



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

Rapporto sui risultati della procedura di consultazione

15 maggio 2024

Indice

1	Oggetto della procedura di consultazione	3
2	Svolgimento della procedura di consultazione	3
3	Valutazione generale	4
4	Pareri espressi sui singoli articoli dell'AP-LDPA	8
4.1	Articolo 1	8
4.2	Articolo 2	8
4.3	Articolo 3	9
4.4	Articolo 5	9
4.5	Articolo 6	9
4.5	Articolo 7	10
4.6	Articolo 8	11
4.7	Articolo 9	12
4.8	Articolo 10.....	12
4.9	Articolo 11.....	13
4.10	Articolo 12.....	13
4.11	Articolo 13 capoverso 2	13
4.12	Articolo 14.....	14
4.13	Articolo 15.....	14
4.14	Articolo 16.....	14
4.15	Articolo 17.....	15
4.16	Articolo 18.....	15
4.17	Articolo 19.....	15
4.18	Articolo 20.....	16
4.18	Articolo 21.....	17
4.19	Articolo 22.....	17
4.20	Articolo 23.....	17
4.20	Allegato 1	18
4.21	Allegato 2	18

1 Oggetto della procedura di consultazione

Al momento dell'acquisto di un biglietto aereo vengono raccolti diversi dati relativi al passeggero. Questo set di dati, conosciuto a livello internazionale come «Passenger Name Record» (PNR), contiene oltre al nome e all'indirizzo del passeggero anche alcune informazioni relative al suo bagaglio e alle modalità di pagamento. Molti Stati hanno riconosciuto il potenziale del PNR e utilizzano questi dati da diversi anni per combattere il terrorismo e altre forme gravi di criminalità. Anche la Svizzera deve poter utilizzare il PNR. La legge sui dati dei passeggeri aerei costituisce la necessaria base legale. Trattando tali dati, la Svizzera attribuisce grande importanza a una maggiore sicurezza, adempiendo contemporaneamente i propri impegni internazionali.

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

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

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

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

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

2 Svolgimento della procedura di consultazione

Dal 13 aprile 2022 al 31 luglio 2022 si è svolta la consultazione sull'avamprogetto della LDPA, ai sensi dell'articolo 3 capoverso 2 della legge sulla consultazione (LCo)¹. A seguire sono presentati i risultati della procedura di consultazione.

Complessivamente sono pervenuti 56 pareri:

¹ RS 172.061

Cantoni	25 (AG, AI, AR, BE, BL, BS, FR, GE, GL, GR, JU, LU, NE, NW, OW, SG, SH, SO, SZ, TG, TI, VD, VS, ZG, ZH)
Partiti	6 (Alleanza del centro, PLR, I Verdi, PS, UDC, PPS)
Associazioni mantello nazionali dei Comuni, delle città e dell'economia	2 (USS, economiesuisse)
Altre organizzazioni e istituzioni	14 (Aerosuisse, AlgorithmWatch, TAF, Società Digitale, easyjet, Aeroporto di Zurigo, CDDGP, CCPCS, privatim, FSA, CPS, STV, SWISS, ASA)
Privati	2 (R.S., Law_firm)
Rinuncia esplicita a esprimere un parere	7 (UR, MPC, TF, TPF, USI, USAM, SSDP)

Il presente rapporto è un riassunto dei risultati della consultazione e indica quali disposizioni sono state accolte in modo positivo, negativo o con riserva oppure con eventuali proposte di modifica. Nel caso dei partecipanti che si sono espressi soltanto su singole disposizioni, senza approvare o respingere esplicitamente il progetto di legge, si parte dal presupposto che accettino in linea di massima l'avamprogetto (AP-LDPA) e che le loro osservazioni o richieste di modifica riguardino solo le disposizioni oggetto del loro parere. Per le motivazioni dettagliate dei partecipanti si rimanda alla versione originale dei loro pareri².

3 Valutazione generale

A) Pareri favorevoli : 40

25 Cantoni (escluso UR)

2 partiti (Alleanza del centro, PLR)

13 organizzazioni/associazioni (Aerosuisse, TAF, easyjet, economiesuisse, Aeroporto di Zurigo, CDDGP, CCPCS, USS, CPS, STV, SWISS, FSFP, ASA)

Una netta maggioranza dei partecipanti (40) è in linea di principio favorevole al progetto e alla prevista introduzione del trattamento sistematico dei dati dei passeggeri aerei allo scopo di sostenere le autorità nel prevenire, investigare e perseguire reati terroristici e altri reati gravi. Molti di loro ritengono opportuno creare una nuova legge in materia (AG, AR, BL, BS, FR, GE, GL, GR, JU, LU, NW, OW, SG, SH, SO, SZ, TG, TI, VD, VS, ZG, ZH, AdC, PLR, CDDGP, CCPCS, USS, CPS, STV, SWISS, FSFP).

Diversi partecipanti motivano la loro approvazione anche con la solidarietà verso il resto dell'Europa e l'adempimento degli obblighi internazionali. Per poter stare al passo con le autorità

² [fedlex-data-admin-ch-eli-dl-proj-2021-80-cons_1-doc_6-de-pdf-a.pdf](#)

di perseguimento penale internazionali, è indispensabile l'istituzione di un'autorità legittimata a livello nazionale a trattare i dati PNR (BS, VD, Alleanza del centro, PLR, USS, STV, FSFP).

Anche la formulazione tecnologicamente neutrale dell'avamprogetto, che consente di reagire ai futuri sviluppi tecnologici senza sottoporre la legge a una revisione, è evidenziata positivamente da diversi partecipanti (AR, GR, NW, OW, TI, CCPCS, CPS).

Molti partecipanti hanno accolto con favore il previsto posizionamento organizzativo dell'UIP presso l'Ufficio federale di polizia fedpol (AR, BL, BS, GR, NW, OW, SH, SZ, TG, ZG, CDDGP, CCPCS).

Anche il modello di distacco proposto, secondo il quale l'UIP è composta da collaboratori federali e cantonali, è sostenuto da numerosi partecipanti. Ciò consentirebbe un trasferimento di competenze dall'UIP ai Cantoni, il che potrebbe essere particolarmente utile per l'elaborazione dei profili di rischio e delle liste d'osservazione (AR, BL, BS, GR, NW, OW, SH, TG, CDDGP, CCPCS).

I partecipanti favorevoli al progetto tematizzano anche altri punti (cfr. 4 e i pareri originali) riassunti a seguire:

- **Oneri di personale supplementari per i Cantoni**

Gran parte dei Cantoni ritiene che il progetto comporterà a livello cantonale oneri di personale supplementari di cui non si conosce ancora né la portata definitiva, né la futura ripartizione tra i Cantoni. Di conseguenza molti Cantoni vedono in modo critico e rifiutano una loro partecipazione paritetica al personale della nuova unità federale (cfr. 4.18 ad art. 20 AP-LDPA).

