Senato della Repubblica

Camera dei deputati

Schema di decreto legislativo recante attuazione 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

Atto del Governo n. 8

Schede di lettura

DOSSIER - XVIII LEGISLATURA

aprile 2018

Senato della Repubblica

SERVIZIO STUDI
Ufficio ricerche sulle questioni istituzionali, giustizia e cultura
TEL. 06 6706-2451 - studi1@senato.it - @SR_Studi

Dossier n. 8

Camera dei deputati

SERVIZIO STUDI
Dipartimento Istituzioni
Tel. 06 6760-3855 - st_istituzioni@camera.it - @CD_istituzioni

Ha collaborato l'Ufficio Rapporti con l'Unione europea

Atti del Governo n. 8

AC0086

I N D I C E

La disposizione di delega e la direttiva 5
Articolo 1 *(Oggetto e ambito di applicazione)* 10
Articolo 2 *(Definizioni)* 13
Articolo 3 *(Finalità dei trattamenti)* 15
Articolo 4 *(Sistema Informativo)* 16
Articolo 5 *(Modalità di trasferimento dei dati PNR al Sistema informativo)* 18
Articolo 6 *(Unità d'informazione sui passeggeri (UIP) nazionale)* 19
Articolo 7 *(Uffici incaricati dei controlli di polizia di frontiera)* 21
Articolo 8 *(Trattamento dei dati PNR)* 22
Articolo 9 *(Trattamento dei dati API)* 23
Articolo 10 *(Periodo di conservazione dei dati PNR e trasformazione in forma anonima)* 24
Articolo 11 *(Conservazione dei dati API)* 26
Articolo 12 *(Trasferimento dei dati PNR alle autorità competenti nazionali)* 27
Articolo 13 *(Trasferimento dei dati PNR alle UIP degli Stati membri)* 29
Articolo 14 *(Trasferimento dei dati PNR alle autorità competenti degli Stati membri)* 31
Articolo 15 *(Trasferimento dei dati PNR da parte di Stati membri)* 32
Articolo 16 *(Richiesta dei dati PNR da parte delle autorità competenti nazionali)* 33
Articolo 17 *(Modalità dì scambio delle informazioni)* 34
Articolo 18 *(Trasferimento dei dati PNR a Europol)* 35
Articolo 19 *(Trasferimento dei dati PNR a Paesi terzi)* 37
Articolo 20 *(Autorità nazionale di controllo)* 39
Articolo 21 *(Responsabile per la protezione dei dati)* 40
Articolo 22 *(Protezione dei dati personali)* 41
Articolo 23 *(Diritti degli interessati)* 43
Articolo 24 *(Sanzioni)* 44
Articolo 25 *(Statistiche)* 46

Articolo 26 *(Disposizioni transitorie e finali)* 47
Articolo 27 *(Clausola di neutralità finanziaria)* 48

Documenti all’esame delle istituzioni dell’UE 49
Procedure di contenzioso 49

La disposizione di delega e la direttiva

Lo schema di decreto legislativo è adottato in attuazione della disposizione di delega recata dall'articolo 1 della legge 25 ottobre 2017, n. 163 (*Legge di delegazione europea 2016-2017)*, per il recepimento delle direttive elencate nell'allegato A, tra cui è ricompresa la direttiva 2016/1148.

E' previsto che gli schemi di decreto legislativo di recepimento delle ventotto direttive contenute nell'allegato A, debbano essere preliminarmente sottoposti all'esame delle competenti Commissioni parlamentari per l'espressione del relativo **parere**.

Per quanto riguarda i **termini, le procedure, i princìpi e i criteri direttivi** della delega, è fatto rinvio alle disposizioni previste dagli articoli 31 e 32 della legge 24 dicembre 2012, n. 234. La legge reca inoltre, all'art. 12, specifici criteri direttivi per l'attuazione della direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) ai fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

L'articolo 31, comma 1, della legge n. 234 del 2012 dispone che il termine per l'esercizio delle deleghe conferite al Governo con la legge di delegazione europea sia di **quattro mesi antecedenti il termine di recepimento** indicato in ciascuna delle direttive . Per le direttive il cui termine così determinato sia già scaduto alla data di entrata in vigore della legge di delegazione europea, o scada nei tre mesi successivi, la delega deve essere esercitata entro **tre mesi dalla data di entrata in vigore della legge stessa**. Per le direttive che non prevedono un termine di recepimento, il termine per l'esercizio della delega è di dodici mesi dalla data di entrata in vigore della legge di delegazione europea.

L'articolo 31, comma 5, della legge n. 234 del 2012 prevede inoltre che il Governo possa adottare **disposizioni integrative e correttive** dei decreti legislativi emanati in base alla delega conferita con la legge di delegazione entro **24 mesi** dalla data di entrata in vigore di ciascun decreto legislativo, sempre nel rispetto dei princìpi e criteri direttivi fissati dalla legge stessa.

Il **termine di recepimento** della direttiva 2016/681 è fissato – dalla medesima - al 25 maggio 2018. La legge di delegazione europea è entrata in vigore il 21 novembre 2017 (quindi il termine del 25 gennaio 2018 per il relativo recepimento veniva a scadenza nei tre mesi successivi alla data del 21 novembre 2017) ed ha trovato dunque applicazione, per l'esercizio della delega legislativa, il termine di tre mesi dalla data di entrata in vigore della legge medesima fissato, quindi, 21 febbraio 2018. Considerato che l'articolo 31, comma 3, della legge 234 del 2012 prevede che qualora il termine fissato per l'espressione del parere parlamentare scada nei trenta giorni che precedono il termine per l'esercizio della delega o **successivamente**, il termine per la delega è prorogato di tre mesi, il termine finale per l'esercizio della delega legislativa è fissato al **21 maggio 2018**.

L’articolo 12 della legge di delegazione europea, come già ricordato, reca **specifici principi e criteri direttivi** per l’attuazione 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.

Preliminarmente si ricorda che i "reati gravi" sono definiti in un elenco allegato (II) alla direttiva, che comprende tra l'altro fatti di associazione criminale, di narcotraffico, di violenza sessuale, di "corruzione", nonché vari altri reati gravi contro la vita e l'incolumità delle persone, oppure contro il patrimonio. La direttiva impone inoltre (articolo 3, n. 9) che i fatti in questioni siano puniti con una pena detentiva pari almeno a tre anni.

L’art. 12 prevede due **principi di delega ulteriori** rispetto a quelli previsti in via generale dalla legge di delegazione europea (che rinvia all’art. 32 della legge n. 234/2012 – v. *infra*).

Nella relazione illustrativa alla legge di delegazione di evidenziava come la direttiva (UE) 2016/681, recando prescrizioni di dettaglio, lasci scarsa discrezionalità al legislatore nazionale, in sede di recepimento.

Si prevede dunque che il Governo dovrà, in sede di attuazione, collocare **l’Unità d'informazione sui passeggeri (UIP),** di cui all’articolo 4 della direttiva, presso il **Ministero dell’Interno** – Dipartimento della Pubblica Sicurezza (comma 1, lettera a). Tale scelta - precisa la relazione illustrativa alla legge di delegazione - è strettamente connessa al fatto che i dati raccolti, costituendo un patrimonio informativo rilevante in materia di prevenzione e accertamento dei reati, sono destinati ad essere trattati **a fini di polizia**. Il secondo criterio di delega (comma 1, lettera b) prevede che il trasferimento a cura dei vettori aerei dei dati del PNR comprenda **anche i voli intra-UE**[1].

Per quanto riguarda i **princìpi e criteri direttivi generali di delega** indicati dall’art. 32 della legge n. 234 del 2012:

a) le amministrazioni direttamente interessate provvedono all'attuazione dei decreti legislativi con le ordinarie strutture, secondo il principio della massima semplificazione dei procedimenti;

b) ai fini di un migliore coordinamento con le discipline vigenti sono introdotte le occorrenti modificazioni alle discipline stesse, anche attraverso il riassetto e la semplificazione della normativa;

c) gli atti di recepimento di direttive dell'Unione europea non possono prevedere l'introduzione o il mantenimento di livelli di regolazione superiori a quelli minimi richiesti dalle direttive stesse (c.d. *gold plating*);

[1] La direttiva definisce "volo extra-UE" un volo di linea o non di linea effettuato da un vettore aereo in provenienza da un Paese terzo e che deve atterrare nel territorio di uno Stato membro oppure in partenza dal territorio di uno Stato membro e che deve atterrare in un Paese terzo, compresi, in entrambi i casi, i voli con scali nel territorio di Stati membri o di Paesi terzi.

d) ove necessario, al fine di assicurare l'osservanza delle disposizioni contenute nei decreti legislativi, sono previste sanzioni amministrative e penali per le infrazioni alle disposizioni dei decreti stessi. In ogni caso le sanzioni penali sono previste "solo nei casi in cui le infrazioni ledano o espongano a pericolo interessi costituzionalmente protetti";

e) al recepimento di direttive o di altri atti che modificano precedenti direttive o di atti già attuati con legge o con decreto legislativo si procede apportando le corrispondenti modificazioni alla legge o al decreto legislativo di attuazione;

f) nella redazione dei decreti legislativi si tiene conto delle eventuali modificazioni delle direttive comunque intervenute fino al momento dell'esercizio della delega;

g) quando si verificano sovrapposizioni di competenze tra amministrazioni diverse o comunque siano coinvolte le competenze di più amministrazioni statali, i decreti legislativi individuano le procedure per salvaguardare l'unitarietà dei processi decisionali, l'efficacia e la trasparenza dell'azione amministrativa, nel rispetto dei princìpi di sussidiarietà e delle competenze delle regioni e degli enti territoriali;

h) le direttive che riguardano le stesse materie o che comunque comportano modifiche degli stessi atti normativi vengono attuate con un unico decreto legislativo, compatibilmente con i diversi termini di recepimento;

i) è sempre assicurata la parità di trattamento dei cittadini italiani rispetto ai cittadini degli altri Stati membri dell'Unione europea e non può essere previsto in ogni caso un trattamento sfavorevole dei cittadini italiani.

Per quanto riguarda il procedimento per il **parere delle competenti Commissioni parlamentari**, la disposizione segue lo schema procedurale disciplinato in via generale dall'articolo 31, comma 3, della legge 234 del 2012.

Esso prevede che gli schemi di decreto legislativo, una volta acquisiti gli altri pareri previsti dalla legge, siano trasmessi alle Camere per l'espressione del parere e che, decorsi **quaranta giorni dalla data di trasmissione**, i decreti siano emanati anche in mancanza del parere.

