativo al trasferimento di dati PNR verso Paesi terzi.

L'UE ha finora concluso accordi sull'utilizzo dei dati PNR con gli USA[23] e l'Australia[24].

Un accordo negoziato con il Canada, siglato il 6 maggio 2013, che avrebbe dovuto sostituire quello del 2006, ha dovuto essere rinegoziato dopo che la CGUE, nel suo parere del 26 luglio 2017[25], è giunta alla conclusione che tale accordo è in contrasto con la Carta dei diritti fondamentali dell'Unione europea[26].

20 Causa C-817/19, Ligue des droits humains v Conseil des ministres; causa C-148/20, 149/20, 150/20, AC/DF/BD v Deutsche Lufthansa AG.

21 Comunicazione della Commissione del 21 settembre 2010 sull'approccio globale al trasferimento dei dati del codice di prenotazione (PNR) verso paesi terzi, COM/2010/492 final

22 Comunicazione della Commissione del 24 luglio 2020 al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni sulla strategia dell'UE per l'Unione della sicurezza, COM/2020/605 final, pag. 26

23 Accordo tra gli Stati Uniti d'America e l'Unione europea sull'uso e il trasferimento delle registrazioni dei nominativi dei passeggeri al dipartimento degli Stati Uniti per la sicurezza interna, GU L 215 del 11.8.2012, pag. 5

24 Accordo tra l'Unione europea e l'Australia sul trattamento e sul trasferimento dei dati del codice di prenotazione (Passenger Name Record — PNR) da parte dei vettori aerei all'Agenzia australiana delle dogane e della protezione di frontiera, GU L 186 del 14.7.2012, pag. 4

25 Parere 1/15 della Corte (Grande Sezione) del 26 luglio 2017, ECLI:EU:C:2017:592

26 Carta dei diritti fondamentali dell'Unione europea, GU C 202 del 7.6.2016, pag. 389

Nel febbraio 2020 la Commissione europea è stata incaricata di avviare i negoziati con il Giappone. Nello stesso anno ha dimostrato alla Svizzera il suo interesse a concludere un accordo bilaterale concernente il PNR. Nel 2021 sono state avviati i colloqui esplorativi.

Regno Unito

Il Regno Unito è stato il primo Stato membro dell'UE a disporre di un sistema PNR funzionante. Tratta i dati PNR sin dal 2004.

Nel quadro dei negoziati sulla Brexit, il Regno Unito ha concordato con l'UE di proseguire lo scambio di dati PNR. Si è impegnato inoltre a rendere accessibili all'Ufficio europeo di polizia (Europol) e all'Unità di cooperazione giudiziaria dell'Unione europea (Eurojust) nonché alle autorità di contrasto degli Stati membri dell'UE le analisi allestite su loro richiesta[27].

USA

Come conseguenza degli attacchi terroristici dell'11 settembre 2001 gli Stati Uniti avevano imposto per mezzo dell'«Aviation and Transportation Security Act»[28] alle compagnie aeree di concedere alle autorità statunitensi l'accesso ai dati PNR di tutti i voli che atterrano, partono o transitano nel territorio degli USA. Da allora, il Governo statunitense mira alla raccolta, al trattamento e alla registrazione di dati PNR. Il primo accordo con la Svizzera concernente la trasmissione di dati PNR è entrato in vigore il 29 marzo 2005, ma aveva una validità limitata di tre anni e mezzo. L'accordo PNR del 23 dicembre 2008[29] adottato dal Consiglio federale ha per contro una validità illimitata.

I dati PNR sono trattati conformemente alle prescrizioni in materia di protezione dei dati applicabili al sistema di registrazione (System of Records Notice, SORN) per il monitoraggio automatizzato (Automated Targeting System, ATS), gestito dal Dipartimento della Sicurezza interna degli Stati Uniti (US Department of Homeland Security, DHS), Ufficio delle dogane e della protezione delle frontiere (US Customs and Border Protection). L'ATS SORN sancisce che il Governo USA è tenuto a garantire ai dati PNR rilevati nei voli tra gli Stati Uniti e la Svizzera sostanzialmente la stessa protezione concessa dall'accordo del 2007 tra gli Stati Uniti e l'UE sul trattamento dei dati PNR. Dall'11 agosto 2012 un accordo riveduto tra gli USA e

27 Accordo sugli scambi commerciali e la cooperazione tra l'Unione europea e la Comunità europea dell'energia atomica, da una parte, e il Regno Unito di Gran Bretagna e Irlanda del Nord, dall'altra, GU L 149 del 30.4.2021, pag. 10, art. 542–562.

28 Public Law 107–71, 19 novembre 2001, 115 STAT. 597, online: https://www.gpo.gov/fdsys/pkg/PLAW107publ71/pdf/ PLAW107publ71.pdf (28.08.2018)

29 RS **0.748.710.933.6**

l'UE[30] disciplina l'utilizzo e il trasferimento di dati PNR. Nel gennaio 2021 è stata adottata una valutazione dell'accordo[31].

Data l'assenza di una base legale nel suo diritto interno, la Svizzera non riceve alcun dato PNR per i voli operati dagli USA verso la Svizzera.

Canada

Dal 2009 i dati PNR e API di voli operati dalla Svizzera verso il Canada sono trasmessi alle autorità competenti canadesi. La pertinente base legale è costituita dal Memorandum of Understanding Between the Canada Border Services Agency and the Swiss Federal Office for Civil Aviation Concerning Advance Passenger Information/Passenger Name Record del 17 marzo 2006[32]. I dati PNR possono essere utilizzati unicamente per l'identificazione di persone per le quali sussiste il pericolo che:

- importino merci in relazione al terrorismo o a reati terroristici,
- commettano altri reati gravi di natura transnazionale (compresa la criminalità organizzata), o
- abbiano un possibile legame con tali reati.

Le autorità canadesi conservano i dati PNR durante 42 mesi, sempreché la persona non sia oggetto di un procedimento. Trascorsi 24 mesi, i dati vengono pseudonimizzati.

La comunicazione di dati PNR da parte del Canada Border Services Agency a un'altra autorità canadese è ammessa unicamente in singoli casi e soltanto dopo aver valutato la rilevanza delle informazioni PNR specifiche da divulgare. Sono messi a disposizione soltanto gli elementi PNR che sono palesemente necessari date le circostanze. In tutti i casi occorre sempre fornire la quantità minore possibile di informazioni. La trasmissione di dati PNR da parte delle autorità canadesi a uno Stato terzo è ammessa laddove un trattato internazionale lo preveda.

Data l'assenza di una base legale nel suo diritto interno, la Svizzera non riceve alcun dato PNR per i voli operati dal Canada verso la Svizzera.

3 Punti essenziali del progetto

La LDPA proposta intende permettere alla Svizzera di utilizzare in futuro il PNR quale strumento consolidato per la lotta al terrorismo e ai reati gravi. Si tratta infatti di uno strumento che è già in uso da circa 20 anni in particolare negli USA, in Canada e nel Regno Unito e da diversi anni anche negli Stati membri dell'UE.

30 Accordo tra gli Stati Uniti d'America e l'Unione europea sull'uso e il trasferimento delle registrazioni dei nominativi dei passeggeri al dipartimento degli Stati Uniti per la sicurezza interna, GU L 215 dell'11.8.2012, pag. 5.

31 Relazione della Commissione al Parlamento europeo e al Consiglio sulla valutazione congiunta dell'accordo tra gli Stati Uniti d'America e l'Unione europea sull'uso e il trasferimento delle registrazioni dei nominativi dei passeggeri al dipartimento degli Stati Uniti per la sicurezza interna, COM/2021/18 final

32 Consultabile all'indirizzo: https://www.newsd.admin.ch/newsd/message/attachments/2242.pdf

L'UE è il principale partner in materia di sicurezza della Svizzera e, di conseguenza, rappresenterà in futuro anche il principale partner nello scambio di dati PNR. È per tale ragione che l'avamprogetto della LDPA si ispira alla direttiva PNR dell'UE.

Con la LDPA la Svizzera intende soddisfare i propri obblighi internazionali. Particolarmente vincolanti sono le tre risoluzioni del Consiglio di sicurezza dell'ONU[33] che impongono agli Stati membri di rafforzare le proprie capacità di raccolta, trattamento e analisi di dati PNR. Inoltre, su mandato del Consiglio di sicurezza dell'ONU, l'Organizzazione internazionale dell'aviazione civile (OACI) ha sviluppato, in collaborazione con l'Organizzazione mondiale delle dogane (OMD), i governi degli Stati membri, le imprese di trasporto aereo e i fornitori di servizi, standard per la trasmissione dei dati dei passeggeri aerei. I cosiddetti PNR Reporting Standard sono vincolanti per tutti gli Stati membri dell'OACI e quindi anche per la Svizzera. Gli USA, infine, assoggettano la permanenza della Svizzera nel Visa Waiver Program al trattamento dei dati dei passeggeri aerei (cfr. sopra n. **Fehler! Verweisquelle konnte nicht gefunden werden.**).

3.1 La normativa proposta

La LDPA costituisce il requisito giuridico affinché anche la Svizzera possa trattare dati dei passeggeri aerei e gestire un sistema di informazione ad hoc.

I dati dei passeggeri aerei vengono raccolti al momento della prenotazione dei biglietti aerei, a prescindere dall'utilizzo che ne farà lo Stato ai fini della lotta alle forme gravi di criminalità. Tali dati non devono pertanto essere raccolti specificamente per gli scopi della presente legge.

Complessivamente, le imprese di trasporto aereo devono trasmettere 19 diverse categorie di dati (all. 1 LDPA).

Questo trattamento dei dati da parte dello Stato riguarda tutti i passeggeri sui voli charter e di linea da e verso la Svizzera.

Prima della partenza di un volo da o verso la Svizzera le imprese di trasporto aereo sono tenute a trasmettere i dati all'UIP, collocata in seno a fedpol, in due fasi distinte definite dalla legge (art. 2). Ciò consente alle competenti autorità federali e cantonali di adottare tempestivamente le misure appropriate nei confronti di persone sospette al loro arrivo o alla loro partenza dal Paese.

Le imprese di trasporto aereo devono garantire la trasmissione puntuale dei dati e il rispetto delle prescrizioni tecniche (art. 4). Devono inoltre informare i passeggeri aerei per iscritto in merito al trattamento dei loro dati da parte dello Stato (art. 5).

Se un'impresa di trasporto aereo viola in parte o in toto tali obblighi è soggetta alle sanzioni di cui agli articoli 23–25. Non vi è violazione dell'obbligo se l'impresa di trasporto aereo dimostra che ha adottato tutte le misure tecniche e organizzative ragionevolmente esigibili per adempiere i propri obblighi.

Gli articoli 6–12 disciplinano il trattamento dei dati.

33 Risoluzione 2178 (2014) adottata dal Consiglio di sicurezza nella 7272ª sessione del 24 settembre 2014, risoluzione 2396 (2017) adottata dal Consiglio di sicurezza nella 8148ª sessione del 21 dicembre 2017, risoluzione 2482 (2019) adottata dal Consiglio di sicurezza nella 8582ª sessione del 19 luglio 2019.

I dati dei passeggeri aerei possono essere trattati soltanto a fini di prevenzione, accertamento, indagine e perseguimento dei reati terroristici e di altri reati gravi. I pertinenti reati sono riportati nell'allegato al presente rapporto. I risultati di un trattamento che non sono conformi a tale scopo sono cancellati immediatamente (art. 6).

La competenza per il trattamento dei dati incombe all'UIP, il nuovo servizio che sarà collocato in seno a fedpol.

I dati trasmessi dalle imprese di trasporto aereo, in una prima fase, sono confrontati automaticamente con diversi sistemi di informazione di polizia della Confederazione. Tale confronto consente, da un lato, di identificare, arrestare e/o eventualmente estradare le persone ricercate a livello nazionale e internazionale e, dall'altro, di completare le informazioni relative a reati pianificati o non chiariti. In una seconda fase, tali dati sono verificati manualmente e, se del caso, accedendo a ulteriori sistemi di informazione di polizia o della Confederazione quali SIMIC, ORBIS o il sistema di informazione dell'Ufficio federale della dogana e della sicurezza dei confini (UDSC) (art. 7).

Se la verifica produce un riscontro positivo, la corrispondenza è trasmessa al servizio responsabile della segnalazione da cui è scaturita la corrispondenza, ossia le autorità di perseguimento penale della Confederazione e dei Cantoni o il Servizio delle attività informative della Confederazione (SIC) (art. 8). Il servizio responsabile della segnalazione in seguito deciderà in merito alle eventuali misure da adottare.

I dati dei passeggeri aerei possono essere confrontati anche con i profili di rischio e le liste d'osservazione che sono elaborati dall'UIP sulla base di proprie analisi o su richiesta delle autorità di perseguimento penale o del SIC. I profili di rischio descrivono combinazioni di dati che forniscono indizi di attività criminali correlate al terrorismo o a forme gravi di criminalità. Nelle liste d'osservazione sono contenuti elementi dei dati PNR o relativi a persone (p. es. indirizzi di posta elettronica, numeri di telefono) di cui occorre seguire il monitoraggio nel quadro di reati terroristici o altri reati gravi. Grazie al confronto con i dati PNR, questi due strumenti aiutano le autorità di perseguimento penale a individuare persone ancora sconosciute alla polizia, a identificare membri di organizzazioni criminali o a riconoscere potenziali vittime della tratta di esseri umani. Le liste d'osservazione possono essere utilizzate soltanto per alcune fattispecie penali definite dal Consiglio federale all'interno di un'ordinanza, in particolare in relazione a reati terroristici o a reati collegati alla criminalità organizzata (art. 9).

La LDPA tiene già conto della nuova LPD, la cui entrata in vigore è prevista per settembre 2023. Quest'ultima prende atto della rapida evoluzione tecnologica e mira a un'ampia armonizzazione con il diritto UE in materia di protezione dei dati.

Nel complesso, i dati dei passeggeri aerei sono trattati unicamente in occasione del confronto con i sistemi di informazione di polizia, con i profili di rischio e le liste d'osservazione (cfr. commento all'art. 9). Successivamente solo una minima parte di essi è oggetto di un ulteriore trattamento. Nello specifico, sono interessati i dati dal cui confronto è scaturita una corrispondenza e per i quali sussiste pertanto un certo sospetto. Soltanto nella fase successiva del trattamento sarà possibile verificare se tale sospetto è giustificato. Infatti, prima di sottoporre le corrispondenze a ulteriore

trattamento occorre accertare la loro plausibilità. Si tratta quindi di dati per i quali è stato avvalorato un sospetto legame con il terrorismo o con forme gravi di criminalità.

Per contro, la stragrande maggioranza dei dati dei passeggeri aerei non sarà più trattata in seguito al confronto e sarà pseudonimizzata trascorsi sei mesi dalla loro ricezione (art. 14). Quest'ultima procedura consiste nel fornire uno pseudonimo a dati personali quali nome, numero di telefono, indirizzo di posta elettronica o numero di carta di credito in modo da non poterli più attribuire a una persona. Diversamente dall'anonimizzazione, la pseudonimizzazione può essere revocata. Al Tribunale amministrativo federale (TAF) spetta decidere se sussistono le circostanze che giustificano una tale misura (art. 15).

I dati dei passeggeri aerei sono cancellati cinque anni dopo la loro introduzione nel sistema di informazione PNR (art. 16). Si tratta di una durata di conservazione fondamentale sul piano operativo, dato che le indagini sui reati che si intendono contrastare con i dati PNR si protraggono spesso per diversi mesi o persino diversi anni[34].

La protezione dei dati è attuata anche sul piano tecnico, come prescritto dall'articolo 7 nLPD. L'accesso al sistema di informazione PNR è ad esempio limitato a un numero ristretto di persone (art. 13 cpv. 2). È esclusa in particolare la possibilità di accesso diretto da parte delle autorità di perseguimento penale della Confederazione e dei Cantoni. Questa delimitazione è giustificata dalla scelta di distinguere l'UIP sul piano organizzativo dalle unità inquirenti (art. 19). L'automatismo previsto per la pseudonimizzazione e la cancellazione dei dati dei passeggeri aerei si iscrive ugualmente nel contesto della protezione tecnica dei dati.

