23.xxx

Messaggio concernente la legge sui dati dei passeggeri aerei

del …

Onorevoli presidenti e consiglieri,

con il presente messaggio vi sottoponiamo, per approvazione, il disegno di legge sui dati dei passeggeri aerei.

Gradite, onorevoli presidenti e consiglieri, l'espressione della nostra alta considerazione.

…

In nome del Consiglio federale svizzero:

La presidente della Confederazione, Viola Amherd
Il cancelliere della Confederazione, Viktor Rossi

Compendio

Il presente disegno di legge intende consentire alla Svizzera di trattare, al pari di numerosi altri Paesi, in modo sistematico i dati dei passeggeri aerei allo scopo di sostenere le autorità federali e cantonali nella lotta alle gravi forme di criminalità.

Situazione iniziale

Negli ultimi decenni il numero di passeggeri nel traffico aereo è cresciuto vistosamente su scala globale. Un siffatto incremento rappresenta una sfida non solo per l'infrastruttura degli aeroporti, ma anche per le autorità incaricate dei controlli all'ingresso e alla partenza dal territorio nazionale. Finita la fase delle restrizioni ai viaggi dovute alla pandemia da COVID-19, secondo i dati provvisori forniti dall'Ufficio federale dell'aviazione civile già nel 2023 sono stati registrati nuovamente più di 53 milioni di passeggeri partiti dalla Svizzera o giunti in Svizzera a bordo di voli charter o di linea.

Malgrado questo numero elevato di passeggeri in entrata e in uscita dal Paese, deve essere sempre possibile identificare le persone che si servono del traffico aereo per perseguire i loro scopi criminali, soprattutto quando si tratta di gravi forme di criminalità, quali i reati terroristici e altri reati gravi.

Il terrorismo e le gravi forme di criminalità hanno spesso carattere transfrontaliero.

Per tale ragione, 69 Paesi utilizzano già attualmente le informazioni sui passeggeri aerei quale strumento di lotta alle gravi forme di criminalità.

Al momento dell'acquisto di un biglietto aereo vengono raccolti dati dei passeggeri aerei di cui le imprese di trasporto aereo hanno bisogno 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), è composto di 19 categorie di dati e contiene tra l'altro il nome e l'indirizzo dei passeggeri come pure informazioni relative ai loro bagagli e alle modalità di pagamento.

Il trattamento dei dati dei passeggeri aerei permette di individuare non solo persone già note alle autorità di perseguimento penale, ma anche persone che, per quanto risultino ancora sconosciute, presentano un legame con le gravi forme di criminalità. Ciò permette, ad esempio, di riscontrare combinazioni di dati che ricorrono frequentemente in relazione alla tratta di esseri umani o al traffico di stupefacenti.

Attualmente l'utilizzo del PNR viene promosso in tutto il mondo. Tre risoluzioni del Consiglio di sicurezza dell'ONU, vincolanti anche per la Svizzera, impongono alla comunità internazionale di trattare i dati dei passeggeri aerei ai fini della prevenzione del terrorismo.

Con la direttiva (UE) 2016/681, l'Unione europea 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 dal suo territorio verso l'UE e viceversa sono tenute a comunicare i dati PNR dei loro passeggeri.

Se è vero che oggi i dati PNR dei voli operati dalla Svizzera sono comunicati agli Stati membri dell'UE, al Regno Unito, alla Norvegia e agli Stati Uniti, è altresì vero che la Svizzera, dal canto suo, non può trattare in modo sistematico tali dati fintanto che non disporrà di una base giuridica e di un sistema PNR nazionale.

Senza un sistema PNR, la Svizzera, a differenza degli altri Stati Schengen, non può contare su informazioni essenziali per la salvaguardia della sicurezza pubblica concernenti persone che fanno ingresso sul suo territorio e quindi nello spazio Schengen.

Per giunta, sempre più Stati minacciano le imprese di trasporto aereo svizzere, in assenza di una comunicazione dei dati PNR, di infliggere loro pene pecuniarie ingenti e persino di revocare loro i diritti di atterraggio. Ciò avrebbe conseguenze esiziali sul piano economico.

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 Stati Uniti senza visto, per turismo o affari, per una durata massima di 90 giorni.

Contenuto del progetto

La legge sui dati dei passeggeri aerei (LDPA) costituisce la base giuridica che autorizza la Confederazione a trattare i dati dei passeggeri aerei. Il PNR permetterà alla Svizzera di sapere se un passeggero aereo è potenzialmente pericoloso o se è ricercato, prima che entri nel Paese o che lo lasci. Sulla scorta di queste informazioni, le autorità competenti, in particolare quelle di polizia e di perseguimento penale, decideranno se il passeggero in questione deve essere sottoposto a un esame approfondito o addirittura arrestato.

Un nuovo servizio, collocato in seno all'Ufficio federale di polizia (fedpol) e denominato «unità d'informazione sui passeggeri» (UIP) tratterà i dati dei passeggeri aerei a beneficio delle autorità competenti. 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. Non appena registrati, questi dati vengono automaticamente confrontati con diversi sistemi d'informazione di polizia nonché con i profili di rischio e le liste d'osservazione.

Dopo aver verificato manualmente le corrispondenze così ottenute, l'UIP le comunica alle autorità competenti della Confederazione e dei Cantoni, affinché possano adottare tempestivamente le misure necessarie. Il catalogo dei

reati allegato alla LDPA riporta le fattispecie penali che giustificano la comunicazione dei dati dei passeggeri aerei a un'autorità.

Conformemente ai risultati della consultazione, il disegno di LDPA tiene conto di diversi elementi chiave definiti dalla Corte di giustizia dell'UE nella sua sentenza, segnatamente la durata di conservazione ridotta per i dati dei passeggeri aerei che non presentano alcun indizio di gravi forme di criminalità e lo snellimento del catalogo dei reati.

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

Utilità dei dati PNR nella lotta al terrorismo e alle gravi forme di criminalità: esempi

Esempio 1: impedire l'entrata nel Paese in caso di sospetto di terrorismo

La signora X prenota su Internet un volo da una città canadese verso la Svizzera, indicando le informazioni richieste per la prenotazione, tra cui il suo nome, i suoi dati di contatto e la sua data di nascita.

La compagnia aerea trasmette queste informazioni in un periodo compreso tra le 48 e le 24 ore prima del volo alle UIP del Paese di partenza e di destinazione.

Le UIP procedono a un confronto automatico di questi dati con i sistemi d'informazione di polizia cui hanno accesso. Nel quadro di tale confronto l'UIP svizzera ottiene una corrispondenza. Gli specialisti dell'UIP verificano quindi, per sicurezza, la corrispondenza manualmente per accertarne la fondatezza. Il risultato: la signora X è registrata nel Sistema d'informazione Schengen (SIS) per sostegno e appartenenza a un'organizzazione terroristica.

L'UIP trasmette in seguito la corrispondenza all'autorità competente in Svizzera (di norma una polizia cantonale o fedpol). L'autorità svizzera competente invia senza indugio una richiesta alle autorità del Paese di partenza allo scopo di impedire che la signora X possa imbarcarsi sul volo verso la Svizzera.

Il giorno successivo la signora X si reca all'aeroporto per prendere il volo. Non avendo con sé alcun bagaglio, si dirige direttamente al gate. Al momento dell'imbarco, la polizia ferma la signora X, le impedisce di salire a bordo dell'aereo e la trae in arresto.

I dati PNR permettono di identificare persone nei sistemi d'informazione di polizia prima che possano imbarcarsi su un volo nonché di rafforzare la cooperazione internazionale di polizia.

Esempio 2: prevenire la tratta di esseri umani a fini di sfruttamento sessuale

Una polizia cantonale sta indagando su un trafficante di esseri umani. È al corrente del fatto che un collegamento aereo da una città dell'Europa dell'Est

verso Zurigo viene regolarmente utilizzato per far entrare in Svizzera giovani donne a fini di sfruttamento sessuale. Le donne sono accompagnate da una persona la cui identità è ancora ignota. La polizia cantonale sa anche che i biglietti aerei sono prenotati sempre presso la stessa agenzia di viaggio con la stessa carta di credito. Il sospetto è che l'accompagnatore sia un trafficante di esseri umani e che si tratti della medesima persona che acquista i biglietti per sé e le giovani donne presso l'agenzia di viaggi pagando con la carta di credito.

La polizia cantonale contatta l'UIP, chiedendole di introdurre i dati attualmente noti dell'accompagnatore, ossia numero di carta di credito e agenzia di viaggio, in una lista d'osservazione. L'UIP verifica la richiesta e si impegna da quel momento in poi a confrontare i dati dei passeggeri che si recano in aereo dalla città dell'Europa dell'Est in questione a Zurigo con la lista d'osservazione.

Trascorse alcune settimane, l'UIP osserva una corrispondenza tra un passeggero e la lista d'osservazione. Verifica pertanto la corrispondenza manualmente e inoltra in seguito l'informazione alla polizia cantonale. La polizia cantonale è pronta a intervenire: l'uomo dall'identità ancora ignota verrà fermato al momento dell'ingresso nel Paese e interrogato. L'interrogatorio e altre indagini confermeranno il sospetto che si tratti di un trafficante di esseri umani.

La polizia cantonale chiede a questo punto all'UIP di verificare se negli ultimi sei mesi l'uomo abbia viaggiato sulla stessa rotta insieme ad altre giovani donne. L'incaricato della protezione dei dati dell'UIP verifica se la richiesta soddisfa tutte le condizioni legali e la inoltra successivamente al Tribunale amministrativo federale. Quest'ultimo decide che è lecito accedere ai dati relativi ai voli in questione degli ultimi sei mesi e consultarli.

L'UIP effettua consultazioni individuali da cui emerge che l'uomo negli ultimi sei mesi ha viaggiato più volte su questa rotta insieme ad altre potenziali vittime.

Queste informazioni supplementari permetteranno alla polizia cantonale di condurre indagini in modo mirato e di identificare altre vittime, liberandole dalle grinfie della rete di trafficanti di esseri umani.

I dati PNR possono contribuire a individuare e prevenire la tratta di esseri umani e a proteggerne le vittime.

Indice

Messaggio

1 Situazione iniziale

1.1 Panoramica

Chi prenota un volo mette a disposizione delle imprese di trasporto aereo direttamente oppure indirettamente, tramite l'agenzia di viaggio, svariate informazioni che sono in seguito conservate nel rispettivo sistema di prenotazione anche dopo la conclusione del viaggio. Tali informazioni 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, sul numero di bagagli o su altre persone che viaggiano con lui. Questi dati costituiscono il cosiddetto set di dati dei passeggeri aerei, denominato anche «Passenger Name Record», in breve PNR.

Attualmente 69 Paesi chiedono alle imprese di trasporto aereo questi dati al fine di disporre di informazioni su persone ricercate a livello nazionale o internazionale in relazione al terrorismo o ad altri reati gravi (gravi forme di criminalità), prima che entrino o partano dal loro territorio. Ulteriori Stati sono in procinto di introdurre l'utilizzo dei dati PNR.

Inoltre, tre risoluzioni[1] del Consiglio di sicurezza dell'ONU, vincolanti anche per la Svizzera, sollecitano gli Stati membri a rafforzare le proprie capacità per raccogliere, diffondere e analizzare i dati PNR e a utilizzare questi ultimi per la lotta al terrorismo.

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 lotta ai reati di terrorismo e sostiene gli Stati nella creazione di un sistema PNR nazionale.

Con la direttiva (UE) 2016/681[2] (direttiva PNR) l'UE impone agli Stati membri di creare sistemi PNR nazionali. La direttiva non costituisce uno sviluppo dell'acquis di Schengen e non è pertanto giuridicamente vincolante per la Svizzera. Tuttavia la Svizzera è interessata dalla sua trasposizione, dato che

1 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.

2 Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dai 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.

le imprese di trasporto aereo vengono obbligate a trasmettere dati PNR per i voli operati dalla Svizzera verso l'UE.

Anche la Svizzera intende in futuro servirsi dei dati PNR per combattere le gravi forme di criminalità. La necessaria base giuridica sarà introdotta con la presente legge. La Svizzera potrà così soddisfare i propri obblighi internazionali e fornire un contributo significativo, a livello nazionale e internazionale, nella lotta alle gravi forme di criminalità.

Le imprese di trasporto aereo svizzere trasmettono già oggi i dati PNR relativi ai voli operati dalla Svizzera verso altri Paesi. Tra i destinatari di tali dati, oltre agli Stati membri dell'Unione europea, vi sono il Regno Unito, la Norvegia, il Canada e gli Stati Uniti.

Nel giugno 2018 gli Stati Uniti hanno dichiarato per la prima volta che la permanenza della Svizzera nel «Visa Waiver Program» (VWP) è vincolata al suo utilizzo dei dati PNR per la lotta alle gravi forme di criminalità. Questo programma consente ai cittadini svizzeri di recarsi negli Stati Uniti senza visto, per turismo o affari, per una durata massima di 90 giorni.

Pertanto, il PNR assume per la Svizzera una rilevanza non solo sul piano della politica di sicurezza, ma anche economica. Per giunta, sempre più Stati minacciano le imprese di trasporto aereo svizzere, in assenza di una comunicazione dei dati PNR, di infliggere loro pene pecuniarie ingenti e di revocare loro i diritti di atterraggio.

1.2 Necessità di agire e obiettivi

A livello internazionale, la Svizzera è tenuta a introdurre un sistema PNR e a contribuire così alla lotta alle gravi forme di criminalità. L'introduzione di questo sistema nel Paese è dettata anche da ragioni di sicurezza nazionale e da un numero crescente di considerazioni di carattere economico.

Tuttavia, come emerso anche nel quadro della procedura di consultazione condotta nel 2022, occorre sempre trovare il giusto equilibrio tra queste istanze in materia di politica di sicurezza ed economica e quelle legate alla protezione dei dati.

Per trattamento s'intende qualsiasi operazione relativa ai dati (personali), segnatamente la raccolta, la registrazione, la conservazione, l'utilizzazione e la modificazione. Tale nozione comprende anche l'archiviazione, la cancellazione o la distruzione di dati nonché la comunicazione di dati (personali), ossia la loro trasmissione o il fatto di renderli accessibili (cfr. art. 5 lett. d ed e della legge federale del 25 settembre 2020[3] sulla protezione dei dati [LPD]).

3 RS **235.1**

Diversi Stati, tra cui i principali partner economici della Svizzera, chiedono già da tempo i dati PNR alle imprese di trasporto aereo.

Nel 2003 la Svizzera ha concluso per la prima volta con gli Stati Uniti un accordo che prevede la comunicazione dei dati. La comunicazione 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.

I dati PNR sono comunicati anche agli Stati membri dell'UE in relazione a voli operati dalla Svizzera verso il loro territorio. Tale comunicazione si basa 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 la comunicazione dei dati dei passeggeri aerei agli Stati membri dell'UE richiedenti sarà ammessa fino alla creazione della pertinente base legale. Ciò a condizione che i passeggeri aerei siano informati nelle condizioni di trasporto in merito alla comunicazione dei loro dati e vi abbiano dato il loro consenso. Per mezzo di una procedura analoga è stata resa anche possibile la comunicazione di dati alla Norvegia.

Da allora l'IFPDT ha ribadito a più riprese la necessità di creare rapidamente in Svizzera le necessarie basi giuridiche. La comunicazione reciproca di dati sarà sancita sulla base di trattati internazionali.

Affinché la Svizzera possa in futuro trattare sistematicamente dati PNR per la lotta al terrorismo e ad altri reati gravi, occorre tanto una base giuridica formale, come quella che s'intende creare con il presente disegno di legge, quanto un sistema d'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), una legge federale sulla raccolta e l'utilizzo di dati PNR. Al contempo ha chiesto di 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.

Il 13° aprile 2022 il Consiglio federale ha avviato la procedura di consultazione concernente l'avamprogetto di LDPA, che si è conclusa a fine luglio 2022.

1.3 Alternative esaminate e soluzione scelta

Orientamento al diritto dell'UE

L'avamprogetto di LDPA posto in consultazione si ispira ampiamente alla direttiva PNR dell'UE. In tal modo s'intende agevolare la conclusione di un accordo con l'UE sullo scambio reciproco di dati PNR. Il numero di passeggeri aerei che raggiungono la Svizzera dall'UE rappresenta infatti oltre un terzo del volume totale dei passeggeri registrati presso gli aeroporti svizzeri. Per la Svizzera è quindi di fondamentale importanza ricevere questi dati.

L'interesse a scambiare dati PNR è reciproco, anche in ragione dello status della Svizzera quale Stato associato allo spazio Schengen: la Svizzera non deve rappresentare infatti un porto franco che consente di entrare nello spazio Schengen senza dati PNR.

Il 21 giugno 2022, mentre la LDPA era ancora in fase di consultazione, la Corte di giustizia dell'UE (CGUE) ha pronunciato una sentenza[4] (sentenza CGUE) in cui ha interpretato le disposizioni della direttiva PNR come conformi alle pertinenti norme della Carta dei diritti fondamentali[5] dell'Unione europea (Carta dei diritti fondamentali).

La CGUE ha precisato in particolare che:

- soltanto la lotta contro reati *gravi*, conformemente al principio di proporzionalità, può giustificare le gravi ingerenze che la direttiva PNR può comportare nei diritti fondamentali garantiti[6];
- una durata di conservazione di sei mesi per tutti i dati vada considerata ammissibile;
- una durata di conservazione fino a cinque anni è giustificabile se dai dati scaturiscono indizi obiettivi di un reato terroristico o di un altro reato grave.

La sentenza CGUE non è giuridicamente vincolante per la Svizzera. La Svizzera è pertanto in linea di massima libera di scegliere l'approccio da adottare nei confronti di questa sentenza. Tuttavia, se dovesse confermare la sua intenzione di armonizzare in toto la LDPA con la direttiva PNR, sarebbe tenuta a tener conto della nuova interpretazione di quest'ultima e, di conseguenza, della sentenza CGUE.

Diversi partecipanti alla procedura di consultazione sulla LDPA si richiamano a questa sentenza nel formulare le loro richieste. Queste ultime sono ampiamente considerate nel presente disegno di legge.

4 Causa C-817/19, ECLI:EU:C:2022:491.
5 Carta dei diritti fondamentali dell'Unione europea, GU C 326 del 26.10.2012, pag. 391
6 Causa C-817/19, ECLI:EU:C:2022:491, punto 148.

In virtù delle diverse modifiche apportate, la LDPA continua a poggiare sulla direttiva PNR.

Opzione scelta

L'opzione scelta si basa sull'avamprogetto di LDPA ed è stata rielaborata sulla base dei risultati della procedura di consultazione.

Sono state inoltre considerate anche diverse richieste formulate nell'ambito della consultazione che prendevano spunto dalla sentenza CGUE.

Il presente disegno di legge contempla quindi:

- una riduzione della durata di conservazione dei dati che non forniscono indizi di gravi forme di criminalità;
- uno snellimento del catalogo dei reati (limitazione alle gravi forme di criminalità);
- una maggiore protezione dei dati;
- un'estensione del diritto di accesso delle persone interessate.

La presente opzione integra nel disegno di LDPA elementi importanti della sentenza CGUE, senza ripercussioni significative per l'efficienza e l'efficacia del PNR quale strumento di lotta alle gravi forme di criminalità.

Il disegno permette pertanto di conciliare l'esigenza pubblica di sicurezza con l'interesse privato a una protezione sufficiente dei dati personali.

Considerazioni di natura legislativa

Il Consiglio federale ha esaminato la possibilità di creare le necessarie basi giuridiche relative al PNR non all'interno di una nuova legge, bensì di leggi federali già vigenti quali la legge federale del 21° dicembre 1948[7] sulla navigazione aerea (LNA) o la legge federale del 16 dicembre 2005[8] sugli stranieri e la loro integrazione (LStrI).

Ne sarebbe risultata una base giuridica caotica e, quindi, divergente dall'interesse delle imprese di trasporto aereo o dei passeggeri. La LDPA è inoltre incentrata su obiettivi non solo di politica di sicurezza, ma anche economici, il che è compatibile soltanto in misura limitata con le suddette leggi. Per tale ragione il Consiglio federale ha rinunciato a queste opzioni.

Una nuova legge che disciplini in maniera esaustiva il trattamento dei dati dei passeggeri aerei offre per contro la massima trasparenza in particolare alle persone che viaggiano in aereo e che saranno oggetto del trattamento dei dati previsto. Per queste ultime risulterà infatti più semplice riconoscere per quale

[7] RS **748.0**
[8] RS **142.20**

scopo e a quali condizioni i loro dati sono trattati dallo Stato e sapere di quali diritti godono in qualità di passeggeri.

L'opzione scelta è giustificata anche dal carattere internazionale del PNR. Consente infatti di individuare rapidamente in che modo il PNR è disciplinato in Svizzera, agevolando dunque la comunicazione con gli Stati partner.

Una legge sui dati dei passeggeri aerei comprendente tutte le disposizioni rilevanti in materia di PNR permette altresì di rendere il quadro giuridico chiaramente riconoscibile anche per le imprese di trasporto aereo interessate.

Per queste ultime derivano inoltre alcuni nuovi obblighi. In futuro, saranno infatti chiamate a comunicare i dati PNR non solo ai servizi esteri competenti in materia di PNR, ma anche all'unità d'informazione sui passeggeri (UIP) svizzera. L'estensione di tale obbligo di comunicazione riguarderebbe oltre 237 imprese di trasporto aereo che nel 2023 hanno trasportato più di 53 milioni di passeggeri dalla Svizzera all'estero e viceversa a bordo di voli charter o di linea.

1.4 PNR e altri dati dei passeggeri aerei

Dati API

Prima del passaggio al nuovo millennio il numero di passeggeri nel traffico aereo di linea e charter aveva fatto registrare un'enorme crescita a livello globale tale da mettere a dura prova le infrastrutture aeroportuali e le risorse di personale delle autorità competenti per il controllo al confine. Sempre più spesso si è rivelato impossibile controllare *tutti* i passeggeri e i loro bagagli.

Con i dati API che devono essere trasmessi «anticipatamente» («in advance» in inglese) dalle imprese di trasporto aereo, le autorità competenti per il controllo al confine ricevono le necessarie informazioni relative ai passeggeri aerei, prima della loro entrata e partenza, al fine di poterle verificare in modo selettivo sulla base di una valutazione del rischio.

In seguito agli attacchi terroristici dell'11 settembre 2001, gli Stati Uniti hanno iniziato a utilizzare i dati API anche ai fini della lotta al terrorismo.

Con la direttiva 2004/82/CE[9] (direttiva API), l'UE ha obbligato gli Stati membri a creare le necessarie basi giuridiche per l'utilizzo dei dati API al fine di agevolare i controlli al confine e combattere l'immigrazione illegale.

9 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.

La direttiva API è parte dell'acquis di Schengen ed è pertanto giuridicamente vincolante per la Svizzera. Dal 2008 la Svizzera obbliga le imprese di trasporto aereo a raccogliere dati API e a trasmetterli all'autorità competente sulla base dell'articolo 104 LStrI.

Solo dal 2019 i dati API possono essere utilizzati in Svizzera anche per la lotta alla criminalità organizzata internazionale e al terrorismo (cfr. 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	

A differenza dei dati PNR, i dati API non sono raccolti automaticamente al momento della prenotazione dei biglietti aerei, ma devono essere rilevati dalle imprese di trasporto aereo, direttamente prima della partenza, ai fini del loro utilizzo da parte dello Stato. La Svizzera impone inoltre alle imprese di trasporto aereo di rilevare e trasmettere i dati API soltanto per voli specifici, giudicati a rischio, provenienti da Stati terzi.

A seguito dell'introduzione del PNR, i dati API figureranno in futuro all'interno della categoria 18 del set di dati dei passeggeri (cfr. all. 1 LPDA), a condizione che i dati siano effettivamente disponibili. Tali dati sono disponibili soltanto qualora lo Stato in cui è previsto l'atterraggio di un volo ne abbia richiesto la trasmissione anticipata. I dati API, in seguito al loro trasferimento nella categoria 18 del set di dati dei passeggeri aerei, sottostanno ugualmente al diritto applicabile ai dati PNR.

Revisione API

Alla fine del 2022 la Commissione europea ha proposto all'interno di due progetti di regolamento un nuovo disciplinamento dei dati API[10]. Uno dei due progetti di regolamento (API Border), che regolamenta l'utilizzo dei dati API per i controlli all'entrata sul territorio è vincolante per tutti gli Stati aderenti allo spazio Schengen e pertanto anche per la Svizzera. Questo progetto di regolamento non è tuttavia rilevante ai fini della LDPA.

L'altro progetto di regolamento (API Police), che concerne la raccolta e la comunicazione di dati API per scopi di prevenzione, accertamento, indagine e azione penale riguardo ai reati di terrorismo e ai reati gravi, non è invece rilevante ai fini Schengen ed è vincolante soltanto per gli Stati membri dell'UE.

La Commissione europea suppone che la modifica API non potrà essere trasposta *prima* del 2030.

API Police prevede che i dati API possano essere in futuro trattati nell'UE soltanto nel quadro del PNR. Le imprese di trasporto aereo dovrebbero inoltre essere tenute a rilevare tali dati in maniera automatizzata, a condizione che i documenti lo consentano.

Resta ancora da vedere fino a che punto la Svizzera intende introdurre questa novità. Infatti, come accennato, API Police, in quanto atto giuridico non rilevante ai fini Schengen, non è giuridicamente vincolante per la Svizzera.

Per la Svizzera resta tuttavia ancora aperta la questione se i dati API, diversamente dalle intenzioni dell'UE, debbano continuare a essere trattati anche al di fuori del PNR. Questa scelta potrebbe essere in particolare giustificata nel caso di voli in provenienza da Stati che non dispongono di un sistema PNR e che sono pertanto tenuti a comunicare sistematicamente alla Svizzera soltanto i dati API. Tra questi Stati rientrano attualmente la Russia e diversi Stati del Medio Oriente.

Oltre a non convergere sul piano temporale con il progetto legislativo svizzero in corso relativo al PNR, *allo stato attuale* non si intravede neanche alcuna

10 Proposta di regolamento del Parlamento europeo e del Consiglio sulla raccolta e sul trasferimento delle informazioni anticipate sui passeggeri (API) al fine di migliorare e agevolare i controlli alle frontiere esterne, che modifica il regolamento (UE) 2019/817 e il regolamento (UE) 2018/1726 e abroga la direttiva 2004/82/CE del Consiglio, COM/2022/729 final; proposta di regolamento del Parlamento europeo e del Consiglio sulla raccolta e sul trasferimento di informazioni anticipate sui passeggeri a fini di prevenzione, accertamento, indagine e azione penale riguardo ai reati di terrorismo e ai reati gravi, e che modifica il regolamento (UE) 2019/818, COM/2022/731 final.

convergenza sul piano giuridico tra la modifica API e la LDPA. Per tale ragione la modifica non è stata presa in considerazione nell'ambito del presente disegno di legge.

Elenco dei passeggeri

L'articolo 21*f* LNA autorizza le autorità di perseguimento penale a richiedere «elenchi dei passeggeri» alle imprese di trasporto aereo «per la prevenzione o il perseguimento di crimini e delitti». Le imprese di trasporto aereo sono tenute a fornire i seguenti dati su richiesta delle autorità di perseguimento penale, per quanto «li abbiano già rilevati nell'ambito della loro normale attività»:

a. cognome, nome, indirizzo, data di nascita, cittadinanza e numero del documento di viaggio;
b. data, ora e numero del volo;
c. luogo di partenza, di transito e destinazione finale del trasporto;
d. eventuali compagni di viaggio;
e. informazioni relative al pagamento, in particolare il metodo di pagamento e il mezzo di pagamento impiegato;
f. dati concernenti il servizio presso il quale è stato prenotato il trasporto.

Diversamente da quanto avviene per il PNR, gli elenchi dei passeggeri non possono essere trattati in modo sistematico.

Nel messaggio del 31 agosto 2016[11] concernente la revisione parziale 1+ della legge sulla navigazione aerea il Consiglio federale aveva affermato al riguardo quanto segue:

«A complemento dei meccanismi di controllo in essere impiegati in maniera capillare e standardizzata per prevenire attentati contro la navigazione aerea, al fine di garantire la sicurezza dell'aviazione e contrastare la criminalità si dovrà prevedere anche la possibilità di controllare i passeggeri individualmente, e a seconda del rischio, sulla base degli elenchi dei passeggeri. Strumenti analoghi sono già previsti sia nella legislazione doganale sia nel diritto degli stranieri allo scopo di contrastare le infrazioni contro il diritto doganale e la migrazione illegale. Per prevenire e svolgere inchieste su atti criminali si dovrà prevedere l'obbligo per le imprese di trasporto aereo di mettere a disposizione delle competenti autorità di perseguimento penale, su loro richiesta, gli elenchi dei passeggeri».