Come già ricordato, qualora il termine fissato per l'espressione del parere parlamentare scada nei trenta giorni che precedono il termine per l'esercizio della delega o successivamente, il termine per la delega è **prorogato di tre mesi**. Si intende in tal modo permettere al Governo di usufruire in ogni caso di un adeguato periodo di tempo per l'eventuale recepimento nei decreti legislativi delle indicazioni emerse in sede parlamentare.

Il comma 9 del medesimo articolo 31 prevede altresì che ove il Governo **non intenda conformarsi ai pareri espressi dagli organi parlamentari** relativi a **sanzioni penali** contenute negli schemi di decreti legislativi, ritrasmette i testi alle Camere, con le sue osservazioni e con eventuali modificazioni. Decorsi venti giorni dalla data di ritrasmissione, i decreti sono emanati anche in mancanza di nuovo parere.

Alla copertura degli oneri recati dalle spese eventualmente previste nei decreti legislativi attuativi, nonché alla copertura delle minori entrate eventualmente derivanti dall'attuazione delle direttive, qualora non sia possibile farvi fronte con i fondi già assegnati alle competenti amministrazioni, si provvede a carico del

Fondo per il recepimento della normativa europea, di cui all'articolo 41-bis della legge n. 234/2012.

Lo stesso comma 3 prevede inoltre che, in caso di incapienza del Fondo per il recepimento della normativa europea, i decreti legislativi attuativi delle direttive dai quali derivano nuovi o maggiori oneri sono emanati solo successivamente all'entrata in vigore dei provvedimenti legislativi che stanziano le occorrenti risorse finanziarie, in conformità all'articolo 17, comma 2, della legge di contabilità e finanza pubblica (legge 31 dicembre 2009, n. 196).

È altresì previsto il parere delle **Commissioni parlamentari competenti anche per i profili finanziari** sugli schemi dei decreti legislativi in questione, come richiesto dall'articolo 31, comma 4, della legge 24 dicembre 2012, n. 234, che disciplina le procedure per l'esercizio delle deleghe legislative conferite al Governo con la legge di delegazione europea.
In particolare, il citato comma 4 dell'articolo 31 prevede che gli schemi dei decreti legislativi recanti recepimento delle direttive che comportino conseguenze finanziarie sono corredati della **relazione tecnica**, ai sensi dell'articolo 17, comma 3, della legge di contabilità pubblica (legge n. 196/2009). Su di essi è richiesto anche il parere delle Commissioni parlamentari competenti per i **profili finanziari**.
E' previsto che il Governo, ove non intenda conformarsi alle condizioni formulate con riferimento all'esigenza di garantire il rispetto dell'articolo 81, quarto comma, della Costituzione, **ritrasmette** alle Camere i testi, corredati dei necessari elementi integrativi d'informazione, per i pareri definitivi delle Commissioni parlamentari competenti per i profili finanziari, che devono essere espressi entro venti giorni.

La direttiva (UE) 2016/681 in sintesi

La direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, prevede:

• il trasferimento, a cura dei vettori aerei, dei dati del codice di prenotazione dei passeggeri (PNR) dei voli extra-UE[2];

• il trattamento di tali dati da parte delle autorità competenti degli Stati membri dell'Unione Europea (UE), a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

Ai fini della direttiva, si intende per "codice di prenotazione" (PNR) le informazioni relative al viaggio di ciascun passeggero comprendenti i dati necessari per il trattamento e il controllo delle prenotazioni a cura dei vettori aerei, siano esse registrate in sistemi di prenotazione, in sistemi di controllo delle partenze utilizzati per la registrazione dei passeggeri sui voli, o in altri sistemi equivalenti con le stesse funzionalità.

I dati del codice di prenotazione raccolti dai vettori aerei sono elencati all'allegato I e comprendono:

1. il codice PNR di identificazione della pratica;
2. la data di prenotazione/emissione del biglietto;
3. le date di viaggio;
4. il nome;
5. indirizzo, recapito telefonico e indirizzo di posta elettronica;
6. le informazioni sui viaggiatori abituali;
7. l'itinerario di viaggio;
8. l'agenzia di viaggio;
9. lo status di viaggio del passeggero, inclusi conferme, check-in, precedenti assenze all'imbarco o passeggero senza prenotazione;
10. PNR scissi/divisi;
11. osservazioni generali (comprese tutte le informazioni sui minori non accompagnati di età inferiore a 18 anni);
12. i dati sull'emissione del biglietto;
13. le informazioni sul posto, compreso il numero di posto assegnato;
14. le informazioni sul *code share* (codici comuni);
15. le informazioni sui bagagli;
16. il numero di viaggiatori e altri nomi figuranti nel PNR;
17. le informazioni anticipate sui passeggeri (API) eventualmente raccolte (tra cui: tipo, numero, Paese di rilascio e data di scadenza del documento, cittadinanza, cognome, nome, sesso, data di nascita, compagnia aerea, numero di volo, data di partenza, data di arrivo, aeroporto di partenza, aeroporto di arrivo, ora di partenza e ora di arrivo);
18. cronistoria delle modifiche dei dati PNR.

[2] Viene definito "volo extra-UE" un volo di linea o non di linea effettuato da un vettore aereo in provenienza da un Paese terzo e che deve atterrare nel territorio di uno Stato membro oppure in partenza dal territorio di uno Stato membro e che deve atterrare in un Paese terzo, compresi, in entrambi i casi, i voli con scali nel territorio di Stati membri o di Paesi terzi;

Articolo 1
(Oggetto e ambito di applicazione)

Gli articoli del **Capo I** dello schema di decreto recano disposizioni di carattere generale.

L'**articolo 1** individua l'oggetto del decreto che consiste nel **recepimento dei contenuti della direttiva (UE) 2016/681 del 27 aprile 2016**, del Parlamento europeo e del Consiglio sull'uso del codice di prenotazione (PNR). Tale direttiva si propone di rafforzare il sistema di controllo avente ad oggetto le informazioni che ciascun passeggero fornice ai vettori aerei in fase di prenotazione del volo (cd. dati PNR), con finalità di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

Più nel dettaglio, la **direttiva PNR** introduce l'obbligo per i vettori aerei di trasmettere informazioni specifiche elencate nell'allegato I (c.d. dati PNR) riguardanti i passeggeri di voli extra-UE e intra-UE, in ingresso e in uscita dal territorio dello Stato, all'Unità d'informazione sui passeggeri («UIP»), appositamente istituita e avente la funzione principale di individuare, attraverso l'analisi dei dati PNR, i passeggeri implicati in reati di terrorismo o in altri reati gravi.

In particolare, ai sensi del **comma 1**, il decreto disciplina:

1) il **trasferimento** da parte dei vettori aerei dei **dati PNR dei voli *extra* UE e dei voli *intra* UE**. A tale riguardo, come indicato nel criterio direttivo specifico della delega contenuta nell'art. 12 della legge di delegazione europea 2016-2017 (L. n. 163/2017), il Governo in sede di recepimento si è avvalso della facoltà riconosciuta dall'articolo 2 della direttiva comunitaria di **estendere l'applicazione dell'obbligo di trasmissione dei dati PNR anche in relazione ai voli intra-UE**;
2) il **trattamento di tali dati** da parte delle autorità competenti, ivi incluse le operazioni di raccolta, uso, conservazione e scambio con gli Stati membri.

Il **comma 2** estende l'oggetto del decreto anche alla **disciplina del trattamento dei c.d. dati API**, ossia dei dati relativi ai passeggeri che fanno ingresso nel territorio dello Stato italiano, che i vettori aerei hanno l'obbligo di trasmettere ai competenti uffici di polizia di frontiera.

Si segnala in merito che tale disciplina è oggetto di un'altra direttiva europea – ossia la direttiva 2004/82/CE (cd. direttiva API) – che è stata già recepita nel nostro ordinamento con il **decreto legislativo 2 agosto 2007, n. 144**.

In particolare, la **direttiva API** ha introdotto l'obbligo per i vettori aerei di trasmettere agli Uffici incaricati di effettuare i controlli di polizia di frontiera determinate informazioni anagrafiche (c.d. «dati API»), relative ai passeggeri trasportati su voli extra-UE che fanno ingresso nel territorio dello Stato, con la finalità di

migliorare l'efficienza delle verifiche di frontiera e di prevenire l'immigrazione irregolare.

In attuazione della direttiva il vigente D.Lgs. n. 144/2007 ha previsto l'istituzione del Sistema informativo frontaliero *Border Control System* (BCS), presso il Ministero dell'interno, Dipartimento della pubblica sicurezza, Direzione centrale dell'immigrazione e della polizia delle frontiere, per la raccolta e il trattamento dei dati API.

La **scelta di assorbire** nello schema di decreto in esame anche la **regolamentazione dei dati API** è motivata – secondo quanto si legge nella relazione illustrativa – «dall'identità dell'oggetto, ossia l'obbligo di trasmissione di informazioni relative ai passeggeri, e l'identità del soggetto su cui tale onere grava, ovvero i vettori aerei».

In tale contesto, si è valutata innanzitutto la problematicità del mantenimento di due diverse discipline normative a livello nazionale, soprattutto in relazione alla duplicazione dei relativi sistemi informativi e degli adempimenti per i vettori aerei. Inoltre, si è tenuto conto del fatto che alcune specifiche disposizioni della direttiva PNR fanno esplicito riferimento ai dati API, a partire da quanto previsto nell'Allegato I, in base al quale i dati API rappresentano una parte dei dati PNR.

Pertanto, l'armonizzazione in una disciplina unitaria contenuta nello schema in esame, con la conseguente abrogazione della normativa di attuazione della direttiva API dal momento dell'entrata in vigore di tutti i provvedimenti di attuazione dello schema in esame (cfr. art. 26, co. 1), è parsa al legislatore delegato, come esplicitato nella relazione illustrativa, una misura di semplificazione, nonché l'opzione di maggior salvaguardia dei principi di necessità e non eccedenza in materia di protezione dei dati personali.

In base alla relazione illustrativa tale scelta troverebbe **fondamento normativo** nei principi di massima semplificazione dei procedimenti e della normativa, enunciati dall'art. 32 della L. 234/2012 come principi generali di delega per l'attuazione del diritto dell'Unione europea, che sono richiamati dal combinato disposto dell'art. 1, co. 1 dell'art. 12 della legge di delegazione n. 163/2017.

Sul punto il **parere del Garante per la privacy** osserva che l'inserimento dei dati API e la loro regolamentazione nello schema di decreto legislativo in esame, «oltre ad apparire non strettamente necessario, potrebbe rivelarsi non proporzionale, attesa la mancanza di ogni valutazione d'impatto in merito e considerati i differenti ambiti regolati dalla rispettiva disciplina.». Tale osservazione muove in particolare dalla considerazione che la direttiva 2016/681/UE lascia impregiudicata la disciplina recata dalla direttiva API e che il regime di raccolta dei dati stabilito dal D.Lgs. n. 244 del 2007, che si intende abrogare, presenta punti di difformità rispetto al contenuto della direttiva PNR.