L'UIP, che tratta i dati conformemente alla LDPA, deve essere collocata in seno a fedpol (art. 19) ed essere composta, in parti uguali, di collaboratori della Confederazione e dei Cantoni (art. 20).

3.2 Compatibilità tra i compiti e le finanze

I danni che la (grave) criminalità arreca alle persone coinvolte e all'economia sono ingenti. Il chiarimento di tali reati e la condanna dei loro autori sono due elementi cardine che vanno di pari passo con la giustizia in uno Stato di diritto. Per le vittime, sono spesso la condizione per un nuovo inizio.

La prevenzione di tale reati risulta ancora più importante. La sicurezza è un bene determinante per il bene e il benessere di una società.

Il PNR fornisce un contributo fondamentale in tal senso.

Infatti, non solo consente di perseguire i criminali di alto profilo e di alleviare in modo mirato gli oneri per le autorità di perseguimento penale, ma contribuisce anche in modo decisivo a individuare tempestivamente la pianificazione di reati gravi e a impedire che questi ultimi vengano commessi.

34 Relazione della Commissione al Parlamento europeo e al Consiglio sulla valutazione congiunta dell'accordo tra gli Stati Uniti d'America e l'Unione europea sull'uso e il trasferimento delle registrazioni dei nominativi dei passeggeri al dipartimento degli Stati Uniti per la sicurezza interna, COM/2021/18 final, pag. 9.

- Attualmente le autorità di perseguimento penale devono chiedere alle singole imprese di trasporto aereo in modo mirato gli itinerari dei criminali di alto profilo nel traffico aereo internazionale, con un conseguente notevole dispendio di tempo. Importanti legami tra esponenti della criminalità organizzata restano pertanto spesso nascosti. Il PNR consente alle autorità di perseguimento penale di ricorrere a pacchetti di dati compatti, i cosiddetti set di dati PNR, che sono raccolti sistematicamente e registrati in modo centralizzato. Questo set di dati, oltre a evidenziare gli itinerari di viaggio, contiene indicazioni sui viaggiatori e le persone che viaggiano insieme a loro, come pure sulla frequenza e la destinazione dei viaggi. Il PNR rappresenta pertanto per le autorità di perseguimento penale uno strumento fondamentale per ottenere con maggiore facilità e rapidità le informazioni importanti relative a persone indiziate, alle loro abitudini di viaggio e ai loro legami.
- La criminalità segue sovente determinati schemi comportamentali che possono essere individuati con maggiore facilità grazie al PNR. Ciò permette pertanto di individuare tempestivamente e prevenire reati pianificati.

Il PNR si serve di dati raccolti al momento della prenotazione dei voli. Gli oneri per le imprese di trasporto aereo si limitano alla trasmissione di questi dati al servizio statale competente. Il PNR non comporta pertanto per queste imprese notevoli oneri supplementari, ragion per cui può essere considerato uno strumento efficiente. Inoltre, può essere anche ritenuto uno strumento efficace, come spiega il fatto che viene impiegato da ormai circa 20 anni e in oltre 60 Paesi, tra cui USA, Canada, Australia, Regno Unito e Stati membri dell'UE, per combattere i reati terroristici e altri reati gravi.

L'introduzione del PNR in Svizzera dovrebbe comportare spese ricorrenti limitate principalmente al trattamento dei dati trasmessi dalle imprese di trasporto aereo. I risultati del trattamento dei dati saranno a disposizione innanzitutto delle autorità di perseguimento penale della Confederazione e dei Cantoni, agevolandone i compiti.

È previsto che i Cantoni si facciano carico dei costi per la metà dell'organico, vale a dire dei collaboratori da loro distaccati presso l'UIP. Questa ripartizione dei costi rispecchia il fatto che la sicurezza del Paese e la protezione della popolazione sono un compito congiunto della Confederazione e dei Cantoni. Poiché il PNR è un progetto che va oltre i confini cantonali, ma anche del Paese, è opportuno che la Confederazione si faccia carico dei rimanenti costi, ad esempio di quelli legati alla creazione del necessario sistema di informazione.

3.3 Attuazione

In aggiunta ai dati PNR che le saranno forniti in futuro in caso di adozione della LDPA, la Confederazione, ed eventualmente la Segreteria di Stato della migrazione (SEM), riceve già oggi dalle imprese di trasporto aereo i dati API di determinati voli giudicati a rischio provenienti da Stati terzi e diretti in Svizzera. Dal 2015 tali dati sono trattati in modo automatizzato in virtù degli articoli 104*a* e 104*b* LStrI.

Conformemente agli standard tecnici internazionali dell'OACI, dell'OMD e dell'Associazione del trasporto aereo internazionale (IATA), occorre prevedere una

cosiddetta «single window», ovvero un'unica interfaccia per la trasmissione di dati PNR e API. Ciò dovrebbe permettere di sgravare le imprese di trasporto aereo da inutili oneri.

In occasione della realizzazione del sistema PNR svizzero occorrerà pertanto definire a livello tecnico una «single window», per i dati API e PNR. Di conseguenza, le imprese di trasporto aereo potranno fornire i dati a un'unica interfaccia che li smisterà, a sua volta, automaticamente all'UIP o alla SEM.

4 Commento ai singoli articoli

1. Legge federale sul trattamento dei dati dei passeggeri aerei per la lotta ai reati terroristici e ad altri reati gravi

Sezione 1: Oggetto

Art. 1 Oggetto

La presente disposizione illustra i contenuti più importanti della legge che, oltre al trattamento e all'analisi dei dati dei passeggeri aerei, disciplina anche gli obblighi delle imprese di trasporto aereo. Questi obblighi non costituiscono tuttavia una novità assoluta; le imprese di trasporto aereo sono tenute infatti ad adempierli da anni nei confronti di Stati Uniti e Canada e, dal 2018, anche nei confronti degli Stati membri dell'UE. La novità è rappresentata dal fatto che tali obblighi vigono ora anche nei confronti della Svizzera.

Le categorie di *dati dei passeggeri aerei* da trattare sono elencate nell'allegato 1 della LDPA. Queste 19 categorie di dati corrispondono a quelle indicate nella direttiva PNR dell'UE. I dati si riferiscono solo ai passeggeri aerei, e non ai membri dell'equipaggio. Inoltre comprendono anche i dati personali ai sensi dell'articolo 5 lettera a nLPD. La LDPA costituisce la base legale per il trattamento di tali dati.

Il trattamento deve essere ammesso soltanto ai fini del contrasto di reati di particolare gravità che rappresentano un pericolo serio per la sicurezza pubblica. L'articolo 6 capoversi 2 e 3 stabilisce di quali fattispecie concrete del Codice penale e del diritto penale accessorio si tratta.

L'articolo 6 capoverso 3 nLPD impone che la persona in questione debba essere informata circa la finalità del trattamento o che il trattamento debba essere previsto dalla legge[35]. Ne deriva che le imprese di trasporto aereo sono tenute a informare i passeggeri che i loro dati sono trattati conformemente alla presente legge al fine di combattere efficacemente il terrorismo e altri reati gravi (cfr. art. 5).

Nel diritto vigente non è prevista alcuna definizione di *impresa di trasporto aereo*, ragion per cui tale nozione viene precisata nell'articolo 1 lettera b. La definizione si basa su quella elaborata nel quadro della legge del 25 settembre 2020 sul CO_2 (art. 2

35 Messaggio del 15 settembre 2017 concernente la legge federale relativa alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati, FF **2017** 5939, in particolare 6016

lett. i)[36]. Questa definizione è necessaria per la LDPA, visto soprattutto che le imprese di trasporto aereo sono ora tenute e a comunicare puntualmente i dati dei passeggeri aerei (art. 4). Inoltre devono informare i loro passeggeri riguardo al trattamento dei loro dati in virtù della presente legge (art. 5). Le violazioni dei diritti sono punite dall'articolo 23.

Non sono considerate imprese di trasporto aereo quelle che rientrano nella cosiddetta aviazione leggera, ad esempio i voli d'istruzione, le esercitazioni di volo, i voli di controllo, i voli a scopo turistico, l'aviazione sportiva come pure i voli privati.

Sezione 2: Obblighi delle imprese di trasporto aereo

Art. 2 Trasmissione dei dati dei passeggeri aerei all'UIP

Le imprese di trasporto aereo sono tenute a trasmettere all'UIP i dati dei passeggeri aerei menzionati all'allegato 1 del presente avamprogetto per tutti i voli da o verso la Svizzera (cpv. 1). Anche i voli ricadenti sotto la giurisdizione svizzera che atterrano all'Euroairport Basel-Mulhouse-Freiburg (con il codice aeroportuale IATA «BSL») sono considerati come voli verso la Svizzera, anche se l'aeroporto si trova al di fuori del territorio svizzero. Lo stesso vale per i voli in partenza dallo stesso aeroporto verso l'estero.

I dati dei passeggeri aerei vanno trasmessi all'UIP in due diversi momenti, ossia non prima di 48 ore e non oltre 24 ore dall'orario previsto di partenza nonché immediatamente dopo la chiusura dell'imbarco (cpv. 2). La prima trasmissione dei dati, per quanto fornisca solo dati provvisori, permette all'UIP di disporre di un determinato margine di tempo fino all'arrivo del volo, con evidenti vantaggi soprattutto in caso di brevi voli. La seconda trasmissione consente invece di comunicare in modo definitivo i dati di tutti i passeggeri presenti a bordo.

Le imprese di trasporto aereo non possono trasmettere all'UIP dati personali degni di particolare protezione[37] ai sensi dell'articolo 5 nLPD. Qualora tali dati dovessero essere comunque erroneamente trasmessi, l'UIP, una volta individuato l'errore, dovrà provvedere immediatamente a cancellarli (cpv. 3).

La trasmissione dei dati può avvenire secondo il metodo PULL o il metodo PUSH. Il metodo PULL prevede che l'UIP acceda al sistema di prenotazione delle compagnie aeree, mentre nel caso del metodo PUSH sono le imprese di trasporto aereo a procedere alla trasmissione. Il metodo PUSH è quello che offre un livello più elevato di protezione e deve pertanto trovare applicazione nella realizzazione del sistema PNR in Svizzera. Ciò viene concretizzato con la nozione di trasmissione dei dati. Le modalità di trasmissione sono rette dai pertinenti standard dell'OACI. I «PNR Reporting Standards» sono stati sviluppati dall'OACI su incarico del Consiglio di sicurezza dell'ONU e in collaborazione con l'OMD, con i governi degli Stati membri, le compagnie aeree e i fornitori di servizi. Le norme sono vincolanti per tutti gli Stati membri dell'OACI, e pertanto anche per la Svizzera. Non è pertanto necessaria

36 https://www.bafu.admin.ch/dam/bafu/de/dokumente/klima/rechtliche-grundlagen/definition-luftverkehrsunternehmen.pdf.download.pdf (disponibile soltanto in tedesco e in francese)

37 Per la definizione v. glossario in allegato.

un'ulteriore regolamentazione a livello di legge. Il costante sviluppo tecnologico rende tuttavia indispensabile poter precisare le modalità tecniche ove necessario. Il capoverso 4 autorizza pertanto fedpol a emanare le pertinenti disposizioni a livello di ordinanza (cpv. 4).

Art. 3 Trasmissione dei dati dei passeggeri aerei alle autorità estere

Le imprese di trasporto aereo trasmettono già oggi i dati dei passeggeri aerei a Stati verso cui sono destinati i voli dalla Svizzera, ad esempio agli USA e al Canada. In entrambi i casi, la base per la trasmissione dei dati è rappresentata da accordi esistenti con la Svizzera. È prevista la conclusione di un accordo anche con l'UE.

Gli accordi garantiscono che i dati trasmessi godano all'estero di una protezione dei dati equiparabile a quella sancita in Svizzera. Inoltre con la conclusione di tali accordi la Svizzera può beneficiare anche della reciprocità nel ricevere i dati dei passeggeri aerei dall'altro Stato contraente.

Art. 4 Obbligo di diligenza

Le imprese di trasporto aereo sono tenute a trasmettere i dati di *tutti* i passeggeri puntualmente (cfr. art. 2 cpv. 2) e conformemente alle prescrizioni tecniche (cfr. art. 2 cpv. 4). Ci si attende dunque che adottino tutte le misure ragionevolmente esigibili per adempiere a tale obbligo. In caso contrario, sono applicabili le sanzioni previste dall'articolo 23.

Nella fase di prenotazione di un biglietto aereo i dati dei passeggeri aerei vengono inseriti perlopiù manualmente dal passeggero stesso o da un collaboratore dell'aeroporto o dell'agenzia di viaggio. Ne consegue che i dati PNR contengono spesso errori. Quanti più sono gli errori che si verificano accidentalmente o persino volontariamente in occasione dell'inserimento dei dati, tanto meno questi ultimi saranno utilizzabili.

Sarebbe in ogni caso sproporzionato imporre alle imprese di trasporto aereo di verificare che tutti i dati dei passeggeri aerei siano corretti. Tuttavia, poiché la qualità dei dati è decisiva per un trattamento efficace ai sensi della presente legge, le imprese di trasporto aereo devono concepire il loro sistema di prenotazione in modo tale che i dati inseriti in modo manifestamente errato (p. es. nome «Aaaaa» o indirizzo di posta elettronica sprovvisto di @) non vengano accettati dal sistema. Tali misure sono considerate ragionevolmente esigibili (cfr. art. 23 cpv. 2 lett. b).

Art. 5 Obbligo di informazione

Le imprese di trasporto aereo devono informare per iscritto i passeggeri aerei che i loro dati, oltre a essere utilizzati in relazione al loro volo, saranno anche trattati ai sensi della LDPA. Un'indicazione in tal senso può essere inserita nelle loro condizioni generali.

L'obbligo di informazione ai sensi dell'articolo 5 è giustificato anche se l'informazione ribadisce quanto già previsto dall'articolo 20 capoverso 1 lettera b nLPD, visto in particolare che i dati dei passeggeri aerei sono trattati

- in due contesti totalmente diversi, uno pratico, l'altro giuridico (gestione tecnica della prenotazione del volo / attuazione della LDPA),
- per diversi scopi (prenotazione del volo / lotta alla criminalità) e
- e sotto una diversa responsabilità (impresa di trasporto aereo / fedpol).

L'informazione oltre a specificare che i dati sono trasmessi all'UIP, deve anche indicare in modo riconoscibile lo scopo del trattamento dei dati (cfr. art. 6 cpv. 3 nLPD). Le ulteriori modalità relative all'obbligo di informare le persone interessate risulteranno dall'ordinanza concernente la nLPD.

Sezione 3: Trattamento dei dati

Art. 6 Principi

Il trattamento dei dati deve essere consentito soltanto se sono implicati reati di particolare gravità che rappresentano un serio pericolo per la sicurezza pubblica. Il capoverso 3 specifica di quali fattispecie concrete del Codice penale e del diritto penale accessorio si tratta.

I *reati terroristici e gli altri reati gravi* sono descritti nei capoversi 2 e 3, senza tuttavia essere menzionati in modo concreto. Vengono suddivisi per l'appunto due tipi di reati: quelli terroristici e gli altri reati gravi.

Per *terroristici* ai sensi della LDPA s'intendono tutti i reati, indipendentemente dalla pena comminata, rientranti tra le fattispecie di cui al numero 22 dell'allegato 1 LSIS. I reati terroristici sono indicati nell'allegato 1 del presente rapporto.

La maggior parte dei reati sono crimini e vengono pertanto puniti con una pena detentiva massima di oltre tre anni (art. 10 cpv. 2 CP). Per contro, le seguenti fattispecie di reato sono considerate delitti ai sensi dell'articolo 10 capoverso 3 CP:

- pubblica intimidazione (art. 258 CP),
- pubblica istigazione a un crimine o alla violenza (art. 259 CP),
- sommossa (art. 260 cpv. 1 CP),
- associazioni illecite (art. 275ter CP).

Tali reati ricadono nella categoria dei reati terroristici soltanto se sono anche di matrice terroristica.