- **Orientamento agli attuali standard tecnici e coordinamento con il settore del trasporto aereo**

Per **PLR, Aerosuisse, economiesuisse, Aeroporto di Zurigo, STV, SWISS e ASA** è fondamentale che la Svizzera segua gli attuali standard tecnici, in modo che i dati richiesti possano essere generati e messi a disposizione delle autorità senza grandi oneri aggiuntivi a partire dai sistemi in uso presso le imprese di trasporto aereo. Le modalità di raccolta e di trattamento dei dati definite a livello di ordinanza devono essere elaborate d'intesa con il settore del trasporto aereo. I requisiti eccessivi che eccedono gli standard internazionali saranno respinti. L'obiettivo è evitare la creazione, nel settore dei viaggi internazionali, di ulteriori ostacoli che potrebbero compromettere la competitività della Svizzera.

Non è ancora possibile una valutazione sufficiente degli effetti sulle imprese di trasporto aereo. Anche l'obbligo di diligenza e le sanzioni in caso di violazioni degli obblighi da parte delle imprese di trasporto aereo sarebbero definite in modo troppo poco concreto (ASA).

- **Protezione dei dati**

Diversi partecipanti alla consultazione ritengono che la protezione dei dati e dei diritti della personalità dei passeggeri aerei sia fondamentalmente garantita dall'AP-LDPA: infatti soltanto il personale dell'UIP centrale potrà accedere ai dati dei passeggeri per svolgere i propri compiti. Allo stesso tempo, migliorerebbe così la tutela del personale di volo e vi sarebbe compatibilità con gli Stati esteri, tra cui i Paesi membri dell'UE, (USS). Un partecipante (BL) è favorevole al fatto che la raccolta e l'utilizzo dei dati PNR siano disciplinati conformemente alla protezione dei dati e al trattamento dei dati previsti dalla direttiva PNR. È inoltre considerato positivo che il progetto di legge sia orientato alla nuova legislazione sulla protezione dei dati, che il trattamento dei dati sia consentito soltanto per scopi legali e che, in caso di riscontri, dopo il confronto automatico sia obbligatorio verificare le corrispondenze e la loro plausibilità manualmente. In questo modo, la protezione dei dati dei passeggeri è sufficientemente garantita (Alleanza del centro). **PLR** accoglie con favore l'obbligo delle imprese di trasporto aereo di informare i passeggeri sulla raccolta e sul trattamento dei loro dati PNR in quanto contribuisce in modo

significativo alla protezione dei diritti della personalità. Nonostante ciò, l'UIP e le autorità di perseguimento penale dovranno comunque attenersi obbligatoriamente ai principi applicabili della minimizzazione dei dati e della limitazione della durata di archiviazione.

È stata sollevata la questione di una sorveglianza indipendente (Incaricato federale della protezione dei dati e della trasparenza o Incaricato cantonale della protezione dei dati e della trasparenza) delle attività dell'UIP in termini di protezione dei dati, questione che non è stata trattata né nell'avamprogetto né nel rapporto esplicativo. Una sorveglianza puramente interna da parte del servizio di protezione dei dati di fedpol non è considerata sufficiente, poiché fedpol stessa conduce indagini di polizia (SH). In considerazione della notevole quantità di dati e del relativo potenziale di abuso, sarebbe opportuno includere informazioni sulla sicurezza dei dati già nel rapporto esplicativo (BE).

- **Conservazione dei dati**

Il termine di cinque anni per la conservazione dei dati (in forma pseudonimizzata ai sensi dell'art. 16 cpv. 1 AP-LDPA) è considerato relativamente lungo. Secondo PLR, per evitare di incorrere nell'accusa di conservazione preventiva dei dati sproporzionata o di contraddire la giurisprudenza europea, la conservazione dei dati andrebbe adeguata alla sentenza della Corte di giustizia dell'Unione europea (CGUE) recentemente pubblicata e dovrebbe essere mantenuto il diritto d'accesso ai sensi dell'articolo 18 capoverso 1 in combinato disposto con gli articoli 25-28 della nuova legge federale sulla protezione dei dati (nLPD)³.

- **Obbligo di comunicazione della revoca della pseudonimizzazione**

Nella sua versione attuale, l'AP-LDPA non prevede che la revoca della pseudonimizzazione sia comunicata (a posteriori) all'interessato. In base all'articolo 33 della legge federale sulle attività informative (LAI)⁴ esiste, invece, un obbligo di comunicazione per quanto riguarda la sorveglianza mediante misure di acquisizione soggette ad autorizzazione, che in alcuni casi comporta una possibilità di ricorso. Alla luce del diritto internazionale e della giurisprudenza del Tribunale federale sugli articoli 8 e 13 della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU)⁵, risulta opportuno valutare se un analogo obbligo di comunicazione a posteriori, compresa la possibilità di ricorso, sia necessario anche nell'ambito della LDPA. Tantopiù che in questi casi il passeggero è inconsapevolmente interessato da un atto dello Stato soggetto ad autorizzazione e riguardante i suoi dati personali. L'eventuale comunicazione dovrà essere effettuata dall'UIP (TAF).

- **Operabilità UIP**

Nell'ambito della lotta al terrorismo e ai reati gravi di cui all'elenco dei reati, lo scambio immediato di informazioni è considerato obbligatorio. È indispensabile che le informazioni possano essere scambiate, trattate e analizzate 24 ore su 24, 7 giorni su 7. L'operabilità continua dell'UIP deve quindi essere garantita 24 ore su 24, 7 giorni su 7 (AG, PLR).

<u>B) Pareri con riserve di base:</u> 1 (PS)

PS ritiene delicato il trattamento sistematico dei dati di tutti i passeggeri aerei per motivi di economia dei dati, proporzionalità e protezione dei dati. Esisterebbero rischi soprattutto per quanto riguarda la sicurezza dei dati e il loro potenziale uso improprio. Il progetto di legge va

³ RS 235.1; entrata in vigore della nuova legislazione sulla protezione dei dati: 01.09.2023

⁴ RS 121

⁵ RS 0.101

migliorato in particolare per quanto riguarda la trasmissione dei dati dei passeggeri aerei alle autorità di perseguimento penale, la durata di conservazione di questi dati e i prerequisiti per la loro trasmissione a servizi esteri.

C) Pareri contrari: 8

(I Verdi, UDC, PPS, AlgorithmWatch, Società Digitale, FSA, R.S., Law_firm)

I partecipanti che rifiutano chiaramente l'avamprogetto avanzano essenzialmente le argomentazioni seguenti.

Tutti i passeggeri aerei sono sottoposti, senza alcun motivo o sospetto, alla sorveglianza di massa, che prevede una conservazione preventiva dei dati personali. Quest'ultima è sproporzionata e costituisce una massiccia violazione dei diritti fondamentali dei passeggeri (UDC, I Verdi, PPS, AlgorithmWatch, Società Digitale, Law_Firm, FSA).