Pertanto il Garante suggerisce «una rivisitazione delle disposizioni che riguardano il trattamento dei dati API, facendo salve quelle sole disposizioni

conformi alle puntuali previsioni della direttiva 681, espungendo le altre, qualora volte a modificare il D.Lgs. n. 144/2007».

Il terzo comma dell'articolo 1, definisce l'**ambito di applicazione**, precisando che l'attuazione della Direttiva non pregiudica l'applicazione degli accordi o delle intese bilaterali o multilaterali sullo scambio di informazioni tra autorità competenti entrati in vigore con Stati membri dell'Unione europea entro il 24 maggio 2016 (data di entrata in vigore della direttiva), in quanto compatibili con la Direttiva stessa, né l'applicazione degli obblighi derivanti da accordi bilaterali o multilaterali conclusi con Stati terzi, ossia non appartenenti all'Unione europea.

Articolo 2
(Definizioni)

L'**articolo 2** reca disposizioni di carattere definitorio. Oltre a recepire le definizioni contenute nella direttiva 2016/681, rientrano, in particolare, nella definizione di «**autorità competenti nazionali**» (co. 2, lett. b)):

- le Forze di polizia di cui all'articolo 16, co. 1, della L. 121/1981 (Polizia di Stato, Arma dei Carabinieri, Guardia di Finanza);
- la Direzione Investigativa Antimafia;
- gli Organismi di informazione e sicurezza facenti parte del Sistema di Informazione per la Sicurezza della Repubblica, di cui agli articoli 4, 6 e 7 della Legge n. 124/2007 (Dipartimento delle informazioni per la sicurezza-DIS, Agenzia informazioni e sicurezza esterna-AISE e Agenzia informazioni e sicurezza interna-AISI);
- la Direzione Nazionale Antimafia e Antiterrorismo;
- le Autorità giudiziarie competenti a perseguire i reati di terrorismo e i reati gravi.

Per **Unità di informazione sui passeggeri (UIP) nazionale**, ossia l'autorità competente in materia di prevenzione e repressione dei reati di terrorismo e dei reati gravi, che ai sensi della direttiva spetta a ciascuno Stato membro individuare, s'intende l'Unità istituita presso il Dipartimento della pubblica sicurezza del Ministero dell'interno, nell'ambito della Direzione centrale della polizia criminale (co. 2, lett. o)).

In tale previsione trova attuazione un altro criterio direttivo specifico della delega contenuta nell'art. 12 della legge di delegazione europea 2016-2017 (L. n. 163/2017), che prevede di collocare l'Unità d'informazione sui passeggeri presso il Ministero dell'Interno – Dipartimento della Pubblica Sicurezza (comma 1, lettera a).

Tale scelta - precisava la relazione - è strettamente connessa al fatto che i dati raccolti, costituendo un patrimonio informativo rilevante in materia di prevenzione e accertamento dei reati, sono destinati ad essere trattati a fini di polizia.

Assumono rilievo, soprattutto ai fini dell'accorpamento delle discipline delle direttive 2016/681/UE e 2004/82/CE, anche le definizioni di:

- «dati PNR», con cui s'intendono le informazioni relative al viaggio di ciascun passeggero consistenti nei dati di cui all'allegato I della direttiva 2016/681, necessari per il trattamento e il controllo delle prenotazioni da parte dei vettori aerei e contenuti nel codice di prenotazione (co. 1, lett. a));
- «dati API», con cui si intende parte dei dati PNR, comprendenti il tipo, il numero, paese di rilascio e la data di scadenza del documento di viaggio

utilizzato, la cittadinanza, il nome completo, sesso, la data e il luogo di nascita, il valico di frontiera di ingresso nel territorio italiano, la compagnia aerea, il numero di volo, la data di partenza e di arrivo, l'ora di partenza, l'ora di arrivo e la durata del volo, l'aeroporto di partenza e di arrivo, il numero complessivo dei passeggeri trasportati con tale volo, il primo punto di imbarco (co. 3, lett. c)).

Articolo 3
(Finalità dei trattamenti)

L’articolo 3 apre il **capo II** (artt. 3-11) che disciplina le finalità del trattamento dei dati raccolti a norma dello schema di decreto. A tal fine, la disposizione considera la diversa tipologia dei dati a cui associa due distinte finalità.

Da un lato, i **dati PNR** sono trattati, in ossequio alla direttiva 2016/681/UE, per fini di **prevenzione e repressione dei reati di terrorismo e dei reati gravi**.

Si ricorda in proposito che i "reati gravi" sono definiti in un elenco allegato (II) alla direttiva, che comprende tra l'altro fatti di associazione criminale, di narcotraffico, di violenza sessuale, di "corruzione", nonché vari altri reati gravi contro la vita e l'incolumità delle persone, oppure contro il patrimonio. La direttiva impone inoltre (articolo 3, n. 9) che i fatti in questioni siano puniti con una pena detentiva pari almeno a tre anni.

Dall’altro, la finalità del trattamento dei **dati API**, raccolti e resi disponibili agli Uffici incaricati dei controlli di polizia di frontiera secondo le disposizioni del decreto, è di **migliorare i controlli delle frontiere esterne e prevenire l’immigrazione illegale**.

La disposizione specifica che il trattamento dei dati API può essere esteso ai voli intra-UE in caso di ripristino temporaneo dei controlli di frontiera.

Articolo 4
(Sistema Informativo)

L'**articolo 4** prevede **l'istituzione del "Sistema Informativo"** attraverso il quale verranno raccolti, trattati e trasferiti i dati del codice di prenotazione (PNR), di cui alla direttiva (UE) 2016/681, e le informazioni anticipate sui passeggeri (API), di cui alla direttiva 2004/82/CE del Consiglio (co. 1).

Attualmente, i dati API, per le finalità e alle condizioni previste dal D.Lgs. 2 agosto 2007, n. 144, recante l'attuazione della citata Direttiva API, sono raccolti e trattati nel sistema informativo frontaliero *Border Control System* (BCS). Pertanto, a regime, tale sistema dovrebbe essere sostituito dal Sistema previsto dall'articolo in commento.

Il Sistema è istituito **presso il Dipartimento della Pubblica Sicurezza** del Ministero dell'Interno, a cui sono attribuite anche le funzioni di **titolare del trattamento** ai sensi di quanto previsto dal Codice per la protezione dei dati personali. Le funzioni di **responsabile del trattamento** sono invece attribuite a due diverse articolazioni del Dipartimento, ossia la Direzione centrale della polizia criminale per quanto concerne i dati PNR e la Direzione centrale dell'immigrazione e della polizia delle frontiere con riferimento ai dati API (co. 2).

Le interrogazioni del Sistema possono essere effettuate esclusivamente per le finalità indicate dall'articolo 3 dello schema e da parte del personale titolare di un specifico profilo di autorizzazione (co. 3 e 4).

La **disciplina tecnica del Sistema** viene demandata ad uno o più **decreti di natura non regolamentare** adottati, entro tre mesi dalla data di entrata in vigore del decreto, dal Ministro dell'interno, sentito il Garante per la protezione dei dati personali (comma 5).

A tale riguardo, nel **parere reso dal Garante per la privacy** si evidenzia che l'utilizzo di un Sistema Informativo unitario rappresenta un «utile elemento di semplificazione degli adempimenti in carico ai vettori aerei». Esso richiede l'adozione di opportune misure tecniche e organizzative al fine di garantire il rispetto dei principi di necessità, di proporzionalità e di finalità nel trattamento dei dati PNR e dei dati API, che il Garante si riserva di valutare una volta che saranno adottati i decreti ministeriali ai sensi della disposizione da ultimo citata.

Si fa rinvio ad uno specifico decreto per disciplinare le modalità di trasferimento delle informazioni dall'UIP agli organismi del comparto "*intelligence*", secondo la procedura prevista per l'adozione di disposizioni regolamentari ai sensi della L. n. 124 del 2007 sul sistema di informazione per la sicurezza della Repubblica (comma 6).

Viene richiamato in proposito l’art. 43 della L. 124 del 2007, ai sensi del quale le disposizioni regolamentari sono emanate con uno o più decreti del Presidente del Consiglio dei ministri adottati anche in deroga all'articolo 17 della legge 23 agosto 1988, n. 400, e successive modificazioni, previo parere del Comitato parlamentare per la sicurezza della Repubblica e sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR). Tali decreti stabiliscono il regime della loro pubblicità, anche in deroga alle norme vigenti.

Il comma 7 stabilisce i formati di dati e i protocolli informatici che il Sistema informativo deve utilizzare.

Ai sensi del comma 8, i vettori aerei che non effettuano voli secondo un programma operativo pubblico specifico e che non possiedono l'infrastruttura necessaria a supportare i formati di dati e i protocolli di trasmissione di cui al comma 7 devono **trasferire i dati PNR** con un mezzo elettronico che offra adeguate garanzie rispetto alle misure di sicurezza tecniche, individuato dall’Unità d’informazione sui passeggeri nazionale con apposita prescrizione, sarebbe opportuno prevedere che venga "sentito il Garante per la protezione dei dati personali".

A tale riguardo, nel proprio **parere** il **Garante per la privacy** ha osservato che sarebbe opportuno prevedere il parere del Garante sulla decisione dell’UIP. Ha inoltre sottolineato che sembrerebbe più coerente collocare il comma 8 all'interno del successivo articolo 5 dello schema, recante le modalità di trasferimento dei dati PNR al Sistema Informativo.

Articolo 5
(Modalità di trasferimento dei dati PNR al Sistema informativo)

L’**articolo 5** prevede l’**obbligo** per i vettori aerei di **trasferire al Sistema informativo i dati PNR** relativi ai voli in partenza, in arrivo o facenti scalo nel territorio nazionale raccolti nello svolgimento della loro attività (comma 1).

La relazione illustrativa esplicita che in tale disposizione confluisce la disciplina dell’obbligo dei vettori aerei di trasmettere i dati API, in quanto tali dati, rappresentando un sottoinsieme dei dati PNR, sono trasferiti contestualmente agli altri dati inclusi nel codice di prenotazione.

La trasmissione deve avvenire con «metodo push» con mezzo elettronico.

I vettori aerei devono utilizzare, per il trasferimento dei dati PNR, "i formati di dati e i protocolli informatici comuni individuati con la decisione di esecuzione 2017/759/UE della Commissione, del 28 aprile 2017” (comma 2). Tuttavia, nelle more dell'adeguamento dei propri sistemi informatici, i vettori possono utilizzare mezzi elettronici di trasmissione ulteriori (comma 3).