11 FF **2016** 6401, in particolare 6408

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

Già nella Strategia della Svizzera per la lotta al terrorismo del 18 settembre 2015[12] il Consiglio federale aveva menzionato il PNR come possibile misura per impedire ingressi, partenze e transiti di persone sospettate di terrorismo.

Il presente disegno di legge è annunciato nel messaggio del 29 gennaio 2020[13] sul 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».

L'utilizzo del 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».

Poiché il quadro di sviluppo finanziario dei dipartimenti è definito ora sulla base degli obiettivi di legislatura, le risorse necessarie per il progetto e per il futuro impiego del PNR sono state richieste tramite la pianificazione del fabbisogno per il quadro di sviluppo del DFGP per l'anno 2025 e seguenti.

1.6 Interventi parlamentari

Il presente messaggio non comporta lo stralcio di alcun intervento parlamentare.

2 Procedura preliminare, in particolare procedura di consultazione

2.1 Testo sottoposto a consultazione

Dal 13 aprile al 31 luglio 2022 i Cantoni, i partiti politici e le cerchie interessate hanno avuto l'opportunità di esprimersi, nel quadro di una procedura di consultazione, in merito all'avamprogetto di LDPA.

L'avamprogetto era ispirato alla direttiva PNR dell'UE. Lo scopo era di creare i presupposti ottimali per un accordo sullo scambio reciproco di dati PNR tra la Svizzera e l'UE. L'UE rappresenta infatti il principale partner economico e in materia di sicurezza della Svizzera. Inoltre il traffico di persone tra UE e

12 FF **2015** 6143, in particolare 6148
13 FF **2020** 1565, in particolare 1684

Svizzera risulta intenso, assumendo pertanto rilevanza anche nell'ottica del PNR.

2.2 Riassunto dei risultati della procedura di consultazione

Nel quadro della procedura di consultazione, svoltasi dal 13 aprile a fine luglio 2022, 49 partecipanti hanno fatto pervenire il loro parere.

40 partecipanti hanno giudicato l'avamprogetto in modo positivo o neutrale:

25 Cantoni	*Il Cantone di Uri è l'unico a non essersi espresso sul progetto*
2 partiti	Alleanza del Centro, PLR
13 organizzazioni/associazioni	Aeroporto di Zurigo, Aerosuisse, ASA, CCPCS, CDDGP, CPS, easyJet, economiesuisse, FSFP, FST, SWISS, TAF, USS

I Cantoni hanno sottolineato l'importanza del PNR in materia di politica di sicurezza e hanno accolto perlopiù positivamente i miglioramenti che l'utilizzo del PNR dovrebbe apportare nella lotta alle gravi forme di criminalità. Alcuni di essi hanno criticato l'obbligo di dover distaccare e finanziare metà dei collaboratori dell'UIP.

I rappresentanti del settore dell'aviazione si sono espressi invece in modo neutrale sul piano della politica di sicurezza, auspicando una regolamentazione pragmatica, ispirata alle norme internazionali. Al riguardo hanno precisato che occorre a ogni costo evitare che si giunga a uno «swiss-finish».

Nove interpellati hanno espresso inoltre un parere critico o negativo:

4 partiti	PS, i Verdi, UDC, Partito Pirata
3 organizzazioni	AlgorithmWatch, FSA, Società digitale
2 privati	R.S., LAW FIRM

Richiamandosi alla sentenza CGUE, la maggioranza dei partecipanti ha giudicato negativamente in particolare il periodo di conservazione uniforme per *tutti* i dati (cinque anni secondo quanto previsto nell'avamprogetto) nonché la portata del catalogo dei reati. Diversi partecipanti hanno inoltre criticato la scarsa importanza attribuita alla protezione dei dati, evocando in larga misura la sentenza CGUE e proponendo misure di miglioramento.

Spiegazioni più dettagliate sono riportate nel rapporto del 1° marzo 2024[14] sui risultati della procedura di consultazione.

2.3 Valutazione dei risultati della procedura di consultazione

È obiettivo dichiarato del Consiglio federale di lanciare con il PNR un chiaro segnale in materia di politica di sicurezza, a livello nazionale e internazionale: le gravi forme di criminalità non devono destabilizzare la nostra società.

Tuttavia, ciò non deve andare a detrimento della protezione dei dati. Dalla consultazione emerge infatti quanto sia fondamentale trovare un giusto equilibrio tra gli interessi della collettività perseguiti dall'utilizzo del PNR e i diritti della personalità dell'individuo garantiti dal diritto fondamentale.

La sentenza CGUE, cui hanno rinviato diversi interpellati, ha avuto un effetto non trascurabile sull'esito della consultazione.

Sebbene tale sentenza non abbia alcun effetto vincolante per la Svizzera, nel presente disegno di legge il Consiglio federale tiene conto di alcuni suoi elementi chiave, nella misura in cui siano stati invocati nel quadro della procedura di consultazione e non compromettano in linea di massima l'efficacia dell'utilizzo del PNR. La sentenza riconosce peraltro che i dati PNR possono essere utilizzati in conformità con il diritto fondamentale.

Come rilevato nella sentenza, riguardo al periodo di conservazione occorre operare una distinzione tra i dati che forniscono indizi obiettivi per ritenere che il passeggero aereo possa rappresentare un pericolo in materia di reati terroristici o di gravi forme di criminalità e i dati che non forniscono invece alcun indizio in questo senso. Secondo la CGUE, un periodo di conservazione di cinque anni è giustificato soltanto per i dati contenenti indizi obiettivi di gravi forme di criminalità. Tutti gli altri dati devono pertanto essere cancellati dopo sei mesi.

Singoli pareri espressi nell'ambito della procedura di consultazione sottolineano giustamente l'importanza economica della LDPA. La Svizzera deve in effetti continuare a far parte del traffico aereo internazionale se intende preservare sul territorio i posti di lavoro nel settore dell'aviazione e del turismo e l'attrattiva in generale della piazza economica svizzera. L'utilizzo del PNR diventa una condizione viepiù necessaria in tale ottica. Sempre più Stati lasciano infatti intendere di voler subordinare l'autorizzazione a effettuare voli verso il proprio territorio all'utilizzo del PNR.

[14] www.admin.ch > Diritto federale > Procedure di consultazione > Procedure di consultazione concluse > 2022 > DFGP

Ugualmente motivata da ragioni economiche è la richiesta che la Svizzera ottemperi, nell'attuazione tecnica del PNR, alle norme internazionali onde scongiurare costi aggiuntivi per le imprese di trasporto aereo e gli aeroporti derivanti da esose soluzioni ad hoc. Tuttavia anche questa richiesta è in contrasto con alcune esigenze in materia di protezione dei dati formulate nel quadro della consultazione.

Il Consiglio federale giudica rilevanti le richieste di differenziazione del periodo di conservazione dei dati dei passeggeri aerei e di snellimento del catalogo dei reati.

Benché non sia stato richiesto esplicitamente, soprattutto la differenziazione della durata di conservazione dei dati dei passeggeri aerei necessita di diverse modifiche a livello di legge che concernono in particolare:

- la distinzione tra dati contrassegnati che presentano indizi obiettivi di un legame con gravi forme di criminalità e dati che non presentano simili indizi e che non devono pertanto essere contrassegnati,
- la possibilità di revocare il contrassegno se gli ulteriori accertamenti da parte delle autorità competenti non confermano gli indizi o se il sospetto iniziale su una persona ricercata si rivela infondato,
- una differenziazione del diritto di accesso per i dati di voli risalenti a più di sei mesi.

3 Diritto comparato, in particolare rapporto con il diritto europeo

UE

Diversi Stati membri dell'UE hanno iniziato a trattare dati PNR in virtù del loro diritto nazionale già prima del 2016. Il 27 aprile 2016 il Parlamento europeo e il Consiglio hanno adottato la direttiva (UE) 2016/681. La direttiva, entrata in vigore il 24 maggio 2016, ha come scopo di armonizzare le disposizioni relative al PNR degli Stati membri, di evitare l'incertezza giuridica e le lacune in materia di sicurezza e di garantire lo stesso livello di protezione dei dati in tutti gli Stati membri. La Danimarca è l'unico Stato membro non vincolato da tale direttiva[15]. Tuttavia, nel frattempo ha aderito volontariamente allo scambio d'informazioni PNR tra gli altri Stati membri dell'UE.

La direttiva PNR armonizza tra l'altro le competenze delle UIP che sono responsabili per la gestione operativa all'interno dei rispettivi Stati membri (art. 4), il trattamento lecito dei dati (in particolare art. 6) nonché gli obblighi dei vettori aerei riguardanti i trasferimenti di dati (art. 8).

15 Direttiva PNR, consid. 40

A distanza di due anni la Commissione europea ha riesaminato la direttiva PNR e ne ha illustrato i risultati in una relazione del 24 luglio 2020[16] al Parlamento europeo e al Consiglio. Nel complesso, la Commissione ha constatato che il PNR risulta uno strumento efficace nella lotta al terrorismo e alle gravi forme di criminalità. Senza l'uso dei dati PNR, non sarebbe stato possibile procedere a diverse indagini approfondite o ad arresti. Gli Stati membri dell'UE ribadiscono inoltre la necessità sul piano operativo di conservare i dati PNR per un periodo di cinque anni a prescindere dalla presenza di un sospetto. Sostengono tuttavia che il miglioramento della qualità dei dati continui a rappresentare una sfida.

Nella sentenza del 21 giugno 2022 la CGUE ha confermato la compatibilità della direttiva PNR con la Carta dei diritti fondamentali dell'UE, interpretando le disposizioni della direttiva come conformi alle pertinenti norme della Carta.

L'UE ha finora concluso accordi sull'utilizzo reciproco dei dati PNR con gli Stati Uniti[17] e l'Australia[18].

Nel 2017 la CGUE si è occupata in un parere delle questioni relative ai trattati dell'UE con gli Stati terzi[19], nello specifico di un accordo previsto con il Canada. La CGUE chiedeva in particolare che il Canada cancellasse i dati PNR dell'UE immediatamente dopo la partenza della persona in questione. Attualmente l'accordo con il Canada non è stato ancora concluso.

Nel febbraio 2020 la Commissione europea è stata incaricata di avviare i negoziati con il Giappone.

Nello stesso anno la Commissione europea ha dimostrato alla Svizzera il suo interesse a concludere un accordo bilaterale concernente il PNR. Alla fine del 2020 la Commissione europea e la Svizzera, rappresentata dal DFAE, dall'UFAC e da fedpol, hanno avviato i colloqui esplorativi, che sono stati condotti in modo molto costruttivo.

La Commissione europea ha salutato inoltre con favore l'intenzione della Svizzera di tener conto della sentenza CGUE per quanto riguarda il periodo ridotto di conservazione e lo snellimento del catalogo dei reati.

16 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

17 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.

18 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.

19 CGUE, parere 1/15 del 26 luglio 2017, ECLI:EU:C:2017:592

L'8 febbraio 2023 la Commissione europea ha proposto a Svizzera, Norvegia e Islanda l'avvio di negoziati per gli accordi bilaterali concernenti il PNR. Intende peraltro condurre tali trattative in modo parallelo, ma separato con i tre Stati associati a Schengen. La Svizzera necessita a tal fine di un mandato negoziale. In occasione della sua seduta del 1° novembre 2023 il Consiglio federale ha adottato il pertinente progetto con riserva dell'approvazione da parte delle Commissioni di politica estera delle Camere federali e della Conferenza dei governi cantonali, le quali hanno alla fine approvato il mandato negoziale.

Regno Unito

Il Regno Unito è stato il primo Stato membro dell'UE a disporre di un sistema PNR funzionante e 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. Il Regno Unito e l'UE hanno negoziato a tal fine un accordo relativo al PNR che è stato inserito nell'articolo 542 e seguenti dell'Accordo sugli scambi commerciali e la cooperazione tra l'UE e il Regno Unito («Trade and Cooperation Agreement», TCA)[20].

In seguito alla Brexit, la Svizzera ha concluso con il Regno Unito un accordo di polizia[21]. Tuttavia, poiché tale accordo non costituisce alcuna base per un ampio scambio reciproco di informazioni sui dati PNR, la Svizzera procederà presumibilmente a stipulare un accordo separato relativo al PNR con il Regno Unito.

Stati Uniti

Come conseguenza degli attacchi terroristici dell'11 settembre 2001 gli Stati Uniti avevano imposto, con l'«Aviation and Transportation Security Act»[22], alle imprese di trasporto aereo di concedere alle autorità statunitensi l'accesso ai dati PNR di tutti i voli che atterrano, partono o transitano nel territorio degli Stati Uniti.

Il primo accordo PNR concluso dagli Stati Uniti con la Svizzera è entrato in vigore il 29 marzo 2005, ma aveva una validità limitata di tre anni e mezzo. L'accordo successivo è entrato in vigore il 23 dicembre 2008[23].

20 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.
21 RS **0.360.367.1**
22 www.congress.gov/bill/107th-congress/senate-bill/1447
23 RS **0.748.710.933.6**

Il Governo degli Stati Uniti si impegna con l'accordo a garantire ai dati PNR provenienti dalla Svizzera la stessa tutela prevista per i dati dall'UE[24].

Canada

Dal 2009 i dati PNR e API di voli operati dalla Svizzera verso il Canada sono trasmessi alle autorità competenti canadesi. La comunicazione dei dati si basa sul «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[25].

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 simili reati.

Le autorità canadesi pseudonimizzano i dati PNR trascorsi 24 mesi e li cancellano dopo 42 mesi, sempreché la persona in questione non sia oggetto di un procedimento.

L'accordo prospetta alla Svizzera la possibilità di ricevere dati PNR e API dal Canada, non appena la necessaria base giuridica per il trattamento di dati PNR sarà stata introdotta in Svizzera.

4 Punti essenziali del progetto

I dati PNR sono utilizzati in tutto il mondo da 69 Paesi: Stati Uniti, Canada e Regno Unito si avvalgono di questo strumento da una ventina d'anni, mentre gli Stati membri dell'UE vi fanno ricorso da alcuni anni.

La LDPA proposta intende permettere alla Svizzera di utilizzare in futuro il PNR quale strumento consolidato per la lotta alle gravi forme di criminalità e pertanto di adempiere ai suoi obblighi internazionali.

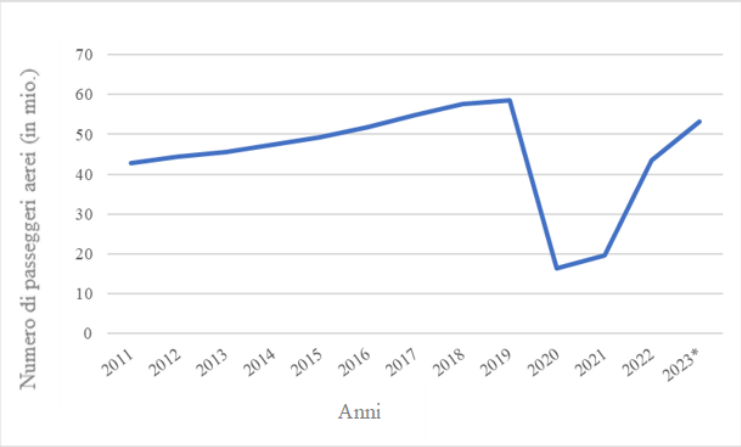
24 Cfr. Accordo tra gli Stati Uniti d'America e l'Unione europea sull'uso e il trasferimento delle registrazioni dei nominativi dei passeggeri al dipartimento degli Stati Uniti per la sicurezza interna, GU L 215 dell'11.8.2012, pag. 5.

25 Cfr. comunicato stampa del Consiglio federale del 17 marzo 2006, consultabile all'indirizzo www.admin.ch > Documentazione > Comunicati stampa > «Firmato con il Canada un accordo concernente i dati dei passeggeri aerei»

Particolarmente vincolanti sono le tre risoluzioni del Consiglio di sicurezza dell'ONU citate in precedenza, che impongono agli Stati membri di introdurre il PNR ai fini della lotta al terrorismo.

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, norme 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.

Diversi Stati, tra cui importanti partner economici della Svizzera, chiedono già da tempo la trasmissione dei dati PNR alle imprese di trasporto aereo che operano voli verso la Svizzera. Possono essere soggette all'obbligo di trasmissione dei dati anche le imprese di trasporto aereo che operano voli dalla Svizzera. Più di recente alcuni Stati hanno minacciato di revocare i diritti di atterraggio, nel caso in cui non dovessero ricevere anticipatamente i dati PNR. In tal caso la Svizzera rischierebbe di veder ridotta significativamente, a medio o a lungo termine, la propria inclusione nel traffico aereo internazionale, la cui importanza per la Svizzera trova conferma nel numero di passeggeri a bordo di voli di linea e charter internazionali registrati ogni anno presso gli aeroporti svizzeri.



Numero di passeggeri aerei partiti dalla Svizzera o giunti in Svizzera a bordo di voli charter o di linea (fonte: UFAC).
*2023: numero di passeggeri provvisorio.

Gli Stati Uniti, infine, assoggettano la permanenza della Svizzera nel VWP (v. n. 1.1) al trattamento di dati PNR.

Il disegno di LDPA è ispirato alla direttiva PNR. Esso tiene anche conto dei contenuti essenziali della sentenza CGUE, nella misura in cui siano stati invocati nel quadro della procedura di consultazione e non compromettano sostanzialmente l'efficacia del PNR.

4.1 La normativa proposta

Le imprese di trasporto aereo raccolgono i dati dei passeggeri aerei in occasione della prenotazione di un biglietto aereo e li utilizzano per gestire i voli. Questi dati sono utilizzati dagli Stati in un secondo momento.

La LDPA costituisce la base giuridica che permette alla Confederazione di trattare sistematicamente, ai fini della lotta alle gravi forme di criminalità, i dati dei passeggeri che viaggiano su voli di linea e charter in arrivo o in partenza dalla Svizzera. Le fattispecie penali rilevanti figurano nell'allegato 2 LDPA.

La competenza per il trattamento dei dati dei passeggeri aerei è affidata all'UIP, collocata in seno a fedpol. L'UIP può essere quindi considerata come una prestatrice di servizi dello Stato nel settore della sicurezza.

Gli articoli 2–4 LDPA disciplinano gli obblighi delle imprese di trasporto aereo.

Le imprese di trasporto aereo devono comunicare complessivamente 19 categorie di dati dei passeggeri aerei. Queste categorie figurano nell'allegato 1 del disegno di legge e costituiscono insieme il set di dati dei passeggeri aerei. A dover essere comunicati sono i set di dati di *tutti* i passeggeri di voli charter e di linea in arrivo o partenza dalla Svizzera. I dati devono essere comunicati durante il lasso di tempo previsto per legge prima del decollo da o verso la Svizzera. Destinataria dei dati è l'UIP svizzera (art. 2).

Dalle imprese di trasporto aereo ci si attende che adottino tutte le misure ragionevolmente esigibili per comunicare i dati puntualmente e nel rispetto delle prescrizioni tecniche (art. 3).

Al momento della prenotazione del biglietto, le imprese di trasporto aereo devono inoltre informare i loro passeggeri in modo adeguato e in forma precisa, trasparente, comprensibile e facilmente accessibile che i loro dati saranno trattati dallo Stato in virtù della presente legge (art. 4).

Se non rispettano tali obblighi o non lo fanno in maniera sufficiente, le imprese di trasporto aereo sono soggette a sanzioni ai sensi dell'articolo 31. Non vi è invece violazione degli obblighi legali se provano di aver adottato tutte le misure tecniche e organizzative ragionevolmente esigibili per adempierli.

Gli articoli 5–11 LDPA disciplinano il trattamento dei dati da parte dell'UIP

Nel complesso, i dati dei passeggeri aerei trasmessi all'UIP sono trattati attivamente soltanto in occasione del confronto automatico dei dati di cui all'articolo 6. Questa fase del trattamento permette di effettuare una prima selezione.

Non appena giungono nel sistema d'informazione dell'UIP, tali dati sono confrontati automaticamente con i sistemi d'informazione di polizia nonché con i profili di rischio e le liste d'osservazione registrati (art. 6).

Successivamente l'UIP dovrà verificare manualmente le corrispondenze eventualmente ottenute («hit»). Soltanto in seguito potrà comunicarle a un'autorità competente di cui all'articolo 1 capoverso 2. Le corrispondenze che non sono state confermate nell'ambito della verifica manuale vanno cancellate senza indugio (cfr. art. 22).

I risultati del confronto automatico di dati permettono alle autorità competenti:

- di individuare i reati di cui all'allegato 2 che non sono ancora oggetto di un'indagine o di un procedimento penale in corso (cfr. art. 5 cpv. 1 lett. a);
- di completare le informazioni relative a un'indagine o a un procedimento penale in corso per un reato di cui all'allegato 2 o relative a reati dello stesso allegato 2 non ancora chiariti (cfr. art. 5 cpv. 1 lett. a);
- di fermare ed eventualmente arrestare persone che, per via di un reato di cui all'allegato 2, sono ricercate a livello nazionale o internazionale (cfr. art. 5 cpv. 1 lett. a nonché lett. b n. 1);
- di far espiare la pena detentiva a persone che sono state condannate con decisione passata in giudicato per un reato di cui all'allegato 2 (cfr. art. 5 cpv. 1 lett. b n. 2).

Una volta comunicati, i dati interessati sono contrassegnati dall'UIP. I dati contrassegnati saranno automaticamente soggetti a una durata di conservazione più lunga rispetto a quelli che non sono stati comunicati a un'autorità competente e che non sono stati quindi contrassegnati (cfr. art. 21).

Dopo questa fase di trattamento, i dati dei passeggeri aerei possono essere comunicati a un'autorità competente e in seguito contrassegnati soltanto:

- su richiesta di tale autorità conformemente all'articolo 8; o
- insieme a un indizio ai sensi dell'articolo 9 ricevuto dall'UIP.

L'articolo 11 disciplina una forma particolare di comunicazione dei dati dei passeggeri aerei che *non* prevede alcun contrassegno dei dati: il Servizio delle attività informative della Confederazione (SIC) riceve i dati dei passeggeri aerei di determinate rotte per trattarli autonomamente, a condizione che ciò

sia necessario all'adempimento dei suoi compiti ai sensi dell'articolo 6 capoverso 1 lettera a numeri 1–5 della legge federale del 25 settembre 2015[26] sulle attività informative (LAIn) e finalizzato alla lotta di un reato di cui all'allegato 2 LDPA. I dettagli relativi al trattamento da parte del SIC e il termine di conservazione ammesso sono retti dalla LAIn (cfr. all. 3 n. 1 LDPA).

La distinzione tra dati contrassegnati e non contrassegnati consente di adempiere alla richiesta formulata in occasione della procedura di consultazione, secondo cui i dati dei passeggeri aerei che non presentano indizi relativi a un reato di cui all'allegato 2 (dati non contrassegnati) dovrebbero essere conservati per un periodo più breve rispetto ai dati contrassegnati.

Un'autorità competente ai sensi dell'articolo 1 capoverso 2 può giungere alla conclusione di non avere più bisogno dei dati comunicati dall'UIP, per esempio quando gli indizi che hanno portato alla comunicazione dei dati non sono confermati o il sospetto iniziale nei confronti di una persona oggetto di una segnalazione di ricerca si rivela infondato. Non appena riceve la relativa informazione dall'autorità competente interessata, l'UIP revoca il contrassegno dei dati in questione (art. 10). Questi ultimi risulteranno pertanto non contrassegnati e saranno soggetti alle pertinenti conseguenze giuridiche (cfr. art. 18 e 21).

Gli articoli 12–15 LDPA disciplinano le modalità di utilizzo dei profili di rischio e delle liste d'osservazione nel quadro del confronto automatico dei dati. Il Consiglio federale verifica l'utilizzo di questi strumenti.

Il profilo di rischio permette di cercare nei dati dei passeggeri aerei combinazioni di dati ricorrenti nel caso di determinati reati di cui all'allegato 2 e in particolare del crimine organizzato (tratta di esseri umani; art. 12). Poiché tale ricerca non riguarda un reato di cui all'allegato 2 già noto alle autorità, il profilo di rischio non conterrà alcun dato che riguarda una persona fisica identificata o identificabile e che rappresenta pertanto un dato personale ai sensi dell'articolo 5 lettera a LPD.

Per contro, i dati che concernono una persona fisica o giuridica identificata o identificabile sono utilizzati nelle liste d'osservazione ai sensi degli articoli 13 e 14. Le liste d'osservazione permettono di cercare nei dati dei passeggeri aerei indizi concreti relativi a un reato di cui all'allegato 2 noto alle autorità, ad esempio il nome di una persona ricercata o il numero di una carta di credito utilizzata a più riprese da un'organizzazione criminale.

In casi eccezionali e soltanto previa approvazione del giudice dei provvedimenti coercitivi competente, possono essere inseriti all'interno di una lista d'osservazione anche i dati di terzi (art. 14). Questi dati devono permettere di risalire al luogo di soggiorno ancora ignoto di una persona accusata di un reato

26 RS **121**

di cui all'allegato 2 o condannata con decisione passata in giudicata per tale reato e ricercata, affinché possa espiare la pena detentiva.

L'utilizzo di questi strumenti deve essere verificato dal Consiglio federale (art. 15).

Gli articoli 17–26 LDPA contengono disposizioni in materia di protezione dei dati di cui l'UIP deve tener conto nel trattare i dati dei passeggeri aerei.

Con la revisione totale del diritto in materia di protezione dei dati, la Svizzera si adegua agli sviluppi dell'UE in tale ambito[27]. La presente legge tiene conto del nuovo diritto in materia di protezione dei dati entrato in vigore il 1° settembre 2023.

Gli articoli 17–26 LDPA contengono perlopiù norme che precisano la LPD e prevalgono su di essa. Talune disposizioni menzionano, per ragioni di trasparenza, le norme della LPD o vi rinviano.

L'articolo 17 illustra le basi legali in materia di protezione dei dati applicabili all'UIP e alle autorità che ricevono e trattano dati conformemente al presente disegno di legge.

I dati non contrassegnati, che comprendono anche i dati il cui contrassegno è stato revocato in virtù dell'articolo 10, sono pseudonimizzati un mese dopo la loro comunicazione all'UIP e beneficiano pertanto sul piano tecnico di una protezione accresciuta (art. 18).

Il periodo durante il quale i dati non contrassegnati sono attribuibili a una determinata persona è quindi limitato a un mese. Diversamente dall'anonimizzazione, la pseudonimizzazione può essere revocata. A tal fine è necessaria l'autorizzazione del Tribunale amministrativo federale (TAF; art. 19 e 20).

I dati non contrassegnati sono cancellati automaticamente dopo sei mesi. Questo periodo breve di conservazione risponde a una richiesta formulata a più riprese nel quadro della procedura di consultazione.

I dati contrassegnati possono essere invece conservati per cinque anni, a condizione che il loro contrassegno non sia stato precedentemente revocato conformemente all'articolo 10. Trascorso tale termine, sono cancellati automaticamente (art. 21).

Agli altri dati che potrebbero pervenire all'UIP in virtù della LDPA si applicano i termini di cancellazione previsti dall'articolo 22.

27 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 5941

L'articolo 24 statuisce che per ogni trattamento automatizzato occorre allestire un verbale elettronico. Quest'ultimo permette di risalire, anche a posteriori, all'autore, al tipo e all'ora del trattamento automatizzato e ai dati oggetto del trattamento. I verbali devono essere registrati al di fuori del sistema d'informazione PNR (riguardo al luogo di registrazione v. n. 6.1) e sono accessibili soltanto alle poche persone che ne necessitano ai fini dell'adempimento dei loro compiti di sicurezza, vigilanza e sorveglianza.

L'articolo 26 conferisce ai passeggeri aerei il diritto di ottenere informazioni sui dati che li riguardano che sono trattati sulla base della presente legge. Nel ricevere queste informazioni, la persona in questione non deve tuttavia poter apprendere di essere oggetto di un eventuale procedimento in corso.

Questo rischio sussiste allorché l'informazione concerne dati relativi a un volo risalente a più di sei mesi prima. In quel momento la maggior parte dei dati del volo in questione sono infatti già stati cancellati; i dati restanti sono quelli contrassegnati che devono essere quindi conservati per un periodo di cinque anni (art. 21).

In caso di richieste di accesso che riguardano dati relativi a un volo risalente a più di sei mesi, fedpol comunica pertanto *sistematicamente* alla persona richiedente che l'informazione sarà differita, rinviando alla possibilità di chiedere all'IFPDT di verificare se eventuali dati che la riguardano sono trattati in modo lecito e se sussistono interessi preponderanti che giustificano il mantenimento del segreto.

