MARINE AVIATION & TRANSPORT INSURANCE REVIEW

LA DISCIPLINA NAZIONALE SUI DATI PNR NEL TRASPORTO AEREO

Doriano Ricciutelli
Istruttore certificato dell´ENAC

Il 21 maggio 2018 è stato emanato il decreto legislativo n. 53 che attua la direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR), finalizzato a prevenire, accertare, procedere alle indagini e all'azione penale nei confronti dei reati di terrorismo e dei gravi crimini e, quindi, in sintesi a proteggere con maggiore efficacia la vita e l'incolumità delle persone.

Si tratta nella sostanza delle informazioni relative al viaggio aereo di ciascun passeggero gestite dalle compagnie aeree per fini commerciali (si veda per approfondimenti MAT n. 3/2015, pag. 23) e nel caso in cui con una singola prenotazione vengano acquistati più biglietti - fattispecie non contemplata dalla direttiva comunitaria di riferimento - il PNR deve contenere informazioni relative a tutti i soggetti cui la prenotazione si riferisce.

In via preliminare, va detto che il decreto disciplina il trasferimento, a cura dei vettori aerei (*metodo push*), dei dati dei voli extra-UE e dei voli intra-UE (questi ultimi introdotti grazie all'opzione dell'art. 2 della citata direttiva europea inglobata nell'art. 12 della legge 25 ottobre 2017, n. 163 di delegazione europea 2016/2017), nonché le modalità di trattamento degli anzidetti dati e le relative operazioni di raccolta, uso conservazione e scambio con gli Stati membri.

È bene rimarcare che il trasferimento dei dati deve rispondere alle indicazioni fornite dall'art. 1 della decisione di esecuzione (UE) 2017/759 della Commissione, del 28 aprile 2017, sui protocolli

comuni e i formati che i vettori aerei devono utilizzare, uniformando tale attività secondo gli orientamenti sul PNR dell'ICAO, organizzazione che ha peraltro sollecitato gli Stati contraenti a implementarne gli standard anche in occasione dell'ultima (39^) Assemblea (WP/2013 EX/75 del 10/8/2016).

In aggiunta - come elemento significativamente rilevante - va considerato che nell'ambito di applicazione del nuovo strumento normativo - in una logica di razionalizzazione delle risorse disponibili protesa ad evitare sterili frammentazioni e onerose duplicazioni - rientra anche il trattamento dei dati API (Advanced Passenger Information), riservato agli uffici di frontiera nazionali attraverso l'impiego del Border Control System (BCS), trasmessi dalle compagnie aeree e relativi ai passeggeri in ingresso nel territorio italiano sulla scorta della direttiva 82/2004 (UE) e (sinora) del decreto attuativo n.144/2007 che difatti viene abrogato da questo atto legislativo n. 53.

In proposito, giova sottolineare che il trattamento dei dati API è rivolto verso differenti finalità rispetto al trattamento concernente il PNR e, segnatamente, quelle connesse al miglioramento dei controlli proprio delle frontiere aeree esterne ed interne dell'UE e della prevenzione dell'immigrazione illegale presso gli aeroporti italiani.

Infatti, vale la pena di rammentare che, in caso di ripristino dei controlli di frontiera previsto dal regolamento (UE) 2016/399 (Codice Schengen) ai confini interni, il *processing* dei dati API si estende con tutta evidenza anche ai voli interni intra-unionali.

Procedendo sul solco delle novità salienti sotto il profilo organizzativo-strutturale, il decreto istituisce un "Sistema Informativo" presso il Dipartimento della Pubblica Sicurezza opportunamente strutturato per occuparsi, in parallelo, di entrambi i suesposti trattamenti dati, rispettivamente, attraverso l'opera della Direzione Centrale della Polizia Criminale per quanto riguarda il PNR e della Direzione Centrale dell'Immigrazione e della Polizia delle Frontiere per l'API, garantendone le rispettive, necessarie gestioni tecniche e informatiche, sulla base delle disposizioni di un emanando decreto del Ministro dell'Interno.

Muovendo ora sul terreno delle modalità d'intervento, si prevede che i vettori forniscano elettronicamente al succitato Sistema Informativo del Dipartimento i dati sui voli extra UE e intra-UE originanti, in arrivo o facenti scalo in Italia, raccolti nel corso dello svolgimento di routine delle attività di compagnia.

In ogni caso risulta assolutamente determinante la focalizzazione dei momenti in cui si esplica la trasmissione dati: chiariamo che la norma indica puntualmente il "periodo compreso tra le ventiquattro e le quarantotto ore antecedenti l'orario previsto per la partenza" e "immediatamente dopo la chiusura del volo quando non è più possibile l'imbarco o lo sbarco dei passeggeri".