A tale riguardo, il **Garante per la privacy** osserva che sarebbe opportuno prevedere che le specifiche tecniche di tali mezzi elettronici di trasmissione siano oggetto di un preventivo parere da parte del Garante medesimo.

I dati PNR devono essere trasferiti in due momenti distinti. Un primo trasferimento avviene **tra le 24 e le 48 ore antecedenti l’orario** previsto per la **partenza del volo**. Immediatamente **dopo la chiusura del volo**, quando non è più possibile l’imbarco o lo sbarco dei passeggeri, i vettori aerei trasferiscono nuovamente di dati, anche mediante aggiornamento dei precedenti (comma 4).

I dati possono essere trasferiti anche in un momento precedente quelli indicati in caso di pericolo imminente e concreto che possa essere commesso un reato di terrorismo o un altro grave reato (co. 5).

Nell’ipotesi in cui vengano trasferiti **dati diversi** da quelli richiesti in base alla normativa europea (allegato I della direttiva PNR), l’Unità di informazione sui passeggeri nazionale provvede alla loro immediata cancellazione (co. 6).

Articolo 6
(Unità d'informazione sui passeggeri (UIP) nazionale)

L'**articolo 6** disciplina **composizione e funzioni dell'Unità d'informazione sui passeggeri (UIP) nazionale**.

Ai sensi di tale disposizione (comma 2) l'UIP nazionale è l'organo deputato a **ricevere dai vettori aerei i dati PNR** e, soprattutto, l'organo competente ad **analizzare**, prima dell'arrivo o della partenza del volo, **i dati** ricevuti per individuare eventuali passeggeri che potrebbero essere implicati in reati di terrorismo o in altri reati gravi per i quali è necessario procedere ad ulteriori verifiche da parte delle autorità competenti.

Inoltre, spetta all'Unità nazionale:

- **comunicare alle autorità competenti nazionali** o di altri Stati membri, in caso di richiesta motivata, **i dati PNR** o i risultati del loro trattamento;
- **scambiare** tali **dati con le Unità di altri Stati membri** secondo le modalità previste nel capo III dello schema in esame;
- **aggiornare i criteri** sulla base dei quali sono effettuate le valutazioni finalizzate a individuare i **passeggeri che potrebbero essere implicati in reati** di terrorismo o in altri reati gravi.

Con riferimento alle funzioni dell'UIP nazionale, l'articolo 6, comma 2, lettera *a)*, dello schema prevede il possibile avvalimento, da parte dell'UIP nazionale, di un "operatore economico qualificato" per la ricezione dei dati PNR dei vettori aerei.

In questa eventualità, nel parere del Garante della privacy si segnala l'opportunità di «prevedere che l'operatore venga designato quale responsabile esterno del trattamento».

In attuazione del criterio direttivo previsto dalla legge dei delegazione europea (art. 12, L. n. 163 del 2017), il regolamento prevede che l'UIP nazionale sia incardinata presso il Dipartimento della pubblica sicurezza del Ministero dell'interno (si cfr., *supra*, art. 2, co. 2, lett. *o)*).

Il comma 1 dell'articolo in commento prevede che l'unità sia **composta da personale delle forze di polizia** (Polizia di stato, Carabinieri e Guardia di Finanza) e rimette **l'organizzazione e la pianta organica** dell'Unità ad un **decreto del Ministro dell'interno**, di concerto con il Ministro dell'economia, al pari di come avviene per l'organizzazione interna di tutte le articolazioni del Dipartimento della pubblica sicurezza (art. 5, co. 7, L. n. 121/1981).

Per quanto concerne il contingente di personale, esso viene stabilito con decreto del Ministero dell'interno per il personale appartenente ai ruoli della

Polizia di Stato, mentre per quanto riguarda il personale delle altre forze di polizia con dPCM, su proposta del Ministro dell'interno, di concerto con il Ministro dell'economia e con i Ministri interessati (art. 6, co. 2, L. n. 121/1981).

Articolo 7
(Uffici incaricati dei controlli di polizia di frontiera)

L’**articolo 7** individua, in conformità alle previsioni oggi contenute nel D.Lgs. n. 144 del 2007 di attuazione della direttiva API, gli **uffici incaricati di effettuare i controlli delle persone alle frontiere** esterne attraverso le quali i passeggeri entrano nel territorio dello Stato, come gli **organi incaricati del trattamento dei dati API** per agevolare tali controlli al fine di prevenire l’immigrazione irregolare.

Tale disposizione chiarisce che i dati API, pur essendo parte dei dati PNR e venendo quindi trattati dall'UIP nazionale al pari degli altri dati contenuti nel codice di prenotazione, devono essere altresì trattati, ai sensi della Direttiva API, dagli Uffici incaricati di svolgere i controlli di polizia di frontiera per le finalità previste dalla stessa Direttiva.

In merito la relazione illustrativa esplicita che, pertanto, il Sistema informativo dovrà essere strutturato tecnicamente in modo da consentire il trattamento dei dati PNR ad opera dell’Unità nazionale e il contemporaneo trattamento del sottoinsieme dei soli dati API da parte degli uffici di frontiera, nel rispetto della diversa finalità.

Articolo 8
(Trattamento dei dati PNR)

L'**articolo 8** definisce le **modalità operative del trattamento** dei dati PNR, specificando in particolare come l'Unità nazionale procede all'analisi di tali dati per l'individuazione dei passeggeri sospettati (comma 1).

A tal fine, infatti l'UIP può **mettere a confronto i dati PNR con le informazioni contenute nella Banca dati delle forze di polizia**, e le altre banche dati europee ed internazionali che possano contenere informazioni utili per prevenire i reati di terrorismo o i reati gravi.

Per quanto riguarda le banche dati nazionali, si fa esplicito rifermento al Centro elaborazione dati (CED) istituito ai sensi dell'art. 8 della legge n. 121/1981 nell'ambito del Servizio per il Sistema Informativo Interforze (S.S.I.I.) della Direzione centrale della Polizia criminale, interna al Dipartimento della pubblica sicurezza.

L'UIP può altresì trattare i dati sulla base di **criteri predeterminati dalla stessa Unità**, dopo aver sentito le autorità competenti nazionali, nel **rispetto dei principi proporzionalità, specificità e non discriminazione** (comma 2). Anche le modalità di analisi devono essere non discriminatorie (comma 3).

In **caso di riscontro positivo**, ove cioè sia individuato un passeggero sospettato di essere implicato in un reato di terrorismo o in reati gravi, all'esito di un trattamento automatizzato dei dati PNR, si prevede l'obbligo di procedere altresì ad un esame non automatizzato sul singolo caso per verificare la necessità di adozione di provvedimenti da parte delle autorità nazionali competenti, sulla base delle norme vigenti (comma 4).

Infine, si precisa che l'adozione di provvedimenti da parte delle autorità competenti non pregiudica il diritto di entrare nel territorio dello Stato delle persone che godono del diritto di libera circolazione all'interno dell'UE in conformità alle disposizioni contenute nel D.Lgs. n. 30 del 2007, di attuazione della direttiva 2004/38/CE relativa al diritto dei cittadini dell'Unione e dei loro familiari di circolare e di soggiornare liberamente nel territorio degli Stati membri (comma 5).

Articolo 9
(Trattamento dei dati API)

L’**articolo 9** definisce le **modalità operative del trattamento** dei dati API.

In proposito, si stabilisce che il Sistema informativo rende consultabili i dati API agli uffici incaricati dei controlli di polizia di frontiera immediatamente dopo la chiusura del volo, quando non è più possibile effettuare operazioni di imbarco e di sbarco dei passeggeri.

I dati non necessari per le finalità di prevenzione dell’immigrazione irregolare sono resi invisibili agli Uffici incaricati dei controlli di polizia di frontiera entro ventiquattro ore dalla loro comunicazione ovvero dopo l’ingresso dei passeggeri nel territorio dello Stato.

I dati rilevanti per la citata finalità restano nella disponibilità degli uffici di frontiera per sei mesi dal loro ricevimento.

Attualmente, il D.Lgs. n. 144 del 2007, di attuazione della direttiva API, stabilisce, all’articolo 4, che i competenti uffici incaricati dei controlli di polizia di frontiera, nonché dell'Agenzia delle dogane e della Guardia di finanza, laddove incaricati normativamente dei controlli di polizia di frontiera, registrano i dati comunicati in via provvisoria e, dopo l'ingresso dei passeggeri, cancellano entro ventiquattro ore dalla ricezione, i dati che non sono necessari per il contrasto dell'immigrazione illegale. In deroga a tale disposizione generale, i medesimi dati possono essere conservati per un periodo non superiore a sei mesi, qualora si tratti di dati destinati a confluire per legge nel CED, quando, a seguito di specifica segnalazione, i dati si rendano indispensabili in relazione alla prevenzione di un pericolo per l'ordine pubblico o la sicurezza nazionale o ad attività d'indagine in corso.

Articolo 10
(Periodo di conservazione dei dati PNR e trasformazione in forma anonima)

L'**articolo 10** stabilisce le **condizioni per la conservazione** dei dati PNR, fissando innanzitutto il principio in base al quale i dati PNR sono conservati all'interno del Sistema informativo per un periodo di **cinque anni** dalla loro trasmissione da parte dei vettori aerei (comma 1).

Ciononostante, **decorsi sei mesi** dal loro trasferimento, i dati vengono resi anonimi mediante un'operazione di **mascheramento** di una serie di elementi che potrebbero servire a identificare direttamente gli interessati a cui i dati PNR si riferiscono. Tali elementi vengono esplicitamente individuati mediante elencazione al comma 2.

Si ricorda che ai sensi dell'art. 2, co. 1, lett. b) dello schema, per "mascheramento dei dati" si intende l'operazione attraverso la quale vengono resi non visibili alla consultazione le informazioni che consentono l'identificazione diretta dell'interessato.

Tuttavia, al comma 3 si prefigura l'ipotesi che **allo scadere del periodo di sei mesi**, sia ancora consentita la **comunicazione dei dati PNR integrali**. Ciò può avvenire solo se necessario per corrispondere a una richiesta debitamente motivata, formulata ai sensi del precedente articolo 6, comma 2, lettera c).

In tali ipotesi, il comma 3 richiede altresì la **preventiva autorizzazione**:

a) dell'Autorità giudiziaria nel caso in cui la richiesta sia formulata nell'ambito di un procedimento penale o per l'applicazione di una misura di prevenzione personale o patrimoniale ai sensi del Codice delle leggi antimafia (D.Lgs. n. 159/2011); o

b) del Vice Capo della Polizia, nel caso in cui la richiesta sia formulata per le finalità di prevenzione dei reati di terrorismo e dei reati gravi.