I diritti d'accesso ai dati relativi a voli risalenti a non oltre sei mesi sono invece retti dalla LPD.

Anche altre disposizioni, disciplinate in altre sezioni della legge, sono rilevanti sul piano della protezione dei dati, in particolare:

- l'articolo 5 capoverso 1: scopo del trattamento dei dati;
- l'articolo 5 capoverso 2: restrizioni nel trattamento da parte dell'UIP di dati degni di particolare protezione;
- l'articolo 6 capoversi 2 e 3 e l'articolo 7 come pure i rinvii a quest'ultimo contenuti negli articoli 8 e 9: obbligo di verificare manualmente i risultati del trattamento prima di comunicarli a un'autorità competente;
- l'articolo 16 capoverso 2: accesso limitato al sistema d'informazione PNR.

Possono essere considerate come misure tecniche volte a garantire la protezione dei dati (cfr. art. 7 cpv. 2 LPD):

- il confronto (art. 6), la pseudonimizzazione (art. 18) e la cancellazione (art. 21) automatici dei dati dei passeggeri aerei; nonché

- la verbalizzazione del trattamento dei dati (art. 24).

Inoltre, gli articoli 27 capoverso 2 e 28 capoverso 4 contemplano misure organizzative volte a garantire la protezione dei dati. Lo scopo è ridurre il rischio che possano essere scambiati in modo informale contenuti rilevanti in materia di protezione dei dati.

Infine, quali misure tecniche volte a garantire la protezione dei dati (cfr. art. 7 LPD) sono previste la pseudonimizzazione (art. 18) e l'anonimizzazione dei dati (art. 23).

Gli articoli 27 e 28 riguardano l'organizzazione e il personale dell'UIP.

L'UIP è collocata in seno a fedpol (art. 27) ed è composta, in parti uguali, di collaboratori della Confederazione e di collaboratori distaccati dai Cantoni. I Cantoni si assumono i costi relativi allo stipendio dei collaboratori durante la durata dell'impiego e versano i contributi previsti dal diritto delle assicurazioni sociali. Questa soluzione tiene conto del fatto che l'UIP apporta prevalentemente benefici nella lotta alla criminalità a livello cantonale. I dettagli del distacco del personale presso l'UIP sono stabiliti dalla Confederazione e dai Cantoni all'interno di una convenzione. Il Consiglio federale è autorizzato a concludere con i Cantoni simili convenzioni (art. 28).

Gli articoli 31 e 32 disciplinano le sanzioni amministrative.

Le imprese di trasporto aereo che non rispettano i loro obblighi ai sensi degli articoli 3 e 4 o lo fanno in maniera insufficiente possono essere sanzionate. Non vi è invece violazione degli obblighi legali se provano di aver adottato tutte le misure tecniche e organizzative ragionevolmente esigibili per adempierli (art. 31 cpv. 4).

4.2 Compatibilità tra compiti e finanze

I danni che le (gravi) forme di criminalità arrecano alle persone coinvolte e all'economia sono ingenti. Il chiarimento di tali reati e la condanna dei loro autori sono elementi cardine in uno Stato di diritto. Per le vittime, la punizione degli autori è spesso la condizione per un nuovo inizio nella loro vita personale.

La sicurezza è un bene fondamentale per il benessere di una società e la sua prosperità. Tuttavia, la sicurezza ha il suo prezzo.

Come emerge anche nel quadro del presente progetto, questo prezzo non è di mera natura economica: infatti, sebbene i controlli contribuiscano in modo determinante alla sicurezza pubblica, possono condurre in alcuni casi a restrizioni dei diritti della personalità di una persona, anche laddove quest'ultima non rappresenti alcun problema di sicurezza.

L'utilizzo del PNR è uno strumento consolidato a livello internazionale di lotta alle gravi forme di criminalità. Con la sua introduzione, la Svizzera contribuisce a rafforzare la sicurezza sul piano sia nazionale sia internazionale.

In passato ogni singola persona veniva controllata all'entrata e all'uscita dal Paese. Alla luce della rapida crescita del traffico aereo registrata negli ultimi 30 anni, è stato necessario ridurre il numero di controlli sistematici dei viaggiatori effettuati sul posto adottando un approccio basato sui rischi. Tuttavia, ai fini della salvaguardia della sicurezza resta indispensabile identificare le persone colpevoli di aver commesso un reato grave o che perseguono tale scopo.

Il PNR rende possibile tutto ciò, come dimostrano i successi conseguiti dagli Stati membri dell'UE. Peraltro, nella sua sentenza del 21 giugno 2022 la CGUE ha riconosciuto che ai fini della lotta alle gravi forme di criminalità l'utilizzo del PNR è compatibile con la protezione dei diritti fondamentali.

L'utilizzo del PNR non comporta oneri regolamentari significativi per le imprese di trasporto aereo. Gli oneri cui sono confrontati si limitano alla comunicazione tempestiva dei dati disponibili al servizio statale competente e all'informazione dei viaggiatori. L'utilizzo del PNR non comporta pertanto per queste imprese particolari oneri supplementari.

L'utilizzo del PNR non è soltanto efficiente, ma anche efficace, come dimostra il fatto che viene impiegato da ormai circa 20 anni e, attualmente, in oltre 69 Paesi, tra cui Stati Uniti, Canada, Stati membri dell'UE, Australia e Regno Unito, per combattere i reati terroristici e altri reati gravi e come dimostrano chiaramente anche le statistiche e i rapporti allestiti da determinati Paesi.

È previsto che i Cantoni distacchino metà dell'organico dell'UIP e si facciano carico dei relativi costi per il personale. Questa ripartizione dei costi rispecchia il fatto che la sicurezza del Paese e la protezione della popolazione dalle gravi forme di criminalità sono un compito congiunto della Confederazione e dei Cantoni. Per contro, i costi legati alla creazione dell'infrastruttura tecnica e i costi di gestione sono interamente a carico della Confederazione.

4.3 Attuazione

In aggiunta ai dati PNR che le saranno forniti in futuro in virtù della LDPA, la Confederazione, ed eventualmente la Segreteria di Stato della migrazione (SEM), ricevono 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 automaticamente in virtù degli articoli 104*a* e 104*b* LStrI.

Conformemente alle norme tecniche internazionali dell'OACI, dell'OMD e dell'Associazione del trasporto aereo internazionale (IATA), occorre prevedere una cosiddetta «single window», ovvero un'unica interfaccia comune per

la comunicazione 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. Nel quadro della procedura di consultazione questa soluzione è stata accolta favorevolmente dall'Associazione svizzera degli aerodromi e da SWISS.

5 Commento ai singoli articoli

Sezione 1: Disposizioni generali

Art. 1 Oggetto e scopo

Questa disposizione illustra i contenuti più importanti e lo scopo della presente legge.

Cpv. 1

Lett. a

Le imprese di trasporto aereo sono tenute a comunicare all'UIP i dati dei passeggeri aerei per i voli operati da o verso la Svizzera.

Tale obbligo, in linea di massima, non costituisce tuttavia una novità assoluta; le imprese di trasporto aereo sono infatti tenute ad adempierlo da anni nei confronti di Stati Uniti, Canada e degli Stati membri dell'UE. L'unica novità consiste nell'obbligo di comunicare i dati dei passeggeri aerei anche all'UIP.

Lett. b

Oltre agli obblighi per le imprese di trasporto aereo, la legge disciplina anche il trattamento dei dati dei passeggeri aerei da parte dei servizi competenti.

Tali dati possono essere trattati se servono a combattere le gravi forme di criminalità (cfr. cpv. 4).

Lett. c

La presente legge definisce inoltre l'organizzazione dell'unità nazionale svizzera incaricata del trattamento dei dati dei passeggeri aerei. La denominazione in uso a livello internazionale, *unità d'informazione dei passeggeri, PIU* nella forma abbreviata, deve essere adottata anche in Svizzera.

L'UIP deve essere collocata in seno a fedpol (cfr. art. 27) ed essere composta di collaboratori della Confederazione e dei Cantoni (cfr. art. 28).

Cpv. 2

Lo scopo della presente legge è di offrire sostegno alle autorità della Confederazione e dei Cantoni nella lotta alle gravi forme di criminalità (cfr. all. 2).

A usufruire delle prestazioni dell'UIP in virtù della presente legge sono le autorità di polizia e di perseguimento penale della Confederazione e dei Cantoni, i servizi delle attività informative della Confederazione, ossia il Servizio delle attività informative della Confederazione (SIC) e il Servizio informazioni dell'esercito, nonché le autorità di esecuzione cantonali ai sensi dell'articolo 9 LAIn.

Le autorità di perseguimento penale della Confederazione comprendono tra l'altro anche il Servizio federale di sicurezza (art. 4 lett. b della legge del 19 marzo 2010[28] sull'organizzazione delle autorità penali)[29].

Cpv. 3

Nel diritto vigente non è prevista alcuna definizione di *impresa di trasporto aereo*, ragion per cui tale nozione viene ora precisata nella presente legge. La definizione si basa su quella che era stata elaborata nel quadro della legge del 25 settembre 2020[30] sul CO_2 (art. 2 lett. i). Per impresa di trasporto aereo s'intende un'impresa che dispone di un'autorizzazione di esercizio, o di un'autorizzazione equivalente, per il trasporto professionale di persone per via aerea.

Non sono invece considerate imprese di trasporto aereo quelle rientranti nella nozione della cosiddetta aviazione leggera, che include 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. Sono ugualmente esclusi dal campo d'applicazione della legge i voli militari o destinati allo svolgimento di altri compiti sovrani nonché i voli di ricerca e salvataggio.

La definizione di imprese di trasporto aereo assume un'importanza fondamentale, dato che queste ultime sono ora assoggettate alla presente legge. Le imprese di trasporto aereo svizzere ed estere sono tenute a comunicare all'UIP i dati dei passeggeri aerei tempestivamente e conformemente alle prescrizioni tecniche (cfr. art. 2 e 3). Devono inoltre informare i passeggeri in modo adeguato del trattamento dei dati ai sensi della presente legge (cfr. art. 4). Eventuali violazioni di tali obblighi sono punibili in virtù dell'articolo 31.

Cpv. 4

L'allegato 1 della presente legge menziona i dati dei passeggeri aerei che devono essere comunicati dalle imprese di trasporto aereo e trattati ai sensi della presente legge.

I dati dei passeggeri aerei sono suddivisi complessivamente in 19 categorie che costituiscono il set di dati dei passeggeri aerei. Le categorie di dati corri-

28 RS **173.71**

29 Messaggio del 10 settembre 2008 concernente la legge federale sull'organizzazione delle autorità penali della Confederazione (Legge sull'organizzazione delle autorità penali, LOAP), FF **2008** 7093, in particolare 7117

30 FF **2020** 6901, in particolare 6902; oggetto respinto nella votazione popolare del 13 giugno 2021.

spondono alla direttiva PNR e tengono conto nella loro formulazione dell'interpretazione che la CGUE, nella sua sentenza del 21 giugno 2022, impone agli Stati membri dell'UE.

Le imprese di trasporto aereo raccolgono i dati dei passeggeri aerei in occasione della prenotazione di un biglietto aereo. Esse necessitano di tali dati ai fini della gestione del volo. Il trattamento dei dati in virtù della presente legge si limita ai dati già disponibili e avviene pertanto soltanto in un secondo momento.

Un caso speciale è costituito dai dati API che, ove disponibili, devono essere comunicati dalle imprese di trasporto aereo in quanto parte del set di dati dei passeggeri aerei (categoria 18). Questi dati non sono raccolti in occasione della prenotazione, ma devono essere rilevati dalle imprese di trasporto aereo se lo Stato lo richiede (cfr. art. 104 LStrI). Di conseguenza, nel quadro del PNR vanno comunicati all'UIP quale categoria 18 soltanto se sono *disponibili*.

Molte delle 19 categorie di dati non contengono dati che permettono di identificare una persona. Non trattandosi quindi di dati personali (cfr. art. 5 lett. a LPD), il loro trattamento non rientra nel campo d'applicazione della riveduta legge sulla protezione dei dati (art. 2 LPD).

I dati personali sono contenuti nelle seguenti categorie del set di dati dei passeggeri aerei:

- *categoria 4:* nome/i e cognome/i del passeggero aereo;
- *categoria 5:* indirizzo e dati di contatto, compresi il recapito telefonico e l'indirizzo di posta elettronica del passeggero aereo;
- *categoria 6:* informazioni su eventuali carte di credito utilizzate e indirizzo di fatturazione;
- *categoria 8:* programma «frequent flyer»: status e numero del passeggero aereo;
- *categoria 9:* nome dell'agente dell'agenzia di viaggio che ha effettuato la prenotazione del biglietto;
- *categoria 12:* informazioni sui minori non accompagnati di età inferiore a 18 anni, nome e recapito degli accompagnatori alla partenza e all'arrivo nonché del collaboratore dell'aeroporto che accompagna il minore alla partenza e all'arrivo;
- *categoria 17:* numero di viaggiatori nonché nomi e cognomi di altri passeggeri figuranti nei dati PNR;
- *categoria 18:* dati API (cfr. art. 104 cpv. 3 LStrI), che sono al contempo dati personali: (a) generalità (cognome, nome, sesso, data di nascita, cittadinanza) del passeggero aereo; (b) numero, Stato di rilascio, tipo e data di scadenza del documento di viaggio utilizzato; (c) numero, Stato di rilascio, tipo e data di scadenza del visto o del

titolo di soggiorno utilizzato, nella misura in cui l'impresa di trasporto aereo disponga di questi dati;

- *categoria 19:* ogni modifica dei dati dei passeggeri aerei. La presente categoria contiene dati personali, se tali dati hanno subito modifiche in seguito alla prenotazione.

I dati dei passeggeri aerei possono essere trattati, secondo la presente legge, esclusivamente per la lotta alle gravi forme di criminalità. Per gravi forme di criminalità s'intendono i reati menzionati nel catalogo dei reati di cui all'allegato 2 con indicazione delle fattispecie penali determinanti previste dal Codice penale (CP)[31] o dal diritto penale accessorio. L'allegato 2 suddivide tali fattispecie in reati terroristici (n. 1) e altri reati gravi (n. 2).

Il catalogo dei reati si fondava originariamente sulle categorie di reato contemplate dalla direttiva PNR e attribuendo loro le fattispecie rilevanti previste dall'allegato 1 della legge del 12 giugno 2009[32] sullo scambio di informazioni con gli Stati Schengen (LSIS), che è stato ampliato nell'ambito di PRÜM[33]. Tale ampliamento, benché non ancora in vigore, è stato già considerato nella presente legge. Lo stesso vale per un ulteriore ampliamento dell'allegato LSIS, attualmente in fase di elaborazione. A differenza dell'allegato 1 LSIS, il catalogo dei reati rilevante per il PNR tiene conto ora anche dei casi gravi di spionaggio.

Per *terroristici* ai sensi della LDPA si intendono i reati rientranti nella fattispecie di cui al numero 22 dell'allegato 1 LSIS. La fattispecie penale di sommossa (cfr. art. 260 cpv. 1 CP) non fa invece più parte del catalogo dei reati rilevante per il PNR, conformemente alle richieste formulate nell'ambito della procedura di consultazione.

La maggior parte di questi reati sono crimini e sono pertanto punibili con una pena massima di *oltre* tre anni (cfr. art. 10 cpv. 2 CP). Per contro, le seguenti fattispecie di reato sono considerate delitti (cfr. art. 10 cpv. 3 CP) e sono punite con una pena massima di tre anni:

- pubblica intimidazione (art. 258 CP),
- pubblica istigazione a un crimine o alla violenza (art. 259 CP).

La maggior parte dei reati elencati nel catalogo è considerata terroristica soltanto se presenta effettivamente anche una matrice terroristica (cfr. all. 2 n. 1). Tale matrice è ravvisabile laddove l'autore commetta o minacci di commettere il reato in questione al fine di influenzare o modificare l'ordinamento

31 RS **311.0**
32 RS **362.2**
33 Decreto federale che approva e traspone nel diritto svizzero l'Accordo tra la Svizzera e l'UE sul potenziamento della cooperazione transfrontaliera (cooperazione Prüm) e il Protocollo tra la Svizzera, l'UE e il Principato del Liechtenstein riguardante l'accesso a Eurodac a fini di contrasto, FF **2021** 2332 pagg. 10–16

dello Stato (cfr. art. 23*e* della legge del 21 marzo 1997[34] sulle misure per la salvaguardia della sicurezza interna [LMSI]).

Quali *altri reati gravi* l'allegato 2 menziona:

- al numero 2.1, i crimini riportati nell'allegato 1 LSIS summenzionato, nonché
- al numero 2.2, i crimini in relazione allo spionaggio.

Il catalogo degli altri reati gravi è stato notevolmente snellito in risposta a diverse richieste che i partecipanti alla consultazione avevano formulato in relazione alla sentenza CGUE. In particolare sono stati stralciati i reati il cui perseguimento penale compete all'Ufficio federale della dogana e della sicurezza dei confini (UDSC), in quanto non costituiscono gravi forme di reato.

Il catalogo dei reati comprende ora soltanto le fattispecie penali che

a) secondo la CGUE presentano *in modo esplicito* un «livello di gravità indubbiamente elevato» (punto 149) o, quali gravi forme di criminalità, un «collegamento diretto con il trasporto aereo di passeggeri» (punto 154) o, ancora, un «carattere transnazionale» (punto 155); oppure

b) conformemente al diritto svizzero prevedono una pena minima applicabile, che può essere intesa come una peculiarità del diritto nazionale e che permette di dedurre una particolare gravità del reato (a contrario dal punto 151 seg.).

Alla luce della mutata situazione geopolitica, nel catalogo dei reati sono state aggiunte tre fattispecie penali correlate allo spionaggio (n. 2.2). Queste gravi forme di spionaggio costituiscono crimini ai sensi dell'articolo 10 capoverso 2 CP e sono punite con una pena minima applicabile.

Sezione 2: Obblighi delle imprese di trasporto aereo

Art. 2 Comunicazione dei dati dei passeggeri aerei

Per comunicazione s'intende ogni trasmissione di dati personali o il fatto di renderli accessibili (cfr. art. 5 lett. e LPD).

L'articolo 2 definisce i dettagli che regolano la comunicazione dei dati dei passeggeri aerei da parte delle imprese di trasporto aereo. La violazione di tali obblighi può comportare sanzioni (cfr. art. 31).

In sede di consultazione era stato chiesto di introdurre una disposizione che regolamentasse l'uso ammissibile e la cancellazione dei dati dei passeggeri aerei da parte delle imprese di trasporto aereo. Non è possibile dare seguito alla richiesta. Le imprese di trasporto aereo necessitano infatti di tali dati per gestire la prenotazione e il volo. La durata di conservazione di questi dati

34 RS **120**

presso le imprese di trasporto aereo è determinata pertanto dalle esigenze operative di queste ultime e dai principi vigenti in materia di protezione dei dati.

Cpv. 1

L'articolo 2 stabilisce che tutte le imprese di trasporto aereo (cfr. art. 1 cpv. 3) che operano voli da o verso la Svizzera sono tenute a comunicare i dati dei passeggeri aerei all'UIP svizzera (cpv. 1).

Anche i voli ricadenti sotto la giurisdizione svizzera che atterrano all'Euroairport di Basilea-Mulhouse-Friburgo (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 contrassegnati dal medesimo codice aeroportuale IATA operati dall'Euroairport di Basilea-Mulhouse-Friburgo verso un aeroporto non svizzero.

Per converso, in caso di voli nazionali i dati dei passeggeri aerei non vanno comunicati, anche ove siano effettuati da imprese di trasporto aereo di cui all'articolo 1 capoverso 3.

Cpv. 2

I dati dei passeggeri aerei sono rilevati al momento della prenotazione di un biglietto aereo. Se il biglietto è prenotato presso un'impresa di trasporto aereo svizzera, i pertinenti dati sono conservati in Svizzera. Se il biglietto è invece prenotato dalla Svizzera presso un'impresa di trasporto aereo con sede all'estero, i pertinenti dati non saranno più conservati in Svizzera, bensì nello Stato in cui ha sede l'impresa. Il passeggero aereo che effettua quest'ultimo tipo di prenotazione comunica i propri dati autonomamente «all'estero» o acconsente alla loro comunicazione.

Il capoverso 2 è pertanto applicabile solo alle imprese di trasporto aereo svizzere, e non a quelle estere. Le prime possono comunicare i dati dei loro passeggeri a un'UIP estera soltanto se un trattato internazionale con la Svizzera lo prevede (cfr. art. 29).

Se il volo è stato invece prenotato dalla Svizzera presso un'impresa di trasporto aereo estera, la comunicazione transfrontaliera dei dati è retta dal diritto (estero) applicabile a tale impresa.

Le parti contraenti della Svizzera possono essere uno Stato estero o un organismo internazionale. Nel presente contesto, quale organismo internazionale va menzionata in particolare l'UE.

Se la parte contraente con cui la Svizzera negozia tale trattato garantisce una protezione adeguata dei dati (cfr. art. 16 cpv. 1 LPD), la Svizzera non è chiamata a concordare alcuna norma specifica per la protezione dei dati che essa stessa comunica. Per la comunicazione dei dati ai sensi del capoverso 2 è pertanto sufficiente un trattato internazionale che si limiti a disciplinare la reciprocità in materia di comunicazione dei dati.

Per contro, nel caso in cui la parte contraente non garantisca una protezione adeguata dei dati, il trattato internazionale, oltre alla reciprocità di cui sopra,

dovrà prevedere anche norme da osservare nel trattamento dei dati dei passeggeri aerei comunicati dalla Svizzera. In questo modo la parte contraente sarà in grado di garantire una protezione adeguata dei dati provenienti dalla Svizzera (cfr. art. 16 cpv. 2 lett. a LPD).

Le imprese di trasporto aereo svizzere comunicano già oggi i dati dei passeggeri aerei a Stati verso cui sono destinati i voli dalla Svizzera, ad esempio agli Stati Uniti e al Canada. In entrambi i casi, un accordo con la Svizzera rappresenta la base giuridica per la comunicazione dei dati. Entrambi gli accordi garantiscono inoltre la comunicazione dei dati anche all'UIP svizzera, non appena con la presente legge sarà introdotta la base giuridica necessaria al trattamento dei dati dei passeggeri aerei.

Ulteriori accordi sono in programma. Il pertinente mandato negoziale con l'UE è in fase di preparazione. L'accordo andrà a sostituire la disposizione transitoria attualmente in vigore (v. n. 1.2).

Cpv. 3

I dati dei passeggeri aerei vanno trasmessi all'UIP entro due diversi termini, ossia entro un periodo compreso tra le 48 ore le 24 ore prima dell'orario previsto di partenza nonché immediatamente dopo la chiusura dell'imbarco. La comunicazione di dati entro il primo termine, per quanto fornisca solo dati provvisori, permette all'UIP di disporre di un determinato margine di tempo fino all'arrivo del volo, il che è di fondamentale importanza soprattutto in caso di brevi voli. La comunicazione dei dati immediatamente dopo la chiusura dell'imbarco consente di *aggiornare* i dati già pervenuti e fornisce un quadro definitivo dei passeggeri aerei che effettivamente entrano in Svizzera o lasciano il Paese. L'UIP non può più consultare e pertanto nemmeno trattare i dati che le erano stati comunicati entro i termini previsti, laddove essi riguardino passeggeri aerei che non si sono imbarcati sul volo previsto.

Grazie alla comunicazione scaglionata, l'UIP può concentrarsi dopo l'imbarco sui dati che sono stati aggiornati o aggiunti.

Le imprese di trasporto aereo procedono autonomamente a comunicare i dati dei passeggeri aerei all'UIP. Il cosiddetto metodo PUSH corrisponde non solo alla raccomandazione dell'OACI[35], ma anche all'articolo 8 della direttiva PNR.

Cpv. 4

La presente disposizione conferisce al Consiglio federale la competenza per disciplinare i dettagli da osservare nell'ambito della comunicazione dei dati. I dettagli *tecnici* da definire comprendono tra l'altro i formati consentiti applicabili alla comunicazione dei dati dei passeggeri.

35 OACI, Guidelines on Passenger Name Record (PNR) Data, n. 2.7.3, reperibile sul sito www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_en.pdf

Il Consiglio federale si atterà alle prescrizioni dell'OACI che sono vincolanti per tutti gli Stati membri e quindi anche per la Svizzera. Queste norme internazionali garantiscono che la comunicazione dei dati avvenga in tutto il mondo secondo principi uniformi. S'intendono così evitare oneri supplementari per le imprese di trasporto aereo dovuti a differenti regolamentazioni in ciascun singolo Paese. Laddove sarà necessario precisare le prescrizioni internazionali, il Consiglio federale si baserà quanto più possibile sulle soluzioni dell'UE. In questo modo verrà dato seguito a quanto avevano chiesto i rappresentanti del settore dell'aviazione in sede di consultazione, ossia di rinunciare a uno «swiss finish» e, di conseguenza, a norme speciali per la Svizzera.

Art. 3 Obbligo di diligenza

Le imprese di trasporto aereo sono tenute a comunicare all'UIP i dati dei passeggeri aerei tempestivamente e conformemente alle prescrizioni tecniche (cfr. art. 2 cpv. 3 e 4).

Adottano inoltre tutte le misure ragionevolmente esigibili per adempiere a tale obbligo. In caso contrario, sono soggetti alle sanzioni previste dall'articolo 31.

Art. 4 Obbligo di informazione

L'articolo 4 impone alle imprese di trasporto aereo di informare *in modo adeguato* i passeggeri aerei, quando prenotano un biglietto aereo, che i loro dati comunicati al momento della prenotazione saranno trattati non solo in relazione al volo, ma anche conformemente alla LDPA.

L'articolo 13 dell'ordinanza del 31 agosto 2022[36] sulla protezione dei dati (OPDa) precisa la nozione di adeguatezza, sancendo che l'informazione deve avvenire in forma precisa, trasparente, comprensibile e facilmente accessibile.

Nel rapporto esplicativo sull'OPDa, l'Ufficio federale di giustizia rileva quanto segue: «In altri termini, ciò significa che il titolare del trattamento deve scegliere le modalità di comunicazione di modo che le informazioni più importanti siano sempre trasmesse alla persona interessata dal trattamento dei suoi dati personali al primo livello di comunicazione. Se la comunicazione avviene su un sito Internet, ad esempio, potrebbe costituire una buona pratica il fatto di mettere a disposizione in modo immediato tutte le informazioni essenziali, p. es. tramite una panoramica strutturata. La persona che desidera informazioni supplementari potrà cliccare su queste prime informazioni per aprire una finestra contenente maggiori dettagli. Occorre tuttavia precisare che la comunicazione mediante un sito Internet non è sempre sufficiente: la

36 RS **235.11**

persona interessata deve sapere che troverà tali informazioni su un determinato sito»[37].

Affinché i passeggeri possano esercitare i loro diritti, le imprese di trasporto aereo devono fornire in virtù dell'articolo 4 della presente legge almeno le seguenti informazioni:

- la menzione che i dati dei passeggeri aerei sono comunicati a fedpol;
- il titolo completo della presente legge quale base giuridica per il trattamento dei dati dei passeggeri aerei;
- il rinvio al diritto d'accesso di cui all'articolo 26;
- i dati di contatto di fedpol;
- il nome del servizio estero, se i dati sono comunicati all'estero.

Se un'impresa di trasporto aereo non rispetta il suo obbligo di informazione ai sensi dell'articolo 4 o non lo fa in maniera sufficiente, è soggetta a sanzioni ai sensi dell'articolo 31.

Si potrebbe rinunciare all'obbligo di informazione, poiché il trattamento dei dati dei passeggeri aerei è già previsto dalla legge (cfr. art. 19 LPD). Il fatto che tale obbligo sia comunque contemplato nella LDPA è tuttavia giustificato, visto 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 alle gravi forme di criminalità); e
- sotto una diversa responsabilità (impresa di trasporto aereo / fedpol).

Per quanto riguarda la comunicazione automatica al SIC delle rotte aeree disciplinata dall'articolo 11, l'IFPDT avrebbe preferito un obbligo di informazione più esteso per le imprese di trasporto aereo. In tale contesto, ricorda che la comunicazione automatica delle informazioni tramite un servizio ad hoc non deve avere come effetto un allentamento dell'obbligo di informazione.

Sezione 3: Trattamento dei dati da parte dell'UIP

Art. 5 Principi

Cpv. 1

Il capoverso 1 disciplina lo scopo del *trattamento dei dati*.