Per *gravi* ai sensi della LDPA s'intendono due categorie di reati, ossia i crimini di cui all'allegato 1 della LSIS, ove siano attribuibili a una delle categorie di reato ai sensi della direttiva PNR dell'UE (cfr. allegato 2 della presente legge), e i reati il cui perseguimento penale compete all'UDSC e per cui è comminata una pena detentiva massima di almeno tre anni.

Sia i reati terroristici sia i reati gravi sono definiti per legge. Nell'allegato 2 le categorie di reato PNR sono raffrontate alle corrispondenti categorie dell'allegato 1 LSIS. In questo modo è possibile stabilire quali crimini riportati nel catalogo dei reati della LSIS vadano considerati reati gravi ai sensi dell'articolo 6 capoverso 3 lettera a. Ciò permette quindi di individuare chiaramente quali reati ai sensi della LSIS rientrino nel catalogo dei reati PNR giustificando il trattamento dei dati dei passeggeri aerei.

Malgrado si fondano su una solida base legale, i reati di cui al capoverso 3 lettera b il cui perseguimento penale compete all'UDSC devono essere indicati all'interno di un'ordinanza. Questa valenza dichiarativa serve alla certezza del diritto e alla trasparenza (cpv. 4). Tale soluzione consente infatti con maggiore facilità di apportare eventuali modifiche al diritto penale accessorio.

Un'attuale panoramica di tutte le fattispecie penali determinanti sono riportate nell'allegato al presente rapporto.

I risultati ottenuti dal trattamento dei dati dei passeggeri aerei che permettono di prevenire, accertare o perseguire reati diversi da quelli menzionati vanno cancellati immediatamente.

Tale obbligo vale anche per il SIC, ugualmente autorizzato a trattare i dati dei passeggeri aerei per combattere i reati terroristici e altri reati gravi, ma soltanto nella misura in cui il trattamento serva anche ad adempiere i propri compiti di cui all'articolo 6 capoverso 1 lettera a numeri 1 nonché 3–5 della legge federale del 25 settembre 2015[38] sulle attività informative.

L'UIP può trattare i dati personali degni di particolare protezione soltanto in maniera limitata. Le imprese di trasporto aereo non sono infatti autorizzate a trasmetterle tali dati (cfr. art. 2 cpv. 3). Qualora dovesse comunque ricevere simili dati, l'UIP è tenuta a cancellarli immediatamente. I dati personali degni di particolare protezione possono tuttavia pervenire laddove i dati dei passeggeri aerei vengano confrontati con i sistemi di informazione o l'UIP acceda a tali sistemi (cfr. art. 7). È inoltre ipotizzabile che tali dati possano entrare in gioco nell'elaborazione dei profili di rischio e delle liste d'osservazione su richiesta di un'autorità. Per tale ragione occorre statuire all'articolo 6 capoverso 5 che l'UIP è autorizzata a trattare esclusivamente i seguenti dati personali degni di particolare protezione:

- i dati biometrici[39] che identificano in modo univoco una persona fisica;
- i dati concernenti procedimenti e sanzioni amministrativi e penali.

Se riceve altri dati personali degni di particolare protezione, l'UIP è tenuta a cancellarli immediatamente. Tale principio si applica a tutti i compiti assolti dall'UIP in virtù della presente legge.

Art. 7 Confronto dei dati con i sistemi di informazione

I dati dei passeggeri aerei sono confrontati automaticamente con diversi sistemi di informazione di polizia non appena giungono nel sistema di informazione PNR (cfr. 1).

La legge non menziona alcuna tecnologia specifica, bensì soltanto lo scopo del confronto. La formulazione tecnologicamente neutra garantisce che i sistemi di informazione in questione possano essere sostituiti senza richiedere una revisione della norma. Oltre a questo vantaggio, contribuisce anche a rafforzare il senso della disposizione e a limitare il confronto allo stretto necessario, rivelandosi dunque convincente anche sul piano della protezione dei dati.

38 RS **121**
39 Per la definizione v. glossario in allegato.

Il confronto automatico serve alla prima identificazione, alla localizzazione ed eventualmente all'arresto di persone che giungono in Svizzera o partono dalla Svizzera per via aerea o che sono ricercate a livello nazionale o internazionale in relazione a reati terroristici o ad altri reati gravi (art. 6 cpv. 2 e 3). Inoltre può anche fornire informazioni utili in relazione a reati non chiariti o pianificati. Le corrispondenze che non rientrano tra gli scopi definiti dalla legge vanno cancellate immediatamente (cfr. art. 6 cpv. 5).

Il confronto automatico di tutti i dati dei passeggeri aerei è effettuato con i seguenti sistemi di informazione di polizia:

- il sistema di ricerca informatizzato di polizia (art. 15 della legge federale del 13 giugno 2008[40] sui sistemi d'informazione di polizia della Confederazione [LSIP]);
- la parte nazionale del Sistema d'informazione Schengen (art. 16 LSIP);
- il sistema di informazione della Polizia giudiziaria federale (art. 10 e 11 LSIP)[41];
- il sistema informatizzato di gestione e indice informatizzato delle persone e dei fascicoli (art. 18 LSIP).

Il *sistema di ricerca informatizzato di persone e oggetti (RIPOL)* contiene informazioni su persone oggetto di segnalazioni di ricerca, informazioni relative a reati non chiariti, a persone coinvolte in un reato, a titolari di documenti di identità di origine sospetta nonché altre informazioni utili a far luce su reati. RIPOL offre sostegno alle autorità competenti della Confederazione e dei Cantoni in particolare quando si tratta di arrestare persone e prevenire pericoli per la sicurezza pubblica. Il confronto dei dati dei passeggeri aerei con RIPOL contribuisce non solo al successo della ricerca, ma anche a ottenere risultati nelle indagini su reati terroristici o altri reati gravi ai sensi del presente avamprogetto che non sono stati ancora chiariti. Chi è autorizzato a effettuare un confronto con RIPOL riceve automaticamente anche le corrispondenze con la banca dati Automated Search Facility (ASF) di Interpol. Quest'ultima contiene informazioni su persone, su veicoli rubati come pure su documenti di identità rubati o smarriti.

Il *sistema d'informazione Schengen (SIS)* contiene segnalazioni di persone e oggetti (p. es. relative a documenti di identità rubati) ricercati all'interno dello spazio Schengen. Il confronto dei dati dei passeggeri con il SIS può condurre all'arresto di persone che sono ricercate a livello internazionale e quindi da estradare, che sono citate a comparire, nell'ambito di un procedimento penale, dinanzi al tribunale oppure che sono sottoposte a sorveglianza discreta poiché si ritiene abbiano commesso un reato grave.

Diversamente da RIPOL e SIS, i seguenti due sistemi di informazione contengono anche informazioni su indagini in corso condotte dalla Confederazione e dai Cantoni. È pertanto opportuno che siano ugualmente utilizzati per il confronto automatico con i dati dei passeggeri aerei.

40 RS **361**
41 RS **361.2**

Il *sistema d'informazione della Polizia giudiziaria federale* (*JANUS*) comprende informazioni relative alle indagini di polizia giudiziaria della Confederazione come pure alle indagini preliminari e alle indagini di polizia giudiziaria dei Cantoni (art. 10 LSIP). Contiene inoltre informazioni importanti sulla collaborazione della Polizia giudiziaria federale con le autorità di perseguimento penale dei Cantoni e con le autorità estere nella lotta alla criminalità internazionale e organizzata (art. 11 LSIP).

Il *sistema informatizzato di gestione e indice informatizzato delle persone e dei fascicoli dell'Ufficio federale di polizia (IPAS)* contiene informazioni su indagini in corso di polizia giudiziaria e sull'attività preventiva di polizia delle autorità nazionali ed estere di perseguimento penale, in particolare la Polizia giudiziaria federale o il servizio competente di Interpol.

Le corrispondenze («hit») ottenute tramite confronto automatico devono essere verificate manualmente dall'UIP prima di essere trasmesse all'autorità competente (cpv. 3). In questo modo s'intende evitare che le corrispondenze trasmesse possano portare all'adozione di misure a causa di una registrazione errata, volontaria o accidentale, dei dati dei passeggeri aerei. L'obbligo di verifica deriva dall'articolo 6 capoverso 5 della nLPD, secondo cui chi tratta dati personali deve accertarsi della loro esattezza.

Malgrado la verifica manuale, spesso non è comunque possibile chiarire tutte le domande e in particolare fugare completamente ogni dubbio in merito all'identità della persona.

Altri interrogativi possono riguardare i motivi della segnalazione. Il trattamento dei dati dei passeggeri aerei è infatti consentito soltanto se serve a combattere i reati terroristici o altri reati gravi. È possibile valutare se la corrispondenza ottenuta riguarda tali reati solo quando le fattispecie penali sono note o quando sono considerate sussistenti sulla scorta di informazioni di base. A differenza di RIPOL dove i dettagli relativi al reato e la stessa fattispecie sono indicati, le corrispondenze prodotte da un confronto con il SIS indicano semplicemente la categoria di reato (p. es. «omicidio»), ma non i fatti o la fattispecie in questione. Per risalire a queste informazioni occorre pertanto accedere ad altri sistemi di informazione. In caso contrario, la corrispondenza andrà immediatamente cancellata a causa della mancanza di informazioni sufficienti su un reato terroristico o su un altro reato grave. Occorre inoltre procedere alla cancellazione anche nel caso in cui la segnalazione nel SIS si basi su una fattispecie di reato non contenuta nell'elenco dei reati PNR.

Gli accessi effettuati nel quadro dell'accertamento della plausibilità permettono di verificare le corrispondenze generate dal primo confronto riguardo all'identità della persona e al motivo della segnalazione. In questo modo viene garantito che il trattamento dei dati dei passeggeri aerei avvenga nel rispetto dello scopo della legge e che alle competenti autorità di perseguimento penale e al SIC vengano trasmessi i dati delle persone corrette.

Per verificare la plausibilità dell'identità di una persona e dei motivi della segnalazione occorre accedere manualmente, una volta effettuato il confronto automatico, ai seguenti sistemi di informazione:

a) per verificare la plausibilità dell'identità di una persona:

- SIMIC (legge federale del 20 giugno 2003[42] sul sistema d'informazione per il settore degli stranieri e dell'asilo [LSISA]): il sistema d'informazione centrale sulla migrazione contiene dati d'identità delle persone registrate (p. es. cognome, nome, data di nascita) e fornisce informazioni sullo statuto di soggiorno di cittadini stranieri che soggiornano in Svizzera,
- ORBIS (art. 109*c* lett. f LStrI): il sistema nazionale visti fornisce informazioni sulle domande di visto e accesso ai dati di tutte le persone in possesso di un visto per lo spazio Schengen. Una persona può essere ad esempio identificata sulla base del numero di passaporto verificabile;

b) per verificare la plausibilità dei motivi della segnalazione:

- registro nazionale di polizia (art. 17 LSIP)[43]: fornisce indicazioni sulle comunicazioni dei Cantoni,
- SIRENE-IT (art. 5 dell'ordinanza N-SIS dell'8 marzo 2013[44]): l'accesso a questo sistema d'informazione permette, grazie a informazioni di base complementari, di attribuire una segnalazione nel SIS a una fattispecie penale concreta correlata alla criminalità organizzata o al terrorismo,
- I-24/7 (art. 352 cpv. 1 CP): contiene informazioni che consentono di risalire ai motivi di segnalazioni internazionali (Interpol),
- Sistema di informazione dell'UDSC: contiene in particolare informazioni importanti sulle fattispecie penali il cui perseguimento penale compete a questa autorità.

Se del caso occorre accedere anche al sistema di informazione con cui è stato effettuato il confronto automatico, non solo per chiarire il motivo della segnalazione ma anche per risalire all'autorità competente cui andrà trasmessa la corrispondenza in caso di esito positivo della verifica.

La procedura a due fasi garantisce che i dati vengano trattati il meno possibile. Il loro trattamento in seguito al confronto automatico di cui al capoverso 1 si limita infatti ai dati fondati su un primo sospetto. Con l'accesso di cui al capoverso 3 il trattamento viene circoscritto ai dati per i quali la verifica manuale ha confermato il primo sospetto. I restanti dati non sono pertanto più considerati.

Il confronto automatico e l'accesso manuale ai rispettivi sistemi richiedono modifiche della LStrI (ORBIS), della LSIP (RIPOL, JANUS, registro nazionale di polizia) nonché della LSISA (SIMIC). Tali modifiche sono indicate nell'allegato 3 della LDPA. Alla luce della revisione in corso della legislazione doganale, l'eventuale base legale necessaria per l'accesso manuale al sistema di informazione dell'UDSC sarà illustrata soltanto in un secondo momento, all'interno del messaggio.

42 RS **142.51**
43 RS **361.4**
44 RS **362.0**

Art. 8 Trasmissione

Le corrispondenze sottoposte a verifica possono essere trasmesse alle autorità di perseguimento penale della Confederazione e dei Cantoni nonché al SIC. Le autorità di perseguimento penale della Confederazione comprendono anche il commissariato Guardie della sicurezza aerea (SIBEL) in seno al Servizio federale di sicurezza di fedpol (art. 4 lett. b della legge del 19 marzo 2010[45] sull'organizzazione delle autorità penali, LOAP) nonché l'UDSC (art. 4 lett. c LOAP).

L'UIP trasmette le corrispondenze sottoposte a verifica ai sensi dell'articolo 7 capoverso 3 all'autorità

- che è responsabile della segnalazione da cui è scaturita la corrispondenza o
- (in caso di segnalazione da parte di un altro Stato) che deve decidere se e quali misure devono essere adottate sulla base della trasmissione da parte dell'UIP.

Art. 9 Confronto dei dati con i profili di rischio e le liste d'osservazione

L'UIP deve poter elaborare profili di rischio e liste d'osservazione per il trattamento dei dati dei passeggeri aerei (cpv. 1). Affinché questi strumenti possano essere impiegati in modo efficace, è indispensabile disporre di conoscenze specialistiche, esperienza e informazioni di base. Ciò è reso possibile dal fatto che:

- l'UIP è composto di collaboratori che dispongono di conoscenze specialistiche proprie delle pertinenti autorità federali e cantonali (v. commenti all'art. 20),
- le autorità di perseguimento penale della Confederazione e dei Cantoni nonché il SIC possono chiedere che vengano elaborati profili di rischio e liste d'osservazione (cpv. 1).

Il capoverso 2 costituisce la base legale affinché l'UIP possa confrontare i dati dei passeggeri aerei con i profili di rischio e le liste d'osservazione che ha elaborato.

I profili di rischio e le liste d'osservazione possono riguardare soltanto informazioni attribuibili a una categoria di dati di cui all'allegato 1 della legge. Tale soluzione permette di escludere che possano essere trattati dati personali degni di particolare protezione quali l'etnia o la confessione religiosa (cfr. art. 2 cpv. 3).

I *profili di rischio* descrivono combinazioni di dati che, sulla base dell'esperienza, ricorrono maggiormente in caso di attività criminali correlate a reati terroristici o ad altri reati gravi. I profili di rischio devono coprire i diversi reati menzionati all'interno dell'elenco dei reati. Tuttavia devono essere composti soltanto dalle categorie di dati classificate come dati dei passeggeri aerei nell'allegato 1 del presente avamprogetto (cpv. 3).

Le *liste d'osservazione* si compongono di informazioni già note che sono attribuibili a una delle categorie di dati di cui all'allegato 1 della legge e che concernono persone od organizzazioni sospettate di aver commesso o di pianificare un reato terroristico o altri reati gravi. Grazie al confronto dei dati dei passeggeri aerei con le liste

45 RS **173.71**

d'osservazione è possibile ad esempio cercare determinati indirizzi di posta elettronica, numeri di telefono o numeri di carta di credito allo scopo di individuare nessi e relazioni ancora sconosciuti con persone sospettate di aver commesso un reato terroristico o un altro reato grave. Ciò permette pertanto di identificare in particolare persone collegate ad autori di reati già noti o membri di organizzazioni criminali (cpv. 4).

I profili di rischio e le liste d'osservazione sono verificati regolarmente riguardo alla loro fondatezza ed efficacia (cpv. 5). I contenuti che non soddisfano più questi requisiti sono cancellati dall'UIP.