Il progetto di legge arriva nel momento sbagliato. Presso la CGUE è ancora pendente un ricorso della Germania. Allo stesso tempo, in Svizzera è ancora in fase di elaborazione una direttiva per la gestione dei dati API. La Svizzera rischia di adottare una legge che potrebbe dover essere modificata in modo sostanziale non appena sarà definita la direttiva sui dati API o sarà disponibile una nuova sentenza della CGUE. Le riflessioni e le decisioni della CGUE andrebbero prese adeguatamente in considerazione e il presente avamprogetto fondamentalmente riconsiderato (UDC, I Verdi, PPS, Law_Firm, FSA).

La trasmissione di tutti i dati dei passeggeri aerei in assenza di un sospetto fondato creerebbe un'enorme quantità di dati inutili ai fini della lotta contro il terrorismo (AlgorithmWatch, Società Digitale, PPS).

La valutazione di questi dati dovrebbe rimanere di competenza del Servizio delle attività informative della Confederazione (SIC), che se ne è finora occupato in maniera limitata. Un'UIP dovrebbe servire solo a coordinare lo scambio di informazioni in Svizzera e all'estero e potrebbe essere gestita con un onere di personale estremamente ridotto (UDC). Si dovrebbe evitare di creare nuovi meccanismi di sorveglianza non trasparenti e l'uso dei PNR dovrebbe restare ristretto ed efficace (I Verdi).

La conservazione generalizzata di tutti i dati personali per sei mesi o in forma pseudonimizzata per cinque anni è una misura inutile e troppo costosa. I periodi definiti di sei mesi o cinque anni sono troppo lunghi per motivi sia finanziari che di protezione dei dati (UDC, I Verdi, PPS, Società Digitale, Law_Firm).

Lo scambio di dati personali deve avvenire esclusivamente sulla base di un sospetto e soltanto con Stati in cui vi siano indizi di pericoli di terrorismo o di reati gravi connessi ai voli (UDC).

Questa proposta di legge comprometterebbe anche il segreto professionale degli avvocati e di altre categorie professionali legalmente protette (FSA).

Sono necessari una solida protezione dei dati e un diritto d'accesso che l'AP-LDPA tuttavia non offre (AlgorithmWatch, Società Digitale, PPS, Law_Firm).

Per chi è soggetto alla legge, non è chiaro in base a quali dati vengano creati i profili di rischio e le liste d'osservazione e come vengano trattati i suoi dati in questo contesto (I Verdi, PPS, Società Digitale, AlgorithmWatch, Law_Firm, FSA).

Il catalogo dei reati per i quali i PNR possono essere utilizzati va ben oltre il terrorismo e i reati gravi (I Verdi, PPS, Società Digitale, AlgorithmWatch, FSA).

4 Pareri espressi sui singoli articoli dell'AP-LDPA

4.1 Articolo 1

In relazione alla lettera a, **AG** chiede che il trattamento dei dati dei latitanti condannati in giudicato sia esplicitamente menzionato nel testo di legge. Secondo **ZH**, anche l'aviazione privata dovrebbe essere soggetta all'AP-LDPA.

FSA chiede che l'ordine delle lettere a e b venga modificato.

4.2 Articolo 2

Capoverso 1

PPS e **R.S.** sostengono che, poiché la CGUE limita chiaramente a casi speciali la raccolta dei dati per i voli all'interno dell'UE, si dovrebbe rinunciare alla raccolta dei dati per la maggior parte dei voli nell'area Schengen.

Capoverso 2

Per **I Verdi**, **Società Digitale**, **AlgorithmWatch** e **R.S.** non è chiaro perché la trasmissione debba avvenire in due momenti diversi. La doppia trasmissione porta soltanto a una doppia quantità di dati. Chiedono che i dati non vengano trasmessi prima del completamento dell'imbarco. Per **PPS** è incomprensibile il motivo per cui non viene regolamentata la cancellazione dei dati dei passeggeri che non prendono il volo.

Capoverso 3

PPS e **R.S.** lamentano la mancanza di un'istanza competente che verifichi la cancellazione dei dati personali degni di particolare protezione.

FSA chiede un rimando alla legge sulla protezione dei dati: «[...] trasmettere dati personali degni di particolare protezione ai sensi dell'articolo 5 lettera c della legge federale del 25 settembre 2020⁶ sulla protezione dei dati (LPD)».

Capoverso 4

GR, **NE**, **SO** e **TI** accolgono favorevolmente il capoverso 4, secondo il quale fedpol definisce le modalità tecniche relative alla trasmissione dei dati. **BL** sottolinea che è ancora possibile prenotare un volo con nomi falsi. Le imprese di trasporto aereo dovrebbero almeno poter garantire che al momento dell'imbarco – dove viene comunque effettuato un controllo dell'identità – sia verificato il nome fornito al momento della prenotazione. In caso contrario, il confronto dei dati con i sistemi di informazione ai sensi dell'articolo 7 AP-LDPA è inutile.

PS, **I Verdi**, **Società Digitale** e **AlgorithmWatch** chiedono che i principi della trasmissione dei dati tra le imprese di trasporto aereo e fedpol siano disciplinati nell'articolo 2 capoverso 4 AP-LDPA e i dettagli in un'ordinanza del Consiglio federale. Secondo **PPS** e **R.S.**, fedpol dovrebbe definire i dettagli tecnici del trasferimento dei dati insieme all'Incaricato federale della protezione dei dati e della trasparenza, a cui dovrebbe spettare la decisione finale.

Per **ASA**, non è possibile procedere a una valutazione sufficiente dell'impatto sulle imprese di trasporto aereo. L'obbligo di diligenza risulta essere un concetto elastico.

FSA chiede di integrare il testo con «La trasmissione è protetta in particolare dalla crittografia end-to-end. fedpol rende pubblici i dettagli tecnici stabiliti per la trasmissione».

⁶ RS 235.1

4.3 Articolo 3

SO accoglie con favore questa disposizione.

I Verdi, Società Digitale e AlgorithmWatch criticano che anche la trasmissione dei dati all'estero debba essere regolamentato nell'AP-LDPA in modo da garantire la sicurezza dei dati durante il trasferimento. Queste organizzazioni chiedono inoltre di prevedere esplicitamente che un trattato internazionale possa essere concluso soltanto con gli Stati che garantiscono un'adeguata protezione dei dati. **FSA** chiede di integrare il testo in questo senso: «a condizione che il rispettivo diritto nazionale garantisca una protezione adeguata o appropriata dei dati».

4.4 Articolo 5

ZH ritiene l'obbligo di informazione qui menzionato superfluo, in quanto la legge prevede che le informazioni corrispondenti vengano raccolte e trattate.

Per **I Verdi, PPS, AlgorithmWatch, Società Digitale e R.S.** è indispensabile che prima della prenotazione dei biglietti i passeggeri siano attivamente informati in modo comprensibile e ben visibile sull'uso dei PNR. Le informazioni devono elencare tutti i dati che verranno trasmessi e i passeggeri devono fornire il loro consenso consapevolmente. Inoltre, la Confederazione dovrebbe chiarire le procedure e le sanzioni per il caso in cui le imprese di trasporto aereo non rispettino l'obbligo di informazione. **FSA** chiede che nel testo sia indicato «in forma appropriata, comprensibile e facilmente accessibile», anziché «per iscritto».