37 Rapporto esplicativo dell'Ufficio federale di giustizia del 31 agosto 2022 concernente l'ordinanza sulla protezione dei dati, pag. 35; www.bj.admin.ch > Stato & Cittadino > Protezione dei dati > Nuovo diritto in materia di protezione dei dati > Cos'è stato fatto finora, 2022 – Adozione delle nuove ordinanze (OPDa e OCPD)

I dati PNR devono poter essere utilizzati per combattere gravi forme di criminalità a titolo sia preventivo sia repressivo. L'elenco di cui al capoverso 1 distingue infatti tra scopo:

- *preventivo,* nel senso di individuare e prevenire tali reati (cfr. in particolare art. 6 cpv. 1 lett. a LAIn, art. 2*a* lett. f della legge federale del 7 ottobre 1994[38] sugli Uffici centrali di polizia giudiziaria della Confederazione e i centri comuni di cooperazione di polizia e doganale con altri Stati [LUC] nonché le leggi di polizia cantonali); e
- *repressivo,* nel senso di far luce su tali reati e ricercare gli imputati (cfr. in particolare art. 15–21 del Codice di procedura penale [CPP][39]) e i condannati per tali reati con decisione passata in giudicato che non hanno ancora scontato o non hanno scontato interamente la pena.

Sono previste limitazioni a questi scopi in caso di utilizzo di profili di rischio (art. 12) e di liste d'osservazione (art. 13 e 14).

Cpv. 2

I dati degni di particolare protezione (cfr. art. 5 lett. c LPD) non sono contenuti nei profili di rischio o nelle liste d'osservazione né all'interno dei dati dei passeggeri aerei di cui all'allegato 1.

Nel verificare le corrispondenze risultanti dal confronto automatico (cfr. art. 6 cpv. 2 e 3), l'UIP potrebbe tuttavia imbattersi in simili dati.

Quest'ultima può trattare questi dati soltanto laddove si tratti di dati di cui al capoverso 2, ossia:

- dati biometrici che identificano in modo univoco una persona fisica, per esempio impronte digitali, immagini del viso o dell'iride o registrazioni vocali;
- dati concernenti procedimenti o sanzioni amministrativi e penali; rientrano in tale novero anche le informazioni sugli atti materiali di polizia (misure di sicurezza e di protezione)[40].

Tutti gli altri dati degni di particolare protezione risultanti dal trattamento dei dati dei passeggeri aerei devono essere cancellati senza indugio dall'UIP (cfr. art. 22 lett. a).

38 RS **360**
39 RS **312**
40 Secondo la DTF **130** I 369, pag. 380 per atto materiale s'intende un'azione amministrativa effettiva e informale che si contraddistingue in particolare per il fatto di non mirare a produrre un effetto giuridico, bensì un risultato reale, pur potendo interferire sulla situazione giuridica di privati (originale in tedesco).

Art. 6 Confronto automatico dei dati

Il confronto automatico dei dati cui sono sottoposti tutti i dati dei passeggeri aerei deve avvenire entro un periodo di tempo limitato, ossia *immediatamente* dopo la trasmissione di tali dati all'UIP, ed è avviato automaticamente (cpv. 1).

Questo confronto serve a effettuare una prima distinzione dei dati dei passeggeri aerei tra:

- quelli che non hanno prodotto alcuna corrispondenza e che, fatti salvi gli articoli 8–11, non possono più essere trattati in modo approfondito, e
- quelli che hanno prodotto una corrispondenza e devono pertanto essere sottoposti a ulteriore verifica (cpv. 2 e 3) ed eventualmente comunicati all'autorità competente per l'ulteriore trattamento (cfr. art. 7).

Se la verifica ai sensi del capoverso 2 dà esito positivo, l'UIP comunica all'autorità competente, quale risultato del confronto automatico, i dati dei passeggeri aerei in questione (cfr. art. 7) e contrassegna i dati comunicati. L'autorità che riceve i dati dall'UIP decide in seguito le eventuali misure.

I dati contrassegnati sottostanno a un periodo di conservazione di cinque anni. Per contro, i dati non contrassegnati sono pseudonimizzati dopo un mese (cfr. art. 18) e cancellati automaticamente dopo ulteriori cinque mesi (cfr. art. 21).

Cpv. 1

I dati dei passeggeri aerei, non appena giungono nel sistema d'informazione dell'UIP, sono confrontati automaticamente con:

- i dati dei sistemi d'informazione di polizia ai sensi degli articoli 15 e 16 della legge federale del 13 giugno 2008[41] sui sistemi d'informazione di polizia della Confederazione (LSIP) nonché, in virtù dell'articolo 351 CP, con il sistema d'informazione di polizia di Interpol;
- con i profili di rischio ai sensi dell'articolo 12; e
- con le liste d'osservazione ai sensi degli articoli 13 e 14.

Nel caso in cui contenuti di un set di dati dei passeggeri aerei (cfr. all. 1), quali nome e cognome di un passeggero aereo, il suo numero di telefono o indirizzo di posta elettronica, si trovino anche in uno dei due suddetti sistemi d'informazione o in una lista d'osservazione, il confronto automatico dei dati produce una corrispondenza.

Entrambi i sistemi d'informazione con cui i dati dei passeggeri aerei sono confrontati automaticamente sono illustrati qui di seguito nel dettaglio.

41 RS **361**

Il *sistema di ricerca informatizzato di polizia (RIPOL; cfr. art. 15 LSIP)* contiene informazioni su persone segnalate ai fini dell'arresto o della ricerca, informazioni relative a reati non chiariti, a persone coinvolte in un reato nonché altre informazioni utili a far luce su reati. RIPOL offre sostegno alle autorità competenti della Confederazione e dei Cantoni quando si tratta di arrestare persone o prevenire pericoli per la sicurezza pubblica. Il confronto dei dati dei passeggeri aerei con RIPOL può contribuire non solo al successo della ricerca, ma anche a ottenere risultati nelle indagini su reati terroristici o altri reati gravi ai sensi dell'allegato 2 LDPA non chiariti. Chi è autorizzato a effettuare un confronto con RIPOL riceve automaticamente, in caso di confronto, anche le corrispondenze con la banca dati «Automated Search Facility» (ASF) di Interpol. Quest'ultima contiene informazioni su persone ricercate a livello internazionale, su veicoli rubati come pure su documenti di identità rubati o smarriti.

La *parte nazionale del Sistema d'informazione Schengen (N-SIS; cfr. art. 16 LSIP)* comprende le 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 N-SIS può permettere alle autorità competenti di arrestare persone ricercate a livello internazionale, al momento del loro ingresso nel Paese o della loro partenza.

Maggiori dettagli sui profili di rischio e sulle liste d'osservazione utilizzati nell'ambito del confronto automatico sono riportati nei commenti agli articoli 12–14.

Cpv. 2

Il fatto che il confronto automatico dei dati nel sistema d'informazione PNR abbia prodotto una corrispondenza non autorizza di per sé a effettuare una comunicazione all'autorità competente e a contrassegnare i dati (cfr. art. 7 cpv. 1).

L'UIP è chiamata infatti a verificare manualmente ogni singola corrispondenza per evitare che all'autorità competente possano essere comunicati risultanti del confronto che

- non sono conformi allo scopo previsto per il trattamento dei dati (cfr. art. 5 cpv. 1); o
- si riferiscono, per esempio a causa di una registrazione errata del nome, a un'altra persona.

Tali questioni possono essere sovente chiarite soltanto accedendo manualmente a ulteriori informazioni contenute nei sistemi di informazione di polizia e ad altri sistemi d'informazione della Confederazione.

Cpv. 3

Il capoverso 3 menziona i sistemi di informazione cui l'UIP può accedere per verificare le corrispondenze.

Lett. a

Per verificare se la corrispondenza riguarda effettivamente una fattispecie penale ai sensi dell'allegato 2, l'UIP deve accedere manualmente alle informazioni di base sulle circostanze di reato in RIPOL e N-SIS (v. commenti al cpv. 1) nonché nei seguenti sistemi d'informazione di polizia:

- il *sistema nazionale di indagine (SNI, art. 10 e 11 LSIP)* comprende informazioni relative alle indagini di polizia giudiziaria della Confederazione come pure alle indagini preliminari e di polizia giudiziaria dei Cantoni. Inoltre le informazioni sulla collaborazione della Polizia giudiziaria federale (PGF) con le autorità di perseguimento penale e le polizie giudiziarie dei Cantoni nonché con le autorità estere possono rivestire particolare importanza nella lotta alla criminalità organizzata internazionale;
- il *sistema di trattamento dei dati relativi alla cooperazione di polizia internazionale e intercantonale (IPAS, art. 12 LSIP)* contiene tra l'altro informazioni su indagini in corso condotte dalle autorità nazionali ed estere di polizia e di perseguimento penale;
- il *registro nazionale di polizia* (*art. 17 LSIP*) comprende informazioni di base sulle segnalazioni dei Cantoni;
- *SIRENE-IT* (conformemente all'*art. 18 LSIP*) contiene informazioni di base sulle segnalazioni nel sistema d'informazione Schengen nei settori della criminalità organizzata e del terrorismo;
- il *sistema d'informazione di Interpol (I-24/7, art. 350–352 CP)*: questo sistema dell'Organizzazione internazionale di polizia criminale (Interpol) contiene informazioni che consentono di risalire ai motivi delle segnalazioni internazionali.

Lett. b

Per accertare l'identità di una persona sono fondamentali in primis le informazioni registrate sulla persona e sul suo viaggio. A tal fine l'UIP deve poter accedere non solo a RIPOL e N-SIS, ma anche ai seguenti sistemi d'informazione della Confederazione:

- il *sistema nazionale visti (ORBIS, art. 109b LStrI)* 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;
- il *sistema d'informazione centrale sulla migrazione (SIMIC, legge federale del 20 giugno 2003*[42] *sul sistema d'informazione per il settore degli stranieri e dell'asilo, LSISA)* contiene dati personali relativi a cittadini stranieri che vivono o soggiornano in Svizzera (p. es.

42 RS **142.51**

cognome, nome, data di nascita) e al loro statuto di soggiorno. Tramite SIMIC ora è possibile consultare anche i dati provenienti dal sistema d'informazione per il rilascio a stranieri di documenti di viaggio svizzeri e permessi di ritorno ISR (ex art. 111 cpv. 1 LStrI). SIMIC permette così di consultare informazioni tratte dai documenti di viaggio quali nome e luogo d'origine di cittadini stranieri registrati in Svizzera o in possesso di un documento di viaggio rilasciato dalla Svizzera (p. es. titolo di viaggio per rifugiati);

- il *sistema d'informazione svizzero sui documenti d'identità (ISA, art. 11 della legge del 22 giugno 2001*[43] *sui documenti d'identità, LDI)* è gestito da fedpol e contiene i dati personali riportati nei passaporti e nelle carte di identità svizzeri quali nome, luogo d'origine, autorità di rilascio e servizio preposto all'allestimento del documento d'identità.

Le corrispondenze risultanti dal confronto automatico la cui verifica da parte dell'UIP ha dato esito negativo vano cancellate senza indugio (cfr. art. 22 lett. b). In caso di esito positivo, l'UIP ne dà comunicazione all'autorità competente, fornendo anche i pertinenti dati dei passeggeri aerei e contrassegnandoli (cfr. art. 7).

Art. 7 Comunicazione in caso di corrispondenza accertata

Cpv. 1

Solo le corrispondenze risultanti dal confronto automatico dei dati che sono state accertate dall'UIP sulla base di una verifica ai sensi dell'articolo 6 capoverso 2 possono essere comunicate all'autorità competente di cui all'articolo 1 capoverso 2 insieme ai relativi dati dei passeggeri aerei, quali risultati del confronto automatico.

Destinataria di questi risultati del trattamento è l'autorità che, secondo il sistema d'informazione, è indicata come competente nella segnalazione rilevante per l'ottenimento della corrispondenza o che fornisce il profilo di rischio o la lista d'osservazione che ha prodotto la corrispondenza.

È l'articolo 22 lettera b a stabilire quando la verifica di una corrispondenza comporta azioni diverse dalla comunicazione all'autorità competente. Devono quindi essere cancellate senza indugio le corrispondenze:

- non attribuibili o non chiaramente attribuibili a un reato di cui all'allegato 2 (art. 6 cpv. 3 lett. a); o
- per le quali non è confermata l'identità (art. 6 cpv. 3 lett. b).

Infatti, in tali casi la verifica delle corrispondenze risultanti dal confronto automatico ha esito negativo, il che impedisce la comunicazione a un'autorità competente e richiede dunque la cancellazione immediata.

43 RS **143.1**

Cpv. 2

Se la decisione di elaborare un profilo di rischio è stata presa dall'UIP (cfr. art. 12 cpv. 2 lett. b), manca un'autorità richiedente. Lo stesso vale quando l'UIP deve trasmettere un indizio su un reato che potrebbe essere commesso (cfr. art. 9). È inoltre possibile che una segnalazione non menzioni eccezionalmente l'autorità competente.

In tutti questi casi, l'UIP comunica i dati all'autorità di cui all'articolo 1 capoverso 2 che è quella che ha maggiore probabilità di essere competente per l'ulteriore trattamento. In caso di dubbio, l'UIP comunica i dati alla PGF. Se quest'ultima ritiene di non essere competente in materia, trasmette i dati all'autorità che considera competente. Nell'evenienza assai remota, che la PGF non riesca a individuare alcun'autorità competente, dovrà provvedere a cancellare i dati. Non appena l'UIP ne avrà preso conoscenza, revocherà il contrassegno dei dati in questione conformemente all'articolo 10 capoverso 1.

Cpv. 3

L'UIP contrassegna dal punto di vista *tecnico* i dati che sono stati comunicati a un'autorità di cui all'articolo 1 capoverso 2, che sono quindi da quel momento considerati come dati contrassegnati conformemente alla presente legge.

Excursus sui dati contrassegnati

Nella sua sentenza del 21 giugno 2022, la CGUE ha precisato in modo inequivocabile che una durata di conservazione di sei mesi per tutti i dati dei passeggeri aerei è da considerarsi ammissibile. Per contro, una conservazione che ecceda tale durata dovrebbe limitarsi allo stretto necessario a fini di indagini e di perseguimento penale:

«Nei limiti in cui, tuttavia, sono identificati, in casi particolari, elementi obiettivi, come i dati PNR […] che hanno dato luogo a un riscontro positivo verificato, che consentano di ritenere che taluni passeggeri potrebbero presentare un rischio in materia di reati di terrorismo e di reati gravi, un'archiviazione dei loro dati PNR appare ammissibile al di là di tale periodo iniziale»[44].

I dati che l'UIP ha comunicato a un'autorità competente in virtù dell'articolo 7 sono contrassegnati. Questa misura tecnica garantisce il differente trattamento *automatico* previsto dalla legge per i dati:

- che non presentano indizi relativi a gravi forme di criminalità e che, pertanto, non sono contrassegnati, e dopo un mese sono pseudonimizzati automaticamente e dopo ulteriori cinque mesi cancellati automaticamente (cfr. art. 21 cpv. 1); o
- che presentano indizi relativi a gravi forme di criminalità e che, pertanto, sono comunicati a un'autorità e contrassegnati e, in seguito, cancellati automaticamente dopo cinque anni (cfr. art. 21 cpv. 2).

44 Causa C-817/19, ECLI:EU:C:2022:491; punti 248–262.

Un contrassegno è tuttavia revocato, quando un'autorità competente comunica all'UIP che non necessita più dei dati (cfr. art. 10), in quanto gli indizi che hanno portato alla comunicazione dei dati non sono confermati o il sospetto iniziale nei confronti di una persona oggetto di una segnalazione di ricerca si rivela infondato. Una volta revocato il contrassegno, i dati vanno pseudonimizzati e in seguito cancellati o cancellati senza indugio in funzione della loro data di introduzione nel sistema d'informazione (cfr. art. 18 e 21).

Cpv. 4

Le richieste delle autorità competenti indirizzate all'UIP e i dati che quest'ultima comunica all'autorità richiedente devono poter esser comunicati in modo sicuro. Il Consiglio federale è autorizzato a disciplinare, a livello di ordinanza, i dettagli necessari a tal fine. Non si tratta tuttavia solo di definire la modalità di comunicazione, ma anche di chiarire la questione se le autorità devono scambiare i dati in maniera standardizzata tramite i punti di contatto nazionali. Nel caso dei corpi di polizia della Confederazione e dei Cantoni questo ruolo potrebbe essere assolto ad esempio dalla rispettiva Centrale operativa e d'allarme.

Art. 8 Comunicazione su richiesta

Questa disposizione si applica unicamente quando i dati dei passeggeri aerei richiesti *non* sono pseudonimizzati.

Se i dati richiesti sono invece pseudonimizzati, occorre prima chiedere la revoca della pseudonimizzazione (cfr. art. 19 o 20).

Cpv. 1

La comunicazione dei dati ai sensi dell'articolo 8 deve essere sufficientemente concreta e precisa. Per contro, le richieste di tipo generico, non ben specificate che possono produrre una moltitudine di risultati diversi non sono ammesse. Tale esigenza è esplicitata con l'espressione «nel singolo caso».

La richiesta deve altresì esporre in maniera plausibile le ragioni per cui i dati richiesti sono necessari ai fini della lotta a un reato di cui all'allegato 2.

Cpv. 2

L'UIP deve esaminare, sulla base della richiesta ed eventualmente di informazioni supplementari raccolte presso l'autorità richiedente, se i dati dei passeggeri aerei richiesti sono effettivamente collegati a un reato di cui all'allegato 2 (cfr. art. 7 cpv. 1).

I dati dei passeggeri aerei comunicati su richiesta di un'autorità competente devono essere contrassegnati (cfr. art. 7 cpv. 3).

Art. 9 Trasmissione di indizi

Cpv. 1

L'UIP può ricevere da un'UIP estera indizi di un possibile reato imminente di cui all'allegato 2 (cfr. art. 30).

L'UIP deve trasmettere un simile indizio all'autorità competente (cfr. art. 1 cpv. 2), la quale può effettuare, su tale base, accertamenti approfonditi ed eventualmente adottare le opportune misure per prevenire la commissione di tale reato.

Cpv. 2

Tra le altre informazioni che l'UIP comunica, su richiesta, all'autorità competente vi sono i dati dei passeggeri aerei della persona oggetto dell'indizio come pure le eventuali corrispondenze verificate, ottenute mediante un confronto dei dati conformemente all'articolo 6 capoverso 1.

Cpv. 3

In casi urgenti, l'UIP può comunicare immediatamente le informazioni ai sensi del capoverso 2, senza dover attendere una richiesta da parte dell'autorità competente.

Cpv. 4

Applicando per analogia l'articolo 7, l'UIP verifica in particolare se l'indizio trasmesso presenta effettivamente un nesso con il reato di cui all'allegato 2 (cfr. art. 7 cpv. 1).

Se l'UIP non è in grado di determinare con certezza quale autorità è competente per condurre ulteriori accertamenti, trasmette la comunicazione alla PGF che appura la competenza (cfr. art. 7 cpv. 2).

I dati, dopo esser stati trasmessi all'autorità competente, devono essere contrassegnati dall'UIP (cfr. art. 7 cpv. 3).

Art. 10 Revoca di contrassegni

L'autorità competente è in grado di esaminare il sospetto correlato ai dati comunicati in un quadro ben più ampio rispetto all'UIP. In tale contesto può giungere alla conclusione che gli indizi che hanno portato alla comunicazione dei dati non sono confermati o che il sospetto iniziale nei confronti di una persona oggetto di una segnalazione di ricerca si rivela infondato.

In tal caso l'autorità competente deve comunicare all'UIP che non necessita più dei dati che le sono stati trasmessi.

Non appena l'UIP prende conoscenza di questa informazione, è tenuta a revocare il contrassegno dei dati in questione. Questi dati sottostanno in seguito alle regole applicabili ai dati non contrassegnati (cfr. art. 18 e 21).

Occorrerà definire a livello d'ordinanza una procedura che ricordi alle autorità competenti, a intervalli regolari, il loro obbligo di informazione ai sensi

dell'articolo 10. Se tali autorità confermano entro un termine stabilito dall'UIP (p. es. di 10 giorni) che il sospetto nei confronti di una persona per gravi forme di criminalità persiste, i dati restano contrassegnati. Per contro, se l'UIP non riceve alcuna conferma in tal senso, revoca il contrassegno e, in funzione della data di registrazione nel sistema, pseudonimizza o cancella i dati ora non più contrassegnati. Questa procedura permette di evitare che i dati siano contrassegnati in modo ingiustificato e restino pertanto soggetti a un termine di conservazione di cinque anni.

Art. 11 Comunicazione al Servizio delle attività informative della Confederazione

Il SIC riveste una posizione particolare nella lotta ai reati terroristici e agli altri reati gravi. L'acquisizione da parte sua delle informazioni precede spesso le indagini di polizia e il perseguimento penale e serve all'individuazione precoce e alla prevenzione delle minacce alla sicurezza interna ed esterna.

Il SIC deve pertanto aver accesso ai dati grezzi relativi a determinate rotte aeree in vista del loro ulteriore trattamento, contrariamente al Servizio informazioni dell'esercito e alle autorità d'esecuzione cantonali ai sensi dell'articolo 9 LAIn.

Il trattamento dei dati dei passeggeri aerei da parte del SIC è retto dalla LAIn, che è completata di conseguenza (cfr. all. 3 n. 1). La LDPA si limita a disciplinare la comunicazione dei dati e lo scopo lecito del trattamento.

Cpv. 1

Il capoverso 1 precisa semplicemente che il SIC riceve i dati dei passeggeri aerei di determinate rotte aeree predefinite. Tali dati gli sono comunicati automaticamente senza essere in seguito contrassegnati.

Cpv. 2

Il SIC deve poter trattare autonomamente i dati dei passeggeri aerei ai fini dell'adempimento dei propri compiti ai sensi dell'articolo 6 capoverso 1 lettera a LAIn. Tuttavia, non è prevista la concessione al SIC di un accesso diretto al sistema d'informazione PNR. I dati gli sono comunicati automaticamente e soltanto in relazione a determinate rotte predefinite dal Consiglio federale.

Il SIC, conformemente alla presente legge, sottostà nel trattamento dei dati dei passeggeri aerei a un'ulteriore restrizione: può infatti trattare questi dati soltanto ai fini del contrasto dei reati di cui all'allegato 2 rientranti tra i suoi compiti ai sensi dell'articolo 6 capoverso 1 lettera a LAIn.

Il nuovo articolo 16*a* LAIn rinvia in modo esplicito allo scopo previsto dalla presente legge.

L'avamprogetto di LDPA sanciva già questo scopo, che è conforme peraltro alla sentenza CGUE. Quest'ultima trae la seguente ulteriore conclusione:

«Peraltro, il carattere tassativo delle finalità […] della direttiva PNR implica anche che i dati PNR non possono essere conservati in una banca dati unica che possa essere consultata per perseguire tanto queste finalità come altre. Infatti, la conservazione di questi dati in una banca dati siffatta comporterebbe il rischio che detti dati vengano utilizzati per fini diversi»[45].

Dallo scopo sancito al capoverso 2 si deduce infine che il SIC non è autorizzato a estendere lo scopo del trattamento sul piano tecnico. Non è pertanto necessaria alcun'ulteriore regolamentazione all'interno della LDPA.

Sezione 4: Profili di rischio e liste d'osservazione

Art. 12 Profili di rischio

L'articolo 12 fornisce la base legale relativa all'elaborazione e all'utilizzo di profili di rischio e contiene inoltre una definizione di tale strumento.

Grazie a una comprovata esperienza professionale e all'intuito dei collaboratori delle autorità di controllo oggi è ancora possibile individuare, tra la moltitudine di persone in entrata e in uscita dal Paese, determinati soggetti dal profilo criminale finora sconosciuti alle autorità competenti, di esaminarli in dettaglio e interrogarli in maniera approfondita o persino di arrestarli. Tuttavia, occorre considerare con occhio critico queste impressioni personali scaturite in occasione dei controlli, soprattutto perché sono di natura soggettiva e possono dare inconsapevolmente adito a discriminazioni. Per tale ragione e in considerazione del vistoso aumento negli ultimi anni del numero di persone che attraversano i posti di controllo, occorre oggi far maggior ricorso agli strumenti elettronici.

I profili di rischio nel quadro del PNR costituiscono uno di questi strumenti. Analogamente alla lista d'osservazione, sono impiegati nell'ambito del confronto automatico ai sensi dell'articolo 6 e permettono di richiamare l'attenzione sui dati dei passeggeri aerei che presentano combinazioni di dati spesso associate alle gravi forme di criminalità.

Il profilo di rischio impiegato nel quadro del PNR *non* può essere considerato al pari della profilazione (cfr. art. 5 lett. f e g LPD). Il confronto dei dati dei passeggeri aerei con il profilo di rischio non comprende infatti né un'analisi della persona in questione né una previsione sul suo comportamento.

I profili di rischio sono utilizzati per cercare determinati dati che appaiono in forma combinata all'interno di un set di dati dei passeggeri aerei. Una corrispondenza risultante da un confronto conferma unicamente che il set di dati oggetto della corrispondenza contiene la combinazione dei dati ricercata per mezzo del profilo di rischio.

Nella prassi, lo sviluppo dei profili di rischio rappresenta un'enorme sfida. Questo strumento può essere utilizzato in modo efficace soltanto se nella sua

45 Causa C-817/19, ECLI:EU:C:2022:491, punto 235.

concezione le competenze in materia criminologica sono affiancate da comprovata esperienza nel settore della consultazione dei dati.

Tutte le fasi del trattamento automatico devono essere documentate all'interno di un verbale elettronico. Lo stesso vale anche per l'utilizzo dei profili di rischio (cfr. art. 24).

I profili di rischio vanno cancellati non appena non sono più necessari (cfr. art. 22 lett. d).

Il Consiglio federale esegue verifiche riguardo all'utilizzo dei profili di rischio (cfr. art. 15).

Cpv. 1

Determinati crimini si traducono nei set di dati dei passeggeri aerei in combinazioni caratteristiche di dati, come nel caso della criminalità organizzata e, in particolare, della tratta di esseri umani. L'utilizzo di profili di rischio permette di ricercare sistematicamente tali combinazioni all'interno dei set di dati e, pertanto, di raccogliere indizi obiettivi su un reato di cui all'allegato 2 non ancora noto alle autorità.

Diversi partecipanti alla consultazione avevano rilevato con preoccupazione che i profili di rischio potrebbero presentare contenuti discriminatori. Tale preoccupazione è infondata. I profili di rischio *non* sono infatti composti da dati che concernono una persona fisica identificata o identificabile ai sensi dell'articolo 5 lettera e LPD. Di conseguenza, non possono neanche contenere dati personali degni di particolare protezione (cfr. art. 5 lett. c LPD).

Cpv. 2

I profili di rischio sono sempre elaborati dall'UIP.

Un profilo di rischio può scaturire da una richiesta scritta da parte di un'autorità competente ai sensi dell'articolo 1 capoverso 2. Quest'ultima deve indicare nella richiesta quali dati devono essere integrati nel profilo di rischio e a quale scopo.

L'UIP può tuttavia elaborare profili di rischio anche in assenza di tale richiesta, basandosi sulle informazioni che ha raccolto nel corso dell'attività quotidiana delle autorità di polizia e di perseguimento penale in Svizzera e all'estero.

In entrambi i casi, deve esaminare se i contenuti richiesti sono conformi allo scopo previsto e se sono sufficientemente concreti. Se constata che le informazioni fornite dall'autorità richiedente non sono ancora sufficientemente concrete, richiama l'attenzione di quest'ultima su tale aspetto e le offre sostegno nel precisare ulteriormente il profilo di rischio richiesto.

Cpv. 3

L'elaborazione di profili di rischio comporta esigenze elevate sul piano tecnico. Le esperienze raccolte all'estero dimostrano che i profili di rischio producono spesso un numero troppo elevato di corrispondenze.

Ciò è riconducibile alla scarsa precisione dei profili. Questi ultimi dovrebbero infatti contenere idealmente dati a carico e a discolpa.

Per motivi di protezione dei dati (cfr. art. 7 cpv. 3 LPD) e di economia processuale, i profili di rischio non devono mirare a produrre una serie di corrispondenze irrilevanti.

I profili di rischio devono essere pertanto tassativamente testati prima di essere utilizzati. Questi test devono essere condotti esclusivamente con dati generati artificialmente per mezzo di simulazioni.

Cpv. 4

I dati integrati in un profilo di rischio possono essere modificati soltanto dall'UIP, e pertanto da persone fisiche.

Art. 13 Liste d'osservazione

L'articolo 13 fornisce la base legale relativa all'elaborazione e all'utilizzo di liste d'osservazione e contiene inoltre una definizione di tale strumento.

Analogamente al profilo di rischio, le liste d'osservazione sono utilizzate nell'ambito del confronto automatico di tutti i nuovi dati dei passeggeri aerei appena ricevuti (cfr. art. 6 cpv. 1).