Tale autorizzazione deve essere comunicata al responsabile della protezione dei dati personali, nominato ai sensi del successivo art. 21 dello schema, per le verifiche di competenza (comma 4).

In relazione a tale fattispecie, il **Garante della privacy** ha sottolineato che non è chiaro se, a seguito dell'operazione con cui "i dati sono resi anonimi mediante mascheramento", sia ancora possibile re-identificare gli interessati. In tal caso, i dati non possono essere trattati come dati anonimi nell'accezione di cui all'articolo 4, comma 1, lettera n), del Codice (il dato anonimo è "il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile"). Pertanto, secondo il Garante, sarebbe più appropriato modificare la terminologia, utilizzando la nozione di pseudonimizzazione del dato, introdotta dal Regolamento (UE) 2016/679.

Decorso il termine di cinque anni, è prevista la **cancellazione in via definitiva** dal Sistema informativo dei dati PNR secondo le modalità previste nei relativi decreti ministeriali di regolamentazione del Sistema (comma 5).

Costituisce eccezione a tale regola l'ipotesi in cui le informazioni siano state trasferite a una delle autorità nazionali competenti e utilizzate in un caso specifico di prevenzione e repressione dei reati di terrorismo o dei reati gravi. Ove ciò accada, i dati seguono il regime di conservazione previsto nel codice di procedura penale, ovvero quello vigente per i trattamenti per finalità di polizia, ovvero ancora quello relativo ai trattamenti effettuati dagli organismi di *intelligence*.

La disposizione prevede inoltre che **i risultati del trattamento dei dati PNR** effettuato dall'UIP nazionale sono conservati per il tempo strettamente necessario a comunicare eventuali riscontri positivi alle competenti autorità nazionali ovvero alle Unità nazionali degli altri stati membri (comma 6).
Infine, ove riversati nel CED, i dati PNR e i dati API sono sottoposti alla specifica disciplina prevista per il medesimo CED (comma 7).

Articolo 11
(Conservazione dei dati API)

L'**articolo 11** prescrive **l'obbligo dei vettori aerei di cancellare i dati API** trasmessi al Sistema informativo **entro ventiquattro ore** dall'arrivo del volo, come già attualmente previsto dall'omologa previsione contenuta nell'art. 4, co. 3, del D.Lgs. n. 144 del 2007, di attuazione della direttiva API.

L'assenza di una analoga previsione in materia di dati PNR viene motivata nella relazione illustrativa, dal punto di vista formale, con l'assenza di una corrispondente prescrizione nella direttiva PNR e, dal punto di vista sostanziale, con la diversità delle due tipologie di dati. Infatti, mentre i dati API riguardano essenzialmente informazioni anagrafiche, che presentano scarsa utilità per i vettori una volta terminato il volo, i dati PNR comprendono altre informazioni che potrebbero interessare i vettori nell'ambito di eventuali contenzioni sorti nel corso dell'attività di impresa.

Articolo 12
(Trasferimento dei dati PNR alle autorità competenti nazionali)

Il **Capo III** disciplina il trasferimento e lo scambio dei dati contenuti nel codice di prenotazione (dati PNR) e dei risultati del loro trattamento a livello sia interno che internazionale.

La relazione governativa specifica che tale disciplina è introdotta in un'ottica di rafforzamento del meccanismo di condivisione delle informazioni e della cooperazione europea in materia di prevenzione e repressione dei fenomeni criminosi.

L'articolo 12 disciplina la procedura di comunicazione delle informazioni a livello interno, vale a dire la trasmissione dei dati PNR o dei risultati del loro trattamento da parte della UIP nazionale (Unità d'informazione sui passeggeri istituita presso il Ministero dell'interno *ex* art. 2, comma 2), lett. *o)*, e disciplinata dall'art. 6) alle competenti autorità nazionali, enumerate all'art. 2, comma 2, lett. *b)*.

Il **comma 1** specifica che i dati in questione, trasmessi dalla UIP nazionale alle competenti autorità nazionali, sono quelli ricevuti al fine di individuare i passeggeri sospettati di essere implicati in reati di terrorismo o in reati gravi, per i quali si rende necessario procedere a ulteriori verifiche (art. 6, comma 2, lett. *b)*).

La trasmissione di tali dati da parte della UIP nazionale alle competenti autorità nazionali fa seguito all'"esame non automatizzato" dei dati, condotto sul singolo caso dalla UIP nazionale qualora dal "trattamento automatizzato" siano emersi riscontri positivi (art. 8, comma 4).

Le autorità competenti nazionali sottopongono i dati ricevuti ad un "ulteriore trattamento" e adottano provvedimenti idonei a prevenire e reprimere reati di terrorismo o reati gravi.

Sempre per finalità di prevenzione e repressione dei reati di terrorismo, le autorità competenti nazionali hanno facoltà di attivarsi per ottenere dalla UIP nazionale la trasmissione dei dati PNR o dei risultati del loro trattamento.

La trasmissione dei dati PNR o dei risultati del loro trattamento da parte della UIP nazionale alle autorità competenti nazionali è effettuata con strumenti informatici, nel rispetto delle modalità stabilite con i decreti di cui all'articolo 4, comma 5, lettera *f)*.

La lettera f) *(e non la lettera* e)*) dell'art. 4, comma 5, prevede che con decreto ministeriale siano disciplinate le modalità tecniche di trasferimento delle informazioni, con strumenti informatici, dalla UIP nazionale alle autorità competenti nazionali.*

La lettera e)*, erroneamente richiamata nel testo, riguarda il raffronto informatico di dati ai fini della prevenzione dell'immigrazione irregolare.*

Il **comma 2** ribadisce che le decisioni delle autorità competenti nazionali che producono conseguenze giuridiche negative sull'interessato non possono essere adottate esclusivamente sulla base del trattamento automatizzato dei dati PNR.

Già il comma 1 - si ricorda - impone l'"esame non automatizzato" dei dati, condotto sul singolo caso dalla UIP nazionale prima della trasmissione alle autorità competenti nazionali.

Il comma 2 dispone, altresì, che le decisioni delle autorità competenti nazionali non possono essere fondate su ragioni discriminatorie così enumerate (in conformità all'art. 7, paragrafo 6, della direttiva n. 2016/681/UE): origine razziale o etnica, opinioni politiche, religione o convinzioni filosofiche, appartenenza sindacale, stato di salute, vita sessuale od orientamento sessuale dell'interessato.

Nella relazione governativa si osserva che non sembra richiedere un’espressa norma dì trasposizione nell'ordinamento interno la disposizione di cui all’articolo 7, paragrafo 5, della direttiva PNR, sulla base della quale l’ulteriore trattamento delle informazioni operato dalle autorità competenti "non pregiudica le competenze delle autorità di contrasto e giudiziarie nazionali qualora siano individuati altri reati o indizi di reato durante l'azione di contrasto determinata da tale trattamento".

Ciò "in virtù del generale principio del nostro sistema processuale per il quale, in assenza di espressi divieti, le informazioni possono essere utilizzate per le finalità, alle condizioni e con le modalità previste dalle pertinenti disposizioni in vigore".

Articolo 13
(Trasferimento dei dati PNR alle UIP degli Stati membri)

L'articolo 13 - in attuazione dell'art. 9, paragrafi 1, 2 e 4, della direttiva PNR - disciplina la trasmissione dei dati PNR o dei risultati del loro trattamento da parte della UIP nazionale (Unità d'informazione sui passeggeri istituita presso il Ministero dell'interno ex art. 2, comma 2), lett. o), e disciplinata dall'art. 6) alle UIP degli altri Stati membri (autorità competenti in materia di prevenzione e repressione dei reati di terrorismo e dei reati gravi individuate da ciascuno Stato membro, di cui all'art. 2, comma 2), lett. n)).

Il **comma 1** prevede che, in caso di riscontro positivo, la UIP nazionale trasmetta i dati PNR pertinenti e necessari o i risultati del loro trattamento alle UIP di altri Stati membri.

Anche se non espressamente indicato, in analogia a quanto previsto dall'art. 12, sembrerebbe che la trasmissione dei dati PNR o dei risultati del loro trattamento alle UIP di altri Stati membri debba seguire un "riscontro positivo" emerso da un esame individuale non automatizzato dei dati medesimi.

La relazione governativa fa, infatti, cenno ad un "riscontro positivo risultante dall'attività di analisi".

Il **comma 2** disciplina la trasmissione dei dati PNR (o di una loro parte) ovvero dei risultati del loro trattamento da parte della UIP nazionale sulla base di una richiesta della UIP di altro Stato membro.

La richiesta deve essere debitamente motivata in relazione a un caso specifico di prevenzione e repressione dei reati di terrorismo o dei reati gravi.

La UIP nazionale è tenuta a comunicare le informazioni richieste senza ritardo.

Il **comma 3** disciplina la specifica ipotesi di richiesta, da parte di UIP di altro Stato membro, di dati che siano stati resi anonimi mediante il mascheramento di specifici elementi idonei a identificare il soggetto cui si riferiscono.

La "trasformazione in forma anonima" scatta decorsi 6 mesi dal trasferimento dei dati trasmessi dai vettori aerei nel Sistema informativo istituito presso il Dipartimento della Pubblica Sicurezza (articolo 10, comma 2).

In tale caso la trasmissione da parte della UIP nazionale è soggetta alle seguenti condizioni:

- che essa risulti necessaria per corrispondere a una richiesta debitamente motivata pervenuta da autorità competenti di Stati membri (ex articolo 6, comma 2, lettera c));
- che essa sia preceduta da autorizzazione dell'Autorità giudiziaria (nel caso in cui la richiesta sia formulata nell'ambito di un procedimento penale o per

l’applicazione di una delle misure di prevenzione di cui all'art. 10, comma 3, lett. a)) ovvero dal Vice Capo della Polizia-Direttore Centrale della Polizia, per le finalità di prevenzione dei reati di terrorismo e dei reati gravi (art. 10, comma 3, lett. b)).

Il **comma 4** introduce una deroga ai tempi imposti ai vettori aerei per il trasferimento dei dati al Sistema informativo (*ex* art. 5, comma 4, i tempi sono tra 24 e 48 prima dell'orario previsto per la partenza del volo ovvero immediatamente dopo la chiusura del volo).

La deroga scatta nell'ipotesi di pericolo imminente e concreto che possa essere commesso un reato di terrorismo o altro reato grave.

In tale caso la UIP di uno Stato membro può chiedere alla UIP nazionale che i dati PNR siano trasmessi anche in un momento antecedente a quelli sopra indicati (art. 5, comma 4).