Le modalità di verifica, in particolare la responsabilità e la periodicità, devono essere stabilite dal Consiglio federale all'interno di un'ordinanza (cpv. 6 lett. a). Ciò consente di tener conto maggiormente delle esperienze che saranno fatte in futuro con questi strumenti nel trattamento dei dati dei passeggeri aerei.

All'interno dell'ordinanza il Consiglio federale dovrà anche stabilire per quali reati contenuti nel pertinente elenco determinante per il trattamento dei dati dei passeggeri aerei possono essere utilizzate le liste d'osservazione. In tale contesto andrà data priorità ai reati terroristici e ai reati correlati alla criminalità organizzata.

Art. 10 Collaborazione con il SIC

Il SIC riveste una posizione speciale nella lotta ai reati terroristici e ai reati gravi; l'acquisizione da parte sua delle informazioni precede spesso il perseguimento penale e serve all'individuazione precoce e alla prevenzione delle minacce alla sicurezza interna ed esterna.

È pertanto opportuno che il SIC possa trattare autonomamente i dati dei passeggeri aerei ai fini dell'adempimento dei propri compiti. Tuttavia questo trattamento autonomo andrà consentito in maniera rigorosamente limitata. Non è quindi prevista la concessione al SIC di un accesso diretto al sistema di informazione PNR. Al contrario, sarà l'UIP a trasmettergli i dati per via elettronica, per mezzo di una procedura automatizzata, come peraltro previsto dall'articolo 104*b* LStrI per i dati API. La trasmissione automatizzata è opportuna anche a causa del volume dei dati. La trasmissione riguarda i dati dei passeggeri aerei correlati ad aeroporti di partenza e di arrivo che sono stati precedentemente individuati dallo stesso SIC sulla base di una propria valutazione dei rischi. Ciò permette al SIC di sorvegliare gli spostamenti di persone su rotte che comportano rischi per la sicurezza.

Questa proposta è in linea con la soluzione adottata negli articoli 104*a* e 104*b* LStrI per l'utilizzo dei dati API da parte del SIC. Nel messaggio del 3 marzo 2018[46] concernente la revisione della legge federale sugli stranieri, il Consiglio federale ha affermato al riguardo quanto segue:

> «Nel 2015, fondandosi su un rapporto interno e su una perizia dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT), la Delegazione delle Commissioni della gestione ha dichiarato legittimo l'uso dei dati API da parte del SIC sebbene detto Servizio non abbia accesso al sistema. Ai fini della certezza del diritto è tuttavia opportuno creare, nel quadro della presente

46 FF **2018** 1381, in particolare 1418

revisione, una base legale esplicita per quanto riguarda la trasmissione elettronica dei dati API. Inoltre, il SIC deve poter chiedere alla SEM di estendere l'obbligo delle compagnie aeree di comunicare i dati ad altri aeroporti di partenza per prevenire le minacce alla sicurezza interna o esterna rappresentate dal terrorismo, dalla proliferazione di armi e dallo spionaggio».

Il SIC sottostà nel trattamento dei dati dei passeggeri aerei a un'ulteriore restrizione: può infatti trattare questi dati soltanto ai fini del contrasto di reati terroristici e di altri reati gravi rientranti tra i suoi compiti ai sensi dell'articolo 6 capoverso 1 lettera a numeri 1 e 3–5 LAIn (cpv. 2). La seguente tabella evidenzia quali fattispecie autorizzano a tale trattamento. I reati indicati in corrispondenza del numero 1 (terrorismo) autorizzano al trattamento dei dati dei passeggeri aerei soltanto se sono di matrice terroristica. Tale regola si applica a tutte le fattispecie che non presuppongono esplicitamente una matrice terroristica, come nel caso della sommossa (art. 260 CP).

Art. 6 cpv. 1 lett. a n. 1 e 3–5 LAIn	**Fattispecie di cui all'art. 6 cpv. 2 e 3 il cui contrasto autorizza a un trattamento dei dati ai sensi della LAIn**
N. 1: Terrorismo	Pubblica intimidazione; pubblica istigazione a un crimine o alla violenza; sommossa; atti preparatori punibili; organizzazioni criminali e terroristiche; messa in pericolo della sicurezza pubblica con armi; finanziamento del terrorismo; reclutamento, addestramento e viaggi finalizzati alla commissione di un reato di terrorismo; associazioni illecite (art. 258, 259, 260 cpv. 1, 260bis, 260ter, 260^{quater}, 260^{quinquies}, 260^{sexies}, 275ter CP)
	Divieto di organizzazioni (art. 74 della legge federale sulle attività informative[47])
	Disposizioni penali della legge federale del 12 dicembre 2014[48] che vieta i gruppi «Al-Qaïda» e «Stato islamico» nonché le organizzazioni associate (art. 2)
N. 3: Proliferazione di armi nucleari, biologiche o chimiche, compresi i loro sistemi vettori nonché tutti i beni e tutte le tecnologie a duplice impiego civile e militare necessari per la fabbricazione di tali armi (proliferazione NBC), o commercio illegale di sostanze radioattive, materiale bellico e altri beni d'armamento	Delitti e crimini ai sensi della legge del 20 giugno 1997[49] sulle armi (art. 33 cpv. 3)
	Uso delittuoso di materie esplosive o gas velenosi (art. 224 cpv. 1 CP)
	Fabbricazione, occultamento e trasporto di materie esplosive o gas velenosi (art. 226 CP)
	Pericolo dovuto all'energia nucleare, alla radioattività e a raggi ionizzanti (art. 226bis CP)

47 RS **121**
48 RS **122**
49 RS **514.54**

N. 4: Attacchi a infrastrutture nei settori dell'informazione, della comunicazione, dell'energia, dei trasporti e di altro genere, indispensabili per il funzionamento della società, dell'economia e dello Stato (infrastrutture critiche)	Atti preparatori punibili (art. 226ter CP) Inosservanza di provvedimenti di sicurezza interna ed esterna (art. 88 cpv. 2 della legge del 21 marzo 2003[50] sull'energia nucleare [LENu]) Infrazioni con beni nucleari e scorie radioattive (art. 89 cpv. 2 LENu) Acquisizione illecita di dati (art. 143 CP) Danneggiamento di dati (art. 144bis cpv. 3 CP) Abuso di un impianto per l'elaborazione di dati (art. 147 cpv. 1 e 2 CP) Inondazione, franamento (art. 227 n. 1 CP) Danneggiamento d'impianti elettrici, di opere idrauliche e di opere di premunizione (art. 228 n. 1 CP) Danneggiamento (art. 144 cpv. 3 CP) Incendio intenzionale (art. 221 cpv. 1 e 2 CP) Esplosione (art. 223 n. 1 CP)
N. 5: Estremismo violento	Danneggiamento (art. 144 cpv. 3 CP) Incendio intenzionale (art. 221 cpv. 1 e 2 CP) Esplosione (art. 223 n. 1 CP) Uso delittuoso di materie esplosive o gas velenosi (art. 224 cpv. 1 CP) Fabbricazione, occultamento e trasporto di materie esplosive o gas velenosi (art. 226 CP) Inondazione, franamento (art. 227 n. 1 CP) Danneggiamento d'impianti elettrici, di opere idrauliche e di opere di premunizione (art. 228 n. 1 CP) Messa in pericolo della sicurezza pubblica con armi (art. 260^{quater} CP)

Il SIC deve cancellare i dati entro 96 ore dalla loro ricezione (cpv. 3). Con questa durata di conservazione la legge corrisponde a una vigente disposizione del SIC relativa al sistema d'informazione «Memoria dei dati residui». La stessa disposizione è applicabile peraltro anche ai dati API trasmessi automaticamente al SIC.

Art. 11 Trasmissione dei dati dei passeggeri aerei su richiesta

I dati dei passeggeri aerei possono contribuire significativamente al successo delle indagini su reati terroristici o reati gravi. Vanno inoltre utilizzati per chiarire eventuali dettagli. L'UIP deve pertanto essere autorizzata a effettuare su richiesta consultazioni mirate dei dati del sistema di informazione PNR (cpv. 1).

50 RS **732.1**

La consultazione oggetto della richiesta deve essere sufficientemente concreta e, di conseguenza, circoscritta. La richiesta deve inoltre dimostrare in maniera plausibile le ragioni per cui i dati richiesti sono necessari per accertare o prevenire un reato terroristico o un altro reato grave. Le consultazioni generiche, non meglio specificate, che conducono a una moltitudine di risultati più disparati non sono per contro ammesse. Non bisogna pertanto dare alcun seguito a tali richieste.

Il fatto che, oltre alle autorità svizzere già menzionate all'articolo 8, anche l'Ufficio europeo di polizia sia autorizzato a presentare richiesta, senza che la trasmissione dei dati sia subordinata all'esistenza di un trattato internazionale, è attribuibile all'accordo concluso dalla Svizzera con Europol il 24 settembre 2004[51]. L'accordo disciplina la cooperazione nella lotta a gravi forme di criminalità internazionale. Lo scambio di dati tra la Svizzera ed Europol è ammesso soltanto se concerne reati contrastati in virtù sia di tale accordo sia della legge sui passeggeri dei dati aerei. È pertanto esclusa la possibilità di trasmettere a Europol dati su reati che, pur essendo menzionati all'interno dell'accordo, non rientrano nel campo di applicazione della LDPA.

Per converso, se si tratta di reati che non sono oggetto dell'accordo ma che sono considerati reati terroristici o gravi ai sensi della LDPA, l'UIP sarà autorizzata a trasmettere i pertinenti dati a Europol conformemente all'articolo 16 capoverso 1 nLPD. Il Consiglio federale ha infatti confermato che tutti gli Stati membri dell'UE garantiscono una protezione adeguata dei dati[52]. Questo principio è pertanto estendibile anche all'associazione degli Stati membri e quindi a Europol.

Art. 12 Comunicazione in caso di sospetto

Il ricorso a profili di rischio e a liste d'osservazione può permettere di concludere che un reato terroristico o un altro reato grave sia stato commesso, sia ancora in corso o sia pianificato. L'UIP è tenuta a trasmettere alle competenti autorità di perseguimento penale in modo proattivo gli elementi su cui si fonda tale sospetto. Tuttavia la comunicazione deve aver luogo soltanto se il sospetto dell'UIP è concreto, ossia se si riferisce a una determinata persona e se diversi indizi indicano che un reato terroristico o un grave reato sia stato commesso o sia pianificato.

Ogni decisione in merito all'ulteriore procedura compete alle autorità di perseguimento penale cui è stato comunicato il sospetto concreto.

Per dati personali degni di particolare protezione che possono essere trasmessi in virtù del capoverso 2 si intendono i dati biometrici che identificano in modo univoco una persona fisica o i dati concernenti procedimenti e sanzioni amministrativi e penali (cfr. art. 6 cpv. 6). L'UIP non è invece autorizzata a trattare o trasmettere altri dati personali degni di particolare protezione.

51 RS **0.362.2**

52 Elenco degli Stati che garantiscono una protezione adeguata dei dati: https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2021/20211115_Staatenliste_f.pdf.download.pdf/20211115_Staatenliste_f.pdf (non disponibile in italiano)

Sezione 4: Sistema di informazione PNR

Art. 13

Il sistema di informazione PNR è gestito dall'UIP.

L'accesso è limitato ai collaboratori dell'UIP nonché alle persone responsabili della manutenzione e della programmazione del sistema, laddove tale accesso sia strettamente necessario per l'esecuzione di queste loro attività.

Sezione 5: Protezione dei dati

La *necessità* di attribuire un ruolo centrale alla protezione dei dati è dovuta al fatto che nel quadro della lotta ai reati terroristici e ad altri reati gravi vengono raccolti e in seguito trattati anche dati di persone che non presentano alcun legame con tali reati. La raccolta di questi dati è tuttavia inevitabile, salvo rimettere in discussione gli obiettivi previsti dalla legge.

Lo stesso vale per la durata relativamente lunga di conservazione dei dati, che vengono cancellati soltanto trascorsi cinque anni. La relazione della Commissione europea del 24 luglio 2020[53] sul riesame della direttiva PNR spiega al riguardo quanto segue:

> «Solitamente per indagare e perseguire tali reati occorrono mesi e, spesso, anni di lavoro. In quest'ottica, gli Stati membri hanno confermato che il periodo di conservazione di cinque anni è necessario da un punto di vista operativo. La disponibilità di dati storici garantisce che, quando un individuo è accusato di aver commesso un reato grave o di essere coinvolto in attività terroristiche, è possibile riesaminare lo storico dei viaggi e vedere chi ha viaggiato con lui, identificando potenziali complici o altri membri di un gruppo criminale, nonché potenziali vittime.»

La protezione dei dati è garantita non solo dalle disposizioni previste dalla presente sezione, ma anche dall'obbligo per le imprese di trasporto aereo di fornire informazioni in merito al trattamento dei dati (art. 5), dalla procedura a due fasi prevista per il confronto di dati (art. 7) e dal vincolo a concludere trattati internazionali soltanto con gli Stati che garantiscono una protezione dei dati equiparabile a quella della Svizzera (art. 21).

Art. 14 Pseudonimizzazione

I dati dei passeggeri aerei comprendono diverse categorie di dati che permettono di risalire all'identità della persona in questione. Questi dati devono essere automaticamente pseudonimizzati sei mesi dopo la loro introduzione nel sistema di informazione PNR.

Tale regola si applica ai seguenti dati di una persona:

53 Relazione della Commissione al Parlamento europeo e al Consiglio sul riesame della direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, COM/2020/305 final

- nome/i nonché numero e nomi dei compagni di viaggio;
- indirizzo e dati di contatto (indirizzo di posta elettronica, numeri di telefono e di cellulare);
- informazioni su tutte le modalità di pagamento, compreso l'indirizzo di fatturazione;
- informazioni sui viaggiatori abituali («frequent flyer»);
- osservazioni generali contenenti informazioni che potrebbero servire a identificare direttamente il passeggero cui si riferiscono i dati PNR,
- i dati API eventualmente raccolti.

Questi dati non possono pertanto più essere ricollegati alla persona in questione, ma soltanto a uno pseudonimo. Chiunque intenda revocare la pseudonimizzazione necessita di una tavola delle concordanze, conservata accuratamente, in cui ogni pseudonimo utilizzato è associato alla persona in questione.

Conformemente al messaggio concernente la nuova LPD, la pseudonimizzazione costituisce un provvedimento tecnico appropriato per garantire la sicurezza dei dati (art. 8 nLPD)[54]. Nello stesso messaggio il Consiglio federale precisa inoltre che la legge sulla protezione dei dati non si applica ai dati

> «la cui identificazione da parte di un terzo è impossibile (i dati sono stati anonimizzati in modo completo e definitivo) o sarebbe possibile soltanto con uno sforzo che nessun interessato è disposto a fare. Tale regola vale anche per i dati pseudonimizzati[55].»

Il termine di sei mesi antecedente alla pseudonimizzazione corrisponde alla soluzione adottata nella legge federale del 18 marzo 2016[56] sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT), in particolare per la conservazione dei metadati delle telecomunicazioni (art. 26 cpv. 5). Al pari dei dati dei passeggeri aerei, anche questi ultimi dati sono registrati a prescindere dalla presenza di un sospetto, sono attribuibili a una determinata persona e, se del caso, possono esser trattati dallo Stato allo scopo di combattere la criminalità.

Art. 15 Revoca della pseudonimizzazione

Come evidenziato dalla relazione della Commissione europea sul riesame della direttiva PNR, le indagini su reati terroristici e altri reati gravi richiedono anni di lavoro. Le esperienze maturate in Svizzera avvalorano tale affermazione. Deve essere pertanto possibile consultare i dati del sistema di informazione PNR anche nel caso in cui i dati risalgano a più di sei mesi e risultino pertanto pseudonimizzati. Per effettuare simili ricerche di dati storici è necessario poter annullare la pseudonimizzazione.