Tutte le fasi del trattamento automatico devono essere documentate all'interno di un verbale elettronico. Lo stesso vale anche per l'utilizzo delle liste d'osservazione (cfr. art. 24).

La cancellazione dei contenuti di una lista d'osservazione ai sensi dell'articolo 13 è retta dall'articolo 22 lettera d.

Il Consiglio federale esegue verifiche riguardo all'utilizzo delle liste d'osservazione (cfr. art. 15).

Cpv. 1

Le liste di osservazione di cui all'articolo 13 permettono di ricercare, in modo mirato e diretto, nei dati dei passeggeri aerei contenuti correlati a reati di cui all'allegato 2 che sono stati *commessi* e che sono noti alle autorità.

A differenza dei profili di rischio, le liste d'osservazione sono composte esclusivamente da dati concernenti una persona fisica o giuridica identificata o identificabile. Tale nozione riprende la definizione di dati personali in vigore fino all'abrogazione della legge federale del 19 giugno 1992[46] sulla protezione dei dati. Quest'estensione garantisce la possibilità di cercare i numeri di specifiche carte di credito, anche qualora tali carte non appartengano a una persona fisica, bensì a una persona giuridica.

46 RU **2022** 491

Le liste d'osservazione non contengono neanch'esse dati personali degni di particolare protezione, dato che neppure i dati biometrici contenuti nei documenti di viaggio fanno parte di un set di dati dei passeggeri aerei ai sensi dell'allegato 1 (cfr. categoria 18).

Cpv. 2

Il capoverso 2 stabilisce chi può chiedere una lista d'osservazione e quali scopi di trattamento definiti dall'articolo 5 capoverso 1 devono essere osservati nell'elaborazione e utilizzo di tale strumento.

A differenza di quanto previsto per i profili di rischio, l'UIP può elaborare e utilizzare le liste d'osservazione soltanto su richiesta di un'autorità di cui all'articolo 1 capoverso 2 lettera a. Il compito dell'UIP si limita a verificare se i contenuti richiesti siano conformi allo scopo previsto e se sono sufficientemente concreti.

La lista d'osservazione di cui all'articolo 13 può essere elaborata e utilizzata esclusivamente per i seguenti scopi:

- chiarire un reato terroristico e altri reati gravi di cui all'allegato 2 che sono *noti alle autorità* e che sono oggetto di una procedura investigativa o di un procedimento penale (lett. a); o
- ricercare una persona *identificata* che è imputata in relazione a un reato di cui all'allegato 2 (lett. b) o che, in quanto condannata a una pena detentiva con decisione passata in giudicato in relazione a un siffatto reato, cerca di sottrarsi all'espiazione della pena detentiva (lett. c).

Cpv. 3

Le liste d'osservazione possono essere elaborate e modificate soltanto dall'UIP, ossia da persone fisiche.

Art. 14 Integrazione di dati di terzi nella lista d'osservazione

L'articolo 14 prevede una norma speciale per l'integrazione di dati all'interno della lista d'osservazione ai sensi dell'articolo 13. L'inserimento di dati di terzi che non hanno alcun legame con il reato di cui all'allegato 2 permette di ricercare *indirettamente* persone identificate note alle autorità.

I dati di terzi devono permettere di risalire al luogo di soggiorno di persone ricercate in relazione a un reato di cui all'allegato 2. Nello specifico, deve trattarsi di un imputato nel quadro di un procedimento penale in corso o di una persona condannata con decisione passata in giudicato che deve espiare una pena detentiva per un reato di cui all'allegato 2.

L'articolo 270 CPP prevede una regola simile che autorizza la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni di terzi. Questa misura rappresenta tuttavia un'ingerenza molto più incisiva nei diritti

della personalità di terze persone rispetto alla misura prevista dal presente articolo, che dovrebbe rivelarsi peraltro decisamente meno costosa rispetto alla misura di cui all'articolo 270 CPP. Terze persone possono essere oggetto anche di una misura d'osservazione ai sensi dell'articolo 282 CPP.

La cancellazione dei contenuti di una lista d'osservazione ai sensi dell'articolo 14 è retta dall'articolo 22 lettera e.

Il Consiglio federale esegue verifiche riguardo all'utilizzo della lista d'osservazione (cfr. art. 15).

Cpv. 1

Nella lista d'osservazione possono essere integrati, per un periodo limitato, dati di terzi che non hanno alcun legame diretto con un reato terroristico o un altro reato grave di cui all'allegato 2.

La lista d'osservazione ai sensi dell'articolo 14 può essere richiesta per iscritto soltanto da un'autorità di cui all'articolo 1 capoverso 2 lettera a.

In tal caso, la richiesta deve essere indirizzata al giudice dei provvedimenti coercitivi competente per l'autorità in questione. I dati di terzi possono essere infatti integrati in una lista d'osservazione soltanto previa approvazione del competente giudice dei provvedimenti coercitivi.

La lista d'osservazione ha come scopo di permettere alle autorità di risalire, per mezzo dei dati dei passeggeri aerei di un terzo, al luogo di soggiorno di una persona ricercata in quanto imputata in relazione a un reato ai sensi dell'allegato 2 o in quanto, dopo esser stata condannata con sentenza passata in giudicato in relazione a un siffatto reato, cerca di sottrarsi all'espiazione della pena detentiva (art. 13 cpv. 2 lett. b e c).

Per terzo ai sensi dell'articolo 14 si intende una persona talmente vicina alla persona ricercata, sul piano professionale o privato, da rendere probabile l'ipotesi che possa recarsi nel luogo di soggiorno della persona ricercata per farle visita.

Al riguardo occorre tener presente che una lista d'osservazione con contenuti ai sensi dell'articolo 14 può essere efficace soltanto se la terza persona e la persona ricercata intrattengono rapporti nella vita reale e una delle due persone si trova in Svizzera. Se, invece, entrambe le persone si trovano in Svizzera, non avranno bisogno di recarsi in aereo oltre frontiera per incontrarsi. Se, infine, entrambe le persone dimorano all'estero, i dati relativi alla terza persona saranno ugualmente poco utili, dato che l'UIP svizzera dispone normalmente soltanto dei dati dei passeggeri di voli operati da o verso la Svizzera.

Cpv. 2

L'integrazione di tali dati nella lista d'osservazione ha una durata limitata che deve esser stabilita ugualmente dal giudice dei provvedimenti coercitivi.

Nel fissare la durata ammissibile, quest'ultimo ricorrerà verosimilmente a criteri simili a quelli adottati per misure analoghe ai sensi del CPP.

L'UIP deve cancellare i contenuti della lista d'osservazione alla scadenza della data stabilita dal giudice dei provvedimenti coercitivi (cfr. art. 22 lett. e).

Cpv. 3

Il giudice dei provvedimenti coercitivi comunica la sua decisione all'autorità richiedente e all'UIP.

Art. 15 Verifica dei profili di rischio e delle liste d'osservazione

I profili di rischio e le liste d'osservazione sono strumenti essenziali del PNR. Consentono di ottenere rapidamente e con uno sforzo contenuto informazioni che possono risultare importanti nella lotta alle gravi forme di criminalità.

Nel corso della consultazione è stata sollevata la necessità di verificare l'utilizzo di questi due strumenti. Poiché la verifica verterà principalmente sulla funzionalità di questi due strumenti essenziali del PNR, questo compito deve essere attribuito al Consiglio federale.

Cpv. 1

L'articolo 15 statuisce che l'utilizzo di profili di rischio e di liste d'osservazione deve essere oggetto di una verifica da parte del Consiglio federale.

Per poter essere utilizzati, è necessario che questi strumenti siano concepiti in modo tale da permettere di raggiungere gli scopi definiti dalla legge.

I profili di rischio che generano una moltitudine di corrispondenze inutili fanno perdere di vista l'essenziale e tengono inutilmente impegnate diverse risorse. I profili di rischio non sufficientemente precisi non possono essere giustificati dalla necessità.

Lo stesso vale per i profili di rischio che non sono fondati sugli attuali schemi comportamentali, dato che questi ultimi sono costantemente in mutazione. Se i profili di rischio non sono più attuali, non è più necessario utilizzarli e il loro contenuto va cancellato (cfr. art. 22 lett. d).

L'utilizzo delle liste d'osservazione è meno problematico, sebbene possa ugualmente generare inutili corrispondenze, ad esempio quando sono integrati cognomi diffusi senza ulteriori criteri che permettano di definire con maggiore precisione la persona ricercata.

Il motivo principale per cui le liste d'osservazione potrebbero rivelarsi non più necessarie potrebbe risiedere nel fatto che la persona ricercata è stata ritrovata. L'UIP è tenuta a cancellare i contenuti di una lista d'osservazione che non è più necessaria (cfr. art. 22 lett. d ed e).

Cpv. 2

I dettagli di tale verifica devono essere disciplinati a livello di ordinanza. Occorre tuttavia rinunciare alla pubblicazione di un rapporto come invece auspicato da diversi partecipanti alla consultazione. Ragioni di sicurezza e di protezione della personalità impongono infatti di rinunciare alla pubblicazione di un rapporto dall'alto valore informativo.

Sezione 5. Sistema d'informazione PNR

Art. 16

Cpv. 1

Il trattamento dei dati dei passeggeri aerei avviene all'interno del sistema d'informazione PNR. Maggiori dettagli al riguardo sono riportati al numero 6.1.

Cpv. 2

Fedpol gestisce il sistema d'informazione PNR, rivestendo il ruolo di titolare del trattamento ai sensi dell'articolo 5 lettera j LPD.

Fedpol è pertanto tenuto segnatamente:

- ad adottare i provvedimenti tecnici e organizzativi necessari affinché il trattamento dei dati personali sia conforme alle disposizioni sulla protezione dei dati (art. 7 cpv. 1 LPD);
- a garantire, mediante appropriate impostazioni predefinite, che il trattamento dei dati personali sia circoscritto al minimo indispensabile per lo scopo perseguito (art. 7 cpv. 3 LPD);
- a garantire, mediante appropriati provvedimenti tecnici e organizzativi, che la sicurezza dei dati personali sia adeguata al rischio (art. 8 cpv. 1 LPD);
- a tenere un registro delle attività di trattamento (art. 12 LPD);
- a effettuare una valutazione d'impatto sulla protezione dei dati, a condizione che siano adempiute le condizioni per allestire tale valutazione (art. 22 LPD);
- a notificare quanto prima all'IFPDT ogni violazione della sicurezza dei dati che comporta verosimilmente un rischio elevato per la personalità o i diritti fondamentali della persona interessata (art. 24 cpv. 1 LPD);
- a informare la persona interessata sulla violazione della sicurezza dei dati, se ciò è necessario per proteggere la persona interessata o se lo esige l'IFPDT (art. 24 cpv. 4 LPD).

È tenuto inoltre:

- a informare chiunque ne abbia fatto domanda, se dati personali che lo concernono sono oggetto di trattamento (art. 25 LPD, fatte salve le restrizioni ai sensi dell'art. 26 della presente legge);
- a consegnare a chiunque ne abbia fatto richiesta, fatte salve le restrizioni ai sensi dell'articolo 29 LPD, i dati personali trattati in modo automatizzato (art. 28 LPD);
- a trattare l'opposizione, presentata da una persona interessata, alla comunicazione dei suoi dati personali (art. 37 LPD);

- a trattare le richieste di una persona interessata ai sensi dell'articolo 41 LPD.

Gli articoli 17–26 LDPA contengono disposizioni che precisano in parte tali prescrizioni e prevalgono sulle disposizioni generali della LPD.

Cpv. 3 e 4

L'accesso ai dati dei passeggeri aerei e ai risultati del loro trattamento è riservato ai collaboratori che necessitano imperativamente di tale accesso per l'adempimento dei loro compiti. Il diritto d'accesso è attribuito in primo luogo ai collaboratori dell'UIP (lett. a). Anche il consulente per la protezione dei dati di fedpol deve disporre di un'autorizzazione d'accesso ai fini dell'adempimento dei compiti ai sensi della LPD (lett. b).

Devono ugualmente avere diritto d'accesso le persone che sono responsabili dello sviluppo, del perfezionamento o della manutenzione del sistema d'informazione PNR o che forniscono supporto tecnico (lett. c). Tale necessità deriva anche dall'assai ampia definizione di trattamento dei dati.

Per trattamento si intende infatti qualsiasi operazione relativa ai dati personali, indipendentemente dai mezzi e dalle procedure impiegati (cfr. art. 5 lett. d LPD). Il supporto agli utenti può pertanto già costituire un trattamento dei dati. Per quanto riguarda gli aspetti tecnici, entrano in linea di conto per il trattamento del PNR soltanto i fornitori di prestazioni che si sono aggiudicati l'appalto nell'ambito del bando di concorso OMC Alpin 2.0. Alpin 2.0 garantisce un pool di prestazioni di progetto per progetti chiave TIC, grandi progetti TIC o progetti complessi e strategici di tutta l'Amministrazione federale. Le commesse concrete vengono attribuite agli aggiudicatari nell'ambito di una procedura elettronica di mini-gara (concorso). Tutti i fornitori di prestazioni scelti per intervenire nel trattamento devono inoltre aver superato con successo un controllo di sicurezza ampliato.

La gestione e la manutenzione del sistema d'informazione PNR rientrano nella responsabilità del Centro servizi informatici CSI-DFGP e dei suoi collaboratori. A tal fine non viene fatto ricorso a fornitori di prestazioni esterni.

Infine, secondo la lettera d, anche le autorità competenti (cfr. art. 1 cpv. 2) devono poter accedere al sistema d'informazione PNR al fine di ricevere e trattare i dati che le sono comunicati dall'UIP. L'accesso è limitato al «prelievo» di tali dati.

Sezione 6: Protezione dei dati

Art. 17 Principi

I dati dei passeggeri aerei sono trattati non solo dall'UIP, ma anche dalle autorità federali e cantonali cui tali dati sono comunicati ai sensi della presente legge.

Nel quadro della consultazione era stata sottolineata la necessità di statuire nella legge che il trattamento dei dati è retto da basi legali in materia di protezione dei dati differenti in funzione dell'autorità competente.

In una prima fase occorre determinare se si tratta di un'autorità federale o cantonale e, pertanto, se è applicabile il diritto federale o cantonale. Un caso particolare è costituito tuttavia dalle autorità di perseguimento penale (v. commento al cpv. 2).

In una seconda fase occorre, invece, verificare se a una determinata autorità si applicano disposizioni particolari federali o cantonali che prevalgono sul diritto generale federale o cantonale in materia di protezione dei dati.

Cpv. 1

Nel suo messaggio del 15 settembre 2017[47] 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, (di seguito: messaggio concernente la nuova LPD), il Consiglio federale ha rilevato quanto segue:

«Va inoltre osservato che, alla stregua del diritto vigente, il D-LPD disciplina la protezione dei dati in generale. Se il trattamento di dati rientra nel campo d'applicazione di altre leggi federali, in virtù della regola della lex specialis (secondo cui le norme speciali prevalgono sulle norme generali) si applicano in linea di massima le norme sulla protezione dei dati specifiche a un determinato settore».

Quale autorità federale, l'UIP è tenuta a rispettare la LPD nel quadro del trattamento dei dati, salvo disposizione contraria della presente legge. Orbene, le disposizioni in materia di protezione dei dati della presente legge e in particolare gli articoli 17–26 vanno considerate disposizioni speciali e prevalgono pertanto sulla LPD.

Cpv. 2

Le disposizioni in materia di protezione dei dati previste dalla LDPA non si applicano alle autorità che ricevono i dati dall'UIP ai sensi della presente legge. A seconda dell'autorità interessata, non sono neanche applicabili le disposizioni della LPD.

Autorità di perseguimento penale federali e cantonali: nei procedimenti pendenti, la protezione dei dati da garantire è retta dal diritto procedurale applicabile e in particolare dagli articoli 95–103 CPP. Il diritto federale e cantonale in materia di protezione dei dati è applicabile soltanto una volta che il procedimento è chiuso (cfr. art. 99 cpv. 1 CPP). Si applica ugualmente alle procedure amministrative di primo grado (cfr. art. 2 cpv. 3 LPD). Nel messaggio concernente la nuova LPD, il Consiglio federale precisa a tale riguardo quanto segue:

47 FF **2017** 5939, in particolare 6003

«Secondo l'articolo 2 capoverso 3 D-LPD il trattamento di dati personali e i diritti delle persone interessate nei procedimenti giudiziari e nei procedimenti secondo gli ordinamenti procedurali federali sono retti dal diritto procedurale applicabile. La norma disciplina il rapporto tra la LPD e il diritto procedurale e stabilisce come principio generale che le modalità del trattamento di dati personali e i diritti delle persone interessate nell'ambito di procedimenti sono rette esclusivamente dal diritto procedurale applicabile. Il diritto procedurale garantisce anch'esso la tutela della personalità e dei diritti fondamentali di tutte le persone coinvolte assicurando così una protezione equivalente a quella della LPD. Se in questo settore si applicasse la LPD, si correrebbe il rischio di un conflitto normativo e di contraddizioni, che potrebbero intaccare il ponderato sistema del diritto procedurale applicabile»[48].

Autorità di polizia della Confederazione al di fuori di un procedimento penale: la protezione dei dati è retta dalla LPD, sempre che il diritto federale non preveda disposizioni speciali. Simili disposizioni sono presenti nella LSIP, nella LMSI e nell'ordinanza del 30 novembre 2001[49] sull'adempimento di compiti di polizia giudiziaria in seno all'Ufficio federale di polizia.

Autorità di polizia dei Cantoni al di fuori di un procedimento penale: la protezione dei dati è retta dalla legge cantonale sulla protezione dei dati, sempre che il diritto cantonale non preveda disposizioni speciali.

SIC: gli articoli 44–67 LAIn prevalgono sulle disposizioni della LPD.

Autorità d'esecuzione cantonali ai sensi dell'articolo 9 LAIn: ove tali autorità cantonali agiscano da autorità d'esecuzione cantonali ai sensi dell'articolo 46 capoverso 1 LAIn, sottostanno al diritto federale in materia di protezione dei dati, sempre che non prevalgano disposizioni particolari della LAIn. Per contro, se i servizi di informazione cantonali operano nel proprio settore di competenza cantonale, la protezione dei dati da garantire è retta dal diritto cantonale.

Art. 18 Pseudonimizzazione dei dati dei passeggeri aerei

La pseudonimizzazione consiste nel sostituire i dati che permettono di risalire a una persona concreta con indicazioni neutre (pseudonimi). Una tabella delle concordanze specifica lo pseudonimo che corrisponde ai dati di identificazione. La tabella deve essere registrata al di fuori del sistema d'informazione PNR. Fintanto che questa tabella esiste ed è accessibile alle persone autorizzate, la pseudonimizzazione può essere revocata (cfr. art. 19 e 20).

Nel quadro della procedura di consultazione, diversi partecipanti avevano chiesto, in parte richiamandosi alla sentenza CGUE, di ridurre considerevolmente la durata di conservazione dei dati che non necessitano di essere conservati per un periodo più lungo.

48 FF **2017** 5939, in particolare 6005
49 RS **360.1**

Viene quindi implicitamente chiesto che nell'intero campo d'applicazione del PNR sia effettuata una distinzione tra i dati che forniscono indizi obiettivi per ritenere che determinate persone possano rappresentare un pericolo in materia di reati terroristici o di gravi forme di criminalità («dati contrassegnati») e i dati che non forniscono invece alcun indizio in tal senso (altri dati relativi ai passeggeri aerei). La presente legge prevede quindi norme differenti per questi due tipi di dati.

Una di queste norme è rappresentata dalla pseudonimizzazione. Conformemente all'articolo 18, devono essere pseudonimizzati soltanto i dati che non sono stati comunicati a un'autorità competente e che non sono pertanto stati contrassegnati in virtù dell'articolo 7 capoverso 3. Allo stesso modo, i dati il cui contrassegno è stato successivamente revocato (cfr. art. 10) devono essere pseudonimizzati un mese dopo la loro introduzione nel sistema d'informazione PNR.

Conformemente al messaggio concernente la nuova LPD, la pseudonimizzazione costituisce un provvedimento tecnico appropriato per garantire la sicurezza dei dati personali (cfr. art. 8 LPD). Nello stesso messaggio, il Consiglio federale precisa inoltre che la LPD 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»[50].

La pseudonimizzazione consiste nell'attribuire uno pseudonimo ai dati contenuti in un set che permettono di risalire alla persona fisica interessata. Una volta pseudonimizzati, i dati in questione non possono essere più attribuiti a una persona identificata o identificabile, perdendo quindi il loro status di dati personali.

Nel suo messaggio concernente la nuova LPD, il Consiglio federale aggiunge che la pseudonimizzazione è un provvedimento tecnico che deve permettere di «evitare violazioni della sicurezza dei dati, ossia qualsiasi violazione in seguito alla quale, in modo accidentale o illecito, dati personali vanno persi, sono cancellati, distrutti, modificati oppure divulgati o resi accessibili a persone non autorizzate»[51].

Un set di dati dei passeggeri aerei contiene i seguenti dati personali ai sensi dell'articolo 5 lettera a LPD (cfr. all. 1 della presente legge):

- nome/i e cognome/i del passeggero aereo nonché nomi e cognomi di altri passeggeri figuranti nei dati PNR (categorie 4 e 17);
- indirizzo e dati di contatto (categoria 5);
- dettagli sulle carte di credito utilizzate e indirizzo di fatturazione (categoria 6);

50 FF **2017** 5939, in particolare 6011
51 FF **2017** 5939, in particolare 6022

- informazioni sui viaggiatori abituali («frequent flyer»; categoria 8);
- nome dell'agente dell'agenzia di viaggio che ha effettuato la prenotazione del biglietto (categoria 9);
- informazioni sui minori non accompagnati di età inferiore a 18 anni: nome e sesso, età, lingue parlate, nome e recapito dell'accompagnatore alla partenza e relazione di quest'ultimo con il minore, nome e recapito dell'accompagnatore all'arrivo e relazione di quest'ultimo con il minore, nome del collaboratore dell'aeroporto che accompagna il minore alla partenza e all'arrivo (categoria 12);
- dati API (cfr. art. 104 cpv. 3 LStrI), che sono al contempo dati personali: (a) generalità del passeggero aereo (cognome, nome, sesso, data di nascita, cittadinanza); (b) numero, Stato di rilascio, tipo e data di scadenza del documento di viaggio utilizzato; (c) numero, Stato di rilascio, tipo e data di scadenza del visto o del titolo di soggiorno utilizzato, nella misura in cui l'impresa di trasporto aereo disponga di questi dati (categoria 18);
- modifiche successive dei dati dei passeggeri aerei elencati nel set di dati (categoria 19).

I dati personali rientranti in queste categorie di dati devono essere pseudonimizzati.

Contrariamente a quanto avviene per l'anonimizzazione, la pseudonimizzazione può essere revocata a determinate condizioni.

I dati che presentano indizi obiettivi relativi a gravi forme di criminalità, che sono stati comunicati a un'autorità competente di cui all'articolo 1 capoverso 2 in vista di ulteriori accertamenti e che sono stati pertanto contrassegnati dall'UIP (cfr. art. 7) *non* devono invece essere pseudonimizzati.

Cpv. 1

I dati dei passeggeri aerei che *non* contengono indizi obiettivi relativi a gravi forme di criminalità e che, di conseguenza, non sono stati comunicati a un'autorità di cui all'articolo 1 capoverso 2 non sono contrassegnati (cfr. art. 7 cpv. 3). Tali dati sono pseudonimizzati automaticamente un mese dopo la loro introduzione nel sistema d'informazione PNR e non possono più essere attribuiti al passeggero aereo in questione.

I dati contrassegnati non sono invece pseudonimizzati.

Cpv. 2

Se l'autorità competente constata che non necessita più dei dati per i suoi procedimenti, lo comunica all'UIP. Quest'ultima revoca in seguito il contrassegno ai dati in questione (cfr. art. 10 cpv. 2).

In seguito alla revoca del contrassegno, l'UIP provvede a

- *pseudonimizzare* i dati, se il volo cui si riferiscono risale a un periodo compreso tra un mese e sei mesi prima; o

- *a cancellarli*, se il volo risale a oltre sei mesi prima (cfr. art. 21 cpv. 2).

Art. 19 Revoca ordinaria della pseudonimizzazione

Sono pseudonimizzati soltanto i dati personali contenuti in un set che non sono contrassegnati o il cui contrassegno è stato successivamente revocato (cfr. art. 18 cpv. 2).

Malgrado il confronto automatico dei dati dei passeggeri aerei ai sensi dell'articolo 6 e la successiva verifica manuale, il termine di un mese che intercorre fino alla pseudonimizzazione risulta molto breve. Deve essere pertanto possibile consultare i dati del sistema d'informazione PNR anche nel caso in cui risalgano a più di un mese e risultino, in quanto non contrassegnati, pseudonimizzati. Per effettuare simili ricerche di dati storici è necessario poter annullare, se del caso, la pseudonimizzazione.

L'articolo 19 statuisce che la pseudonimizzazione può essere revocata se il TAF considera adempiuti i presupposti legali e approva questa fase del trattamento.

Dal punto di vista tecnico è garantito che la revoca della pseudonimizzazione approvata dal TAF possa essere eseguita soltanto se:

- è effettuata da una persona abilitata a farlo; *e*
- la sentenza del TAF è menzionata o vi si rinvia in maniera sufficiente in altro modo.

Questa fase è verbalizzata affinché sia possibile verificare a posteriori se la pseudonimizzazione è stata eseguita conformemente al diritto (cfr. art. 24).

Secondo gli articoli 19 e 20 la pseudonimizzazione deve essere revocata se un'autorità competente lo richiede.

Se una richiesta d'accesso da parte della persona interessata ai sensi dell'articolo 26 capoverso 1 necessita della revoca della pseudonimizzazione, questa fase può essere effettuata in assenza di una decisione del TAF, quindi *non* in virtù delle disposizioni summenzionate. La pertinente base legale è costituita dall'articolo 25 capoverso 2 lettera b LPD, secondo cui alla persona interessata, nell'accesso accordatole, vanno comunicati «i dati personali trattati in quanto tali».

Tuttavia, occorre verbalizzare anche la revoca della pseudonimizzzione sulla base di una richiesta d'accesso (v. art. 24). Il verbale deve menzionare tale richiesta o rinviarvi in maniera sufficiente in altro modo. Le modalità saranno disciplinate in dettaglio a livello d'ordinanza.

Cpv. 1

Le autorità di cui all'articolo 1 capoverso 2 possono chiedere all'UIP la revoca della pseudonimizzazione.

Cpv. 2 e 3

In un primo momento, l'UIP verifica se la domanda è sufficientemente motivata, ossia se:

- i dati che dovrebbero essere oggetto della revoca della pseudonimizzazione sono ben definiti; tale requisito è soddisfatto quando la domanda di revoca concerne ad esempio una determinata persona. In casi eccezionali debitamente motivati, la domanda di pseudonimizzazione può riguardare anche un intero volo;
- è reso verosimile che la revoca della pseudonimizzazione fornisca informazioni determinanti ai fini del perseguimento di un determinato reato di cui all'allegato 2; le informazioni richieste devono essere descritte nel modo più preciso possibile.

Se la domanda non è motivata o non lo è in maniera sufficiente, l'UIP ne dà comunicazione all'autorità richiedente che ha in seguito la possibilità di apportare correzioni alla propria domanda (cpv. 3).

L'UIP raccomanda di revocare la pseudonimizzazione, laddove ciò permetta sul piano tecnico di ottenere le informazioni ricercate. Non è invece possibile ottenere sul piano tecnico le informazioni ricercate che non sono oggetto di un set di dati dei passeggeri o che risalgono a oltre sei mesi. Tali dati sono infatti già stati cancellati (in quanto non contrassegnati) o non sono stati pseudonimizzati (in quanto contrassegnati).

Se la domanda è sufficientemente motivata, l'UIP la trasmette al TAF, unitamente alla propria raccomandazione.

Cpv. 4 e 5

Il TAF decide su un'eventuale revoca della pseudonimizzazione. La competenza di un tribunale è richiesta anche dal diritto tedesco[52] e austriaco[53]in applicazione dell'articolo 12 paragrafo 3 della direttiva PNR.

Il tempo massimo concesso al TAF è di cinque giorni lavorativi. Tale termine non esenta tuttavia il TAF dal prendere immediatamente una decisione in funzione della gravità del sospetto.

La decisione è definitiva. I ricorsi presso il TAF per decisioni in materia di sicurezza interna o esterna della Svizzera sono inammissibili in virtù dell'articolo 83 lettera a della legge del 17 giugno 2005[54] sul Tribunale federale.

Cpv. 6

Il TAF notifica la sua decisione all'UIP e all'autorità richiedente.