I vettori aerei, su richiesta della UIP nazionale, sono tenuti a trasmettere senza ritardo i dati PNR richiesti (art. 5, comma 5).

Articolo 14
(Trasferimento dei dati PNR alle autorità competenti degli Stati membri)

L’articolo 14 definisce i presupposti in presenza dei quali la UIP nazionale è legittimata a trasmettere le informazioni direttamente alle autorità competenti di altri Stati membri (art. 9, paragrafo 3, della direttiva PNR).

Come principio generale, infatti, le autorità competenti di altri Stati membri dialogano con la UIP nazionale attraverso la UIP del proprio Stato (cfr. il successivo art. 16).

Il **comma 1** dispone che la diretta trasmissione dei dati PNR dalla UIP nazionale alle autorità competenti di altri Stati membri che ne abbiano fatto richiesta possa essere effettuata:

- in presenza di situazioni di emergenza che non consentono di inoltrare la richiesta alla UIP nazionale mediante la UIP del proprio Stato;
- nel rispetto della disciplina sul trasferimento dei dati PNR richiesti da UIP degli Stati membri, recata dai commi 2 e 3 dell'art. 13.

Articolo 15
(Trasferimento dei dati PNR da parte di Stati membri)

L’articolo 15 disciplina le condizioni in presenza delle quali la UIP nazionale può presentare una richiesta di trasmissione di dati PNR (anche parziali) ovvero di risultati del loro trattamento alla UIP di altro Stato membro (art. 9, paragrafi 2 e 4, della direttiva PNR).

Il **comma 1** dispone che la richiesta di trasmissione di dati PNR da parte della UIP nazionale alla UIP di altro Stato membro sia debitamente motivata in relazione a uno specifico caso afferente la prevenzione e repressione di reati di terrorismo o reati gravi.

Una volta ricevute le informazioni richieste da parte della UIP di altro Stato membro, la UIP nazionale è tenuta a trasmetterle alle autorità competenti nazionali ai sensi dell'art. 12, comma 1.

Il **comma 2** (parallelamente a quanto previsto - a parti invertite - dall'art. 13, comma 4) introduce una deroga ai tempi imposti ai vettori aerei per il trasferimento dei dati al Sistema informativo (*ex* art. 5, comma 4, i tempi sono tra 24 e 48 prima dell'orario previsto per la partenza del volo ovvero immediatamente dopo la chiusura del volo).

La deroga scatta nell'ipotesi di pericolo imminente e concreto che possa essere commesso un reato di terrorismo o altro reato grave.

In tale caso la UIP nazionale può chiedere alla UIP di altro Stato membro che i dati PNR siano trasmessi anche in un momento antecedente a quelli sopra indicati (*ex* art. 5, comma 4).

I vettori aerei, su richiesta della UIP di altro Stato membro, sono tenuti a trasmettere senza ritardo i dati PNR richiesti (art. 5, comma 5).

Articolo 16
(Richiesta dei dati PNR da parte delle autorità competenti nazionali)

L’articolo 16 sancisce il principio generale secondo il quale le autorità competenti nazionali dialogano con le UIP di altri Stati membri attraverso la UIP nazionale.

Costituiscono, pertanto, eccezioni le ipotesi in cui le autorità competenti nazionali sono legittimate a rivolgersi direttamente ad una UIP di altro Stato membro (art. 9, paragrafo 3, della direttiva PNR).

Il **comma 1** dispone che le autorità competenti nazionali inoltrano le richieste di dati PNR alle UIP degli altri Stati membri tramite la UIP nazionale.

Il **comma 2** introduce una deroga al principio generale di cui al comma 1 per le situazioni di emergenza che non consentono di inoltrare la richiesta attraverso la UIP nazionale.

In tale caso (parallelamente a quanto previsto dall'art. 14 per le autorità competenti di altri Stati membri) le autorità competenti nazionali possono richiedere direttamente alla UIP di altro Stato membro la trasmissione dei dati PNR, nel rispetto della procedura generale di richiesta tra UIP di cui all'art. 13, comma 2.

L'autorità competente nazionale è tenuta ad inoltrare tempestivamente copia della richiesta alla UIP nazionale.

Articolo 17
(Modalità dì scambio delle informazioni)

L’articolo 17 - in attuazione dell'art. 9, paragrafo 5, della direttiva PNR - disciplina le modalità operative per il trasferimento dei dati PNR o dei risultati del loro trattamento da UIP nazionale a UIP di altro Stato membro (art. 13) e viceversa (art. 15), da UIP nazionale all'autorità competente di altro Stato membro (art. 14), da UIP di altro Stato membro alla competente autorità nazionale (art. 16).

Il **comma 1** prevede che lo scambio dei dati sopra indicati possa avvenire tramite qualsiasi canale esistente di cooperazione internazionale di polizia.

Per la richiesta e per lo scambio di informazioni viene utilizzata la lingua applicabile al canale prescelto.

Il **comma 2** attribuisce alla UIP nazionale il ruolo di punto di contatto italiano nei casi di emergenza.

Articolo 18
(Trasferimento dei dati PNR a Europol)

L'articolo 18 definisce i presupposti e le modalità per la trasmissione dei dati PNR o dei risultati del loro trattamento a Europol (art. 10 della direttiva n. 2016/681/UE).

Per quanto riguarda i presupposti della richiesta, il **comma 1** prevede che Europol possa chiedere la trasmissione di dati PNR quando essi siano "strettamente necessari" per sostenere e rafforzare l'azione degli Stati membri tesa alla prevenzione e repressione di un reato di terrorismo o di altro reato grave, purché si tratti di un reato rientrante nella competenza di Europol ai sensi del regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio dell'11 maggio 2016.

Prevede inoltre che Europol eserciti la propria facoltà di richiesta entro i limiti delle proprie competenze e per l'adempimento dei propri compiti.

Per quanto concerne le modalità di richiesta, il **comma 2** dispone che essa:

- sia formulata con sistemi informatici attraverso l'applicazione SIENA (Secure Information Exchange Network Application);
- sia presentata per il tramite dell'Unità nazionale Europol;
- rechi le motivazioni per le quali Europol ritiene necessaria la trasmissione dei dati richiesti nell'ambito dei presupposti di cui al comma 1.

Sulla base del **comma 3**, l'applicazione SIENA costituisce il mezzo attraverso il quale la UIP trasmette a Europol i dati PNR e condiziona la lingua utilizzata per la richiesta e lo scambio di informazioni.

Con regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio dell'11 maggio 2016 è stata istituita l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) al fine di sostenere la cooperazione tra autorità di contrasto nell'Unione.

L'Agenzia è succeduta all'ufficio Europol, istituito con decisione 2009/371/GAI (la decisione è ancora citata nell'art. 10 della direttiva 2016/681/UE, la cui adozione precede di poco quella del regolamento Europol).

Tra i compiti dell'Agenzia (art. 4 del regolamento) quelli di: coordinare, organizzare e svolgere indagini e azioni operative al fine di sostenere e rafforzare le azioni delle autorità competenti degli Stati membri; fornire sostegno alle attività di scambio di informazioni, operazioni e indagini transfrontaliere degli Stati membri, nonché alle squadre investigative comuni.

L'Unità nazionale Europol - per il tramite della quale deve essere presentata la richiesta di trasmissione di dati PNR - è istituita in ciascun Stato membro quale organo di collegamento tra Europol e le autorità competenti dello Stato membro (art. 7).

Il considerando n. 24 del regolamento ha previsto che Europol mettesse a disposizione l'applicazione di rete per lo scambio sicuro di informazioni (*Secure*

Information Exchange Network Application-SIENA), una rete protetta per lo scambio di dati tesa a facilitare lo scambio d'informazioni tra Stati membri, Europol, altri organismi dell'Unione, Paesi terzi e organizzazioni internazionali.

Il potenziamento delle strutture informatiche di Europol risponde ai diversi obiettivi di individuare rapidamente i collegamenti tra le indagini e i modi operandi comuni dei diversi gruppi criminali, di controllare i dati incrociati e ottenere un quadro chiaro delle tendenze, e, nel contempo, di garantire un livello elevato di protezione dei dati personali delle persone.

Articolo 19
(Trasferimento dei dati PNR a Paesi terzi)

L’articolo 19 - in conformità a quanto disposto dall'art. 11 della direttiva n. 2016/681/UE - stabilisce i presupposti per la trasmissione dei dati PNR o dei risultati del loro trattamento, in relazione a casi individuali, a Paesi terzi.

Il **comma 1** definisce, innanzitutto, il quadro normativo entro cui si inscrive la trasmissione di dati PNR, in relazione a casi individuali, alle autorità competenti di un Paese terzo:

- sono fatte salve le condizioni previste da eventuali accordi internazionali;
- la trasmissione deve conformarsi esclusivamente alle previsioni del provvedimento in esame;
- si applicano le disposizioni del codice per la protezione dei dati personali (decreto legislativo n. 196 del 2003) riguardanti il trasferimento verso Paesi terzi di dati giudiziari ovvero di dati trattati per finalità di polizia.

I principi applicabili al trattamento di dati giudiziari sono contenuti negli art. 21 e 22 del codice per la protezione dei dati personali.

Inoltre, i titoli I e II della Parte II del codice recano, rispettivamente, disposizioni per il trattamento in ambito giudiziario e per il trattamento da parte di forze di polizia.

La trasmissione alle autorità competenti di un Paese terzo è ammissibile in presenza delle seguenti condizioni:

- la richiesta deve essere formulata nel rispetto della procedura generale di richiesta tra UIP (art. 13, commi 2 e 3);
- il trasferimento delle informazioni deve risultare necessario per le finalità di prevenzione e di repressione dei reati di terrorismo e dei reati gravi (art. 3, comma 1);
- il Paese terzo deve impegnarsi a trattare i dati con le garanzie previste dal provvedimento in esame ed eventualmente a trasferire ulteriormente i dati ad altro Paese terzo soltanto per le finalità sopra indicate (prevenzione e repressione dei reati di terrorismo e dei reati gravi) e previa autorizzazione espressa dello Stato italiano.

Il **comma 2** pone le condizioni alle quali i dati PNR possono essere ulteriormente trasferiti senza il previo consenso dello Stato da cui provengono:

- il trasferimento deve risultare indispensabile per rispondere a una minaccia specifica e reale connessa a reati di terrorismo o a reati gravi in uno Stato membro o in un Paese terzo;

- il consenso preliminare dello Stato da cui i dati provengono non può essere ottenuto in tempo utile.

Il **comma 3** - con riferimento all'ipotesi disciplinata al comma 2 - specifica che, qualora uno Stato proceda ad ulteriore trasferimento dei dati PNR senza il preventivo consenso dello Stato dal quale li ha ottenuti, deve darne comunicazione alla UIP di quest'ultimo Stato.