4.5 Articolo 6

SO accoglie con favore questa disposizione.

Secondo **FSA**, i previsti allegati 1 e 2 possono essere sostituiti da un unico allegato. Le seguenti categorie di reato di cui all'allegato 2 AP-LDPA dovrebbero essere escluse: 3, 4, 6, 7, 8, 9, 12, 15, 17, 18, 21, 24, 25, 26. Anche **Società Digitale** avanza una richiesta in tal senso.

Capoverso 1

AG e BL chiedono che il trattamento dei dati dei latitanti condannati in giudicato sia esplicitamente menzionato nel testo di legge.

Società Digitale e AlgorithmWatch chiedono che la protezione dei dati venga integrata e quindi ulteriormente rafforzata, anziché limitata.

Per quanto riguarda l'articolo 6, **PPS e R.S.** affermano che il termine «reato grave» dovrebbe essere definito in modo univoco e la dicitura «altri reati gravi» dovrebbe essere eliminata.

Capoverso 2

BE, GE, ZH e CPS sottolineano che la definizione dei reati di terrorismo dovrebbe rimandare all'allegato 1a dell'ordinanza N-SIS⁷. Secondo **BE**, questa disposizione dovrebbe includere almeno l'articolo 260^{sexies} del Codice penale⁸ (CP) e l'articolo 2 della legge federale che vieta i gruppi «Al-Qaïda» e «Stato islamico» nonché le organizzazioni associate⁹.

⁷ RS 362.0

⁸ RS 311.0

⁹ RS 122

PS, I Verdi, Società Digitale e AlgorithmWatch chiedono che il reato di sommossa di matrice terroristica ai sensi dell'articolo 260 CP venga stralciato dal catalogo dei reati di terrorismo secondo l'articolo 6 capoverso 2 AP-LDPA.

Capoverso 3

Per **AG**, l'espressione «pena detentiva massima di almeno tre anni» necessita di interpretazione e deve essere precisata nel commento agli articoli.

BE, ZH e CPS ritengono che la lettera a sia formulata in maniera troppo restrittiva. Il trattamento dei dati dei passeggeri aerei fornisce agli investigatori uno strumento efficace per individuare le operazioni della criminalità organizzata. Questo aspetto non è sufficientemente considerato nel catalogo dei reati. Di conseguenza, per la definizione di altri reati gravi l'AP dovrebbe rimandare al catalogo dei reati di cui all'allegato 1b dell'ordinanza N-SIS. **BE, BL, GE, PPS e CPS** chiedono che sia prevista una pena detentiva massima di almeno 3 anni per i reati di cui alle lettere a e b. **ZH** propone di eliminare la lettera b. In linea di principio, non è opportuno equiparare gli illeciti penali amministrativi alla lotta contro il terrorismo e i reati gravi. Se si decidesse di non modificare questo punto, le categorie di reato dovrebbero essere disciplinate a livello di legge.

PS, I Verdi, Società Digitale e AlgorithmWatch chiedono che i reati di pirateria di prodotti siano rimossi dal catalogo dei reati gravi secondo l'articolo 6 capoverso 3 lettera a AP-LDPA.

GE nota che lo spionaggio politico (art. 272 CP) e lo spionaggio militare (art. 274 CP) non sono inclusi nel catalogo dei reati, nonostante la categoria 26 (spionaggio industriale). Si tratta di una lacuna nella prevenzione e nell'individuazione dei servizi di spionaggio vietati.

Capoverso 4

ZH propone – come per il capoverso 3 lettera b – di eliminare il capoverso 4. Se si decidesse di non modificare questo punto, le categorie di reato dovrebbero essere disciplinate a livello di legge.

Capoverso 6

BE auspica una spiegazione sulle sanzioni di polizia nel rapporto esplicativo: le misure di sicurezza e di protezione attuate dal sistema di polizia per la gestione delle minacce potrebbero essere molto utili per la valutazione dell'UIP, motivo per cui dovrebbe esserci chiarezza in merito alla trasmissione dei dati di tali informazioni.

PPS afferma che il capoverso 6 è in contrasto con l'articolo 2 capoverso 3 AP-LDPA, che vieta alle imprese di trasporto aereo di trasmettere dati personali degni di particolare protezione. Inoltre, è noto che il dipartimento per la sicurezza nazionale degli Stati Uniti (*US-Department for homeland-security*) vuole accedere a questi dati nella loro interezza. Pertanto, si dovrebbe rinunciare a questi dati («economia dei dati») e il capoverso 6 dovrebbe essere eliminato.

Società Digitale e AlgorithmWatch chiedono che venga esplicitamente dichiarato che i procedimenti e le sanzioni penali riguardano soltanto i reati di terrorismo e gli altri reati gravi. Il trattamento dei procedimenti o delle sanzioni amministrative dovrebbe essere eliminato dalla lettera b.

FSA afferma che la cancellazione rappresenta un trattamento di dati personali degni di particolare protezione e deve essere espressamente menzionata («c. i dati di cui all'art. 2 cpv. 3 [LDPA] al fine di cancellarli»).

4.5 Articolo 7

Capoverso 1

BE propone di chiarire nel rapporto esplicativo in merito all'articolo 7 che il collaboratore UIP distaccato dal Cantone può confrontare i dati con i sistemi di informazione del proprio Cantone. Se la base giuridica non è sufficiente, deve essere creata con la LDPA; solo così si può raggiungere adeguatamente l'obiettivo prefissato dall'articolo 1 capoverso 1 AP-LDPA.

I Verdi, Società Digitale, AlgorithmWatch e FSA chiedono che l'espressione «reati pianificati» (art. 7 cpv. 1 lett. d) venga cancellata perché non è chiaro cosa si intenda. Secondo **FSA**, il termine potrebbe essere definito in altro modo.

Società Digitale e AlgorithmWatch auspicano che questa disposizione indichi esplicitamente che gli scopi di cui alle lettere a-d possono riguardare soltanto il terrorismo e altri reati gravi.

Capoverso 2

LU osserva che sebbene secondo l'articolo 7 capoverso 2 AP-LDPA il confronto automatico vada effettuato «immediatamente dopo la ricezione dei dati», nella pratica, l'utilità delle comunicazioni dipende in gran parte dalla tempestività con cui le ricevono le autorità di perseguimento penale.

PLR ritiene insoddisfacente il concetto generico di «immediatezza». L'ordinanza esecutiva dovrebbe definire il termine entro il quale i dati devono essere confrontati e, se necessario, le autorità di perseguimento penale devono essere informate dei casi sospetti.

Capoverso 3

Per quanto riguarda il capoverso 3, **PS** chiede che i necessari controlli di plausibilità siano eseguiti in modo adeguato durante l'esecuzione e che i dati corrispondenti dei passeggeri aerei siano sistematicamente cancellati se non vi è alcun collegamento con un reato del catalogo.