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

53 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

54 RS **173.110**

Art. 20 Revoca della pseudonimizzazione in caso d'urgenza

La procedura in caso d'urgenza si fonda sull'articolo 31 LAIn.

In caso d'urgenza, il direttore di fedpol deve poter ordinare la revoca della pseudonimizzazione. In seguito deve informarne senza indugio il capo del DFGP che può far sospendere tale revoca (cfr. art. 31 cpv. 1 LAIn).

Quest'ultimo procede in tal senso soltanto se sussistono dubbi riguardo all'urgenza. La decisione di sospensione impone di annullare tutte le azioni già compiute per revocare la pseudonimizzazione e di attendere la decisione del TAF.

Il TAF decide entro tre giorni lavorativi in merito alla domanda del direttore di fedpol (cfr. art. 31 cpv. 2 e 3 LAIn).

In caso di decisione negativa da parte del TAF, tutte le azioni compiute in seguito alla decisione provvisoria ordinata dal direttore di fedpol devono essere completamente annullate.

Art. 21 Durata di conservazione e cancellazione dei dati dei passeggeri aerei

L'articolo 21 concerne esclusivamente i dati dei passeggeri aerei e ne disciplina la cancellazione e pertanto, indirettamente, la durata di conservazione.

La cancellazione di tutti gli altri dati risultanti dal trattamento effettuato dall'UIP o collegati a questo trattamento è retta dall'articolo 22. La cancellazione dei verbali costituisce un'eccezione (cfr. art. 24 cpv. 4).

Sono considerati cancellati ai sensi della presente legge i dati e le informazioni che sono stati cancellati irrevocabilmente e che non possono pertanto essere ripristinati. La cancellazione avviene in modo automatico, sovrascrivendo più volte lo spazio di memoria.

Nella sua sentenza del 21 giugno 2022, la CGUE ha precisato in modo inequivocabile che una durata di conservazione di sei mesi per tutti i dati dei passeggeri aerei *è da considerarsi ammissibile*. Per contro, una conservazione che ecceda tale durata dovrebbe limitarsi allo stretto necessario sul piano delle indagini e del perseguimento penale:

«Nei limiti in cui, tuttavia, sono identificati, in casi particolari, elementi obiettivi, come i dati PNR […] che hanno dato luogo a un riscontro positivo verificato, che consentano di ritenere che taluni passeggeri potrebbero presentare un rischio in materia di reati di terrorismo e di reati gravi, un'archiviazione dei loro dati PNR appare ammissibile al di là di tale periodo iniziale»[55].

Diversi partecipanti alla consultazione hanno sostenuto questo punto di vista, invocando in parte la sentenza CGUE nei loro pareri.

55 Causa C-817/19, ECLI:EU:C:2022:491; punto 259.

L'articolo 21 prevede quindi ora diverse durate di conservazione a seconda dei dati:

- per i dati non contrassegnati: sei mesi;
- per i dati contrassegnati che risalgono a più di sei mesi prima: fino alla revoca del contrassegno e al massimo cinque anni dalla loro introduzione nel sistema d'informazione PNR.

Questa regolamentazione indiretta permette inoltre di precisare che le durate di conservazione autorizzate sono da considerarsi come termini perentori.

Cpv. 1

Una durata di conservazione di sei mesi si applica a tutti i dati dei passeggeri aerei non contrassegnati. Trascorso questo termine, i dati sono cancellati automaticamente.

Cpv. 2

I dati dei passeggeri aerei contrassegnati possono essere conservati per un periodo di cinque anni, dopodiché sono cancellati automaticamente.

Se il contrassegno è revocato prima della scadenza della durata di conservazione prevista per i dati contrassegnati, l'UIP è tenuta, in funzione della loro data di introduzione nel sistema d'informazione PNR, a pseudonimizzare o cancellare immediatamente questi dati che sono nuovamente considerati come dati non contrassegnati (v. commento all'art. 18 cpv. 2).

Art. 22 Cancellazione di altri dati

Contrariamente all'articolo 21 che disciplina la cancellazione dei dati dei passeggeri aerei, l'articolo 22 verte sugli altri dati che possono risultare dal trattamento dei dati dei passeggeri aerei conformemente alla presente legge.

La cancellazione è effettuata «senza indugio», ossia subito dopo aver preso conoscenza delle circostanze che la impongono.

Sono considerati cancellati ai sensi della presente legge i dati e le informazioni che sono stati cancellati irrevocabilmente e che non possono, pertanto, essere più ripristinati. La cancellazione avviene in modo automatico, sovrascrivendo più volte lo spazio di memoria.

Lett. a

In virtù dell'articolo 5 capoverso 2 l'UIP può trattare soltanto i dati biometrici e i dati concernenti procedimenti o sanzioni amministrativi e penali e deve, quindi, cancellare senza indugio tutti gli altri dati personali degni di particolare protezione.

Lett. b

Tutte le corrispondenze risultanti dal confronto automatico devono essere verificate manualmente prima di essere comunicate a un'autorità competente (cfr. art. 6 cpv. 2).

La lettera b definisce in quali circostanze le corrispondenze verificate non vanno comunicate, bensì cancellate immediatamente.

Nello specifico, occorre procedere alla cancellazione quando le corrispondenze non sono chiaramente attribuibili a un reato di cui all'allegato 2 (cfr. lett. b n. 1) o nel caso in cui la persona cercata e il passeggero aereo non corrispondano (cfr. lett. b n. 2).

Lett. c

I dati dei passeggeri aerei che sono stati comunicati a un'autorità di cui all'articolo 1 capoverso 2 e che sono pertanto contrassegnati, sono cancellati automaticamente dopo un periodo di cinque anni, a condizione che il loro contrassegno non sia stato precedentemente revocato (cfr. art. 21 cpv. 2).

La lettera c statuisce che i dati che sono stati comunicati all'autorità competente unitamente ai dati dei passeggeri aerei devono essere cancellati, non appena questi ultimi siano stati cancellati.

Lett. d

I profili di rischio e le liste d'osservazione contengono dati che non sono cancellati in virtù dell'articolo 21. La lettera d prevede pertanto che tali dati debbano essere cancellati, non appena non siano più necessari.

Lett. e

Un caso particolare è costituito dai dati registrati in una lista d'osservazione ai sensi dell'articolo 14. Questi dati devono essere cancellati dopo la scadenza del termine stabilito dal giudice dei provvedimenti coercitivi (cfr. art. 14 cpv. 2). Qualora non dovessero risultare più necessari già prima della scadenza di tale termine, devono essere cancellati conformemente alla lettera d.

Art. 23 Trattamento di dati anonimizzati

I dati sono considerati anonimizzati se non sono più attribuibili a una persona identificata o identificabile e ciò ha carattere irrevocabile.

Con l'anonimizzazione i dati perdono *irrevocabilmente* il loro status di dati personali (cfr. art. 5 lett. a LPD). È proprio il carattere irrevocabile ciò che contraddistingue l'anonimizzazione dalla pseudonimizzazione. Quest'ultima può essere infatti revocata a determinate condizioni (cfr. art. 19 e 20), cosicché i dati possono essere nuovamente attribuiti a una persona identificata o identificabile.

L'UIP può trattare i dati anonimizzati a fini statistici. Può altresì offrirli all'Archivio federale per l'archiviazione (cfr. art. 6 della legge del 26 giugno 1998[56] sull'archiviazione).

56 RS **152.1**

Art. 24 Verbalizzazione del trattamento dei dati

Cpv. 1

Le fasi del trattamento che devono essere verbalizzate sono rette dall'articolo 4 capoverso 2 OPDa. Tale disposizione statuisce infatti che in caso di trattamento automatico dei dati personali occorre verbalizzare almeno la registrazione, modificazione, lettura, comunicazione, cancellazione e distruzione dei dati.

Il diritto svizzero in materia di protezione dei dati non contempla una definizione giuridica della nozione «automatizzato». Secondo le delucidazioni scritte dell'Ufficio federale di giustizia (UFG) del 23 novembre 2022 per «automatizzato» s'intende l'opposto di «manuale». A tale riguardo, l'UFG aggiunge che il trattamento manuale dei dati sottintende l'azione di una persona, mentre quello automatizzato è effettuato da una macchina. Si tratta di un apparecchio caratterizzato da un comando meccanico o elettronico che fa sì che le operazioni da esso eseguite in modo autonomo producano un risultato che risponde a un ordine precedente.

L'UFG sottolinea tuttavia che l'obbligo di verbalizzazione si applica anche ai casi in cui determinati processi di lavoro devono essere effettuati manualmente. Precisa inoltre che la verbalizzazione deve avvenire in particolare quando non è possibile stabilire a posteriori se i dati sono stati trattati conformemente agli scopi per i quali erano stati raccolti o comunicati.

In virtù dell'articolo 4 capoverso 4 OPDa, i verbali devono fornire informazioni:

- sull'identità della persona che ha effettuato il trattamento,
- sul tipo di trattamento,
- sulla data e l'ora del trattamento e
- sull'identità dell'eventuale destinatario dei dati.

I verbali permettono pertanto di verificare a posteriori ogni trattamento dei dati personali.

Cpv. 2 e 3

Il capoverso 2 definisce gli scopi perseguiti dalla verbalizzazione[57]. Il fatto che tali scopi siano enunciati in modo esaustivo esclude la possibilità che i verbali possano essere utilizzati per sorvegliare i collaboratori. Tale possibilità è esclusa anche dalle autorizzazioni d'accesso previste dal capoverso 3.

57 Rapporto esplicativo dell'Ufficio federale di giustizia del 31 agosto 2022 concernente l'ordinanza sulla protezione dei dati, pag. 26; /www.bj.admin.ch > Stato & Cittadino > Protezione dei dati > Nuovo diritto in materia di protezione dei dati > 1. Cos'è stato fatto finora, 2022 – Adozione delle nuove ordinanze (OPDa e OCPD)

Cpv. 4

I verbali sono allestiti in modo automatico e vanno conservati al di fuori del sistema d'informazione PNR. In questo modo viene garantito che i verbali non possano essere manipolati e restino al sicuro, anche in caso di ciberattacco. È prevista la registrazione dei verbali relativi al PNR nell'infrastruttura del CSI-DFGP.

Il rapporto esplicativo sull'OPDa precedentemente menzionato rileva che i verbali debbano essere conservati per almeno un anno (cfr. art. 4 cpv. 5 OPDa). «Questa durata minima non consente tuttavia di conservare i verbali per un periodo di tempo eccessivo. Il periodo di conservazione deve essere proporzionato al fine della sicurezza dei dati»[58].

La presente legge prevede che i verbali relativi al trattamento automatizzato dei dati dei passeggeri aerei siano disponibili un anno in più rispetto ai dati il cui trattamento è stato verbalizzato. Trascorso tale termine, vanno cancellati.

Fino alla loro cancellazione, i verbali devono essere disponibili per fini di controllo e sorveglianza, ma non per l'UIP.

Art. 25 Vigilanza e sorveglianza

Il consulente per la protezione dei dati di fedpol vigila sul rispetto delle norme sulla protezione dei dati all'interno di fedpol in modo indipendente e senza ricevere istruzioni (cfr. art. 26 cpv. 1 e 2 OPDa). Assolve tale compito anche al cospetto dell'UIP.

Funge inoltre da servizio di contatto dell'IFPDT (art. 28 OPDa).

Fedpol è tenuto nei confronti del consulente per la protezione dei dati a concedergli l'accesso a qualsiasi informazione, documento, registro delle attività di trattamento e dato personale necessario all'adempimento dei suoi compiti e a comunicargli eventuali violazioni della sicurezza dei dati.

Nonostante la funzione di assistenza e supervisione[59] attribuita al consulente per la protezione dei dati, la sorveglianza vera e propria è affidata all'IFPDT.

La responsabilità per la conformità del trattamento dei dati personali da parte dell'UIP alle norme in materia di protezione dei dati non incombe né al consulente per la protezione dei dati, né all'IFPDT, bensì soltanto a fedpol, come risulta dal messaggio concernente la nuova LPD[60].

Art. 26 Diritto d'accesso

Le imprese di trasporto aereo sono tenute a informare i loro passeggeri al momento della prenotazione dei biglietti aerei del trattamento dei dati che li riguardano conformemente alla presente legge (cfr. art. 4).

58 Ibidem
59 Ibidem, pag. 17; n. 4.7
60 FF **2017** 5939, in particolare 6024

Le informazioni fornite dalle imprese di trasporto aereo permettono alle persone interessate di esercitare il loro diritto d'accesso ai sensi dell'articolo 26. Le richieste d'accesso vanno presentate a fedpol.

I diritti d'accesso si distinguono in:

- *diritto d'accesso diretto (cpv. 1)*, che si applica ai dati risalenti a non oltre sei mesi ed è retto dagli articoli 25–28 LPD e
- *diritto d'accesso indiretto (cpv. 2)*, che si applica ai dati risalenti a oltre sei mesi ed è retto dall'articolo 8 LSIP.

Questo diverso approccio, adottato in funzione della data cui risalgono i dati, si spiega con il fatto che dopo sei mesi sono conservati soltanto i dati dei passeggeri aerei contrassegnati che sono in fase di trattamento presso l'autorità competente. Ora, l'accesso a dati relativi a un volo risalente a oltre sei mesi potrebbe segnalare al richiedente di essere oggetto di un procedimento in corso e che eventuali sospetti gravano sulla sua persona.

Fornire una simile informazione a una persona sospetta potrebbe così compromettere in modo significativo le indagini preliminari e le procedure investigative in corso.

Se è vero che l'articolo 26 capoverso 2 lettera b LPD prevede in tali casi la possibilità di rifiutare, limitare o differire l'informazione, è altresì vero che, secondo la stessa legge, occorre fornire un'altra informazione alla maggior parte dei passeggeri dello stesso volo, ossia che i loro dati non sono o non sono più trattati, in quanto sono già stati cancellati in virtù dell'articolo 21 capoverso 1.

Nel caso dei dati dei passeggeri aerei, il fatto di rifiutare, limitare o differire l'informazione ai sensi dell'articolo 26 capoverso 2 lettera b LPD sottintende che i dati in questione sono ancora trattati dopo la scadenza del periodo di sei mesi. La persona in questione potrebbe venirne così a conoscenza. I dati dei passeggeri aerei possono essere infatti trattati per un periodo superiore a sei mesi soltanto se sono contrassegnati e sono stati comunicati a un'autorità competente.

Per evitare quest'informazione indesiderata, la LDPA rinvia al diritto d'accesso indiretto ai sensi dell'articolo 8 LSIP.

A prescindere dalla presenza dei dati, in tali casi fedpol fornisce pertanto sempre la stessa risposta, ossia che l'informazione sarà differita. Il richiedente ha tuttavia il diritto di chiedere all'IFPDT di verificare se eventuali dati che lo riguardano sono trattati in modo lecito.

L'IFPDT procede alla verifica se indizi sufficienti lasciano presumere che un trattamento di dati potrebbe violare le disposizioni sulla protezione dei dati (art. 49 cpv. 1 LPD). Informa in seguito il richiedente sulle misure intraprese e sull'esito di un'eventuale inchiesta.

Questa informazione, di carattere elementare per il richiedente, non è mai rifiutata neanche nel quadro del diritto d'accesso indiretto previsto dall'articolo 8 LSIP, quindi neppure alle persone i cui dati sono contrassegnati presso l'UIP e trattati da un'autorità competente di cui all'articolo 1 capoverso 2.

Indipendentemente dalle considerazioni di cui sopra, fedpol deve fornire l'informazione al richiedente appena viene meno l'interesse al mantenimento del segreto, ma al più tardi allo scadere della durata massima di conservazione di cinque anni. Le persone di cui non sono stati trattati dati ne sono informate da fedpol tre anni dopo la ricezione della loro domanda (cfr. art. 8 cpv. 6 LSIP).

Sezione 7: Organizzazione e personale dell'UIP

Art. 27 Organizzazione

Cpv. 1

L'UIP deve essere collocata in seno a fedpol. Quest'attribuzione deriva, da un lato, dallo scopo del trattamento dei dati e, dall'altro, dalla vasta esperienza maturata da fedpol nella gestione di sistemi di informazione, che avrà senza dubbio ripercussioni positive sulla creazione e la gestione del sistema d'informazione PNR.

Cpv. 2

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. È ugualmente indicata in modo esplicito l'indipendenza sul piano del personale, escludendo così l'eventualità che singoli collaboratori possano lavorare contemporaneamente sia presso l'UIP sia presso un'autorità inquirente o di perseguimento penale.

Ciò permette di evitare che queste autorità ricevano in modo informale un accesso privilegiato a informazioni detenute dall'UIP. Tutte le autorità competenti di cui all'articolo 1 capoverso 2, siano esse federali o cantonali, saranno pertanto soggette alle stesse condizioni per ottenere dati dall'UIP.

Per quanto concerne il PNR, l'UIP collocata in seno a fedpol deve fungere da punto di contatto unico sia per le imprese di trasporto aereo sia per le UIP estere.

Ove necessario, garantirà un servizio operativo 24 ore su 24, sette giorni su sette, per poter verificare puntualmente anche in orari marginali i dati dei passeggeri aerei pervenuti.

Art. 28 Personale

L'UIP deve essere composta, in parti uguali, di collaboratori della Confederazione e dei Cantoni. Distaccando i propri collaboratori, i Cantoni partecipano ai costi dell'UIP. Non è prevista una loro partecipazione supplementare.

Poiché i collaboratori cantonali sono integrati *temporaneamente* nella struttura dell'UIP senza cessazione del loro rapporto di lavoro presso il Cantone, questo modello di collaborazione è maggiormente equiparabile al prestito di lavoro propriamente detto, che rappresenta un tipo di fornitura di personale a prestito. Nel suo messaggio del 27 novembre 1985[61] concernente la revisione della legge federale sul servizio di collocamento e la fornitura di servizi, il Consiglio federale osserva al riguardo:

«Il lavoratore non esegue la prestazione dovuta nell'impresa del suo datore di lavoro, ma appunto nell'impresa terza; questa situazione provoca una ripartizione delle funzioni padronali: il diritto di dare istruzioni concernenti lo scopo o la tecnica d'esecuzione del lavoro oppure il comportamento del lavoratore è trasferito, come pure il diritto di esigere la tutela degli interessi e del segreto, all'impresa terza, alla quale ovviamente è imposto anche il dovere di provvedere all'assistenza sociale del lavoratore. Gli altri diritti e obblighi risultanti dal contratto di lavoro, in particolare l'obbligo di corrispondere il salario e il dovere generale di assistenza sociale, continuano a incombere al fornitore di servizi».

Queste considerazioni si applicano per analogia al distacco di collaboratori presso l'UIP.

La Confederazione e i Cantoni devono disciplinare i dettagli relativi al distacco all'interno di una convenzione.

Al riguardo il Commentario basilese relativo alla Costituzione federale (Cost.)[62] 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 giuridica […] è possibile concludere in seguito un contratto con i Cantoni[63].

L'articolo 28 costituisce la base giuridica della convenzione che la Confederazione e i Cantoni devono concludere e definisce in particolare:

- lo scopo e la portata del distacco (cpv. 1),
- il finanziamento (cpv. 2) e
- le disposizioni speciali importanti in materia di diritto del personale (cpv. 3 e 4).

61 FF **1985** III 503, in particolare 510 seg.
62 RS **101**
63 Waldmann Bernhard / Belser Eva Maria / Epiney Astrid (a c. di), Basler Kommentar Bundesverfassung, Basilea 2015, art. 48 n. 37 (trad.)

Il capoverso 5 va inteso come una norma di delega e autorizza il Consiglio federale a disciplinare i dettagli summenzionati all'interno della convenzione con i Cantoni.

La questione se i Cantoni debbano disciplinare tra loro la partecipazione nel quadro di un concordato o in altro modo resta aperta e non necessita di essere regolamentata dal diritto federale.

Cpv. 1

Alla luce del sistema federalista della Svizzera, il lavoro di polizia e il perseguimento penale rientrano 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[64] sull'energia nucleare, nella legge dell'8 ottobre 1992[65] sui trapianti o nella legge del 20 giugno 1997[66] sulle armi.

In tale contesto, la lotta alle gravi forme di reato è intesa come un compito congiunto della Confederazione e dei Cantoni, ciascuno con le sue priorità. Trattando i dati dei passeggeri aerei, l'UIP sostiene in modo equivalente la Confederazione e i Cantoni nell'adempimento di questo compito congiunto.

Per tale ragione, l'UIP deve essere composta, in parti uguali, di collaboratori della Confederazione e dei Cantoni.

Cpv. 2

L'impiego dei collaboratori cantonali in seno all'UIP non comporta la cessazione dell'attuale rapporto di lavoro, ma soltanto una ripartizione del ruolo del datore di lavoro, come nel caso della fornitura di personale a prestito[67].

Il diritto di impartire istruzioni sul piano tecnico e operativo, che include tra l'altro il diritto di fissare gli orari di lavoro, è trasferito a fedpol durante l'impiego presso l'UIP. Il diritto di impartire istruzioni sul piano disciplinare resta invece di competenza dell'autorità che distacca il personale.

I restanti diritti e doveri derivanti dal contratto di lavoro, in particolare l'obbligo di pagare lo stipendio e di versare i contributi previsti dal diritto delle assicurazioni sociali permangono invece di competenza dell'autorità che mette i collaboratori a disposizione dell'UIP.

La Confederazione si assume integralmente i costi relativi all'infrastruttura delle postazioni di lavoro presso l'UIP nonché alla creazione e gestione del sistema d'informazione PNR.

64 RS **732.1**
65 RS **810.21**
66 RS **514.54**
67 Legge del 6 ottobre 1989 sul collocamento (LC; RS **823.11**)

Giova ricordare che in virtù dell'articolo 1 capoverso 1 lettera f della legge del 14 marzo 1958[68] sulla responsabilità, la Confederazione non è solo responsabile dei suoi collaboratori, ma anche di quelli distaccati dai Cantoni e impiegati presso l'UIP.

Cpv. 3

I capoversi 3 e 4 prevedono disposizioni speciali in materia di diritto del lavoro applicabili nel quadro dell'impiego presso l'UIP. Queste disposizioni necessitano di una base giuridica.

Le disposizioni speciali concernono in particolare:

- il diritto condiviso di impartire istruzioni (cpv. 3);
- l'obbligo per i collaboratori di rispettare il segreto professionale (cpv. 4) anche nei confronti del loro datore di lavoro contrattuale.

Il diritto di impartire istruzioni è considerato condiviso in quanto è esercitato sia dal datore di lavoro che distacca il suo personale sia da fedpol o dall'UIP. Quest'ultima esercita il diritto di impartire istruzioni tecniche e operative, il quale comprende tutto ciò che non rientra nel diritto di impartire istruzioni disciplinari, che spetta invece al datore di lavoro contrattuale.

Se durante il proprio impiego presso l'UIP, una persona distaccata denota un comportamento rilevante sul piano disciplinare, fedpol dovrà cercare il dialogo con il datore di lavoro contrattuale. Questi esaminerà in seguito le opportune misure disciplinari da adottare. Nella maggior parte dei casi, le istruzioni saranno sufficienti. In casi eccezionali, occorrerà invece pronunciare ai fini disciplinari la disdetta immediata del rapporto di lavoro. Anche questa possibilità resta di competenza del datore di lavoro contrattuale e non è pregiudicata dal distacco.

Cpv. 4

Il capoverso 4 stabilisce che ai collaboratori dell'UIP è vietato disporre liberamente al di fuori dell'UIP delle informazioni di cui sono venuti a conoscenza durante il loro impiego. Tale regola resta valida anche una volta terminato il loro impiego. In questo modo si vieta in particolare lo scambio informale di dati personali tra l'UIP e l'unità che distacca i propri collaboratori.

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 profili di rischio e le liste d'osservazione. Il modello di distacco sarà così in grado di garantire un trasferimento delle conoscenze dall'UIP alle autorità che distaccano i propri collaboratori.

68 RS **170.32**

Cpv. 5

Nella convenzione che il Consiglio federale deve concludere con i Cantoni occorre stabilire i dettagli relativi al distacco.

Nello specifico, si tratta di concordare, oltre al numero di collaboratori cantonali distaccati, anche le qualifiche auspicate. Particolare attenzione va rivolta ai collaboratori cantonali che hanno una spiccata affinità con i processi digitali. Le ulteriori pretese finanziarie dei collaboratori distaccati, che devono essere anche oggetto della convenzione, riguardano in particolare le spese. Il datore di lavoro contrattuale o il Cantone che distacca i propri collaboratori è tenuto a indennizzarle.

Sezione 8: Conclusione di trattati e di convenzioni e assistenza amministrativa

Art. 29 Conclusione di trattati e di convenzioni

69 Paesi utilizzano già il PNR, chiedendo perlomeno i dati dei passeggeri aerei relativi ai voli che atterrano sul proprio territorio.

L'articolo 2 della presente legge prevede una norma analoga a quella sancita dalla direttiva PNR: le imprese di trasporto aereo devono comunicare all'UIP svizzera i dati dei passeggeri aerei che entrano in Svizzera o ne escono.

Tuttavia, le imprese di trasporto aereo svizzere possono comunicare i loro dati dei passeggeri aerei a un servizio competente estero soltanto se un trattato internazionale concluso dalla Svizzera lo prevede (cfr. art. 2 cpv. 2).

Alla luce dell'articolo 29 che autorizza il Consiglio federale a concludere tali trattati, non è necessaria l'approvazione parlamentare (cfr. art. 166 cpv. 2 Cost.), a condizione che il contenuto del trattato sia conforme alla norma di delega ai sensi del capoverso 2.

Un accordo di questo tipo dovrà essere concluso in particolare con l'UE («organizzazione internazionale»). Sostituirà la soluzione transitoria elaborata di concerto con l'IFPDT che permette attualmente alle imprese di trasporto aereo svizzere di comunicare dati all'UE (v. n. 1.2).

Circa il 72 per cento di tutti i passeggeri registrati presso gli aeroporti svizzeri hanno come destinazione un Paese membro dell'UE o partono da uno di questi ultimi per recarsi in Svizzera. Sebbene questa quota elevata non consenta di dedurre direttamente il volume di dati provenienti dall'UE, mostra comunque che il traffico aereo tra UE e Svizzera è ragguardevole. Un trattato internazionale che disciplini la comunicazione reciproca di dati dei passeggeri aerei è pertanto fondamentale per la Svizzera e per l'UE. Il 1° novembre 2023 il Consiglio federale ha conferito il pertinente mandato negoziale.

Ulteriori trattati sono tra l'altro previsti con la Norvegia e il Regno Unito.

Cpv. 1

L'elenco di cui allegato 1 OPDa riporta gli Stati che garantiscono una protezione adeguata dei dati. La Svizzera può comunicare dati personali a questi Stati senza dover stipulare un trattato internazionale. Tuttavia, la presente legge prevede la conclusione di trattati anche con questi Stati al fine di garantire la comunicazione *reciproca* di dati. Se entrambi gli Stati contraenti constatano che il livello di protezione dei dati garantito reciprocamente è adeguato (cfr. art. 16 cpv. 1 LPD), il trattato si limiterà a regolamentare le modalità relative alla comunicazione reciproca dei dati.

Nel suo rapporto esplicativo concernente l'ordinanza sulla protezione dei dati, l'UFG spiega che l'elenco di Stati menzionati nell'allegato 1 dell'ordinanza «sarà riveduto periodicamente per tenere conto delle prassi di altri Stati e degli sviluppi internazionali, in particolare delle ratifiche della Convenzione 108. Esso non è quindi definitivo e potrebbe ancora essere modificato prima dell'entrata in vigore dell'ordinanza»[69].

Nel messaggio concernente la nuova LPD, il Consiglio federale ha rilevato che per trattato internazionale «non s'intende soltanto una convenzione internazionale sulla protezione dei dati di cui lo Stato destinatario sia parte, come ad esempio la Convenzione STE 108[70] e il suo Protocollo aggiuntivo, e i cui requisiti sono stati trasposti nel diritto nazionale, bensì anche qualsiasi altro trattato internazionale che preveda lo scambio di dati tra gli Stati contraenti e che rispetti sostanzialmente le condizioni della Convenzione STE 108. Può anche trattarsi di un trattato internazionale che il nostro Consiglio ha concluso in virtù dell'articolo 62 lettera b D-LPD [corrispondente all'attuale art. 67 lett. b LPD]» [71].

Cpv. 2

Considerato che la Svizzera non ha ripreso tutte le prescrizioni formulate dalla CGUE, non è escluso che l'accordo con l'UE preveda puntualmente norme più restrittive in materia di protezione dei dati che divergono dalla presente legge. Il capoverso 2 tiene conto di questo fatto, autorizzando il Consiglio federale a concordare, se necessario, all'interno di un trattato trattamenti meno ampi per i dati provenienti dall'UE.