Il trasferimento è annotato in apposito registro per le verifiche da parte del responsabile della protezione dei dati (figura disciplinata dal successivo art. 21).

Articolo 20
(Autorità nazionale di controllo)

Il Capo IV dello schema reca "Disposizioni in materia di dati personali".

È composto dagli articoli 20 (autorità nazionale di controllo), 21 (responsabile per la protezione dei dati), 22 (protezione dei dati personali) e 23 (diritti degli interessati).

L'articolo 20 individua l'**Autorità nazionale di controllo** - istituto che la direttiva (cfr. il suo articolo 15) prevede svolga consulenza e sorveglianza sull'applicazione della direttiva nello Stato membro, insieme assicurando la tutela dei diritti fondamentali in relazione al trattamento dei dati personali.

Siffatta Autorità è individuata nel **Garante per la protezione dei dati personali**.

Le funzioni che il Garante è chiamato ad esercitare sono previste svolgersi secondo le modalità previste dal Codice in materia di protezione dei dati personali (decreto legislativo n. 196 del 2013).

Pertanto i compiti previsti dalla direttiva per l'Autorità nazionale di controllo sono espletati entro l'assetto ordinamentale delle funzioni del Garante, senza che si rendano necessarie modificazioni a fini attuativi.

Nel Codice sono disciplinati i poteri di cui il Garante sia titolare (anche con riguardo ai trattamenti di dati per finalità dì polizia o giudiziari: materia quest'ultima che interseca altra direttiva dell'Unione europea, la n. 680 del 2016, relativa appunto alla **protezione delle persone fisiche** con riguardo al **trattamento dei dati personali** da parte delle autorità competenti a fini di prevenzione, **indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali)**.

È però introdotta la previsione che il Garante esprima - su richiesta dell'interessato, pareri in merito all'esercizio dei diritti di protezione dei dati personali, in relazione alle disposizioni del decreto legislativo recato dallo schema in esame.

Tale previsione è volta a recepire l'articolo 15, par. 4 della direttiva, secondo cui ciascuna autorità nazionale dì controllo, su richiesta, consiglia l'interessato in merito all'esercizio dei diritti derivanti dalle disposizioni adottate conformemente alla medesima direttiva.

Articolo 21
(Responsabile per la protezione dei dati)

L’articolo 21 introduce la figura del responsabile della protezione dei dati PNR oggetto della presente disciplina.

Siffatto responsabile è individuato **entro la Direzione Centrale della Polizia Criminale** del Dipartimento della pubblica sicurezza del Ministero dell’Interno.

La sua designazione è demandata ad un decreto del Capo della Polizia - Direttore Generale della Pubblica Sicurezza.

Il responsabile per la protezione dei dati è figura distinta dal titolare e dai responsabili del trattamento (su cui v. *supra*, l'articolo 4, commi 1 e 2 dello schema; sulla figura del *data protectìon officer* cfr. altra direttiva dell'Unione europea, la n. 679 del 679).

Al responsabile per la protezione dei dati compete la vigilanza sulla correttezza e sulla liceità del trattamento delle informazioni. Inoltre garantisce l’attuazione di tutte le misure tecniche e di sicurezza, nel rispetto di quanto disposto dal Codice per la protezione dei dati personali. Ancora, funge da punto di contatto unico per gli interessati, per tutte le questioni connesse al trattamento dei dati che li riguardino.

La collocazione del responsabile è ritenuta ottemperare ad uno svolgimento delle funzioni "indipendente", secondo il dettato della direttiva (suo articolo 5, par. 2). Si tratta dunque di una posizione di 'alterità' rispetto alla struttura organizzativa dell'Unità d'informazione sui passeggeri (UIP), la quale è l'autorità in materia di previsione e repressione dei reati di terrorismo e dei reati gravi (oggetto dell'articolo 6 dello schema).

In base a tale configurazione del responsabile, si viene a prevedere che esso possa fare segnalazione al Garante per la protezione dei dati personali - qualora il medesimo responsabile, accedendo ai dati trattati dall'UIP, ravvisi un trattamento dei dati effettuato in modo non lecito.

L'attuazione delle disposizioni di questo articolo soggiacciono alla generale clausola di invarianza finanziaria (prevista dall'articolo 27 dello schema). Pertanto l'attuazione dev'essere assicurata con le risorse umane e strumentali disponibili a legislazione vigente.

Articolo 22
(Protezione dei dati personali)

L’articolo 22 sancisce l'**applicabilità** ai trattamenti dei dati personali effettuati ai sensi del presente schema, degli strumenti di tutela previsti dal **Codice per la protezione dei dati personali**.

Si fa qui espressamente richiamo ad alcune disposizioni del Codice.
Sono:

- la Parte II, Titolo II ("Trattamenti da parte di forze di polizia");
- il Titolo III ("Difesa e sicurezza dello Stato"), limitatamente ai trattamenti effettuati dagli organismi dì cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124 - ossia, rispettivamente, il Dipartimento delle informazioni per la sicurezza (DIS), l'Agenzia informazioni e sicurezza esterna (AISE), l'Agenzia informazioni *e* sicurezza interna (AISI);
- gli articoli da 33 a 36 (i quali compongono - del Titolo V, "Sicurezza dei dati e dei sistemi" - il Capo II, Misure minime di sicurezza").

Le disposizioni del Codice si applicano anche per il trattamento di dati personali da parte dei vettori aerei (talché, ad esempio, i vettori aerei devono adempiere all'obbligo di informativa circa i dati personali raccolti previsto dall'articolo 13 del Codice, e sono tenuti a adottare tutte le misure tecniche ed organizzative a tutela della sicurezza e della riservatezza dei dati).

Questa applicabilità ai vettori aerei vale per l'obbligo di informare adeguatamente i passeggeri come anche per l'adozione di adeguate misure tecniche e organizzative a tutela della sicurezza e della riservatezza dei dati personali.

Sono inoltre posti alcuni **obblighi** specifici in capo all'Unità d'informazione sui passeggeri **(UIP)**.

Primo fra questi è la rimozione immediata dei dati PNR trattati in modo che rivelino l'origine razziale o etnica, le opinioni politiche, la religione o le convinzioni filosofiche, l'appartenenza sindacale, lo stato di salute, la vita o l'orientamento sessuale dell'interessato.

Tale previsione risponde all'articolo 15, par. 4 della direttiva.

L'UIP inoltre è chiamata ad adottare misure e procedure tecniche e organizzative adeguate per garantire un livello elevato di sicurezza in relazione ai rischi connessi al trattamento dei dati PNR (anche da parte dei vettori aerei).

L’UIP conserva la documentazione relativa ai sistemi e alle procedure di trattamento. La predetta documentazione riporta l’indicazione dei dati prescritti dall'articolo 15, par. 5 della direttiva.

Ancora, l’UIP conserva i registri delle attività di raccolta, consultazione, comunicazione e cancellazione dei dati. La conservazione è per un periodo di cinque anni - come prescritto dall'articolo 15, par. 6 della direttiva. I registri (che

devono riportare l’indicazione delia finalità, della data e dell'ora dell'operazione e gli elementi relativi all'identità della persona che ha consultato o comunicato ì dati PNR, nonché dei destinatari di tali dati) sono usati esclusivamente a fini di verifica, di autocontrollo, per garantire l'integrità e la sicurezza dei dati o di *audit*.

La documentazione e i registri, a seguito di richiesta, devono essere messi a disposizione del Garante - al quale inoltre sono segnalati i casi di violazione di dati personali (in tali casi, la comunicazione è anche all'interessato, qualora la violazione rischi di arrecare un rilevante pregiudizio ai suoi dati personali o alla sua riservatezza).

Articolo 23
(Diritti degli interessati)

L’articolo 23 riconosce ai soggetti interessati dai trattamenti disciplinati dal presente schema i diritti previsti dall’articolo 10, commi 3, 4 e 5 della legge n. 121 del 1981 (la quale reca: "Nuovo ordinamento dell'Amministrazione della pubblica sicurezza").

Prevede che i diritti siano esercitati previa presentazione di **istanza alla Direzione centrale della polizia criminale** (tramite questa istanza, l’interessato può altresì domandare che ne sia tali diritti venga data apposita evidenza nel Sistema informativo: tale indicazione rimane poi rimuovibile, a richiesta dell’interessato o per effetto di un provvedimento adottato dal Garante ai sensi del Codice per la protezione dei dati personali).

Della presentazione dell'istanza devono essere informati il responsabile della protezione dei dati e l’UIP nazionale (nonché l’UIP dello Stato membro eventualmente interessato).

La Direzione centrale della polizia criminale comunica all'interessato i provvedimenti adottati a seguito delle richieste formulate nell'istanza.

Le disposizioni della legge n. 121 del 1981 sopra richiamate concernono i dati personali raccolti presso l'Amministrazione della pubblica sicurezza.

In particolare, la persona alla quale si riferiscono i dati può chiedere alla Direzione centrale della polizia criminale la conferma dell'esistenza di dati personali che lo riguardino, la loro comunicazione in forma intellegibile e, se i dati risultino trattati in violazione di vigenti disposizioni di legge o di regolamento, la loro cancellazione o trasformazione in forma anonima.

Esperiti i necessari accertamenti, l'ufficio comunica al richiedente, non oltre trenta giorni dalla richiesta, le determinazioni adottate.

L'ufficio può omettere di provvedere sulla richiesta se ne possa conseguire pregiudizio ad azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione della criminalità, dandone informazione al Garante per la protezione dei dati personali.

Chiunque venga a conoscenza dell'esistenza di dati personali che lo riguardano, trattati anche in forma non automatizzata in violazione di disposizioni di legge o di regolamento, può chiedere al tribunale (del luogo ove risiede il titolare del trattamento) di compiere gli accertamenti necessari e di ordinare la rettifica, l'integrazione, la cancellazione o la trasformazione in forma anonima dei dati medesimi.

Secondo il dato riportato dalla relazione tecnica, le istanze presentate ai sensi dell'articolo 10 della legge n. 121 del 1981 vigente sono annualmente circa 6.100. L'aggiungersi di istanze per dati PNR oggetto della disciplina dello schema dovrebbe essere numericamente contenuto, tale da non importare significativo aggravio di carichi di lavoro o incrementi di spesa.

Articolo 24
(Sanzioni)

L'**articolo 24** reca le sanzioni, oggetto dell'articolo 14 della direttiva in recepimento.

Il **comma 1** prevede, infatti, la **sanzione amministrativa pecuniaria da 10.000 a 100.000 euro** nei confronti dei vettori aerei che non trasmettono i dati o li trasmettono con modalità differenti da quelle previste dall'articolo 5 dello schema di decreto in esame o li trasmette in maniera incompleta o errata.