Per **Società Digitale e AlgorithmWatch** non è chiaro quali siano gli «ulteriori» sistemi di informazione. Dovrebbe essere esplicitamente regolamentato a quali sistemi di informazione ha accesso l'UIP. Inoltre, la registrazione degli accessi dovrebbe essere disciplinata a livello di ordinanza.

FSA chiede di integrare il testo con: «Prima che le corrispondenze ottenute automaticamente siano trasmesse all'autorità competente, occorre verificarne la plausibilità manualmente e *senza indugio* [...]». La verifica deve essere documentata». Chiede anche di aggiungere: «[...] per verificarne la correttezza. Il risultato della verifica deve essere documentato».

4.6 Articolo 8

FSA chiede di stralciare l'articolo 8 capoverso 1 lettera b.

BE propone di utilizzare al capoverso 2 lettera a la denominazione «autorità di polizia e di perseguimento penale». Le espressioni «autorità di perseguimento penale» e «esistenza di un reato» sono troppo restrittive e dovrebbero essere riviste.

BL chiede un adeguamento della formulazione: invece di «se la verifica ha confermato l'esistenza di un reato di cui...» propone «se la verifica ha confermato che i dati sono utili a prevenire o perseguire un reato di cui...».

SH considera promettente, in particolare, il confronto automatizzato dei dati dei passeggeri aerei con quelli provenienti dai sistemi di informazione della polizia.

VD chiede l'inclusione dei servizi cantonali delle attività informative nel capoverso 2.

Secondo **ZH**, va indicato in modo esplicito che per facilitare le fasi successive dell'azione penale possono essere trasmessi anche i dati biometrici.

Società Digitale, AlgorithmWatch e FSA chiedono di indicare nella disposizione che l'esistenza di un reato può essere verificata soltanto da un'autorità giudiziaria e non dall'UIP stessa.

4.7 Articolo 9

Secondo **BL**, mancano i requisiti per il confronto dei dati con i profili di rischio e le liste d'osservazione elaborati dall'UIP. Anche questo confronto, inoltre, andrebbe effettuato immediatamente dopo aver ricevuto i dati e non può essere ripetuto a discrezione dell'UIP, se i dati non sono stati pseudonimizzati. Inoltre, deve essere verificata la plausibilità delle corrispondenze prima di trasmettere i dati ad altre autorità, in modo da evitare che gli interessati siano sospettati erroneamente. Queste limitazioni dovrebbero essere fissate nella legge e non delegate al Consiglio federale per una regolamentazione a livello di ordinanza.

LU ritiene molto utile la prevista possibilità di creare profili di rischio e liste d'osservazione e di confrontarli continuamente con i dati dei passeggeri forniti. Il rapporto esplicativo non specifica in quale forma debba essere presentata la richiesta per l'elaborazione di profili di rischio e liste d'osservazione o la decisione dell'UIP, né chi presso l'UIP decida in merito a tale richiesta e neppure come ricorrere contro una decisione negativa. Questi aspetti devono essere presi in considerazione nella stesura della relativa ordinanza. Infine, è necessario esaminare i profili di rischio e le liste d'osservazione anche ai fini della non discriminazione e della parità di trattamento delle persone interessate.

I Verdi, Società Digitale, AlgorithmWatch e FSA chiedono che questo articolo sia stralciato. Questa disposizione introdurrebbe un'indagine incrociata generale priva di motivo o sospetto, che andrebbe ben oltre il già ampio confronto dei dati personali con i sistemi di informazione ai sensi dell'articolo 7 AP-LDPA e sarebbe ovviamente sproporzionata. Se l'articolo 9 non venisse stralciato, si dovrebbe regolamentare con precisione il modo in cui sono effettuate queste analisi, così da creare trasparenza sui profili di rischio e sulle liste d'osservazione e, in particolare, in modo che essi non si basino su alcuna caratteristica direttamente o indirettamente discriminatoria. Inoltre, i risultati della verifica di cui all'articolo 9 capoverso 5 dovrebbero essere pubblicati e dovrebbe essere definita una sorveglianza efficace. **FSA** propone modifiche concrete al testo per il caso in cui la disposizione non dovesse essere stralciata.

PPS e R.S. chiedono di precisare le definizioni di analisi, profili di rischio e liste d'osservazione. Se ciò non fosse possibile, questa disposizione andrebbe stralciata. Inoltre, nell'effettuare i confronti dovrebbe essere esplicitamente vietato l'uso di tecnologie di intelligenza artificiale nell'ambito di sistemi di autoapprendimento («machine learning»).

SG suggerisce di controllare la plausibilità anche dei risultati del confronto dei dati con i profili di rischio e le liste d'osservazione prima di trasmettere i dati corrispondenti alle autorità competenti.

4.8 Articolo 10

PS accoglie con favore la normativa relativamente restrittiva per la trasmissione dei dati dei passeggeri aerei al SIC, raccomandandosi di non allentarla in alcun caso; in particolare, non è concepibile che il SIC abbia un accesso diretto al sistema di informazione PNR.

I Verdi, Società Digitale e AlgorithmWatch e FSA chiedono che l'articolo 10 venga stralciato. Se il Consiglio federale decidesse di non stralciarlo, per garantire la trasparenza, dovrebbero essere pubblicate almeno le rotte selezionate dal SIC e i passeggeri dovrebbero essere attivamente informati della trasmissione generale del loro PNR al SIC prima della prenotazione. Inoltre, i PNR che non generano alcuna corrispondenza presso il SIC vanno cancellati immediatamente (e non dopo 96 ore).

PPS e R.S. chiedono che le rotte selezionate dal SIC siano approvate dalla Commissione della gestione del Parlamento. La legge dovrebbe inoltre indicare chiaramente che i dati trasmessi saranno cancellati direttamente dopo il confronto, se quest'ultimo non ha avuto esito positivo.

4.9 Articolo 11

VD auspica l'inclusione dei servizi cantonali delle attività informative nel capoverso 1.

BE chiede che alla lettera a si utilizzi l'espressione «autorità di polizia e di perseguimento penale». **BE**, **BL** e **CPS** vorrebbero eliminare dal rapporto esplicativo il passaggio «Le consultazioni generiche, non meglio specificate, che conducono a una moltitudine di risultati più disparati» (pag. 31 Rapporto esplicativo). Questa limitazione della possibilità di consultazione non trova alcun fondamento nella formulazione della legge. Deve essere possibile, ad esempio, consultare i dati di tutti i passeggeri di un determinato volo.

LU critica il fatto che né la legge né il rapporto esplicativo menzionino chi presso l'UIP decide in merito alle richieste e se sussistano rimedi giuridici contro tale decisione. **LU** suggerisce di tenere conto anche di questo aspetto nella stesura della relativa ordinanza.

ZH chiede di consentire espressamente la consultazione di set di dati più ampi nell'ambito dell'esame dei modelli comportamentali e di tener conto nel messaggio di tale aspetto.

PPS e **R.S.** chiedono che questa disposizione venga eliminata. **FSA** sollecita la verifica e la documentazione delle richieste e l'aggiunta di un capoverso: «La tutela giurisdizionale è retta dalla legge che disciplina l'attività dell'autorità destinataria».