Cpv. 3

Il capoverso 3 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.

69 Rapporto esplicativo dell'Ufficio federale di giustizia del 31 agosto 2022 concernente l'ordinanza sulla protezione dei dati, pag. 57; /www.bj.admin.ch > Stato & Cittadino > Protezione dei dati > Nuovo diritto in materia di protezione dei dati > 1. Cos'è stato fatto finora, 2022 – Adozione delle nuove ordinanze (OPDa e OCPD)

70 Convenzione del 5 giugno 1997 per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale, RS **0.235.1**

71 FF **2017** 5939, in particolare 6029 seg.

Le questioni fondamentali inerenti alla protezione dei dati o ai diritti e ai doveri delle autorità devono essere per contro sempre oggetto di un trattato internazionale concluso dal Consiglio federale in virtù del capoverso 1.

Art. 30 Assistenza amministrativa

Anche nel caso del PNR, l'assistenza amministrativa deve essere in linea di massima prestata dalle autorità competenti (cfr. art. 1 cpv. 2) conformemente al diritto a esse applicabile.

L'UIP deve prestare assistenza amministrativa soltanto in casi d'urgenza, ossia, come enunciato al capoverso 2, se sussiste il «pericolo imminente» che un reato ai sensi dell'allegato 2 venga commesso all'estero. Sono fatte salve, tuttavia, le disposizioni divergenti di un trattato internazionale.

L'assistenza amministrativa che l'UIP presta a un'UIP estera è pertanto limitata a casi eccezionali debitamente motivati, che giustificano l'intervento dell'UIP in luogo di un'autorità competente di cui all'articolo 1 capoverso 2.

Nel quadro dell'assistenza amministrativa, l'UIP comunica i dati dei passeggeri aerei a un'UIP estera soltanto su richiesta debitamente motivata da parte di quest'ultima. Tale richiesta deve specificare almeno:

- i dati auspicati, indicati in modo preciso;
- quanto questi dati siano necessari per prevenire un reato imminente di cui all'allegato 2.

L'UIP è autorizzata a comunicare i dati soltanto a un'UIP estera facente parte dell'amministrazione di uno Stato che:

- garantisce una protezione adeguata dei dati conformemente all'allegato 1 OPDa (cfr. art. 16 cpv. 1 LPD); o
- sulla base di norme specifiche previste in un trattato internazionale concluso con la Svizzera, garantisce una protezione appropriata dei dati (art. 16 cpv. 2 lett. a LPD).

Se nessuna delle suddette condizioni è soddisfatta, l'UIP rinuncia a comunicare i dati dei passeggeri aerei.

Se i dati richiesti sono pseudonimizzati o degni di particolare protezione, è esclusa ugualmente l'assistenza amministrativa da parte dell'UIP.

Sezione 9: Sanzioni amministrative

Art. 31 Sanzioni in caso di violazione degli obblighi delle imprese di trasporto aereo

Le sanzioni previste dall'articolo 31 costituiscono le cosiddette sanzioni amministrative pecuniarie. Sulla base delle vigenti norme del diritto federale, il Consiglio federale ha descritto questo tipo di sanzione nel suo rapporto del

1° novembre 2018[72] come segue: «semplificando, lo strumento può essere definito come una reazione delle autorità a una violazione avvenuta nel passato di una prescrizione di diritto amministrativo e che consiste nell'imporre alla parte il pagamento di un importo nel quadro di una procedura amministrativa».

Cpv. 1

Una violazione degli obblighi di diligenza e di informazione di cui agli articoli 3 e 4 deve essere sanzionata indipendentemente dal fatto che la Confederazione provi o meno la colpevolezza dell'impresa in questione, come previsto dal 1° ottobre 2015 nell'articolo 122*b* LStrI relativo alle violazioni dell'obbligo di comunicazione delle imprese di trasporto aereo. 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[73].

Cpv. 2

La violazione di un obbligo di cui all'articolo 3 della presente legge è presunta per legge quando l'impresa di trasporto aereo:

- omette di comunicare i dati dei passeggeri aerei o li comunica troppo tardi;
- non osserva le prescrizioni tecniche; o
- non comunica i dati di tutti i passeggeri del volo.

Lo stesso vale quando l'impresa di trasporto aereo non ha informato i suoi passeggeri del trattamento dei dati previsto dall'articolo 4 della presente legge (v. commento all'art. 4).

L'UIP deve fornire la prova che l'impresa di trasporto aereo non ha comunicato i dati conformemente alle prescrizioni legali o non ha informato i suoi passeggeri affatto o in modo adeguato del trattamento dei dati in virtù della presente legge.

Cpv. 3

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

Per converso, 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.

72 Sanzioni amministrative pecuniarie. Rapporto del Consiglio federale in adempimento del postulato 18.4100 della CIP-N del 1° novembre 2018, FF **2022** 776, n. 2.1

73 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** 2195, in particolare 2220

Cpv. 4

Nel rapporto summenzionato, il Consiglio federale ha precisato il concetto di sanzione amministrativa pecuniaria indipendente dalla colpa: «L'autorità amministrativa deve quindi quanto meno provare una colpa in termini di organizzazione (violazione oggettiva di un obbligo di diligenza). L'impresa può anche essere sanzionata in caso di comportamento illecito di un collaboratore responsabile. Questa via di mezzo ha dato buona prova nella prassi relativa al diritto sui cartelli e si lascia trasporre anche alle altre disposizioni che prevedono sanzioni amministrative pecuniarie. Nel complesso, non è quindi necessario intervenire a livello legislativo per quanto riguarda la colpa dei destinatari della sanzione»[74].

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

Cpv. 5

Il capoverso 5 garantisce che anche le violazioni degli obblighi di diligenza verificatesi all'estero possano essere sanzionate. È il caso ad esempio di un'impresa di trasporto aereo che non abbia comunicato affatto, in tempo o in modo completo all'UIP i dati dei passeggeri aerei prima della partenza verso la Svizzera.

Art. 32 Procedimento

Cpv. 1

Fedpol pronuncia le sanzioni previste dall'articolo 31.

Cpv. 2

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. Sono fatte salve tuttavia le violazioni dell'obbligo di informazione di cui all'articolo 4.

Cpv. 3

Il termine di due anni non può essere prorogato.

74 Sanzioni amministrative pecuniarie. Rapporto del Consiglio federale in adempimento del postulato 18.4100 della CIP-N del 1° novembre 2018, FF **2022** 776, n. 4.3.3

Sezione 10: Disposizioni finali

Art. 33 Esecuzione

Le disposizioni di esecuzione costituiscono prescrizioni subordinate o dettagliate che servono all'esecuzione della presente legge. La competenza del Consiglio federale di emanare tali disposizioni si fonda sull'articolo 182 capoverso 2 Cost.

Art. 34 Modifica di altri atti normativi

L'allegato 3 riporta le modifiche che devono essere apportate ad altre leggi in virtù della presente legge. Sono interessate dalle modifiche le seguenti leggi: LAIn, LStrI, LSISA, la legge del 17 giugno 2005[75] sul Tribunale amministrativo federale (LTAF), LSIP e LNA.

L'articolo 351 capoverso 1 CP costituisce la base legale che permette a fedpol di accedere al sistema d'informazione di Interpol (I-24/7). Poiché è collocata in seno a fedpol, l'UIP non necessita di una base legale supplementare per accedervi.

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 non devono essere nuovamente rilevati, ma vanno scissi.

Si parla di *codici comuni* (n. 15) quando un'impresa di trasporto aerea acquista posti a sedere da un'altra impresa responsabile del volo operato. Se un passeggero prenota tale posto, volerà con i codici di entrambe le imprese di trasporto aereo.

Il set di dati dei passeggeri aerei è analizzato in dettaglio anche nei commenti relativi all'articolo 1 capoverso 4.

Allegato 2 Reati terroristici e altri reati gravi

Le categorie di reato comprendono i reati terroristici (n. 1) e altri reati gravi (n. 2). La lotta a tali reati autorizza al trattamento dei dati dei passeggeri aerei in virtù della presente legge.

75 RS **173.32**

Originariamente tali categorie erano ispirate a quelle previste dalla direttiva PNR, cui erano associate le fattispecie penali determinanti ai sensi dell'allegato 1 LSIS, ampliato nell'ambito di PRÜM[76]. Tale ampliamento, sebbene non sia ancora in vigore, è considerato in questa sede. Lo stesso vale per un ulteriore completamento dell'allegato LSIS, che è attualmente in fase di elaborazione.

Inoltre, per via della mutata situazione geopolitica, sono prese in considerazione anche nuove gravi forme di spionaggio.

La seguente tabella riporta le fattispecie penali che sono state integrate nel catalogo dei reati in seguito alla consultazione.

1.7	Attentati contro l'ordine costituzionale (art. 275 CP)
2.1.14.1	Coazione sessuale (art. 189 cpv. 1 CP)
2.1.14.3	Atti sessuali con persone incapaci di discernimento o inette a resistere (art. 191 CP)
2.1.11.5	Sparizione forzata (art. 185bis nonché 260bis cpv. 1 lett. f^{bis} e cpv. 3 CP)
2.2.1.1	Casi gravi di spionaggio politico (art. 272 n. 2 CP)
2.2.1.2	Casi gravi di spionaggio economico (art. 273 terzo comma CP)
2.2.1.3	Casi gravi di spionaggio militare (art. 274 n. 1 quarto comma CP)

In compenso, sempre in seguito alla consultazione e tenuto conto delle spiegazioni della CGUE, il catalogo dei reati è stato snellito in modo significativo, tanto da contenere ora soltanto le fattispecie penali che:

a. secondo la CGUE rivestono un «livello di gravità indubbiamente elevato» (punto 149), presentano «un collegamento diretto con il trasporto aereo dei passeggeri» (punto 154) o un «carattere transnazionale» (punto 155);

b. conformemente al diritto svizzero prevedono una pena minima applicabile, che può essere intesa come una peculiarità del diritto nazionale menzionata dalla CGUE e che permette di dedurre la particolare gravità del reato (a contrario dal punto 151 seg.).

Le fattispecie penali inserite nelle categorie di reato collegate ai casi di spionaggio prevedono ugualmente una pena minima applicabile.

76 Decreto federale che approva e traspone nel diritto svizzero l'Accordo tra la Svizzera e l'UE sul potenziamento della cooperazione transfrontaliera (cooperazione Prüm) e il Protocollo tra la Svizzera, l'UE e il Principato del Liechtenstein riguardante l'accesso a Eurodac a fini di contrasto, FF **2021** 2332 pagg. 10–16

I commenti all'articolo 1 capoverso 4 forniscono spiegazioni supplementari in merito alle fattispecie penali di cui all'allegato 2.

Allegato 3 Modifica di altri atti normativi

1. Legge federale del 25 settembre 2015[77] sulle attività informative

Il SIC riveste una posizione particolare nella lotta ai reati terroristici e agli altri reati gravi. L'acquisizione da parte sua delle informazioni precede spesso le indagini di polizia e il perseguimento penale e serve all'individuazione precoce e alla prevenzione delle minacce alla sicurezza interna ed esterna.

Dopo aver ricevuto i dati dei passeggeri aerei, li confronta nei sistemi d'informazione IASA SIC e ISASA-GEX SIC e tratta eventuali corrispondenze nel sistema che le ha prodotte.

Per i dati di IASA SIC, l'articolo 21 dell'ordinanza del 16 agosto 2017[78] sui sistemi d'informazione e di memorizzazione del Servizio delle attività informative della Confederazione (OSIME-SIC) prevede una durata di conservazione compresa tra i 30 e i 45 anni a seconda del settore interessato. Le corrispondenze in ISASA-GEX SIC sono invece cancellate al più tardi dopo 15 anni (cfr. art. 28 cpv. 1 OSIME-SIC).

I dati dei passeggeri aerei che non hanno prodotto corrispondenze restano nella Memoria dei dati residui fino alla loro cancellazione dopo un mese dalla loro ricezione.

Art. 16a Dati dei passeggeri aerei

Il SIC è l'unica autorità competente che riceve i dati dei passeggeri aerei dall'UIP per trattarli autonomamente. La comunicazione dei dati dei passeggeri aerei è ammessa soltanto per le rotte stabilite precedentemente dal Consiglio federale in un elenco non pubblico. Il tenore del presente articolo è ispirato a quello dell'articolo 20 capoverso 4 LAIn.

Il SIC è tenuto a rispettare lo scopo sancito dall'articolo 11 capoverso 2 LDPA: può infatti confrontare e trattare i dati dei passeggeri aerei nel quadro dell'articolo 6 capoverso 1 lettera a numeri 1–5 LAIn soltanto se è necessario ai fini della prevenzione dei reati di cui all'allegato 2 LDPA (cpv. 2).

Secondo il capoverso 3, i dati che nell'ambito del confronto automatico nei due sistemi d'informazione del SIC non hanno prodotto alcuna corrispondenza devono essere cancellati automaticamente un mese dopo la loro trasmissione al SIC.

77 RS **121**
78 RS **121.2**

2. Legge federale del 16 dicembre 2005[79] sugli stranieri e la loro integrazione

L'articolo 109*b* LStrI costituisce la base legale per il sistema nazionale visti (ORBIS). Quest'ultimo fornisce informazioni sulle domande di visto e riporta 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.

Art. 109c lett. i Consultazione del sistema nazionale visti

La presente disposizione autorizza l'UIP ad accedere ai dati registrati in ORBIS per la verifica dell'identità dei passeggeri aerei (cfr. art. 6 cpv. 3 lett. b LDPA).

3. Legge federale del 20 giugno 2003[80] sul sistema d'informazione per il settore degli stranieri e dell'asilo

La LSISA disciplina il sistema d'informazione utilizzato nel settore degli stranieri e dell'asilo, in breve SIMIC. SIMIC contiene dati personali relativi a cittadini stranieri che vivono o soggiornano in Svizzera (p. es. cognome, nome, data di nascita) e al loro statuto di soggiorno. Tramite SIMIC ora è possibile consultare anche i dati provenienti dal sistema d'informazione per il rilascio a stranieri di documenti di viaggio svizzeri e permessi di ritorno. SIMIC permette così di consultare anche informazioni tratte dai documenti di viaggio quali nome e luogo d'origine di cittadini stranieri registrati in Svizzera o in possesso di un documento di viaggio rilasciato dalla Svizzera (p. es. titolo di viaggio per rifugiati).

Art. 9 cpv. 1 lett. q

La presente disposizione autorizza l'UIP ad accedere ai dati registrati in SIMIC per la verifica dell'identità dei passeggeri aerei (cfr. art. 6 cpv. 3 lett. b LDPA).

4. Legge del 17 giugno 2005[81] sul Tribunale amministrativo federale

Conformemente agli articoli 19 e 20 LDPA, il Tribunale amministrativo federale decide in merito alla revoca della pseudonimizzazione. Questo richiede modifiche alla LTAF.

79 RS **142.20**
80 RS **142.51**
81 RS **173.32**

5. Legge federale del 13 giugno 2008[82] sui sistemi d'informazione di polizia della Confederazione

La LSIP contiene le basi legali relative ai sistemi d'informazione di polizia con i cui dati sono confrontati automaticamente i dati dei passeggeri aerei (cfr. art. 6 cpv. 1 lett. a). Inoltre, l'UIP deve poter accedere manualmente ai dati dei singoli sistemi d'informazione di polizia al fine di verificare la conformità allo scopo legale delle corrispondenze prodotte automaticamente (cfr. art. 6 cpv. 3 lett. a).

Non è invece necessario statuire in modo esplicito l'accesso manuale da parte dell'UIP al sistema di gestione delle pratiche e degli atti ai sensi dell'articolo 18 LSIP al fine di verificare la conformità delle corrispondenze prodotte automaticamente (cfr. art. 6 cpv. 3 lett. a). L'articolo 18 capoverso 7 LSIP prevede infatti già l'accesso per i collaboratori di fedpol.

Ai fini della verifica dell'identità, l'UIP deve poter inoltre accedere anche a RIPOL e N-SIS (cfr. art. 6 cpv. 3 lett. b).

Art. 10 cpv. 4 lett. a^{bis} *Sistema di sostegno alle indagini di polizia giudiziaria della Confederazione*

Art. 11 cpv. 5 lett. b^{bis} *Sistema di trattamento dei dati relativi ai reati federali*

Queste due modifiche autorizzano l'UIP ad accedere manualmente ai dati del Sistema nazionale d'indagine (SNI) per verificare la conformità delle corrispondenze prodotte automaticamente allo scopo legale di cui all'articolo 6 capoverso 3 lettera a.

Art. 12 cpv. 6 lett. b^{bis} *Sistema di trattamento dei dati relativi alla cooperazione di polizia internazionale e intercantonale*

La presente modifica autorizza l'UIP ad accedere manualmente al sistema di trattamento dei dati relativi alla cooperazione di polizia internazionale e intercantonale (IPAS) per verificare la conformità delle corrispondenze prodotte automaticamente allo scopo legale di cui all'articolo 6 capoverso 3 lettera a.

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

La presente modifica autorizza l'UIP a confrontare automaticamente i dati dei passeggeri aerei con i dati del sistema di ricerca informatizzato di polizia (RIPOL), in virtù dell'articolo 6 capoverso 1 lettera a LDPA, e ad accedere manualmente a tale sistema per verificare la conformità delle corrispondenze

82 RS **361**

prodotte automaticamente allo scopo legale di cui all'articolo 6 capoverso 3 lettera a LDPA.

Art. 16 cpv. 2 lett. k^bis *Parte nazionale del Sistema d'informazione Schengen*

La presente modifica autorizza l'UIP a confrontare automaticamente i dati dei passeggeri aerei con i dati della parte nazionale del Sistema d'informazione Schengen (N-SIS), in virtù dell'articolo 6 capoverso 1 lettera a LDPA, e ad accedere manualmente a tale sistema per verificare la conformità delle corrispondenze prodotte automaticamente allo scopo legale di cui all'articolo 6 capoverso 3 lettera a LDPA.

Art. 17 cpv. 4 lett. a^bis *Registro nazionale di polizia*

La presente modifica autorizza l'UIP ad accedere manualmente al Registro nazionale di polizia per verificare la conformità delle corrispondenze prodotte automaticamente allo scopo legale di cui all'articolo 6 capoverso 3 lettera a LDPA.

6. Legge federale del 21 dicembre 1948[83] sulla navigazione aerea

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 31 LDPA.

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[84] sulla esecuzione e sul fallimento).

La nuova norma va applicata in caso di sanzioni in virtù non solo della LDPA, ma anche della LStrI, i cui articoli 122*a* e 122*b* prevedono disposizioni analoghe relative alle sanzioni nei confronti delle imprese di trasporto aereo.

In entrambi i casi la revoca dell'autorizzazione dell'esercizio può avvenire alle seguenti condizioni, ossia se:

- una sanzione ai sensi dell'articolo 31 LDPA o degli articoli 122*a* e 122*b* LStrI è passata in giudicato;
- il suo pagamento è stato più volte sollecitato senza successo.

83 RS **748.0**
84 RS **281.1**

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.

6 Ripercussioni

6.1 Ripercussioni per la Confederazione

Per poter utilizzare il PNR serve un apposito sistema d'informazione e occorre creare l'unità responsabile (UIP) presso fedpol.

Sistema d'informazione PNR

È previsto che la Svizzera adotti il sistema «goTravel» dell'ONU già utilizzato da diversi Paesi.

«goTravel» è un'evoluzione di TRIP, il sistema d'informazione PNR che i Paesi Bassi hanno sviluppato e messo a disposizione dell'ONU.

Da diversi anni, l'ONU mette «goTravel» a disposizione degli Stati membri e li sostiene nell'utilizzo del PNR nel quadro del suo programma di lotta ai viaggi con finalità terroristiche («Countering Terrorist Travel Programme»). In Europa TRIP è utilizzato in Belgio, mentre «goTravel» è impiegato in Lussemburgo e, dal 2022, in Norvegia.

Il fatto che sia in uso in diversi Paesi fa sì che «goTravel» sia in costante evoluzione. L'ONU rende accessibili questi sviluppi agli altri Stati che utilizzano tale sistema d'informazione PNR.

Tuttavia, ai fini di un suo utilizzo in Svizzera, «goTravel» necessiterà di adeguamenti tecnici. Questi adeguamenti saranno avviati dalla Svizzera e attuati dall'ONU.

Soltanto successivamente la versione di «goTravel» adeguata all'utilizzo in Svizzera sarà integrata nell'ambiente informatico del CSI-DFGP, il quale ne verificherà, insieme a fedpol, la funzionalità e la sicurezza.

I dati utilizzati nei test non saranno produttivi, bensì sintetici. Per dati sintetici s'intendono i dati creati artificialmente. Tutti i test saranno effettuati internamente; nessun dato relativo ai test lascerà l'ambiente di test e pertanto il CSI-DFGP. Se la verifica avrà dato esito positivo, «goTravel» sarà ammesso per l'impiego produttivo.

Nel quadro della sua collaborazione con la Svizzera, l'ONU non riceve in alcun modo i dati PNR o i risultati del loro trattamento effettuato in Svizzera. Questi dati sono registrati esclusivamente in Svizzera, nello specifico nell'ambiente informatico del CSI-DFGP, laddove non siano comunicati a un'autorità competente ai sensi della legge (cfr. art. 7–11 e 30).

Non sarà possibile realizzare il progetto sul piano tecnico presso fedpol senza il sostegno di fornitori di prestazioni esterni. Per quanto riguarda le questioni tecniche, entrano in linea di conto soltanto i fornitori di prestazioni che si sono aggiudicati l'appalto prevalentemente nel quadro del bando di concorso OMC Alpin.2.0. Alpin 2.0 garantisce un pool di prestazioni di progetto per progetti chiave TIC, grandi progetti TIC o progetti complessi e strategici di tutta l'Amministrazione federale. Le commesse concrete verranno attribuite agli aggiudicatari nell'ambito di una procedura elettronica di mini-gara (concorso). Tutti i fornitori di prestazioni prescelti dovranno inoltre aver superato con successo un controllo di sicurezza ampliato da parte della Confederazione.

La gestione e la manutenzione della versione di «goTravel» utilizzata dalla Svizzera rientrano nella responsabilità del CSI-DFGP. A tal fine non viene fatto ricorso a fornitori di prestazioni esterni.

Per la protezione dei dati da garantire mediante misure tecniche e organizzative si rimanda al numero **Fehler! Verweisquelle konnte nicht gefunden werden.**.

Costi

I costi di progetto e di esercizio del sistema d'informazione PNR come pure i costi di esercizio dell'UIP sono assunti interamente dalla Confederazione. Il personale si compone in parti uguali di collaboratori della Confederazione e dei Cantoni. Per un funzionamento a pieno regime dell'UIP (24 ore su 24, 7 giorni su 7) l'effettivo del personale dovrebbe ammontare a 30 equivalenti a tempo pieno. Tuttavia, per permettere di raccogliere esperienze con l'utilizzo dei dati PNR, si prevede di aumentare l'organico progressivamente. In una fase iniziale si stima pertanto un fabbisogno minore di personale, adibito a garantire le prestazioni di base dell'UIP.

a) Costi di progetto

Nel quadro del progetto «PNR Svizzera» fedpol crea le basi legali e i presupposti tecnici e organizzativi per il trattamento dei dati dei passeggeri aerei.

Nella fase di avvio del progetto è stato valutato se il sistema d'informazione PNR debba essere acquistato sul mercato o se debba essere il CSI-DFGP a svilupparlo. Poiché lo sviluppo in proprio è giudicato eccessivamente complesso e oneroso, nel quadro di una prova di fattibilità («Proof of Concept», PoC) è stato deciso di valutare se il sistema d'informazione PNR «goTravel» messo a disposizione dall'ONU soddisfa le esigenze e può essere integrato nell'ambiente informatico del CSI-DFGP. Nel giugno 2022 i committenti del progetto PNR hanno optato per «goTravel».

Nel caso in cui «goTravel» dovesse essere realizzato in Svizzera senza grandi adeguamenti, i costi di progetto dovrebbero ammontare a circa 11,5 milioni di franchi (di cui fr. 6,82 mio. con incidenza sul finanziamento) per il periodo 2020–2026. Questi costi sono stati preventivati come indicato di seguito in dettaglio:

	Costi di progetto 2020–2026 ***(in mio. fr.)***
Costi per prestazioni esterne e convenzioni con il fornitore di prestazioni CSI-DFGP	6,82
Costi per il personale interno a fedpol	4,69
Costi complessivi	**11,51**

Attualmente viene condotta una seconda prova di fattibilità più approfondita per verificare in maniera più dettagliata se i nuovi requisiti legali previsti in Svizzera possono essere attuati sul piano tecnico all'interno di «goTravel». Gli adeguamenti e gli sviluppi eventualmente necessari dovrebbero tuttavia essere attuabili soltanto nell'ambito di un ulteriore sviluppo a partire dal 2026.

b) Costi di esercizio del sistema d'informazione PNR e dell'UIP a partire dal 2026 (esclusi i costi per il personale)

L'esercizio del sistema d'informazione PNR e la manutenzione della struttura informatica (hardware, software, reti ecc.) presso il fornitore di prestazioni CSI-DFGP dovrebbero generare costi annuali pari a un massimo di 1,65 milioni di franchi a partire dalla messa in servizio operativa nel 2026. Sono incluse nel calcolo:

- l'infrastruttura del server per l'esercizio di «goTravel» e di tutti i componenti software necessari e la registrazione dei dati PNR nonché
- la registrazione dei verbali (cfr. art. 24).

Il DFGP sta attualmente sondando il mercato per chiarire i costi stimati che dovrebbero derivare dall'acquisto e dalla gestione del gateway di dati per la trasmissione dei dati dei passeggeri aerei da parte delle imprese di trasporto aereo al sistema PNR. Al contempo sono in corso verifiche per la creazione di sinergie con la SEM, che potrebbe utilizzare in futuro lo stesso gateway di dati per ricevere i dati API.

Secondo la pianificazione attuale, l'UIP dovrebbe essere istituita presso la sede principale di fedpol a Berna. I locali sono già disponibili, il che non dovrebbe comportare costi supplementari ragguardevoli. Ulteriori costi saranno generati per le singole postazioni di lavoro secondo la strategia in uso presso l'Amministrazione federale.

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

c) Costi per il personale

Il fabbisogno di personale dell'UIP dipende dagli orari di esercizio di quest'ultima, dal numero di rotte aeree previste nonché dal volume di dati da trattare. È previsto un aumento progressivo dell'organico. In una prima fase,

le prestazioni di base dovrebbero servire a utilizzare i dati PNR e a raccogliere esperienze in tale ambito. Pertanto, inizialmente un fabbisogno limitato di personale dovrebbe essere sufficiente. Ciò dovrebbe garantire un esercizio ridotto dell'UIP (riguardo all'orario di servizio e alla portata delle prestazioni). Per un funzionamento a pieno regime dell'UIP (24 ore su 24, 7 giorni su 7) l'effettivo del personale dovrebbe ammontare a 30 posti a tempo pieno.

A livello di Confederazione, il DFGP (fedpol) e il Dipartimento federale delle finanze (UDSC) mettono a disposizione i loro collaboratori. L'UDSC si è dichiarato pronto a collaborare all'UIP, mettendo a disposizione uno o due equivalenti a tempo pieno, laddove adempia una funzione di controllo delle persone, a titolo di delega, presso gli aeroporti di Basilea e Ginevra. I collaboratori di fedpol, diversamente da quelli dell'UDSC, saranno stabilmente in servizio presso l'UIP. Garantiranno così la continuità del lavoro e la «memoria operativa» in seno all'UIP, in particolare in qualità di membri della direzione dell'UIP, di responsabili dell'assistenza alle imprese di trasporto aereo e di rappresentanti dell'UIP in seno a organismi internazionali.

6.2 Ripercussioni per i Cantoni e i Comuni, per le Città, gli agglomerati e le regioni di montagna

Molte fattispecie penali che verranno contrastate in futuro tramite il PNR rientrano nella competenza in materia di perseguimento penale dei Cantoni. Grazie al PNR, le autorità cantonali di polizia e di perseguimento penale accedono in modo più agevole, rapido e mirato alle informazioni del traffico aereo che sono rilevanti ai fini dell'adempimento dei loro compiti.

I dati PNR consentono alle autorità cantonali di perseguimento penale di ricevere informazioni su persone ricercate a livello nazionale e internazionale che giungono in 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. Grazie all'utilizzo del 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. L'utilizzo del PNR dovrebbe infine fornire anche informazioni utili su reati non ancora chiariti.

Come lo dimostrano le esperienze raccolte all'estero, il PNR, e in futuro la LDPA, contribuiscono notevolmente ad aumentare l'efficienza e l'efficacia del perseguimento penale e della prevenzione della criminalità, con conseguenti ragguardevoli benefici anche per i Cantoni.