La medesima sanzione è irrogata in caso di mancato rispetto dei termini fissati dall'Unità d'informazione nazionale sui passeggeri (UIP) nazionale - ai fini dello scambio dei PNR con le UIP istituite presso gli altri Stati membri e con Europol - disciplinata dall'articolo 6 dello schema di decreto.

Il **comma 2** individua nell'ENAC l'autorità competente ad irrogare le sanzioni. Trova applicazione il procedimento previsto dalla legge n. 689 del 1981 (recante "Modifiche al sistema penale") il quale disciplina le fasi dell'accertamento, notificazione e contestazione delle sanzioni.

Il comma in esame prevede esplicitamente che l'ENAC sia destinataria del rapporto contenente la prova delle eseguite contestazioni o notificazioni, come previsto dall'articolo 17 della citata legge n. 689.

In caso di reiterazione delle violazioni (**comma 3**), l'ENAC può disporre la sospensione (da uno a dodici mesi) oppure la revoca della licenza, autorizzazione o concessione, relative all'attività svolta o al mezzo di trasporto utilizzato, rilasciate dalle autorità italiane.

A tale proposito si rammenta che l'articolo 8-*bis* della legge n. 689 del 1981 stabilisce - in via generale e salvo diverse disposizioni specifiche - che la reiterazione si verifica "quando, nei cinque anni successivi alla commissione di una violazione amministrativa, accertata con provvedimento esecutivo, lo stesso soggetto commette un'altra violazione della stessa indole". Inoltre, si ha reiterazione "quando più violazioni della stessa indole commesse nel quinquennio sono accertate con unico provvedimento esecutivo".

Il **comma 4** stabilisce la **sanzione amministrativa pecuniaria da 5.000 a 50.000 euro** per la mancata cancellazione dei dati API prevista dall'articolo 11 dello schema di decreto (V. sopra). In tali casi l'autorità competente ad irrogare la sanzione è il Garante per la protezione dei dati personali.

Ai sensi del **comma 5**, resta fermo quanto previsto dall'articolo 12, comma 6, del Testo unico immigrazione (di cui al decreto legislativo n. 286 del 1998): esso pone in capo al vettore (aereo, marittimo o terrestre) l'obbligo di accertare che lo straniero trasportato sia in possesso dei documenti richiesti per l'ingresso nel territorio dello Stato e a a riferire all'organo di polizia di frontiera i casi di irregolarità dei passeggeri stranieri a bordo. In caso di mancato assolvimento di tali obblighi, In caso di inosservanza anche di uno solo degli obblighi di cui al

presente comma, si applica la sanzione amministrativa da 3.500 a 5.500 euro per ciascuno degli stranieri trasportati; nei casi più gravi si può disporre la sospensione (da uno a dodici mesi) ovvero la revoca della licenza, autorizzazione o concessione. Anche in questi casi trova applicazione la disciplina dettata dalla sopra menzionata legge n. 689 del 1991.

Articolo 25
(Statistiche)

L’articolo 25 pone in capo al Ministero dell'interno alcuni obblighi di comunicazione di dati concernenti i PNR trasmessi alla UIP nazionale (materia di cui tratta l'articolo 20 della direttiva in recepimento).

In particolare devono essere trasmessi i dati (non contenenti informazioni personali) relativi: al numero totale di passeggeri i cui dati PNR sono stati raccolti e scambiati; il numero dei passeggeri per i quali si sia reso necessario procedere ad ulteriori verifiche in quanto sospettati di essere implicati in reati di terrorismo o in altri reati gravi (secondo la procedura prevista dall'articolo 6, comma 2, lettera *b*), dello schema di decreto in esame).

Articolo 26
(Disposizioni transitorie e finali)

Il **comma 1** prevede che continuino ad applicarsi le disposizioni di cui al decreto legislativo n. 144 del 2007 (recante "Attuazione della direttiva 2004/82/CE concernente l'obbligo per i vettori aerei di comunicare i dati relativi alle persone trasportate"), fino all'emanazione dei **provvedimenti di attuazione** previsti dal presente schema di decreto, agli articoli:

- 4, commi 5 e 6, rispettivamente sulle norme tecniche di funzionamento del Sistema Informativo e sulla trasmissione dei dati dall"UIP nazionale alle omologhe unità degli Stati membri;
- 6, comma 1, sull'organizzazione della UIP nazionale;
- 10, comma 5, sulle modalità cancellazione dei dati PNR allo scadere del periodo di 5 anni.

Dalla data di entrata in vigore dell'ultimo dei provvedimenti di attuazione delle norme qui sopra ricordate, il decreto legislativo n. 144 del 2007 è abrogato.

Ai sensi del **comma 2**, i riferimenti al sistema frontaliero BCS, ovunque ricorrano, devono intendersi riferiti al Sistema Informativo di cui all'articolo 4 dello schema di decreto in esame.

Può ricordarsi come il decreto del Ministro dell'interno 16 dicembre 2010, in attuazione dell'articolo 7 del citato decreto legislativo n. 144 del 2007, individui le modalità tecniche ed operative per la trasmissione da parte dei vettori aerei delle informazioni relative alle persone trasportate mediante il Sistema informativo frontaliero denominato *Border Control System* (BCS) Italia, presso il Dipartimento della pubblica sicurezza del Ministero dell'interno.

Articolo 27
(Clausola di neutralità finanziaria)

L’articolo 27 reca la clausola di neutralità finanziaria.

A tale proposito si rammenta che l'articolo 1, comma 608, della legge di bilancio 2017 (legge n. 232 del 2016) aveva stanziato risorse per l'attuazione della direttiva PNR pari a 5,5 milioni di euro per l'anno 2017, 16 milioni per l'anno 2018, 4,5 milioni a decorrere dal 2019.

Tali risorse sono allocate sui seguenti capitoli nello stato di previsione del Ministero dell'interno:

- 7505 ("Spese per la realizzazione della piattaforma informatica per l'uso dei dati del codice di prenotazione (PNR)" - parte capitale)
- 2563 ("Spese per la gestione e manutenzione della piattaforma informatica per l'uso dei dati del codice di prenotazione (PNR)" - parte corrente)

Nel bilancio di previsione 2018 e triennale per il 2018-2020 (legge n. 205 del 2017), il cap. 7505 reca uno stanziamento di 16 milioni per il 2018; il cap. 2563 reca uno stanziamento pari a 4,5 milioni a decorrere dal 2019.

Inoltre, la relazione tecnica posta a corredo del presente schema segnala che la Commissione europea ha reso disponibili ulteriori 5,98 milioni sul Fondo Sicurezza Interno-Programma Nazionale d'Italia, per il 50% di quota europea, ai fini dell'attuazione della direttiva PNR.

Documenti all’esame delle istituzioni dell’UE

Procedure di contenzioso

Con un parere emesso a richiesta del Parlamento europeo, il 26 luglio 2017, la Corte di giustizia dell'Unione europea ha, tra l'altro, dichiarato non conforme ai diritti fondamentali al **rispetto della vita privata** e alla **protezione dei dati** di carattere personale un **accordo** sul **trattamento dei dati del codice di prenotazione** (accordo PNR), sottoscritto nel 2014 da **Unione europea** e **Canada**.

L'accordo consentiva il **trasferimento sistematico e continuo** dei **dati PNR** di tutti i passeggeri aerei a un'**autorità canadese** ai fini del loro uso e della loro conservazione, nonché del loro **eventuale trasferimento** ulteriore ad **altre autorità e ad altri paesi terzi**, allo scopo di lottare contro il terrorismo e i reati gravi di natura transnazionale. A tal fine, l'accordo previsto contemplava, tra l'altro, una **durata di archiviazione dei dati di cinque anni** nonché obblighi in materia di sicurezza ed integrità dei dati PNR, un mascheramento immediato dei dati sensibili, taluni diritti d'accesso ai dati, di rettifica e di cancellazione e la possibilità di proporre **ricorsi amministrativi o giurisdizionali**.

Pur rilevando che l'ingerenza nei citati diritti fondamentali sarebbe giustificata dal perseguimento di una **finalità d'interesse generale** (garanzia della **sicurezza pubblica** nell'ambito della lotta contro reati di **terrorismo** e reati gravi di natura transnazionale) e che il trasferimento dei dati PNR verso il Canada e il trattamento ulteriore degli stessi sarebbe idoneo a garantire la realizzazione di tale finalità, la Corte ha, tuttavia, ritenuto che varie disposizioni dell'accordo volte a consentire tali attività non siano limitate allo **stretto necessario** e non prevedano norme chiare e precise, costituendo in definita una **violazione dei diritti fondamentali citati**. Di qui la conclusione della Corte che **l'accordo previsto non possa essere concluso nella sua forma attuale**.

La Commissione europea, nell'ottobre 2017, ha conseguentemente iniziato una **nuova procedura** per ottenere l'autorizzazione all'avvio di negoziati per la conclusione di un accordo tra l'Unione europea e il Canada sul trasferimento e sull'uso dei dati del codice di prenotazione *(Passenger Name Record, PNR*) al fine di prevenire e combattere il terrorismo e altri reati gravi di natura transnazionale, che tenga conto dei rilievi contenuti nel parere citato della Corte.

In sede di dibattito a livello istituzionale e accademico europeo, è stata prospettata da taluni l’eventualità che alcuni dei rilievi sollevati dalla Corte di giustizia dell’UE in merito all’accordo UE-Canada sui dati del PNR potrebbero riguardare, in linea teorica, anche taluni profili la **direttiva PNR (2016/681)**.

In particolare, nell’accordo con il Canada e in relazione alla conservazione dei dati, la Corte di Giustizia ha contestato la **mancata differenziazione tra passeggeri in arrivo ed in uscita dal Paese**, affermando che « tale accordo non garantisce che la conservazione e l’uso dei dati PNR dopo la partenza dei passeggeri aerei dal Canada da parte delle autorità canadesi siano limitati allo stretto necessario» (§ 211). La Corte ha specificato (§ 208) che «Per quanto riguarda l’uso dei dati PNR così archiviati, esso dovrebbe […] essere fondato su **criteri oggettivi** per definire **le circostanze e le condizioni** alle quali le autorità canadesi contemplate dall’accordo previsto possano **avere accesso a tali dati** ai fini del loro uso. Del pari, tale uso dovrebbe essere subordinato, salvo casi di urgenza debitamente giustificati, ad un controllo preventivo effettuato o da un giudice, o da un ente amministrativo indipendente la cui decisione che autorizzi l’uso intervenga a seguito di una richiesta motivata di tali autorità presentata, in particolare, nell’ambito di procedure di prevenzione, di accertamento o di esercizio dell’azione penale».