54 Messaggio del 15 settembre 2017 concernente la legge federale relativa alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati, FF **2017** 5939
55 FF **2017** 5939, in particolare 6011
56 RS **780.1**

Una domanda di revoca deve essere presentata all'UIP che, laddove la ritenga sufficientemente motivata, provvederà in seguito a trasmetterla, unitamente alla propria raccomandazione, al Tribunale amministrativo federale (TAF) (cpv. 2). Una domanda è sufficientemente motivata se:

- i dati che dovrebbero essere oggetto della revoca della pseudonimizzazione sono ben definiti. Tale requisito è soddisfatto in particolare quando la domanda di revoca concerne ad esempio una persona o un volo specifico;
- è reso verosimile che la revoca della pseudonimizzazione fornisca informazioni determinanti ai fini della prevenzione, dell'accertamento, dell'indagine e del perseguimento efficaci di un reato terroristico o di un altro reato grave. Le informazioni determinanti richieste devono essere descritte con la maggiore precisione possibile.

Se la domanda non è sufficientemente motivata o se la motivazione è insufficiente, l'UIP ne dà comunicazione all'autorità richiedente che ha in seguito la possibilità di apportare correzioni alla propria domanda.

Il TAF decide su un'eventuale revoca della pseudonimizzazione entro al massimo cinque giorni lavorativi (cpv. 4). La competenza di un tribunale è prevista anche dal diritto tedesco[57] e austriaco[58] in applicazione dell'articolo 12 paragrafo 3 della direttiva PNR dell'UE.

Il tempo massimo di cinque giorni lavorativi non esenta tuttavia il TAF dal prendere immediatamente una decisione in caso di urgenza. L'urgenza si presenta in particolare in caso di minaccia di attentato terroristico.

La chiave tecnica per la revoca della pseudonimizzazione è conservata presso l'UIP. Il suo accesso è protetto. L'UIP può impiegarla soltanto se il TAF ha approvato una domanda di revoca della pseudonimizzazione.

La comunicazione di dati registrati da meno di sei mesi è retta dall'articolo 11 e non richiede il coinvolgimento del TAF.

Art. 16 Durata di conservazione e cancellazione

I dati dei passeggeri aerei sono cancellati automaticamente cinque anni dopo la loro introduzione nel sistema di informazione PNR (cpv. 1).

La durata di conservazione di cinque anni prevista dall'articolo 16 si basa sulla direttiva PNR e garantisce pertanto la compatibilità del sistema PNR svizzero con i sistemi PNR degli Stati membri dell'UE. La compatibilità è un requisito fondamentale per l'accordo sullo scambio reciproco di dati dei passeggeri aerei che la Svizzera intende concludere con l'UE.

La durata di conservazione relativamente lunga deriva in primo luogo dall'impiego dei dati dei passeggeri aerei come strumento per combattere i reati terroristici e altri

57 Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz - FlugDaG), § 5 Abs. 2, BGBl I 117s1484

58 Bundesgesetz über die Verarbeitung von Fluggastdaten zur Vorbeugung, Verhinderung und Aufklärung von terroristischen und bestimmten anderen Straftaten (PNR-Gesetz – PNR-G), § 6 Abs. 2, BGBl. I Nr. 64/2018

reati gravi. Le indagini su questi reati, in particolare quelle intese a individuare reti internazionali, si protraggono spesso per diversi anni. In occasione del riesame della direttiva PNR da parte della Commissione europea, gli Stati membri dell'UE hanno confermato che la durata di conservazione dei dati prevista dalla direttiva PNR è necessaria dal punto di vista operativo. Inoltre le norme concernenti l'accesso da parte delle autorità competenti ai dati conservati dall'UIP e la loro anonimizzazione (ossia alla loro pseudonimizzazione ai sensi dell'art. 14 dell'avamprogetto) hanno dimostrato di essere sufficientemente solide da impedire gli abusi[59].

Per la Svizzera la lunga durata di conservazione dei dati, che nella maggior parte dei casi non sono peraltro neanche correlati a un sospetto, rappresenta un cambiamento di paradigma. Quest'ultimo è giustificato soltanto dallo scopo principale della presente legge, ossia contrastare le gravi forme di criminalità a livello nazionale e internazionale con l'ausilio del PNR.

Il Consiglio federale fissa in un'ordinanza la durata massima di conservazione delle corrispondenze scaturite da confronti di cui agli articoli 7 e 9 (cpv. 2). Ciò permette di tener conto delle diverse procedure in cui le autorità necessitano di dati basati su un sospetto fondato, in particolare le indagini e i procedimenti penali.

Art. 17 Sorveglianza

A livello di ufficio, il servizio di protezione dei dati di fedpol sorveglia l'osservanza delle prescrizioni in materia di protezione dei dati contenute nella presente legge e nella LPD.

La sorveglianza riguarda sia il trattamento dei dati effettuato dall'UIP sia gli aspetti tecnici della protezione dei dati garantiti dal sistema di informazione PNR, quali la pseudonimizzazione dei dati dopo sei mesi e la loro cancellazione automatica dopo cinque anni.

Nonostante la funzione di sorveglianza assolta dal servizio di protezione dei dati di fedpol, è fatta salva la sorveglianza dell'IFPDT prevista dall'articolo 4 nLPD.

Art. 18 Diritto d'accesso

L'articolo 5 prevede che un passeggero aereo sia informato dall'impresa di trasporto aereo sul trattamento dei suoi dati conformemente alla presente legge. Le richieste di accesso ai sensi dell'articolo 18 LDPA e degli articoli 25–28 nLPD devono essere presentate a fedpol.

Tenuto conto dello scopo del trattamento dei dati, resta inteso che l'informazione non può essere sempre comunicata o perlomeno non completamente. fedpol dovrà avvalersi di tale diritto conformemente all'articolo 26 capoverso 2 lettera b nLPD se la comunicazione dell'informazione:

59 Relazione della Commissione al Parlamento europeo e al Consiglio sul riesame della direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, COM/2020/305 final

- è rifiutata in quanto sussiste un interesse pubblico preponderante, in particolare la sicurezza interna o esterna della Svizzera o
- rischia di compromettere un'indagine, un'istruzione o un procedimento giudiziario o amministrativo.

La comunicazione di informazioni è esclusa anche laddove i dati risalgano a più di sei mesi prima e siano pertanto pseudonimizzati. La domanda di revoca della pseudonimizzazione compete, conformemente all'articolo 15 capoverso 1, unicamente alle autorità di perseguimento penale e al SIC.

Se l'UIP ha trasmesso i dati della persona in questione a un'altra autorità, fedpol si consulta con quest'ultima prima di fornire le informazioni. Ciò permette di garantire che eventuali motivi di restrizione del diritto di accesso ai sensi dell'articolo 26 nLPD possano essere presi in considerazione.

Sezione 6: Organizzazione e personale dell'UIP

Art. 19 Organizzazione

L'UIP deve essere collocata in seno a fedpol. Quest'attribuzione deriva, da un lato, dalla finalità del trattamento dei dati e, dall'altro, dalla vasta esperienza maturata da fedpol nella gestione dei sistemi di informazione, che dovrebbe riflettersi, a sua volta, positivamente nella creazione e nella gestione del sistema di informazione PNR.

Vista la particolarità dei dati dei passeggeri aerei, la cui protezione deve essere garantita, è opportuno separare l'UIP sul piano organizzativo dalle unità di fedpol che svolgono compiti di indagine. Qualora intendano richiedere dati all'UIP, queste ultime sottostanno pertanto alle stesse condizioni applicabili anche alle altre autorità di perseguimento penale della Confederazione e dei Cantoni.

L'UIP deve rappresentare il Single Point of Contact (SPOC) per le imprese di trasporto aereo e le autorità estere per quanto concerne i dati PNR. Resta ancora aperta la questione se l'UIP debba garantire un servizio operativo 24 ore su 24, sette giorni su sette. Infatti, sebbene in Svizzera viga un divieto di volo notturno, i dati dei passeggeri aerei sono trasmessi dalle imprese di trasporto aereo anche di notte.

Art. 20 Personale

Il trattamento dei dati dei passeggeri aerei apporta un notevole valore aggiunto per le autorità di perseguimento penale sia della Confederazione sia dei Cantoni.

Visto il sistema federalista della Svizzera, il perseguimento penale rientra generalmente nella competenza primaria dei Cantoni. La Confederazione si adopera invece nel perseguimento di determinati reati gravi ad esempio quelli di terrorismo o di criminalità organizzata e di diversi reati contemplati dal diritto penale accessorio della Confederazione quali le fattispecie contenute nella legge federale del 21 marzo 2003[60] sull'energia nucleare, nella legge del 28 agosto 1992[61] sulla protezione dei

60 RS **732.1**
61 RS **232.11**

marchi, nella legge dell'8 ottobre 2004[62] sui trapianti o nella legge del 20 giugno 1997[63] sulle armi.

La lotta ai reati terroristici e ad altri reati gravi è considerata pertanto un compito congiunto della Confederazione e dei Cantoni, dove ciascuna parte agisce secondo le proprie priorità specifiche beneficiando del sostegno da parte dell'UIP.

La collocazione sul piano organizzativo dell'UIP in seno alla Confederazione è giustificata soprattutto dai risvolti internazionali che comporta l'adempimento dei compiti, il che non significa tuttavia che la Confederazione debba sostenere da sola tutti i costi collegati a questo nuovo compito. Confederazione e Cantoni si fanno infatti carico, in parti uguali, delle spese legate ai collaboratori impiegati presso l'UIP.

Il modello scelto prevede il distaccamento presso l'UIP di propri collaboratori da parte della Confederazione e dei Cantoni per un periodo determinato. Altri modelli di collaborazione particolari come quello qui proposto esistono già presso i centri di cooperazione di polizia di Ginevra e Chiasso[64] come pure presso il Servizio di protezione dei testimoni.

La base per la cooperazione ai sensi della presente legge è rappresentata, da un lato, dalla stessa LDPA e dalla relativa ordinanza e, dall'altro, da una convenzione tra la Confederazione e i Cantoni. Al momento non è ancora chiaro se i Cantoni intendono disciplinare la loro partecipazione nel quadro di un concordato.

Al riguardo il «Basler-Kommentar zur Bundesverfassung»[65] sottolinea quanto segue:

> Poiché la Costituzione federale non prevede che le convenzioni contenenti norme di diritto concluse tra la Confederazione e i Cantoni siano una forma d'atto legislativo a sé stante (art. 163 Cost.), occorre che almeno le condizioni quadro della convenzione siano stabilite da una legge federale (art. 164 Cost.) o, in caso di disposizioni di importanza secondaria, da un'ordinanza. Soltanto in presenza di questa base legale (…) è possibile concludere in seguito una convenzione con i Cantoni.

Oggetto della convenzione tra la Confederazione e i Cantoni è il distacco di collaboratori presso l'UIP.

La legge deve pertanto evidenziare:

- lo scopo del distacco di collaboratori da parte dei Cantoni;
- in quale proporzione Confederazione e Cantoni partecipano alle risorse di personale dell'UIP.

L'UIP si compone in parti uguali di collaboratori della Confederazione e dei Cantoni (cpv. 1). Ogni autorità assume i costi per i propri collaboratori distaccati (cpv. 4).

62 RS **810.21**
63 RS **514.54**
64 Cfr. l'accordo del 2 aprile 2014 sulla gestione nazionale dei centri comuni di cooperazione di polizia e doganale (CCPD) di Ginevra e Chiasso, RS **360.4**
65 Schweizerisches Verfassungsrecht, 3ª ed., Basilea 2016; Waldmann Bernhard /Belser Eva Maria / Epiney Astrid (ed.), Basler Kommentar Bundesverfassung, Basilea 2015, art. 48 n. 37

La legge deve anche indicare che i collaboratori, benché prestino servizio all'interno dell'UIP, continuano a essere impiegati dell'autorità che li ha distaccati la quale resta pertanto il loro datore di lavoro sotto il profilo contrattuale. Questa condizione deriva dal capoverso 2 (diritto di impartire istruzioni condiviso) e dal capoverso 4 già citato.

Le principali differenze rispetto all'attuale rapporto di lavoro necessitano ugualmente di una base legale. Si tratta nello specifico del:

- diritto di fedpol di impartire istruzioni in virtù del rapporto di dipendenza funzionale (cpv. 2), che sostituisce quello del datore di lavoro contrattuale per la durata dell'impiego presso l'UIP;
- l'obbligo del collaboratore di mantenere il segreto (cpv. 3) anche al cospetto del suo datore di lavoro contrattuale.

Il datore di lavoro contrattuale conserva il diritto di impartire istruzioni sul piano disciplinare (cpv. 2) e l'obbligo di assumersi i costi salariali, come pure eventuali spese, indennità per il lavoro straordinario e l'attribuzione di premi. Per i collaboratori dei Cantoni, l'importo di tali indennità è retto dalle disposizioni cantonali in materia.

A complemento delle disposizioni legali, il Consiglio federale può stabilire ulteriori disposizioni a livello di ordinanza (cpv. 5).

Indipendentemente dalla presente legge, l'articolo 1 capoverso 1 lettera f della legge del 14 marzo 1958[66] sulla responsabilità (LResp) si applica ai collaboratori cantonali impiegati presso l'UIP.

Nella convenzione con i Cantoni occorre indicare in particolare le qualifiche richieste per i collaboratori da distaccare presso l'UIP. Sono presi in considerazione soprattutto i collaboratori che vantano conoscenze comprovate in materia di perseguimento penale.

Inoltre la convenzione deve contenere informazioni su come procedere se un collaboratore:

- si rivela inadatto a svolgere il compito;
- adotta un comportamento che potrebbe condurre a misure disciplinari.

Un ulteriore aspetto da regolamentare è la procedura da seguire in caso di disaccordo tra fedpol e un Cantone.

Il capoverso 3 stabilisce che, al di fuori dell'UIP, i collaboratori non dispongono liberamente delle informazioni di cui sono venuti a conoscenza durante il loro impiego presso l'UIP. Tale regola resta valida anche una volta terminato il loro impiego. In questo modo viene vietato lo scambio informale di contenuti che sottostanno alla protezione dei dati tra l'UIP e l'unità distaccante.

È tuttavia auspicabile che i collaboratori, una volta rientrati dal loro impiego presso l'UIP, trasmettano ai loro colleghi le conoscenze metodologiche ivi acquisite in materia di trattamento dei dati dei passeggeri aerei. È il caso ad esempio delle esperienze acquisite nel progettare e impiegare nel modo più efficiente possibile i

66 RS **170.32**

profili di rischio e le liste d'osservazione. Il modello di distacco sarà così in grado di garantire un trasferimento delle competenze dell'UIP alle autorità distaccanti.

Sezione 7: Conclusione di trattati e di convenzioni e assistenza amministrativa

Art. 21 Conclusione di trattati e di convenzioni

La LDPA e la LPD hanno carattere vincolante soltanto per la Svizzera.

Se la Svizzera trasmette dati dei passeggeri aerei a un altro Stato, occorre assicurarsi che il diritto nazionale di quest'ultimo garantisca ai dati trasmessi una protezione equiparabile a quella della Svizzera. L'elenco degli Stati, disponibile in formato elettronico, permette di sapere se un determinato Stato garantisce questa protezione[67].

Se la protezione dei dati è giudicata equiparabile a quella della Svizzera, i dati possono essere comunicati allo Stato in questione anche in assenza di un trattato internazionale (art. 16 cpv. 1 nDSG). Tuttavia l'articolo 21 capoverso 1 della presente legge esige anche in questo caso la conclusione di un trattato internazionale. Soltanto in questo modo la Svizzera è in grado di assicurarsi la reciprocità in materia di trasmissione dei dati per la lotta al terrorismo e ad altri reati gravi e di ricevere i dati dei passeggeri aerei a bordo dei voli operati da questo Stato verso la Svizzera.

Il capoverso 2 conferisce a fedpol la competenza di concludere autonomamente convenzioni con le autorità di altri Stati. Tale competenza è circoscritta ad aspetti operativi, tecnici o amministrativi. Le questioni fondamentali inerenti alla protezione dei dati o i diritti e i doveri delle autorità devono essere per contro sempre oggetto di un trattato internazionale ai sensi del capoverso 1.