Dato che la maggior parte delle misure ai sensi del PNR sono adottate all'arrivo delle persone all'aeroporto, si stima che il trattamento 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.

Costi per il personale

I collaboratori dell'UIP sono distaccati in parti uguali dalla Confederazione e dai Cantoni che si fanno carico, ciascuna parte, dei relativi costi. I dettagli sono stabiliti all'interno di una convenzione tra Confederazione e Cantoni. Nell'ambito della procedura di consultazione, la Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia e la Conferenza dei comandanti delle polizie cantonali della Svizzera hanno giudicato favorevolmente il fatto che i Cantoni partecipino all'UIP distaccandovi il proprio personale. Una convenzione in tal senso viene attualmente elaborata con i Cantoni.

I collaboratori distaccati dai Cantoni presteranno servizio presso l'UIP a tempo determinato. Svolgeranno in primis compiti nell'ambito dell'attività principale dell'UIP, ossia la sorveglianza della comunicazione dei dati all'UIP da parte delle imprese di trasporto aereo come pure la verifica delle corrispondenze risultanti dal confronto dei dati dei passeggeri aerei con i sistemi d'informazione, i profili di rischio e le liste d'osservazione. Questa procedura garantisce il trasferimento delle conoscenze dalla Confederazione ai Cantoni e consente a questi ultimi di massimizzare i benefici offerti dal PNR.

Sarebbe opportuno che i Cantoni designassero almeno una persona di contatto per l'UIP e sarebbe altresì auspicabile che formassero anche specialisti provvisti delle conoscenze necessarie per presentare richieste mirate all'UIP e cooperare strettamente con quest'ultima nel singolo caso.

La LDPA non ha ripercussioni dirette sui Comuni e le regioni di montagna.

6.3 Ripercussioni sull'economia

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 il PNR è già utilizzato da 69 Paesi. Per le imprese di trasporto aereo che sono obbligate a comunicare i dati ai servizi statali competenti, questo compito non rappresenta pertanto una novità.

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. Questa constatazione trova riscontro anche nei pareri pervenuti nel quadro della procedura di consultazione svoltasi dal 13 aprile al 31 luglio 2022.

Va inoltre osservato che la comunicazione dei dati PNR da parte delle imprese di trasporto aereo è sempre più una condizione necessaria per operare voli verso determinate destinazioni. In caso di rinuncia alla LDPA e pertanto al PNR da parte della Svizzera, vi è quindi il rischio che le imprese di trasporto aereo svizzere possano essere sempre più penalizzate e che la Svizzera possa perdere la sua eccellente attuale connessione al traffico aereo internazionale.

Dal punto di vista economico occorre scongiurare nel modo più assoluto tale rischio.

Gli Stati Uniti considerano l'utilizzo del PNR come una condizione per restare nel suo VWP. Tale programma permette ai cittadini svizzeri di soggiornare negli Stati Uniti senza visto per motivi professionali o turistici per un periodo massimo di 90 giorni. Un'esclusione della Svizzera da questo programma potrebbe avere ripercussioni negative su singoli settori dell'economia svizzera.

6.4 Ripercussioni sulla società

In generale

Le gravi forme di criminalità destabilizzano una società e minano la fiducia nello Stato di diritto. Gli strumenti disponibili per contrastare tali crimini sono una condizione essenziale per la salvaguardia della sicurezza pubblica e uno sviluppo positivo della società.

Inoltre, l'osservanza delle prescrizioni in materia di protezione dei dati garantisce che i dati personali siano trattati in modo lecito e nel rispetto del principio di proporzionalità. Le persone interessate hanno per giunta il diritto di essere informate in merito al trattamento dei loro dati e, se del caso, di far verificare la legittimità di tale trattamento.

Anche i bambini sono vittime delle gravi forme di criminalità e necessitano di particolare protezione. Le esperienze raccolte in altri Paesi dimostrano che il PNR è uno strumento efficace per proteggere i minori dalla criminalità organizzata (p. es. tratta di esseri umani) o dalla pedocriminalità.

Excursus: PNR e minori

Di norma, i minori sono accompagnati nei viaggi da almeno uno dei loro genitori, in particolare nel traffico aereo. In tal caso, fino al compimento del dodicesimo anno di età, figurano quali altri viaggiatori, con indicazione della loro data di nascita, nel set di dati dei passeggeri aerei di uno o di entrambi i loro genitori. Tuttavia, se i genitori prenotano un biglietto aereo separatamente per il loro figlio, opzione possibile a partire dal quinto anno di età, il minore disporrà di un proprio set di dati dei passeggeri aerei. Al compimento dei 12 anni di età, i bambini sono considerati come adulti nel settore del trasporto aereo e disporranno sistematicamente di un proprio set di dati dei passeggeri aerei.

I bambini possono tuttavia anche viaggiare da soli. SWISS e Lufthansa prevedono questa possibilità a partire dai cinque anni, sempreché il minore sia accompagnato dal servizio di assistenza offerto dall'impresa di trasporto aereo durante tutta la durata del volo. Solo la Lufthansa registra annualmente circa 70 000 minori che si avvalgono di questo servizio.

In tal caso, la categoria 12 del set di dati dei passeggeri aerei fornisce le informazioni seguenti:

- nome, sesso, lingue parlate da minori non accompagnati di età inferiore a 18 anni;
- nome e recapito dell'accompagnatore alla partenza e relazione di quest'ultimo con il minore;
- nome e recapito dell'accompagnatore all'arrivo e relazione di quest'ultimo con il minore;
- nome e recapito del collaboratore dell'aeroporto che accompagna il minore alla partenza e all'arrivo.

7 Aspetti giuridici

7.1 Costituzionalità

La LDPA impone nuovi obblighi alle imprese di trasporto aereo. La Costituzione attribuisce alla Confederazione la competenza a legiferare in materia di trasporto aereo (cfr. art. 87 Cost.).

La LDPA costituisce la base legale per la gestione di un sistema d'informazione centrale che fornisca informazioni fondamentali per sostenere le competenti autorità della Confederazione e dei Cantoni nell'adempimento dei loro compiti di sicurezza, segnatamente nella lotta ai reati terroristici e ad altri reati gravi. Si tratta di compiti di sicurezza che il CPP attribuisce in parte alla Confederazione in virtù dell'articolo 123 capoverso 1 Cost. (lotta ai reati terroristici ed altri reati gravi che sottostanno alla giurisdizione federale). Queste competenze preesistenti della Confederazione sono fondamentali; gli aspetti inerenti alla sicurezza disciplinati dalla LDPA richiedono inoltre un coordinamento sotto la direzione della Confederazione. La LDPA può pertanto fondarsi sull'articolo 57 capoverso 2 Cost.[85].

7.2 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 (v. nota a piè di pag. n. **Fehler! Textmarke nicht definiert.**). Al contempo attua anche le norme dell'OACI relativi all'aviazione svizzera e garantisce la permanenza del Paese nel VWP degli Stati Uniti. Quest'adesione importante è per il momento soltanto di natura provvisoria (v. n. 1.1).

[85] Rapporto del Consiglio federale in adempimento del postulato Malama 10.3045 del 3 marzo 2010. Sicurezza interna: chiarire le competenze, FF **2012** 3973, in particolare 3999

L'avamprogetto di LDPA era ispirato ampiamente alla direttiva PNR, sebbene quest'ultima non avesse carattere vincolante. La sentenza CGUE ha parzialmente modificato l'interpretazione di questa direttiva. Neanche la sentenza CGUE ha valore vincolante. Tuttavia, alcuni aspetti centrali di questa sentenza sono stati presi in considerazione nel presente disegno, in particolare la riduzione a sei mesi della durata di conservazione dei dati che non forniscono indizi di gravi forme di criminalità e la limitazione del catalogo dei reati alle gravi forme di criminalità.

Il presente disegno di legge si basa sui risultati della procedura di consultazione e tiene conto degli elementi centrali della sentenza CGUE, nella misura in cui i pareri ricevuti in sede di consultazione rinviino a tali elementi e l'efficacia e l'efficienza dell'utilizzo PNR non siano state messe in discussione dalla stessa sentenza.

L'accordo del 21 giugno 1999[86] tra la Confederazione Svizzera e la Comunità europea sul trasporto aereo non è interessato dal presente disegno di legge.

7.3 Forma dell'atto

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

Inoltre, 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 disciplinare il trattamento dei dati dei passeggeri aerei all'interno di una legge formale deriva, infine, anche dalla LPD.

7.4 Subordinazione al freno alle spese

Il progetto non crea nuove disposizioni in materia di sussidi né stabilisce nuovi crediti d'impegno o limiti di spesa. Il progetto non è pertanto subordinato al freno alle spese (cfr. art. 159 cpv. 3 lett. b Cost.).

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

Sussidiarietà

Nel quadro della LDPA, la Confederazione è chiamata ad assumere un nuovo compito, ossia trattare i dati dei passeggeri aerei al fine di comunicarli alle autorità federali e cantonali per combattere le gravi forme di criminalità.

86 RS **0.748.127.192.68**

Ai fini dell'assunzione di nuovi compiti da parte della Confederazione occorre che il principio di sussidiarietà (cfr. art. 5*a* Cost.) sia motivato.

Il carattere internazionale del compito giustifica il trattamento dei dati dei passeggeri aerei da parte della Confederazione:

- questo compito permette alla Svizzera di adempiere diversi dei suoi obblighi internazionali (v. n. 1.1);
- gli Stati Uniti assoggettano la permanenza della Svizzera nel VWP all'attuazione quanto più rapida da parte di quest'ultima dell'utilizzo del PNR;
- lo scambio dei dati dei passeggeri aerei con l'estero richiede la conclusione di trattati internazionali con diversi Stati al fine di garantire la reciprocità con tutti gli Stati e una protezione dei dati appropriata. La competenza per la conclusione di questi trattati è affidata alla Confederazione.

Inoltre poiché, in virtù della Costituzione, compete alla Confederazione legiferare in materia di trasporti aerei, è opportuno che le sia affidato questo nuovo compito (cfr. art. 87 Cost.). L'utilizzo del PNR richiede infatti che l'UIP possa disporre dei dati che le imprese di trasporto aereo le comunicano. Conformemente alla presente legge, oltre all'obbligo di comunicazione, le imprese di trasporto aereo sono soggette anche a sanzioni nel caso in cui non comunichino i dati in tempo o in modo completo all'UIP. La competenza normativa in materia è affidata esclusivamente alla Confederazione.

Equivalenza fiscale

L'equivalenza fiscale deriva dall'articolo 43*a* Cost. Prevede un rapporto equilibrato tra beneficiari di una prestazione, responsabili dei costi e delle decisioni.

L'UIP, che è competente per il trattamento dei dati dei passeggeri aerei, può essere considerata come fornitrice di prestazioni. Mette infatti i risultati del trattamento dei dati dei passeggeri aerei a disposizione delle autorità federali e cantonali, che sono dunque i beneficiari di questo nuovo compito.

Dato che, in virtù della Costituzione, la responsabilità principale in materia di sicurezza interna, e in particolare nel settore della polizia, incombe ai Cantoni, è presumibile che a beneficiare maggiormente del PNR saranno i Cantoni. Neanche la soppressione di determinate categorie di reato in seguito alla procedura di consultazione incide sostanzialmente da questo punto di vista. Sono state cancellate soprattutto le fattispecie penali contemplate dal diritto penale accessorio della Confederazione, che concernono soltanto in maniera marginale i Cantoni. Alla luce di queste considerazioni, è giustificato che la metà dei collaboratori dell'UIP siano messi a disposizione e finanziati dai Cantoni.

L'altra metà dei collaboratori è invece messa a disposizione e finanziata dalla Confederazione, che assume inoltre i costi relativi al progetto, all'infrastruttura necessaria e all'esercizio dell'UIP.

Nel complesso, i Cantoni assumono pertanto meno della metà dei costi legati alla creazione di un sistema PNR in Svizzera.

In sede di consultazione, diversi Cantoni hanno chiesto che la Confederazione assuma interamente i costi. Ciò sarebbe tuttavia in evidente contrasto con il principio di equivalenza fiscale sancito dalla Costituzione, ragion per cui le richieste di tali Cantoni non possono essere accolte.

7.6 Delega di competenze legislative

L'*articolo 2 capoverso 4* conferisce al Consiglio federale la competenza a disciplinare a livello di ordinanza i requisiti tecnici che le imprese di trasporto aereo sono tenute a osservare nel comunicare all'UIP i dati dei passeggeri aerei. A tal fine, il Consiglio federale si ispira alle norme internazionali di OACI, OMD e IATA, che all'occorrenza vanno precisate.

L'*articolo 7 capoverso 4* conferisce al Consiglio federale la competenza a disciplinare i dettagli relativi a una comunicazione sicura dei dati tra l'UIP e le autorità competenti. Non si tratta tuttavia solo di definire la modalità di comunicazione, ma anche di chiarire la questione se le autorità devono scambiare i dati in maniera standardizzata tramite i punti di contatto nazionali. Nel caso dei corpi di polizia della Confederazione e dei Cantoni questo ruolo potrebbe essere assolto ad esempio dalla rispettiva Centrale operativa e d'allarme.

L'*articolo 15 capoverso 2* conferisce al Consiglio federale la competenza a definire i dettagli relativi alla verifica dei profili di rischio e delle liste d'osservazione. Inoltre, dovrà disciplinare la rendicontazione.

L'*articolo 29 capoverso 1* conferisce al Consiglio federale la competenza a concludere autonomamente trattati internazionali sulla comunicazione reciproca di dati dei passeggeri aerei. Quali possibili parti contraenti entrano in linea di conto soltanto gli Stati e le organizzazioni internazionali (UE) che possono garantire una protezione appropriata o, tramite disposizioni specifiche convenute, adeguata dei dati provenienti dalla Svizzera. I trattati devono garantire la reciprocità della comunicazione dei dati.

7.7 Protezione dei dati

La LDPA s'ispira in toto alla nuova LPD entrata in vigore il 1° settembre 2023. Ciò assume una rilevanza ancora maggiore se si considera l'importanza attribuita alla protezione dei dati dalla presente legge. Ciò trova conferma peraltro nei pareri espressi nel quadro della procedura di consultazione condotta nella prima metà del 2022. Diversi di questi pareri si fondano sulla sentenza CGUE. Il disegno di legge tiene conto dei punti centrali di tale sentenza, sebbene quest'ultima non abbia carattere vincolante per la Svizzera. Per esempio, la LDPA prevede la riduzione a sei mesi della durata di conservazione dei dati

che non presentano alcun indizio di gravi forme di criminalità come pure lo snellimento del catalogo dei reati e la conseguente limitazione alle gravi forme di criminalità effettive. Per contro, non sono stati presi in considerazione i contenuti della sentenza che avrebbero limitato considerevolmente l'efficienza e l'efficacia del PNR.

Dati personali

Il set di dati dei passeggeri aerei comprende diverse categorie. I dati personali sono gli unici rilevanti ai fini della protezione dei dati (art. 2 cpv. 1 lett. b LPD). Si tratta dei dati concernenti una persona fisica identificata o identificabile (art. 5 lett. a LPD). Dati di questo tipo sono contenuti nelle categorie 4–6, 8–9, 12, 17 e 18; la categoria 19 *può* contenere dati personali (cfr. all. 1 LDPA). Fanno parte di questi dati, tra gli altri, il nome, il numero di telefono, l'indirizzo del domicilio e l'indirizzo di posta elettronica del passeggero aereo.

I dati dei passeggeri aerei che non presentano alcun indizio relativo a un reato di cui all'allegato 2 e che pertanto non sono contrassegnati, sono pseudonimizzati automaticamente un mese dopo la loro introduzione nel sistema d'informazione PNR (cfr. art. 18). Una volta pseudonimizzati, i dati in questione non possono essere più attribuiti a una persona identificata o identificabile, perdendo quindi il loro status di dati personali. Diversamente dall'anonimizzazione, con cui i dati perdono irrevocabilmente il loro status di dati personali, la pseudonimizzazione può essere revocata (cfr. art. 19 e 20). Il TAF deve autorizzare questa fase del trattamento. Sul piano tecnico è previsto che solo le persone autorizzate possano eseguire questa decisione rinviando alla sentenza in questione.

Nel messaggio concernente la nuova LPD il Consiglio federale evidenzia che la pseudonimizzazione costituisce un provvedimento tecnico appropriato per garantire la sicurezza dei dati (cfr. art. 8 LPD). Afferma 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 […]. Tale regola vale anche per i dati pseudonimizzati»[87].

Dati personali degni di particolare protezione

La legge autorizza unicamente il trattamento dei dati degni di particolare protezione ai sensi dell'articolo 5 capoverso 2. L'UIP può eventualmente entrare in possesso di tali dati nell'ambito della verifica manuale delle corrispondenze risultanti dal confronto automatico (cfr. art. 6 cpv. 3 LDPA).

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

Il disegno di legge tiene conto delle riserve formulate dalla CGUE riguardo la descrizione di singole categorie di dati (cfr. all. 1 LDPA)[88]. È pertanto escluso per legge che l'UIP possa entrare in possesso di dati degni di particolare protezione tramite i dati dei passeggeri aerei. Tuttavia, l'articolo 22 lettera a prevede, a titolo preventivo, che l'UIP debba cancellare senza indugio i dati degni di particolare protezione non menzionati all'articolo 5 capoverso 2.

Durata di conservazione

Il disegno di legge statuisce che i dati non contrassegnati siano cancellati automaticamente sei mesi dopo la loro introduzione nel sistema d'informazione PNR (cfr. art. 21 cpv. 1). In tal senso, riprende quanto illustrato dalla CGUE nella propria sentenza del 21 giugno 2022:

«Pertanto, tenuto conto delle finalità della direttiva PNR e delle esigenze dell'indagine e delle azioni penali in materia di reati di terrorismo e di reati gravi, si deve giudicare che la conservazione dei dati PNR di tutti i passeggeri aerei assoggettati al sistema istituito da tale direttiva, durante il periodo iniziale di sei mesi, senza che vi sia il minimo indizio di una loro implicazione in reati terroristici o in reati gravi, non sembra, in linea di principio, eccedere i limiti dello stretto necessario, nella misura in cui essa consente le ricerche necessarie al fine d'identificare persone che non erano sospettate di partecipazione a reati terroristici o a reati gravi»[89].

Per contro, i dati contrassegnati (cfr. art. 7 cpv. 3) devono essere registrati per un periodo di cinque anni, a condizione che il loro contrassegno non sia stato già revocato (cfr. art. 21 cpv. 2). La CGUE considera anche tale durata di conservazione giustificata. A tale riguardo afferma infatti quanto segue:

«Nei limiti in cui, tuttavia, sono identificati, in casi particolari, elementi obiettivi, come i dati PNR dei passeggeri che hanno dato luogo a un riscontro positivo verificato, che consentano di ritenere che taluni passeggeri potrebbero presentare un rischio in materia di reati di terrorismo e di reati gravi, un'archiviazione dei loro dati PNR appare ammissibile al di là di tale periodo iniziale (…). Infatti, l'identificazione di tali elementi obiettivi sarebbe tale da stabilire un rapporto con le finalità perseguite dai trattamenti ai sensi della direttiva PNR, di modo che la conservazione dei dati PNR relativi a tali passeggeri sarebbe giustificata per il periodo massimo consentito da detta direttiva, ossia per cinque anni»[90].

I dati possono essere contrassegnati e rimanere assoggettati al periodo di conservazione di cinque anni soltanto nella misura del necessario. Tale durata di conservazione diventa superflua nel momento in cui l'autorità competente constata di non aver più bisogno dei dati. Questa circostanza si verifica ad

88 Causa C-817/19, ECLI:EU:C:2022:491, punti 130–140.
89 Causa C-817/19, ECLI:EU:C:2022:491, punto 255.
90 Causa C-817/19, ECLI:EU:C:2022:491, punti 259–260.

esempio quando un'indagine o un procedimento penale evidenzia che gli indizi obiettivi non sono giustificati. In tal caso, la LDPA prevede che l'autorità ne dia comunicazione all'UIP. Quest'ultima procede in seguito a revocare il contrassegno. I dati interessati risulteranno nuovamente non contrassegnati e sottostaranno alle pertinenti disposizioni.

I dati possono essere trattati soltanto per gli scopi previsti dalla legge (art. 6 cpv. 4 LPD).

Conformemente all'articolo 5 capoverso 1, i dati dei passeggeri aerei possono essere trattati soltanto ai fini della lotta alle gravi forme di criminalità. Le fattispecie ammesse figurano nell'allegato 2 della legge. I profili di rischio e le liste d'osservazione possono essere utilizzati soltanto per ulteriori scopi limitati (cfr. art. 12–14).

Prima di procedere alla comunicazione delle corrispondenze risultanti dal confronto automatico, l'UIP è tenuta a verificare se è rispettato lo scopo legale del trattamento (cfr. art. 6 cpv. 3 lett. a). Deve cancellare senza indugio le corrispondenze che non sono conformi a questo scopo (cfr. art. 22 lett. b n. 1).

Tale obbligo di verifica si applica per analogia anche alla comunicazione di altri dati a un'autorità competente (cfr. art. 8 cpv. 2 e art. 9 cpv. 3).

Se sono trattati dati personali occorre accertarsi della loro esattezza (art. 6 cpv. 5 LPD).

L'UIP è tenuta a verificare ciascuna corrispondenza risultante dal confronto automatico dei dati, se del caso, accedendo a sistemi d'informazione supplementari. La verifica deve riguardare anche l'identità del passeggero aereo in questione (cfr. art. 6 cpv. 3 lett. b). Se quest'ultimo non corrisponde alla persona ricercata, la corrispondenza deve essere cancellata senza indugio (cfr. art. 22 lett. b n. 2). Tale obbligo di verifica si applica per analogia anche agli altri risultati del trattamento prima della loro comunicazione a un'autorità competente (cfr. art. 8 cpv. 2 e art. 9 cpv. 3).

La protezione dei dati deve essere garantita per mezzo di provvedimenti tecnici adeguati (art. 7 LPD).

La protezione dei dati è attuata sul piano tecnico mediante automatismi che la LDPA prevede per le diverse fasi del trattamento quali la pseudonimizzazione dei dati non contrassegnati (cfr. art. 18 cpv. 1), la loro cancellazione dopo sei mesi come pure la cancellazione dei dati contrassegnati dopo cinque anni. Queste importanti fasi del trattamento vanno eseguite in modo costante e puntuale, ragion per cui sono automatizzate (cfr. art. 18 cpv. 1 nonché art. 22).

L'elaborazione di profili di rischio comporta esigenze elevate sul piano tecnico. I profili devono infatti fornire soltanto un numero limitato o strettamente necessario di corrispondenze e devono essere pertanto tassativamente testati prima del loro utilizzo. I test sono eseguiti esclusivamente con dati sintetici.

A complemento di questi test, il Consiglio federale verifica l'utilizzo dei profili di rischio. Questo tipo di sorveglianza rappresenta un provvedimento aggiuntivo volto a garantire che la struttura dei profili di rischio sia sempre aggiornata e che il loro utilizzo sia limitato allo stretto necessario (cfr. art. 15).

Per proteggere i dati occorre adottare anche provvedimenti organizzativi (art. 7 LPD).

Un provvedimento organizzativo è rappresentato, sul piano legale, dalla separazione dell'UIP in materia organizzativa e del personale dalle unità che sono potenzialmente destinatarie dei risultati del trattamento eseguito dalla stessa UIP (cfr. art. 27 cpv. 2). Grazie a tale provvedimento e all'obbligo di serbare il segreto cui sono sottoposti i collaboratori dell'UIP (cfr. art. 28 cpv. 4), viene ridotto al minimo sul piano organizzativo e legale il rischio di uno scambio informale da persona a persona.

La presente legge prevede inoltre che in due ambiti l'UIP non possa prendere decisioni in maniera autonoma, ma che dipenda invece da una decisione giudiziaria emanata da:

- il giudice dei provvedimenti coercitivi competente che decide se una lista d'osservazione contenente dati di terzi possa essere utilizzata (cfr. art. 14);
- il TAF che decide se sono adempiuti i presupposti che autorizzano la revoca della pseudonimizzazione per determinati dati (cfr. art.19 e 20).

I provvedimenti tecnici garantiscono ugualmente una sicurezza adeguata dei dati dei passeggeri aerei (art. 8 LPD).

La protezione dei dati individuali è possibile soltanto, se sono adottati al contempo provvedimenti tecnici di carattere generale in materia di sicurezza dei dati. La sicurezza dei dati concerne i dati disponibili e comprende il quadro tecnico e organizzativo generale del trattamento dei dati. Conformemente all'articolo 8 LPD, fedpol è tenuto a prevedere un'architettura di sicurezza adeguata affinché i dati dei passeggeri aerei e i risultati del trattamento siano al sicuro.

Questi dati e risultati sono registrati all'interno dell'Amministrazione federale presso il CSI-DFGP. Lo stesso vale per i verbali che vanno tuttavia registrati separatamente dai dati operativi.

Come menzionato dal Consiglio federale nel messaggio concernente la nuova LPD, la pseudonimizzazione costituisce un provvedimento nel senso sopra indicato[91]. La LDPA contempla la pseudonimizzazione (cfr. art. 18) dei dati non contrassegnati dei passeggeri aerei. Fanno parte di questi dati anche i dati il cui contrassegno è stato revocato a posteriori e che sono stati introdotti nel sistema d'informazione PNR al minimo un mese e al massimo sei mesi prima (cfr. art. 18). La pseudonimizzazione consiste nell'attribuire uno pseudonimo

91 FF **2017** 6941, in particolare 6022

ai dati contenuti in un set che permettono di risalire alla persona fisica interessata.

La pseudonimizzazione, diversamente dall'anonimizzazione, può essere revocata, ma unicamente previa autorizzazione del TAF (cfr. art. 19 e 20). Sul piano tecnico, solo la direzione dell'UIP è autorizzata ad attuare una tale decisione del TAF, nella misura in cui accede alla tavola delle concordanze per revocare la pseudonimizzazione nei limiti autorizzati. Nell'effettuare l'accesso, la persona autorizzata deve ugualmente indicare la decisione con cui il TAF autorizza tale operazione.

Tutti questi provvedimenti motivano quanto affermato dal Consiglio federale nel messaggio summenzionato: «La legge [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»[92].

Analisi del bisogno di protezione e valutazione d'impatto sulla protezione dei dati

Per ogni progetto informatico, l'Amministrazione federale effettua un'analisi preliminare del bisogno di protezione. Il momento dell'analisi è stabilito in base al modello HERMES per la procedura progettuale. L'analisi deve essere effettuata durante la fase di avvio del progetto. In questo modo si garantisce la presa in considerazione della sicurezza informatica sin dall'inizio del progetto.

Per il progetto PNR Svizzera, è stata eseguita un'analisi del bisogno di protezione nel quadro di HERMES che è stata in seguito esaminata dall'incaricato della sicurezza di fedpol e firmata nel marzo del 2021.

Sulla base della LPD, sono stati identificati i rischi in materia di protezione dei dati che derivano dalla trasmissione alla polizia dei dati personali registrati dalle imprese di trasporto aereo e sono state elaborate misure ad hoc nell'ambito di una valutazione d'impatto sulla protezione dei dati (VIPD), tenendo conto dell'analisi del bisogno di protezione.

La VIPD ha individuato 14 rischi potenziali di violazione dei diritti fondamentali («rischi lordi»), contrastati con l'adozione di 22 misure organizzative, giuridiche e tecniche. Queste misure hanno permesso di ridurre al livello «medio» o «minimo» i rischi lordi, che erano stati in parte classificati come «elevati», per quanto riguarda la probabilità di accadimento e l'entità dei danni. La VIPD non presenta pertanto alcun rischio residuo potenzialmente elevato.

Dato che il progetto legislativo non chiede alle imprese di trasporto aereo di registrare dati personali supplementari, per la personalità e i diritti fondamentali delle persone interessate non deriva alcun ulteriore rischio rispetto a quelli residui indicati nella VIPD.

92 FF **2017** 6941, in particolare 6011

Nel suo parere del 5 aprile 2024 sulla VIPD, l'IFPDT ha constatato che la valutazione è stata elaborata accuratamente e che la probabilità che, per una parte dei rischi residui, si verifichino danni ingenti è remota. Il servizio specializzato responsabile del trattamento stima pertanto che i rischi residui individuati siano generalmente ragionevoli. Vista la chiarezza della VIPD, allestita a regola d'arte, l'IFPDT non ha ritenuto necessario sollevare obiezioni, tanto più che, nel valutare i rischi, il proprio margine discrezionale non intende sostituirsi inutilmente a quello dei servizi specializzati.

Allegato (disegno)