4.10 Articolo 12

BE chiede di utilizzare al capoverso 1 l'espressione «autorità di polizia e di perseguimento penale» e di verificare la definizione «concreto».

ZH, **CPS**, **PLR**, **PS** e **FSA** chiedono che il termine «sospetto concreto» presente nel capoverso 1 non venga utilizzato (proposta di formulazione **ZH**: sospetto iniziale, sufficienti indizi di reato, gravi indizi / **PLR**, **CPS**: cancellare «concreto» / **PS**: grave sospetto / **FSA**: sospetto sufficientemente fondato). Deve essere sufficiente che vi siano «indicazioni» o «indizi» di un reato corrispondente. La norma deve pertanto essere adeguata in tal senso.

I Verdi, **Società Digitale**, **AlgorithmWatch** e **FSA** chiedono di usare l'espressione «sospetto sufficientemente fondato». Per quanto riguarda il capoverso 2, queste organizzazioni chiedono di aggiungere che i dati devono essere dati personali degni di particolare protezione di cui all'articolo 6 capoverso 6 AP-LDPA.

FSA sottolinea che, dal punto di vista della sistematica, l'articolo 12 AP-LDPA deve essere collocato tra l'articolo 9 e l'(attuale) articolo 10 AP-LDPA.

R.S. chiede di eliminare «o un altro reato grave».

4.11 Articolo 13 capoverso 2

BL afferma che, in considerazione della quantità di dati e del potenziale di abuso, il Consiglio federale deve definire ulteriori requisiti per la sicurezza dei dati.

Secondo **PS**, per motivi di protezione e sicurezza dei dati, dovrebbero avere accesso al sistema di informazione PNR soltanto i collaboratori soggetti al diritto pubblico. Questo dovrebbe essere indicato a livello di legge in questa disposizione.

Società Digitale e **AlgorithmWatch** chiedono che il capoverso 2 lettera a disciplini dal punto di vista organizzativo chi ha accesso a quali dati. Se i dati devono essere elaborati manualmente, è necessario introdurre un sistema di verifica con una seconda persona. Questi partecipanti, **PPS** e **R.S.** chiedono inoltre di stralciare il capoverso 2 lettera b.

4.12 Articolo 14

Il **PS** ritiene problematico che l'applicazione di questa legge porti all'utilizzo dei dati dei passeggeri aerei senza che ci sia un collegamento con un reato e chiede, pertanto, la seguente modifica: «Il sistema di informazione PNR pseudonimizza automaticamente i dati dei passeggeri aerei tre mesi dopo la loro trasmissione da parte delle imprese di trasporto aereo».

I **Verdi** chiedono che i dati siano cancellati immediatamente dopo il confronto effettuato dall'UIP. Se il Consiglio federale non dovesse rinunciare alla conservazione dei dati, almeno la pseudonimizzazione dovrebbe avvenire più rapidamente, segnatamente in modo automatizzato e immediatamente dopo il confronto dei dati. **Società Digitale, AlgorithmWatch e R.S.** ritengono che il periodo di sei mesi per la pseudonimizzazione sia troppo lungo.

PPS ritiene urgente ridurre drasticamente i termini di conservazione.

FSA chiede che venga definito il termine «pseudonimizzazione» (formulazione suggerita: «La pseudonimizzazione è la sostituzione di nomi e altri elementi identificativi con un contrassegno allo scopo di rendere sostanzialmente più difficile l'identificazione delle persone interessate»).

4.13 Articolo 15

LU sottolinea che, data la grande importanza che si prevede rivestiranno i dati dei passeggeri e l'ampio catalogo di reati, ci si può aspettare un numero considerevole di domande di revoca della pseudonimizzazione già solo da parte delle autorità di perseguimento penale (anche dati di vario genere più vecchi di sei mesi possono essere rilevanti nelle indagini). Bisognerebbe tener conto di tale aspetto per quanto riguarda le capacità necessarie al Tribunale amministrativo federale. **SH** si chiede se la pseudonimizzazione prevista dall'articolo 15 AP-LDPA sia appropriata e se non sarebbe invece meglio mantenere i termini di cancellazione quanto più brevi possibile e sancirli formalmente nella legge.

I **Verdi** chiedono che vi sia il diritto di richiedere la rimozione della pseudonimizzazione necessaria all'esercizio del diritto d'accesso (art. 15 cpv. 1).

TAF afferma che dalla formulazione del capoverso 5 non si può dedurre se il procedimento rimanga pendente dinanzi al Tribunale amministrativo federale per il periodo necessario al completamento degli atti o agli ulteriori accertamenti. A seconda della situazione, potrebbe non essere possibile decidere entro cinque giorni lavorativi.

FSA chiede di integrare il testo con un capoverso 6 («Il Tribunale amministrativo federale pubblica le sue decisioni»).

4.14 Articolo 16

PS ritiene essenziale che i dati raccolti dalle autorità siano conservati dallo Stato soltanto per il tempo strettamente necessario. Da questo punto di vista, sarebbe opportuno ridurre significativamente il termine di conservazione (proposta di formulazione: «I dati dei passeggeri aerei sono cancellati automaticamente due anni dopo la loro introduzione nel sistema di informazione PNR»).

PLR afferma che la conservazione dei dati oltre il periodo consueto, in assenza di qualsiasi indicazione di un reato commesso, costituisce una violazione dei diritti fondamentali dei passeggeri, in particolare perché, ai sensi dell'articolo 18 capoverso 2 AP-LDPA, il diritto d'accesso personale non può più essere esercitato dopo la pseudonimizzazione. Per evitare di incorrere nell'accusa di conservazione preventiva dei dati sproporzionata o di contraddire la giurisprudenza europea, la conservazione dei dati andrebbe adeguata alla sentenza della CGUE e dovrebbe essere mantenuto il diritto d'accesso ai sensi dell'articolo 18 capoverso 1 in

combinato disposto con gli articoli 25-28 nLPD. Anche **SG** fa riferimento a questa sentenza per quanto riguarda il periodo di conservazione.

I Verdi, Società Digitale e AlgorithmWatch chiedono che i dati siano cancellati immediatamente dopo il confronto effettuato dall'UIP e che la durata di conservazione di cui al capoverso 1 sia stralciata. Se il Consiglio federale non dovesse rinunciare alla conservazione dei dati, la pseudonimizzazione dovrebbe almeno avvenire più rapidamente, segnatamente in modo automatizzato e immediatamente dopo il confronto dei dati. Inoltre, è necessario che anche la durata di conservazione dei dati risultanti dal confronto di cui agli articoli 7 e 9 sia specificato nella legge (art. 16 cpv. 2). Si tratta di dati personali degni di particolare protezione che possono essere trattati soltanto se previsto da una base giuridica formale.