Art. 22 Assistenza amministrativa

L'assistenza amministrativa che l'UIP presta a un'UIP estera in assenza di un trattato internazionale che disciplini più dettagliatamente la trasmissione di dati tra la Svizzera e questo Stato è limitata a casi eccezionali debitamente motivati. Non è consentita la trasmissione di dati di passeggeri aerei se nei confronti della persona non sussiste alcun sospetto fondato che stia pianificando o abbia commesso un reato terroristico o un altro reato grave.

La trasmissione è limitata ai dati che dovranno essere sufficientemente precisati dall'UIP richiedente nella propria richiesta. Inoltre questi dati devono essere indispensabili per prevenire una minaccia imminente. La direttiva PNR prevede un'eccezione simile (art. 9 par. 1 e 2).

Una revoca della pseudonimizzazione non è ammessa nell'ambito dell'assistenza amministrativa ai sensi della presente disposizione.

67 https://www.bafu.admin.ch/dam/bafu/de/dokumente/klima/rechtliche-grundlagen/definition-luftverkehrsunternehmen.pdf.download.pdf (disponibile soltanto in tedesco e in francese)

Sezione 8: Sanzioni amministrative

Art. 23 Sanzioni in caso di violazione degli obblighi delle imprese di trasporto aereo

Una violazione degli obblighi di diligenza e di informazione di cui agli articoli 4 e 5 deve essere sanzionata indipendentemente dalla prova della colpa, come previsto dal 1° ottobre 2015 nell'articolo 122*b* LStrI. Il Consiglio federale aveva motivato la rinuncia a tale prova con le ricerche approfondite che avrebbero dovuto essere condotte anche all'estero. Nei fatti la prova della colpa si sarebbe rivelata impossibile[68].

La violazione dell'obbligo da parte di un'impresa di trasporto aereo è ad esempio presunta quando quest'ultima:

- omette di trasmettere i dati dei passeggeri aerei all'UIP o li trasmette troppo tardi;
- non osserva le prescrizioni tecniche di fedpol nello trasmettere i dati dei passeggeri aerei all'UIP; oppure
- non trasmette all'UIP i dati di tutti i passeggeri aerei.

Lo stesso vale quando:

- i dati trasmessi sono manifestamente errati; o
- i passeggeri aerei non sono stati informati per iscritto del trattamento dei loro dati secondo la presente legge (cfr. art. 5).

Una violazione dell'obbligo di diligenza è considerata grave quando è constatata a più riprese o l'insieme dei dati di un volo non vengono forniti. È equiparata a una mancata comunicazione anche la trasmissione di dati perlopiù errati.

Nei casi di lieve entità si può prescindere dall'apertura di un procedimento, ad esempio quando quest'ultimo risulterebbe sproporzionato.

Se l'impresa di trasporto aereo è in grado di dimostrare che, malgrado l'avvenuta contestazione, abbia adottato tutte le misure precauzionali, la sanzione viene meno. Si pensi ad esempio a un'interruzione di corrente a essa non imputabile che ha reso impossibile la trasmissione di dati.

La trasmissione dei dati dei passeggeri aerei dovrebbe aver luogo nella metà dei casi da un aeroporto di partenza situato all'estero. Il capoverso 5 garantisce pertanto che anche le violazioni degli obblighi di diligenza verificatesi all'estero possano essere sanzionate.

Art. 24 Procedimento

Se una violazione dell'obbligo di comunicazione ai sensi dell'articolo 122*b* LStrI è già sanzionata, non può essere passibile di ulteriori sanzioni ai sensi della LDPA. Le

68 Messaggio dell'8 marzo 2013 concernente la modifica della legge federale sugli stranieri (Violazioni dell'obbligo di diligenza e dell'obbligo di comunicazione da parte delle imprese di trasporto aereo, sistemi d'informazione), FF **2013** 2045, in particolare 2220

violazioni dell'obbligo di informazione di cui all'articolo 5 sono invece sanzionabili indipendentemente dalla LStrI, visto che quest'ultima, diversamente dalla LDPA, non punisce tali violazioni.

Allegato 1 Dati dei passeggeri aerei

Lo *status di viaggio* (n. 10) comprende i voli già effettuati e quelli previsti. Da indicare sono le conferme, il check-in, le precedenti assenze all'imbarco e i passeggeri con biglietto aereo ma senza prenotazione.

La *scissione* dei dati (n. 11) si verifica quando le persone effettuano separatamente un viaggio prenotato insieme. In questo caso i dati dei passeggeri aerei in questione devono nuovamente essere rilevati. I dati inizialmente raccolti vengono pertanto scissi.

Si parla di *code share* (n. 15) quando il volo è eseguito da un'impresa di trasporto aereo diversa da quella indicata dal numero del volo.

Allegato 2 Categorie di reato PNR ai sensi dell'art. 6 cpv. 3 lett. a

Sono considerati gravi ai sensi dell'articolo 6 capoverso 3 lettera a della presente legge soltanto i reati di cui all'allegato 1 LSIS puniti con una pena detentiva di più di tre anni e che sono attribuibili a una categoria di reato PNR ai sensi dell'allegato 2 della presente legge.

Nell'allegato 2 le categorie di reato sono raffrontate alle corrispondenti categorie di cui all'allegato 1 LSIS. In questo modo è possibile stabilire quali crimini riportati nel catalogo dei reati della LSIS vadano considerati reati gravi ai sensi dell'articolo 6 capoverso 3 lettera a.

Allegato 3 Modifica di altri atti normativi

1. Legge federale del 20 giugno 2003[69] sul sistema d'informazione per il settore degli stranieri e dell'asilo (LSISA)

Art. 9 cpv. 1 lett. c^{bis} Procedura di richiamo

Vista la formulazione tecnologicamente neutra dell'articolo 7 LDPA concernente il confronto automatico dei dati dei passeggeri aerei con i diversi sistemi di informazione della Confederazione, nella presente disposizione occorre prevedere l'autorizzazione all'accesso manuale a SIMIC da parte dell'UIP.

2. Legge federale del 16 dicembre 2005[70] sugli stranieri e la loro integrazione (LStrI)

Art. 109c lett. f n. 1 Consultazione del sistema nazionale visti

Vista la formulazione tecnologicamente neutra dell'articolo 7 LDPA concernente il confronto automatico dei dati dei passeggeri aerei con i diversi sistemi di informazione della Confederazione, nella presente disposizione occorre prevedere l'autorizzazione all'accesso manuale a ORBIS da parte dell'UIP.

69 RS **142.51**
70 RS **142.20**

3. Legge federale del 17 giugno 2005[71] sul Tribunale amministrativo federale (LTAF)

Art. *36c* Giudice unico

Il Tribunale amministrativo federale esamina, quale autorità indipendente, se la pseudonimizzazione può essere revocata conformemente all'articolo 15 LDPA. Oltre a verificare se la domanda è sufficientemente motivata, pondera gli interessi in materia di sicurezza perseguiti con tale revoca rispetto agli interessi in materia di protezione dei dati.

4. Legge federale del 13 giugno 2008[72] sui sistemi d'informazione di polizia della Confederazione (LSIP)

Art. 10 cpv. 4 lett. d Sistema di sostegno alle indagini di polizia giudiziaria della Confederazione

Art. 11 cpv. 5 lett. b Sistema di trattamento dei dati relativi ai reati federali

Vista la formulazione tecnologicamente neutra dell'articolo 7 LDPA concernente il confronto automatico dei dati dei passeggeri aerei con i diversi sistemi di informazione della Confederazione, gli articoli 10 e 11 LSIP devono prevedere l'autorizzazione al confronto automatico e all'accesso manuale a JANUS da parte dell'UIP.

Art. 15 cpv. 4 lett. a^{bis} Sistema di ricerca informatizzato di polizia

Vista la formulazione tecnologicamente neutra dell'articolo 7 LDPA concernente il confronto automatico dei dati dei passeggeri aerei con i diversi sistemi di informazione della Confederazione, l'articolo 15 LSIP deve prevedere l'autorizzazione al confronto automatico e all'accesso manuale a RIPOL da parte dell'UIP.

Art. 17 cpv. 4 lett. m Registro nazionale di polizia

Vista la formulazione tecnologicamente neutra dell'articolo 7 LDPA concernente il confronto automatico dei dati dei passeggeri aerei con i diversi sistemi di informazione della Confederazione, nella presente disposizione occorre prevedere l'autorizzazione di accesso da parte dell'UIP.

5. Legge federale del 21 dicembre 1948[73] sulla navigazione aerea (LNA)

Art. 29 cpv. 5

Le imprese di trasporto aereo non devono più poter partire dalla Svizzera o atterrarvi liberamente se sono state sollecitate a più riprese senza successo a pagare l'importo derivante da una sanzione ai sensi dell'articolo 26.

71 RS **173.32**
72 RS **361**
73 RS **748.0**

È in particolare impossibile procedere a un'esecuzione nel caso in cui un'impresa di trasporto aereo estera non abbia alcuna sede in Svizzera e le condizioni per un'esecuzione presso un eventuale domicilio speciale non siano soddisfatte (art. 50 della legge federale dell'11 aprile 1889[74] sulla esecuzione e sul fallimento [LEF]).

In questo caso la revoca dell'autorizzazione dell'esercizio può avvenire alle seguenti condizioni, ossia se:

- una sanzione ai sensi dell'articolo 26 LDPA è passata in giudicato;
- il suo pagamento è stato più volte sollecitato senza successo.

Una revoca dell'autorizzazione di esercizio va invocata come ultima ratio e non senza aver prima considerato tutte le ulteriori circostanze non direttamente legate ai pagamenti in sospeso. Per tale ragione, si è rinunciato a introdurre un obbligo legale di revoca dell'autorizzazione di esercizio.

5 Ripercussioni

5.1 Ripercussioni finanziarie e sull'effettivo del personale per la Confederazione

Alla luce dello sviluppo e della gestione di un sistema d'informazione tecnico e della creazione e organizzazione di un'UIP che ne deriva, l'introduzione di un sistema PNR nazionale rappresenta un processo complesso i cui costi possono essere suddivisi in tre categorie: costi di progetto, di gestione e per il personale.

Costi di progetto

La progettazione, lo sviluppo e l'introduzione di un sistema PNR nonché la creazione di un'UIP comportano costi di progetto, la cui entità dipende dalla scelta di utilizzare il sistema PNR dell'ONU «goTravel» (opzione 1) o di acquistare e sviluppare internamente un sistema PNR (opzione 2). Entrambe le opzioni comportano ripercussioni sul finanziamento del progetto, ma non sul contenuto della legge.

- L'opzione 1, ossia la soluzione dell'ONU «goTravel», è il sistema PNR attualmente impiegato dall'ONU. Tale sistema può essere acquisito senza grandi adeguamenti e può essere utilizzato sin da subito. «goTravel» è già in uso presso diversi Paesi. Si tratta dell'opzione al momento privilegiata dal DFGP. Attualmente, oltre alle possibilità tecniche, nell'ambito di una cosiddetta «Proof of Concept» (PoC) viene valutato se sono soddisfatte le esigenze richieste per un sistema PNR svizzero. Le funzionalità mancanti potrebbero essere aggiunte in un secondo momento. I costi di progetto per quest'opzione ammontano a circa 11,6 milioni di franchi (di cui 6,82 mio. di spese con incidenza sul finanziamento) per il periodo 2020-2025.
- L'opzione 2, «Acquisto e sviluppo in proprio di una soluzione PNR», copre sul piano finanziario sia l'acquisto (OMC) e l'adeguamento di un sistema esistente sul mercato sia lo sviluppo in proprio di un sistema da parte della Confederazione. Poiché attualmente l'opzione 1 risulta quella prediletta e viene esaminata dettagliatamente, soltanto in caso di rinuncia a «goTravel» si procederà a verificare in maniera approfondita quali sistemi PNR

74 RS **281.1**

disponibili sul mercato potrebbero essere presi in considerazione o se la Confederazione debba sviluppare autonomamente un proprio sistema. I costi di progetto per l'opzione 2 ammontano per il periodo 2020-2026 a 22,5 milioni di franchi (di cui 16,82 mio. di spese con incidenza sul finanziamento). Conformemente all'articolo 21 della legge del 7 ottobre 2005[75] sulle finanze della Confederazione (LFC) sarebbe necessario richiedere un credito d'impegno.

A maggio 2022 sarà conclusa la valutazione del sistema ONU. A quel punto sarà chiaro se «goTravel» potrà essere integrato nell'ambiente informatico della Confederazione. Se la valutazione avrà un esito positivo si deciderà se adottare l'opzione 1 privilegiata o, in alternativa, l'opzione 2. In caso contrario l'opzione 1 sarà abbandonata in favore dell'opzione 2 che sarà elaborata in maniera più concreta.

Nel messaggio si provvederà a indicare in maniera più dettagliata i costi del progetto PNR svizzero.

In ogni caso, si potrà procedere allo sviluppo o all'adeguamento del sistema soltanto una volta che l'entrata in vigore della base legale sarà stata stabilita in maniera definitiva.

Costi di gestione del sistema di informazione PNR e dell'UIP a partire dal 2025

La gestione del sistema di informazione PNR e dell'infrastruttura PIU comporta costi, in particolare per la locazione di spazi, la manutenzione della struttura TIC (hardware, software, reti ecc.), per il mobilio e per le eventuali apparecchiature tecniche necessarie, nonché costi di ammortamento e per gli acquisti di sostituzione.

I costi concreti dell'infrastruttura e di gestione saranno calcolati ulteriormente nel corso del progetto.

Costi per il personale

Il fabbisogno di personale dell'UIP dipende dalla forma di gestione, dalle rotte aeree che verranno progressivamente introdotte nonché dalla quantità di dati da analizzare. Il fabbisogno di personale è stimato a 20 equivalenti a tempo pieno (ETP) e dovrebbe aumentare, una volta completata la creazione dell'UIP, a 30 ETP.

5.2 Ripercussioni per i Cantoni

Molte fattispecie penali che verranno contrastate in futuro tramite il PNR rientrano nella competenza in materia di perseguimento penale dei Cantoni. Con il sistema di informazione PNR la Confederazione intende fornire alle autorità cantonali di perseguimento penale gli strumenti necessari affinché possano ottenere in modo più semplice e rapido le informazioni che agevolano la prevenzione e la lotta contro le gravi forme di criminalità.

I Cantoni partecipano ai costi dell'UIP distaccando propri collaboratori e facendosi carico della loro retribuzione anche durante il loro impiego in seno all'UIP.

I dati PNR consentono alle autorità cantonali di perseguimento penale di ricevere informazioni su persone ricercate a livello nazionale e internazionale che giungono in

[75] RS **611.0**

Svizzera o sono in procinto di lasciare il Paese per via aerea. Ciò permette ai Cantoni, eventualmente in collaborazione con altre autorità, di adottare tempestivamente le misure necessarie. Con le proprie analisi mirate, l'UIP risponde a un'importante esigenza delle autorità di perseguimento penale. Grazie al sistema PNR i Cantoni non dovranno inoltre più sottoporre alle imprese di trasporto aereo le richieste, dispendiose in termini di tempo, relative al monitoraggio di itinerari utilizzati a scopo criminale. Il sistema dovrebbe infine fornire anche informazioni utili su reati non chiariti.

Nel complesso, la LDPA contribuisce notevolmente ad aumentare l'efficienza e l'efficacia del perseguimento penale e della prevenzione della criminalità, con ragguardevoli benefici anche per i Cantoni.

Ripercussioni finanziarie per i Cantoni

Un sistema PNR svizzero può funzionare efficacemente soltanto se i Cantoni partecipano alla sua gestione mettendo a disposizione il proprio personale. È pertanto previsto che la Confederazione e i Cantoni forniscano e finanzino i collaboratori in parti uguali. I restanti costi, compresi quelli di investimento e di gestione del sistema di informazione PNR, come pure gli altri costi di gestione dell'UIP sono a carico della Confederazione. Gli ulteriori dettagli sono oggetto di una convenzione tra Confederazione e Cantoni. La Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP) e la Conferenza dei comandanti delle polizie cantonali della Svizzera (CCPCS) sostengono la creazione di un sistema PNR nazionale e si dichiarano pronte a partecipare all'UIP mettendo a disposizione del personale. Una convenzione in questo senso sarà elaborata con i Cantoni nella fase di sviluppo del progetto a partire dall'inizio del 2022.