FSA afferma che sarebbe possibile conservare dopo sei mesi una serie di dati selezionati dei passeggeri aerei (pseudonimizzati) se la verifica di cui all'articolo 7 AP-LDPA ha dato esito positivo, se la verifica incrociata ai sensi dell'articolo 9 AP-LDPA ha dato luogo alla trasmissione o se i dati sono stati trasmessi in altro modo rispetto alla prassi consueta (anche su richiesta). Una tale disposizione potrebbe essere inserita in un altro capoverso (proposta di modifica del testo: [...] sei mesi dopo la loro introduzione»). Inoltre, la legge dovrebbe disciplinare la durata massima di conservazione per tutti i dati e non soltanto per quelli di cui all'articolo 16 capoverso 1 AP-LDPA.

PPS e R.S. propongono che i dati vengano cancellati entro 24 ore dall'atterraggio – prevedendo un meccanismo di controllo e sanzione funzionante.

4.15 Articolo 17

LU sottolinea che, in base a questa disposizione, il servizio di protezione dei dati di fedpol sorveglia l'osservanza delle prescrizioni in materia di protezione dei dati. Per adempiere efficacemente a questo compito, occorre garantire che tale servizio abbia accesso a tutti i dati trattati (cfr. art. 6 par. 7 Direttiva (UE) 2016/681).

FSA richiede la seguente integrazione al testo: «Il servizio di protezione dei dati di fedpol sorveglia l'osservanza delle prescrizioni in materia di trattamento dei dati personali ai sensi della presente legge. Il servizio di protezione dei dati pubblica un rapporto annuale sulla sorveglianza».

4.16 Articolo 18

Per **BL** e **PS** non è chiaro come mai i dati pseudonimizzati non siano soggetti al diritto d'accesso e al diritto di accedere ai propri dati personali.

LU afferma che, in linea di principio, il diritto d'accesso dell'interessato dovrebbe essere esteso a tutti i dati, compresi quelli pseudonimizzati, e dovrebbe essere limitato solo in casi eccezionali.

I Verdi, Società Digitale e AlgorithmWatch chiedono di stralciare il capoverso 2. **FSA** chiede lo stralcio dei capoversi 2 e 3.

Per **PPS** e **R.S.** la pseudonimizzazione dei dati comporta un enorme svantaggio per tutti i partecipanti. Se i dati non vengono cancellati entro 24 ore dall'atterraggio, gli interessati devono poter esercitare il diritto d'accesso per l'intero periodo di conservazione dei dati (con o senza pseudonimizzazione).

4.17 Articolo 19

ZH ritiene fondamentale la trasmissione immediata dei dati da parte dell'UIP, soprattutto in caso di persone ricercate. L'UIP dovrà quindi essere attiva 24 ore su 24.

4.18 Articolo 20

AG accoglie con favore l'approccio secondo cui il personale dell'UIP dovrebbe essere composto per metà da collaboratori federali e per metà da collaboratori cantonali. Ciò garantirebbe un trasferimento di conoscenze ai Cantoni.

ZH ritiene importante che tutti i Cantoni contribuiscano in modo adeguato ai costi del personale cantonale presso l'UIP, poiché tutti trarrebbero beneficio dall'aumento della sicurezza.

Anche **SO** esprime un parere positivo sulla partecipazione in termini di personale e rimanda al già noto obbligo di distacco e all'implementazione del trattamento dei dati nell'attività della polizia cantonale, che dovrebbe essere presa in considerazione nel quadro della prossima pianificazione dell'effettivo. Questo onere aggiuntivo per i Cantoni va messo in relazione con i benefici che ne derivano.

BE si dichiara disponibile a partecipare all'organico dell'UIP presso fedpol e a redigere un accordo corrispondente, anche se l'effettivo onere operativo per il Cantone di Berna non può ancora essere quantificato.

ZG sottolinea che, per quanto riguarda l'entrata in vigore della legge, si deve tenere conto del fatto che i Cantoni devono avere il tempo sufficiente per mettere a bilancio i posti corrispondenti.

BL rifiuta una partecipazione paritetica dei Cantoni all'effettivo del personale della nuova unità federale. Tanto più che il rapporto esplicativo contiene solo informazioni rudimentali sulle ripercussioni finanziarie sui Cantoni. Sulla base delle indicazioni attuali, il singolo Cantone difficilmente può stimare quali costi dovrà sostenere. Le informazioni sulle conseguenze finanziarie per i Cantoni dovrebbero essere integrate e specificate di conseguenza.

Anche **FR** critica i criteri di partecipazione all'effettivo del personale e prevede che non gli sarà possibile contribuire.

Allo stesso modo, **TI, NE, VD e VS** contestano la chiave di ripartizione scelta, in quanto comporta un onere eccessivo per i Cantoni.

NE chiede che la chiave di ripartizione tenga conto dell'uso effettivo del PNR da parte delle rispettive autorità cantonali e ritiene troppo breve il periodo di un anno per l'impiego del personale. Infine, ritiene importante che tutte le autorità e le unità interessate siano rappresentate nel PNR.

JU è favorevole a una chiave di ripartizione secondo cui 1/3 del personale è distaccato dai Cantoni e 2/3 dalla Confederazione.

AI sottolinea che, a causa delle dimensioni della sua polizia cantonale, non gli è possibile mettere a disposizione personale per l'UIP.

AR, GR, SH e TG propongono che i costi per i collaboratori siano interamente a carico della Confederazione, analogamente ai Centri di cooperazione doganale e di polizia (CCPD) di Ginevra e Chiasso. Solo in questo modo i Cantoni più piccoli e la polizia, in particolare, potrebbero distaccare personale per questi compiti federali. L'articolo 20 capoverso 4 AP-LDPA deve essere modificato di conseguenza.

Secondo **GL, NW e SZ**, è fondamentale che i Cantoni siano coinvolti fin dall'inizio nei successivi lavori di pianificazione e in particolare nello sviluppo della struttura organizzativa vera e propria. Per **SZ**, dovrebbe essere riesaminato criticamente anche l'impiego di personale sorprendentemente massiccio nonostante l'automazione.

Secondo **GE**, è importante monitorare attentamente gli effetti delle misure previste dalla legge e la sede definita dell'UIP nei casi di competenza cantonale.

GE lamenta inoltre che il rapporto esplicativo non indica se sono previste UIP decentrate anche negli aeroporti più importanti.

A causa della scarsità di risorse nei corpi di polizia cantonali, **FSFP** sostiene la partecipazione paritetica dei Cantoni all'effettivo del personale soltanto in caso di nuove assunzioni.

PPS si chiede perché i Cantoni non si assumano semplicemente i costi invece di fornire metà del personale. **R.S.** afferma che si vogliono introdurre processi complicati.

BL suggerisce, in merito al capoverso 3, che sarebbe opportuno stabilire chiaramente nella legge che l'obbligo di discrezione si applica anche al datore di lavoro contrattuale del personale dell'UIP.

4.18 Articolo 21

SO accoglie con favore questa disposizione.