Oneri di tipo operativo

I Cantoni dovranno ugualmente riflettere in quale misura intendono integrare il trattamento dei dati PNR all'interno dei loro corpi di polizia e quali ripercussioni questa integrazione avrà sull'organizzazione e le risorse. Saranno pertanto chiamati a formare specialisti nei loro corpi di polizia incaricati di trasmettere all'UIP profili, liste d'osservazione e richieste di ricerca di buona qualità e a cooperare strettamente con l'UIP nel singolo caso.

Tuttavia saranno sempre le autorità competenti a dover decidere ed eseguire eventuali misure successive risultanti dall'analisi dei dati PNR.

Dato che la maggior parte delle prime misure sono adottate all'arrivo delle persone all'aeroporto, si stima che l'utilizzo dei dati dei passeggeri aerei comporterà oneri maggiori per i Cantoni che ospitano un aeroporto internazionale rispetto agli altri Cantoni. È pertanto necessario tener conto di questo aspetto.

5.3 Ripercussioni sull'economia e sulla società

La LDPA non comporta in linea di massima nuovi compiti amministrativi per le imprese di trasporto aereo. I dati dei passeggeri aerei sono infatti raccolti al momento della prenotazione dei biglietti aerei, a prescindere dalla presente legge. Inoltre, sono già utilizzati attualmente da oltre 60 Paesi in virtù di obblighi internazionali. La trasmissione dei dati PNR non rappresenta pertanto una novità assoluta per le imprese di trasporto aereo.

Il progetto ha come obiettivo principale il rafforzamento della sicurezza. Un'accresciuta sicurezza all'interno della società è una condizione fondamentale per il mantenimento e il rafforzamento della piazza economica svizzera. Va inoltre osservato che la trasmissione di dati PNR è sempre più una condizione necessaria per operare voli verso determinate destinazioni. Il fatto di restare inclusa nel traffico aereo internazionale riveste per la Svizzera una fondamentale importanza sul piano economico.

Il terrorismo e le forme gravi di criminalità destabilizzano una società e compromettono la fiducia nello Stato di diritto. Gli strumenti disponibili per contrastare tali reati contribuiscono in maniera significativa a uno sviluppo positivo della società.

Gli Stati Uniti che considerano l'utilizzo dei dati PNR come una condizione per restare nel suo «Visa Waiver Program», si attendono che la Svizzera faccia concreti passi avanti nell'introduzione di un sistema PNR nazionale. Tale programma permette ai cittadini di determinati Paesi, tra cui la Svizzera, di viaggiare negli Stati Uniti senza visto per motivi professionali o turistici e di soggiornarvi per un periodo massimo di 90 giorni. Un'esclusione della Svizzera dal «Visa Waiver Program» comporterebbe notevoli svantaggi per la Svizzera in quanto le persone che viaggiano per affari non potrebbero più fare ingresso facilmente negli USA, il che si ripercuoterebbe negativamente sulle relazioni commerciali tra i due Paesi.

Il trattamento di dati personali non fondato su un sospetto rappresenta un cambio paradigmatico per la Svizzera. Tuttavia, l'ingerenza nella sfera privata dei passeggeri aerei si limita principalmente al confronto dei dati con i sistemi di informazione di polizia ai sensi dell'articolo 7 capoverso 1 LDPA. L'obiettivo del PNR, ossia rafforzare la sicurezza dell'intera società, giustifica tale pratica.

6 Aspetti giuridici

6.1 Costituzionalità

La LDPA traccia le linee di un nuovo compito inerente alla politica di sicurezza e al traffico aereo.

Il trattamento dei dati dei passeggeri aerei, quale nuovo compito della Confederazione, è principalmente motivato dalla politica di sicurezza. La salvaguardia della sicurezza interna, compito comune della Confederazione e dei Cantoni (art. 57 cpv. 1 Cost.), resta prioritaria. La LDPA costituisce la base legale per la gestione di un sistema di informazione centrale che fornisca informazioni fondamentali per sostenere le competenti autorità della Confederazione e dei Cantoni nell'adempimento dei loro compiti di sicurezza. La ripartizione delle competenze tra la Confederazione e i Cantoni resta invariata. Alla luce di tali premesse è possibile confermare la costituzionalità della LDPA.

La LDPA è infine strettamente correlata al traffico aereo. Le imprese di trasporto aereo vengono infatti obbligate a trasmettere i dati e devono attendersi sanzioni in caso di violazioni degli obblighi. L'articolo 87 Cost. attribuisce alla Confederazione la competenza esclusiva a legiferare in materia di traffico aereo.

6.2 Compatibilità con gli impegni internazionali della Svizzera

Con la creazione dell'UIP e la regolamentazione del trattamento dei dati dei passeggeri aerei, la Svizzera attua, in qualità di membro dell'ONU, le risoluzioni vincolanti del Consiglio di sicurezza dell'ONU in materia di utilizzo di tali dati. Al contempo attua anche gli standard dell'OACI relativi all'aviazione svizzera e garantisce la permanenza del Paese nel «Visa Waiver Program» degli USA. Questo status importante è per il momento soltanto di natura provvisoria.

L'avamprogetto di LDPA è ispirato ampiamente alla direttiva PNR dell'UE, il che dovrebbe comportare vantaggi ai fini della conclusione di un accordo in materia con l'UE. Esso non ha tuttavia alcuna incidenza sull'accordo del 21 giugno 1999[76] tra la Confederazione Svizzera e la Comunità europea sul trasporto aereo.

6.3 Forma dell'atto

Il presente avamprogetto disciplina il trattamento dei dati dei passeggeri aerei, comprendenti anche i dati personali. Il confronto automatico dei dati dei passeggeri aerei con quelli contenuti nei diversi sistemi di informazione della Confederazione può sfociare in un trattamento ulteriore di dati personali degni di particolare protezione.

Il trattamento dei dati può intaccare il diritto costituzionale alla protezione della sfera privata dei passeggeri aerei, il che è consentito unicamente sulla base di una legge formale (art. 164 cpv. 1 lett. b Cost.).

La necessità di disporre di una legge federale è giustificata anche dal nuovo compito derivante per la Confederazione dall'attuazione della LDPA (art. 164 cpv. 1 lett. e Cost.).

6.4 Rispetto del principio di sussidiarietà e del principio dell'equivalenza fiscale

Secondo il principio di sussidiarietà, in uno Stato federale l'autorità territoriale sovraordinata può assumere un compito o parte di essi unicamente se è in grado di adempierli in modo manifestamente migliore rispetto alle autorità territoriali subordinate (art. 5*a* Cost.). Il principio di sussidiarietà parte implicitamente dal presupposto che l'adempimento dei compiti debba aver luogo per quanto possibile vicino ai cittadini e che questi possano in tal modo influire sul processo politico.

Nel presente caso non è opportuno che i Cantoni si organizzino per primi in vista del trattamento comune dei dati dei passeggeri aerei. Con la presente legge la Confederazione attua tre risoluzioni vincolanti dell'ONU nella misura in cui crea e gestisce un sistema di informazione centrale per il trattamento dei dati dei passeggeri aerei. Tale sistema è destinato in particolare alle autorità di perseguimento penale della Confederazione e dei Cantoni cui sono trasmesse spontaneamente o su richiesta informazioni preziose per l'esecuzione dei loro compiti. La prossimità con la popolazione non è rilevante per questo tipo di adempimento dei compiti. La necessità, per contro, di disporre di una soluzione uniforme costituisce un ulteriore motivo che giustifica l'attribuzione della competenza alla Confederazione (cfr. art. 43*a* cpv. 1 Cost).

76 RS **0.748.127.192.68**

Secondo il principio dell'equivalenza fiscale la comunità che fruisce di una prestazione statale ne assume i costi (art. 43*a* cpv. 2 Cost.).

Il trattamento dei dati dei passeggeri aerei comporta vantaggi sia per la sua portata nazionale sia sul piano concreto per le autorità della Confederazione e dei Cantoni. Una fatturazione specifica ai singoli Cantoni genererebbe oneri considerevoli. Da qui la soluzione pragmatica proposta che i Cantoni mettano a disposizione a loro spese la metà dei collaboratori necessari per il trattamento dei dati dei passeggeri aerei.

6.5 Delega di competenze legislative

L'*articolo 2 capoverso 4* conferisce a fedpol la competenza di precisare, se del caso, a livello d'ordinanza gli standard industriali OACI, OMD e IATA.

L'*articolo 6 capoverso 4* dell'avamprogetto prevede che il Consiglio federale specifichi in un'ordinanza i reati gravi di cui all'articolo 6 capoverso 3 lettera b. Come già spiegato nei commenti a questa disposizione, non si tratta di una delega delle competenze legislative. I reati gravi sono infatti già definiti con chiarezza dall'articolo 6 capoverso 3 lettera b. La concretizzazione delle fattispecie penali serve unicamente alla trasparenza e alla certezza del diritto.

Conformemente all'*articolo 9 capoverso 6* il Consiglio federale definisce ugualmente a livello d'ordinanza i reati determinanti che autorizzano al trattamento ulteriore di dati dei passeggeri aerei nel caso in cui dal confronto con una lista d'osservazione sia emersa una corrispondenza. L'accento è posto sui reati terroristici e quelli correlati alla criminalità organizzata.

L'*articolo 16 capoverso 2* sancisce che il Consiglio federale fissa in un'ordinanza la durata massima di conservazione dei dati risultanti da un confronto. A differenza dei dati dei passeggeri aerei (art. 16 cpv. 1), non è opportuno limitare la durata di conservazione delle corrispondenze di dati dei passeggeri aerei generate da un confronto con i sistemi di informazione di polizia o con i profili di rischio e le liste d'osservazione. In caso contrario si può incorrere nel rischio, a seconda della situazione, che i dati vengano cancellati prima della conclusione di un procedimento. La disponibilità di tali dati deve essere infatti garantita durante un procedimento in corso. La fissazione della durata di conservazione a livello d'ordinanza crea il margine di manovra necessario.

La Costituzione federale non considera le convenzioni contenenti norme di diritto concluse tra la Confederazione e i Cantoni come una forma di atto legislativo a sé stante (cfr. art. 163 Cost.). Occorre pertanto che le condizioni quadro della convenzione siano almeno stabilite da una legge federale (art. 164 Cost.) o, in caso di disposizioni di importanza secondaria, da un'ordinanza. Soltanto in presenza di questa base legale sarà possibile stipulare una convenzione con i Cantoni[77]. Per tale ragione l'*articolo 20 capoverso 5* attribuisce al Consiglio federale la possibilità di stabilire in un'ordinanza le condizioni quadro per una convenzione con i Cantoni in merito al distacco di collaboratori e al loro impiego presso l'UIP.

In virtù dell'*articolo 21 capoverso 1* il Consiglio federale ha la facoltà di concludere autonomamente trattati internazionali sul trattamento dei dati dei passeggeri aerei.

77 BSK BV-Waldmann/Schnyder von Wartensee, art. 48 n. 37

Come parti contraenti entrano in linea di conto esclusivamente gli Stati che garantiscono una protezione dei dati equiparabile a quella della Svizzera. fedpol può concludere convenzioni su aspetti operativi, tecnici o amministrativi a complemento di questi trattati (art. 21 cpv. 2).

6.6 Protezione dei dati

La LDPA s'ispira in toto alla legge del 25 settembre 2020[78] sulla protezione dei dati (nLPD), la cui entrata in vigore è prevista nel 2023. Nel messaggio del 15 settembre 2017[79] il Consiglio federale ha spiegato che la nLPD si prefigge di rafforzare le disposizioni sulla protezione dei dati per far fronte alla rapidissima evoluzione tecnologica. La LDPA è in linea con questo adeguamento del diritto federale in materia di protezione dei dati. Si tratta di un aspetto particolarmente importante dal momento che la protezione dei dati riveste un ruolo centrale nel trattamento dei dati ai sensi della LDPA.

Il set di dati dei passeggeri aerei comprende diverse categorie. A essere rilevanti per la protezione dei dati sono in primis i dati personali. Si tratta di tutte le informazioni concernenti una persona fisica identificata o identificabile (art. 5 lett. a nLPD). Fanno parte di questi dati il nome, il numero di telefono, l'indirizzo del domicilio e l'indirizzo di posta elettronica. In seguito a un confronto con diversi sistemi di informazione della Confederazione (cfr. art. 7 cpv. 1) possono risultare anche dati personali degni di particolare protezione. Secondo la LDPA, questi dati possono essere trattati soltanto se sono di natura biometrica o, al limite, se concernono procedimenti e sanzioni amministrativi e penali. Tutti gli altri dati personali degni di particolare protezione che dovessero emergere in occasione del trattamento dei dati dei passeggeri aerei devono essere cancellati immediatamente (art. 6 cpv. 5).

I dati dei passeggeri aerei possono essere trattati soltanto per gli scopi previsti dalla legge (art. 6 cpv. 4 nLPD), ossia, nel caso della LDPA, esclusivamente per la lotta ai reati terroristici e ad altri reati gravi (art. 6 cpv. 1). I risultati che non sono conformi a questo scopo sono cancellati immediatamente (art. 6 cpv. 5).

Se sono trattati dati personali occorre accertarsi della loro esattezza (art. 6 cpv. 5 nLPD). L'UIP è tenuta a verificare manualmente ciascuna corrispondenza ottenuta dal confronto dei dati dei passeggeri aerei con i sistemi di informazione della Confederazione e ad accertarne la plausibilità (art. 7 cpv. 3).

I dati dei passeggeri aerei sono confrontati con quelli dei sistemi di informazione della Confederazione in due diverse tappe (art. 7 cpv. 1 e 3). In una prima fase vengono confrontati tutti i dati disponibili. Soltanto i dati che corrispondono a quelli contenuti nei sistemi di informazione e che sono pertanto fondati su primi sospetti sono trattati ulteriormente. La loro plausibilità è verificata manualmente e, se del caso, anche tramite accesso mirato a ulteriori sistemi di informazione della Confederazione. Questa seconda fase del trattamento intende innanzitutto garantire l'esattezza della corrispondenza nonché la sua conformità con lo scopo legale del trattamento stesso.

78 FF **2020** 6695
79 FF **2017** 5939

Le corrispondenze che non presentano alcun nesso con i reati terroristici o altri reati gravi di cui all'articolo 6 capoversi 2 e 3 sono cancellati immediatamente. In virtù di questa procedura a due fasi, i dati dei passeggeri aerei possono essere trattati soltanto nella misura in cui ciò sia necessario allo scopo della legge e a garantire l'esattezza dei dati.

La sicurezza dei dati dei passeggeri aerei viene accresciuta dopo sei mesi dalla loro ricezione nel sistema di informazione PNR grazie alla loro pseudonimizzazione (art. 14). Secondo il messaggio sulla revisione totale della legge sulla protezione dei dati, la pseudonimizzazione rappresenta un provvedimento tecnico appropriato per garantire la sicurezza dei dati (art. 8 nLPD)[80]. Nel medesimo messaggio il Consiglio federale dichiara inoltre che la LPD non si applica ai dati

> «che sono stati resi anonimi e la cui identificazione da parte di un terzo è impossibile (i dati sono stati anonimizzati in modo completo e definitivo) o sarebbe possibile soltanto con uno sforzo che nessun interessato è disposto a fare. Tale regola vale anche per i dati pseudonimizzati[81].»