SH, I Verdi, Società Digitale, AlgorithmWatch e R.S. chiedono di prevedere esplicitamente che un trattato internazionale possa essere concluso soltanto con gli Stati che garantiscono un'adeguata protezione dei dati. **FSA** chiede di integrare il testo del capoverso 1 con «[...] una protezione adeguata o appropriata [...]» e il capoverso 2 con «a condizione che il rispettivo diritto nazionale garantisca una protezione adeguata o appropriata dei dati».

PPS chiede che venga chiarito il termine «equiparabile», in quanto non è chiaro se questo possa includere anche «leggermente peggiore».

4.19 Articolo 22

LU raccomanda che la doppia punibilità, come previsto dall'articolo 64 della legge federale sull'assistenza internazionale in materia penale¹⁰, venga ancorata per analogia nell'AP-LDPA, in modo che la norma si applichi anche alla trasmissione dei dati dei passeggeri aerei.

BE chiede di rivedere il termine «fondato».

ZH chiede che il termine «sospetto fondato» sia sostituito da «indizi».

BL afferma che il capoverso 3 comporta una verifica materiale del «sospetto fondato», in quanto secondo il capoverso 2 deve esserci una richiesta motivata e il servizio estero richiedente deve adempiere gli stessi compiti dell'UIP. Secondo **CPS**, la versione tedesca dovrebbe essere allineata a quella francese («se nei confronti della persona interessata non sussiste alcun sospetto»), come nel caso dell'articolo 12.

Per il **PPS** è necessario precisare al capoverso 3 chi decide se esiste un sospetto fondato e propone una commissione composta da 5 giudici federali.

4.20 Articolo 23

SO accoglie con favore questa disposizione.

Capoverso 1

BL propone di sanzionare le violazioni dell'articolo 3 anziché quelle dell'articolo 4.

Capoverso 2

Aerosuisse, economiesuisse e SWISS chiedono che l'articolo 23 capoverso 2 lettera b AP-LDPA sia soppresso. Le imprese di trasporto aereo non sarebbero in grado di verificare l'accuratezza dei dati registrati dai passeggeri o dalle agenzie. Inoltre, non esiste alcuno standard per i dati corretti o errati dei passeggeri; si tratta di informazioni che le imprese di trasporto aereo raccolgono per poter elaborare una prenotazione a livello commerciale.

TAF fa notare che alla lettera d si dovrebbe fare riferimento all'articolo 15 capoverso 4.

Capoverso 5

¹⁰ RS 351.1

Secondo **ASA**, i rischi per le singole imprese di trasporto aereo sono difficili da valutare, in quanto la violazione degli obblighi di diligenza e di informazione di cui agli articoli 4 e 5 AP-LDPA deve essere sanzionata indipendentemente dalla prova della colpa. I rischi non sono trattati nemmeno nel capitolo 6 «Aspetti giuridici» del rapporto esplicativo.

4.20 Allegato 1

SO accoglie con favore l'allegato 1.

AG e **ZH** auspicano che i dati biometrici siano inclusi nell'elenco.

Società Digitale e **AlgorithmWatch** chiedono che tutti i dati siano pseudonimizzati secondo l'allegato 1.

4.21 Allegato 2

SO accoglie con favore l'allegato 2.

BE, ZH, GE e **CPS** sottolineano che per la definizione dei reati di terrorismo occorre un rimando all'allegato 1a dell'ordinanza N-SIS.

I **Verdi, Società Digitale** e **AlgorithmWatch** chiedono che vengano eliminate tutte le categorie di reato che non hanno un collegamento oggettivo diretto con il trasporto di passeggeri aerei. Secondo **FSA**, le seguenti categorie di reato dovrebbero essere escluse dall'allegato 2 in base all'avamprogetto: 3, 4, 6, 7, 8, 9, 12, 15, 17, 18, 21, 24, 25, 26.

Elenco dei Cantoni, dei partiti e delle organizzazioni che hanno trasmesso un parere

(con indicazione delle abbreviazioni utilizzate nel testo)

1. CANTONI

AG	Consiglio di Stato Argovia
AI	Consiglio di Stato Appenzello Interno
AR	Consiglio di Stato Appenzello Esterno
BE	Consiglio di Stato Berna
BL	Consiglio di Stato Basilea Campagna
BS	Consiglio di Stato Basilea Città
FR	Consiglio di Stato Friburgo
GE	Consiglio di Stato Ginevra
GL	Consiglio di Stato Glarona
GR	Consiglio di Stato Grigioni
JU	Consiglio di Stato Giura
LU	Consiglio di Stato Lucerna

NE	Consiglio di Stato Neuchâtel
NW	Consiglio di Stato Nidvaldo
OW	Consiglio di Stato Obvaldo
SG	Consiglio di Stato San Gallo
SH	Consiglio di Stato Sciaffusa
SO	Consiglio di Stato Soletta
SZ	Consiglio di Stato Svitto
TG	Consiglio di Stato Turgovia
TI	Consiglio di Stato Ticino
UR	Consiglio di Stato Uri
VD	Consiglio di Stato Vaud
VS	Consiglio di Stato Vallese
ZG	Consiglio di Stato Zugo
ZH	Consiglio di Stato Zurigo

2. PARTITI RAPPRESENTATI NELL'ASSEMBLEA FEDERALE

Alleanza del Centro	Alleanza del Centro
I Verdi	Partito ecologista svizzero
PLR	I Liberali Radicali
PS	Partito socialista svizzero
UDC	Unione democratica di centro

3. ASSOCIAZIONI MANTELLO NAZIONALI DEI COMUNI, DELLE CITTÀ E DELLE REGIONI DI MONTAGNA

ACS	Associazione dei Comuni Svizzeri
-----	----------------------------------

4. ASSOCIAZIONI MANTELLO NAZIONALI DELL'ECONOMIA

economiesuisse	Federazione delle imprese svizzere
usam	Unione svizzera delle arti e mestieri
USI	Unione svizzera degli imprenditori
USS	Unione sindacale svizzera

5. ALTRE ORGANIZZAZIONI E ISTITUZIONI

Aeroporto di Zurigo	Aeroporto di Zurigo / Flughafen Zürich AG
Aerosuisse	Aerosuisse
AlgorithmWatch	AlgorithmWatch Svizzera
ASA	Associazione svizzera degli aerodromi
CCPCS	Conferenza dei comandanti delle polizie cantonali della Svizzera
CDDGP	Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia
CPS	Conferenza dei procuratori della svizzera
easyjet	easyjet
FSA	Federazione svizzera degli avvocati
FSFP	Federazione Svizzera dei Funzionari di Polizia

MPC	Ministero pubblico della Confederazione
PPS	Partito Pirata Svizzera
Privatim	Conferenza degli incaricati svizzeri per la protezione dei dati
Società Digitale	Società Digitale
SSDP	Società svizzera di diritto penale
STV	Federazione svizzera del turismo
SWISS	SWISS
TAF	Tribunale amministrativo federale
TF	Tribunale federale
TPF	Tribunale penale federale

PRIVATI

Law_Firm	Sylvain Métille, professore ass., Dr jur, avvocato
R.S.	Rolf Sommer