80 Messaggio del 15 settembre 2017 concernente la legge federale relativa alla revisione totale della legge sulla protezione dei dati e alla modifica di altri atti normativi sulla protezione dei dati, FF **2017** 5939, in particolare 6021

81 FF **2017** 5939, in particolare 6011

Allegato

A. Reati terroristici ai sensi dell'articolo 6 capoverso 2

Reati terroristici ai sensi degli articoli 1–4 della decisione quadro 2002/475/GAI	**Applicabile in caso di matrice terroristica:** Pubblica intimidazione; pubblica istigazione a un crimine o alla violenza; sommossa; atti preparatori punibili; organizzazioni criminali e terroristiche; messa in pericolo della sicurezza pubblica con armi; finanziamento del terrorismo; reclutamento, addestramento e viaggi finalizzati alla commissione di un reato di terrorismo; associazioni illecite (art. 258, 259, 260 cpv. 1, 260bis, 260ter, 260^{quater}, 260^{quinquies}, 260^{sexies}, 275ter CP) Divieto di organizzazioni (art. 74 della legge federale sulle attività informative[82]) Disposizioni penali della legge federale del 12 dicembre 2014[83] che vieta i gruppi «Al-Qaïda» e «Stato islamico» nonché le organizzazioni associate (art. 2)

B. Reati gravi ai sensi dell'articolo 6 capoverso 3 lettera a

Allegato II della direttiva PNR	**Reati considerati dal diritto svizzero[84]**
Partecipazione a un'organizzazione criminale	Organizzazioni criminali e terroristiche (art. 260ter CP)
Tratta di esseri umani	Matrimonio forzato, unione domestica registrata forzata; tratta di esseri umani (art. 181*a*, 182 cpv. 1, 2 e 4 CP)
Sfruttamento sessuale di minori e pedopornografia	Esposizione a pericolo dello sviluppo di minorenni: atti sessuali con fanciulli, promovimento della prostituzione, pornografia (art. 187 n. 1, 195 lett. a e art. 197 cpv. 4 CP)
Traffico illecito di stupefacenti e sostanze psicotrope	Disposizioni penali della legge sugli stupefacenti[85] (art. 19 cpv. 2 e 20 cpv. 2 LStup)

82 RS **121**
83 RS **122**
84 Reati di cui all'allegato I della legge sullo scambio di informazioni con gli Stati Schengen (RS **362.2**), per i quali è comminata una pena detentiva superiore a tre anni.
85 RS **812.121**

Allegato II della direttiva PNR	Reati considerati dal diritto svizzero[84]
Traffico illecito di armi, munizioni ed esplosivi	Messa in pericolo della sicurezza pubblica con armi (art. 260^{quater} CP)
	Delitti e crimini ai sensi della legge sulle armi[86] (art. 33 cpv. 3 LArm)
Corruzione	Corruzione attiva; corruzione passiva; corruzione di pubblici ufficiali stranieri (art. 322ter, 322^{quater}, 322^{septies} CP)
Frode	Truffa; abuso di un impianto per l'elaborazione di dati; abuso di carte-chèques o di credito; contraffazione di merci; bancarotta fraudolenta e frode nel pignoramento (art. 146 cpv. 1 e 2, 147 cpv. 1 e 2, 148, 155 n. 2, 163 n. 1 CP)
	Truffa in materia di prestazioni e di tasse (art. 14 cpv. 4 della legge federale sul diritto penale amministrativo[87])
Riciclaggio di proventi di reato e falsificazione di monete	Contraffazione di monete; alterazione di monete; importazione, acquisto e deposito di monete false, riciclaggio di denaro (art. 240 cpv. 1, 241 cpv. 1, 244 cpv. 2, 305bis n. 2 CP)
Criminalità informatica/cibercriminalità	Acquisizione illecita di dati; danneggiamento di dati; abuso di un impianto per l'elaborazione di dati (art. 143, 144bis cpv. 3, 147 cpv. 1 e 2 CP)
Criminalità ambientale, compresi il traffico illecito di specie animali protette e il traffico illecito di specie e di essenze vegetali protette	Irradiazione ingiustificata di persone (art. 43 cpv. 2 della legge sulla radioprotezione[88])
Favoreggiamento dell'ingresso e del soggiorno illegali	Incitazione all'entrata, alla partenza o al soggiorno illegali (art. 116 cpv. 1 lett. a, a^{bis} e c in combinato disposto con cpv. 3 della legge sugli stranieri e la loro integrazione[89])
Omicidio volontario, lesioni personali gravi	Omicidio intenzionale; assassinio; omicidio passionale; lesioni gravi; mutilazione di organi genitali femminili (art. 111, 112, 113, 122, 124 CP)

86 RS **514.54**
87 RS **313.0**
88 RS **814.50**
89 RS **142.20**

Allegato II della direttiva PNR	Reati considerati dal diritto svizzero[84]
Traffico illecito di organi e tessuti umani	Crimini ai sensi della legge sui trapianti[90] (art. 69 cpv. 2)
	Crimini ai sensi della legge sulle cellule staminali[91] (art. 24 cpv. 3 LCel)
Rapimento, sequestro e presa di ostaggi	Estorsione; sequestro di persona e rapimento; circostanze aggravanti di un sequestro di persona o di un rapimento; presa d'ostaggio; atti compiuti senza autorizzazione per conto di uno Stato estero (art. 156, 183, 184, 185, 271 n. 2 e 3 CP)
Furto organizzato e rapina a mano armata	Furto; rapina (art. 139 n. 3, 140 CP)
Traffico illecito di beni culturali, compresi oggetti d'antiquariato e opere d'arte	---
Contraffazione e pirateria di prodotti	Contraffazione di merci (art. 155 n. 2 CP)
	Violazione del diritto al marchio; uso fraudolento del marchio; uso, contrario al regolamento, di un marchio di garanzia o di un marchio collettivo; uso di indicazioni di provenienza non pertinenti (art. 61 cpv. 3, 62 cpv. 2, 63 cpv. 4, 64 cpv. 2 della legge sulla protezione dei marchi[92])
	Violazione del diritto di design (art. 41 cpv. 2 della legge sul design[93])
	Violazione del diritto d'autore; lesione di diritti di protezione affini (art. 67 cpv. 2, 69 cpv. 2 della legge sul diritto d'autore[94])
	Violazione del brevetto (art. 81 cpv. 3 della legge sui brevetti[95])
Falsificazione di atti amministrativi e traffico di documenti falsi	Falsificazione dei pesi e delle misure; monete e bolli di valore esteri; falsità in documenti; conseguimento fraudolento di una falsa attestazione; documenti esteri; falsità in atti formati da pubblici ufficiali o funzionari (art. 248, 250, 251 n. 1, 253, 255, 317 n. 1 CP)

90 RS **810.21**
91 RS **810.31**
92 RS **232.11**
93 RS **232.12**
94 RS **231.1**
95 RS **232.14**

Allegato II della direttiva PNR	**Reati considerati dal diritto svizzero[84]**
Traffico illecito di sostanze ormonali e altri fattori di crescita	Disposizioni penali della legge sulla promozione dello sport[96] (art. 22 cpv. 2 LPSpo) Crimini ai sensi della legge sugli agenti terapeutici[97] (art. 86 cpv. 2 e 3 LATer)
Traffico illecito di materie nucleari o radioattive	Pericolo dovuto all'energia nucleare, alla radioattività e a raggi ionizzanti; atti preparatori punibili (art. 226bis, 226ter CP) Inosservanza di provvedimenti di sicurezza interna ed esterna; infrazioni con beni nucleari e scorie radioattive (art. 88 cpv. 2 e 89 cpv. 2 della legge federale sull'energia nucleare[98])
Stupro	Violenza carnale (art. 190 CP)
Reati che rientrano nella competenza giurisdizionale della Corte penale internazionale	Genocidio; crimini contro l'umanità; gravi violazioni delle Convenzioni di Ginevra; attacchi contro persone e beni di carattere civile; trattamento medico ingiustificato, lesione dell'autodeterminazione sessuale e della dignità umana; reclutamento e impiego di bambini-soldato; metodi di guerra vietati; impiego di armi vietate (art. 264, 264*a*, 264*c*–*h* CP)
Dirottamento di aeromobile/nave	Estorsione; sequestro di persona e rapimento; presa d'ostaggio (art. 156, 183, 185 CP)
Sabotaggio	Danneggiamento; incendio intenzionale; esplosione; uso delittuoso di materie esplosive o gas velenosi; fabbricazione, occultamento e trasporto di materie esplosive o gas velenosi; inondazione, franamento; danneggiamento d'impianti elettrici, di opere idrauliche e di opere di premunizione (art. 144 cpv. 3, 221 cpv. 1 e 2, 223 n. 1, 224 cpv. 1, 226, 227 n. 1, 228 n. 1 CP)
Traffico di veicoli rubati	Ricettazione (art. 160 CP)
Spionaggio industriale	---

96 RS **415.0**
97 RS **812.21**
98 RS **732.1**

C. Reati gravi ai sensi dell'articolo 6 capoverso 3 lettera b

Reati il cui perseguimento penale compete all'Ufficio federale della dogana e della sicurezza dei confini (UDSC) e per i quali è comminata una pena detentiva massima di almeno tre 3 anni

1. Truffa in materia di prestazioni e di tasse; falsità in documenti; conseguimento fraudolento di una falsa attestazione; soppressione di documenti; favoreggiamento (art. 14 cpv. 4, 15, 16 cpv. 1 e 17 n. 1 della legge federale sul diritto penale amministrativo [DPA][99]).
2. I reati seguenti, nella misura in cui il loro perseguimento penale compete all'UDSC e sono correlati a un reato preliminare per il quale è comminata una pena detentiva massima di almeno tre anni:
   art. 37 della legge federale sull'imposizione degli autoveicoli (LIAut)[100];
   art. 39 della legge federale sull'imposizione degli oli minerali (LIOm)[101].
3. Gli ulteriori reati seguenti:

   art. 36 cpv. 2 in combinato disposto con art. 40 LIAut;

   art. 38 cpv. 2 in combinato disposto con art. 42 LIOm;

   art. 86 cpv. 1, 2, 3 in combinato disposto con art. 90 cpv. 1 della legge sugli agenti terapeutici (LATer)[102]

   art. 26 cpv. 2 in combinato disposto con art. 27 della legge sulla circolazione delle specie di fauna e di flora protette (LF-CITES)[103];

   art. 63 cpv. 1 e 2 in combinato disposto con art. 65 della legge sulle derrate alimentari (LDerr)[104];

   art. 26 cpv. 1 in combinato disposto con art. 31 cpv. 3 della legge federale sulla protezione degli animali (LPAn)[105].

99 RS **313.0**
100 RS **641.51**
101 RS **641.61**
102 RS **812.21**
103 RS **453**
104 RS **817.0**
105 RS **455**

Glossario

Dati API	Dati che le imprese di trasporto aereo devono trasmettere a uno Stato prima della partenza di determinati voli (API: «Advance Passenger Information»). In Svizzera i dati API sono disciplinati dagli articoli 104 e 104*a* della legge federale sugli stranieri e la loro integrazione (RS *142.20*). *Rilevanza per il PNR: i dati API costituiscono una categoria di dati all'interno del set di dati PNR*
Trattamento di dati	Qualsiasi operazione relativa a dati personali, indipendentemente dai mezzi e dalle procedure impiegati, segnatamente la raccolta, la registrazione, la conservazione, l'utilizzazione, la modificazione, la comunicazione, l'archiviazione, la cancellazione o la distruzione di dati. *Rilevanza per il PNR: la legge sui dati dei passeggeri aerei prevede il trattamento di dati per combattere il terrorismo e altri reati gravi e disciplina la loro protezione in modo complementare alla legge sulla protezione dei dati.*
Dati personali degni di particolare protezione	→ Dati personali che possono essere trattati soltanto a determinate condizioni. Sono considerati degni di particolare protezione: 1. i dati concernenti le opinioni o attività religiose, filosofiche, politiche o sindacali; 2. i dati concernenti la salute, la sfera intima oppure l'appartenenza a una razza o a un'etnia; 3. i dati genetici; 4. i → dati biometrici; 5. i dati concernenti i procedimenti o le sanzioni amministrativi e penali; 6. i dati concernenti le misure di assistenza sociale.

	Rilevanza per il PNR: dati personali degni di particolare protezione possono risultare dal confronto dei dati dei passeggeri aerei con altri sistemi d'informazione della Confederazione o dall'accesso a questi sistemi nell'intenzione di rendere plausibili i dati. Il presente avamprogetto di legge sui dati dei passeggeri aerei autorizza tuttavia il loro trattamento soltanto se si tratta di → dati biometrici o di dati concernenti procedimenti o sanzioni amministrativi e penali (cfr. art. 6 cpv. 6). Tutti gli ulteriori dati personali degni di particolare protezione vanno cancellati immediatamente.
Dati biometrici	Dati personali relativi a caratteristiche fisiche, fisiologiche e comportamentali di un individuo ottenuti tramite un processo tecnico specifico e che permettono di identificare univocamente una persona o di confermarne l'identificazione. Si tratta ad esempio di impronte digitali, immagini del viso o dell'iride o registrazioni della voce. I dati biometrici sono considerati → dati personali degni di particolare protezione che possono essere trattati soltanto a determinate condizioni. *Rilevanza per il PNR: il trattamento dei dati dei passeggeri aerei può produrre dati biometrici in caso di confronto con i dati dei sistemi d'informazione o di accesso a tali sistemi. Il servizio competente è autorizzato a trattare questi dati per gli scopi definiti dalla legge.*
Set di dati	Diversi dati collegati da un nesso logico e consecutivi di lunghezza fissa o variabile. *Rilevanza per il PNR: il set di dati di un passeggero aereo si compone di 19 categorie di dati, raccolte in occasione della prenotazione di un biglietto aereo. Di norma a ogni passeggero aereo corrisponde un set di dati. Sempre più*

	Stati utilizzano tali set di dati per combattere il terrorismo e altri reati gravi. La Svizzera intende sancire il trattamento di questi set di dati nella legge sui dati dei passeggeri aerei, il cui avamprogetto sarà inviato in procedura di consultazione nella prima metà del 2022.
anonimizzare	Sinonimo di → pseudonimizzare *Rilevanza per il PNR: mentre la direttiva PNR dell'UE utilizza la nozione di anonimizzare, il pertinente decreto legislativo dell'Italia impiega invece la nozione di pseudonimizzare.*
pseudonimizzare	I dati sono da considerarsi pseudonimizzati quando è loro attribuito uno pseudonimo e non possono più essere attribuiti a una persona specifica. La pseudonimizzazione può essere revocata da un servizio legittimato sostituendo lo pseudonimo con il nome corrispondente. A partire da quel momento i dati possono di nuovo essere attribuiti alla persona in questione. La tavola delle concordanze permette di ricollegare uno pseudonimo alla persona specifica. Ciononostante, i dati pseudonimizzati sono ancora considerati dati personali ai sensi della protezione dei dati, fintanto che la tavola delle concordanze è ancora disponibile. *Rilevanza per il PNR: i dati dei passeggeri aerei trattati in Svizzera conformemente alla legge sui dati dei passeggeri aerei, sono pseudonimizzati automaticamente dopo sei mesi. La decisione sull'eventuale revoca della pseudonimizzazione spetta al Tribunale amministrativo federale.*
Dati personali	Indicazioni concernenti una persona fisica identificata o identificabile. Una persona fisica è identificabile se può essere identificata direttamente o indirettamente, ad esempio tramite le informazioni risultanti dalle circostanze o dal contesto (numero d'identificazione, dati di

	localizzazione, elementi specifici riguardanti le sue caratteristiche fisiche, fisiologiche, genetiche, psichiche, economiche, culturali o sociali). L'identificazione può avvenire in base a un solo elemento (numero di telefono, numero dell'immobile, numero AVS, impronte digitali) o correlando varie informazioni (indirizzo, data di nascita e stato civile). La mera possibilità teorica che qualcuno possa essere identificato non è sufficiente per supporre che sia identificabile. I dati personali comprendono anche i → dati personali degni di particolare protezione per i quali il diritto in materia di protezione dei dati sancisce una protezione maggiore. *Rilevanza per il PNR: il set di dati del passeggero aereo che le imprese di trasporto aereo sono tenute a trasmettere all'UIP, contiene anche dati personali, ma non quelli degni di particolare protezione. Qualora dovessero comunque essere trasmessi quelli degni di particolare protezione, l'UIP è obbligato per legge a cancellarli.*
Visa Waiver Program	Il programma di esenzione dal visto («Visa Waiver Program») permette ai cittadini di determinati Paesi di recarsi negli Stati Uniti senza visto per motivi professionali o turistici (scopo del viaggio «visita») per una durata massima di 90 giorni. *Rilevanza per il PNR: per continuare a far parte del Visa Waiver Program degli Stati Uniti, la Svizzera è tenuta a introdurre una normativa sul PNR.*