Non sfugge qui la circostanza che, nei casi contingenti causati dal pericolo imminente e concreto della commissione di reati di terrorismo e di altri gravi crimini fondato su una attenta valutazione della potenziale minaccia, venga confacentemente contemplato l'obbligo di trasferimento dei dati anche in anticipo rispetto ai predetti, circostanziati termini temporali.

Alla stregua di queste premesse, il legislatore ha inteso poi assegnare ad un ufficio del Ministero dell'Interno, i.e. un'articolazione inquadrata nell'anzidetta Direzione Centrale della Polizia Criminale e con l'intervento - come soggetto legittimato - del personale delle forze di Polizia (cui sia stata preventivamente rilasciata la necessaria credenziale di autenticazione), l'istituzione dell'UIP (Unità Informazione Passeggeri), ovverosia un unico organismo in grado di garantire trasparenza e, nel contempo, di ridurre i costi a carico dei vettori.

Nel novero delle funzioni svolte dall'UIP rileva, *inter alia,* la ricezione dei dati PNR, anche avvalendosi di un operatore economico qualificato e, a seguire, prima dell'arrivo o della partenza del volo, l'attività di analisi dei dati pervenuti indirizzata alla individuazione dei passeggeri (che non sono necessariamente già noti alle autorità) sospettati di essere implicati nei menzionati reati per i quali occorre procedere a ulteriori verifiche da parte degli organi competenti, incluso l'Europol.

Nel mentre l'UIP, sulla base di richieste motivate e limitatamente a singoli casi, è chiamata a comunicare alle autorità nazionali o dei paesi europei o alla Europol, i dati PNR o i riscontri ottenuti a seguito della prefata, relativa analisi.

Nel quadro delle relazioni interne dell'Unione Europea si introduce un virtuoso e proficuo circuito collaborativo realizzabile tramite scambi informativi tra le UIP nazionali degli Stati membri dei dati correlati o necessari alle indagini o il risultato del loro trattamento, che può riguardare sia situazioni di ordinaria prassi investigativa, sia fattispecie emergenziali, ove sia presente il rischio della perpetrazione di atti terroristici o criminali - come detto - di seria natura.

Merita una riflessione separata l'ipotesi del trasferimento dei dati PNR a paesi terzi che, fatte salve circostanze peculiari introdotte da specifici accordi internazionali, è consentito esclusivamente se conforme anche alle norme del decreto legislativo di attuazione della direttiva (UE) 2016/680, tesa ad assicurare il rispetto del presente decreto, e previa autorizzazione dello Stato italiano, eccetto il caso in cui sia indispensabile per rispondere ad una aggressione specifica in uno Stato membro o uno Stato terzo.

Soffermandoci agli aspetti che caratterizzano le modalità applicative del trattamento dei dati, osserviamo una serie di interventi che l'UIP deve effettuare nel corso del suindicato processo di analisi.

Intanto, gioca un ruolo rilevante il confronto del PNR con le informazioni contenute nel CED e nelle altre banche dati nazionali, europee (SIS) ed internazionali (Interpol), accompagnato da un trattamento dei dati improntato a criteri predeterminati, periodicamente aggiornati e confortati dal parere delle autorità competenti nazionali (forze di polizia, DIA, Direzione Nazionale Antimafia e Antiterrorismo e le Autorità giudiziarie che perseguono, *ratione materiae*, i reati summenzionati) e nell'osservanza del principio di proporzionalità e di non discriminazione.

Su questi aspetti ci preme mettere nel necessario rilievo la considerazione che il sistema PNR davvero rappresenti innanzitutto un formidabile volano per lo sviluppo delle prossime attività pertinenti alla polizia giudiziaria in quanto capace di schiudere una fonte inesauribile e sempre aggiornata di opportunità per una ricerca inve -

stigativa incisivamente mirata a combattere le più gravi forme di fenomenologia criminale.

Ciò detto, è utile precisare che a seguito di riscontri positivi di un singolo caso, derivanti da un trattamento automatizzato, questi vengono sottoposti dall'UIP a un esame (stavolta) non automatizzato, al fine di appurare l'effettiva e concreta esigenza di adottare ulteriori "provvedimenti e misure" da parte delle predette autorità nazionali che non debbono, comunque, pregiudicare il diritto di ingresso nel territorio dello Stato delle persone che beneficiano della libera circolazione all'interno dell'UE.

Si soggiunga che, secondo le puntuali indicazione della direttiva 2016/681, i dati PNR sono conservati per un periodo di cinque anni dal momento dalla trasmissione da parte dei vettori e, dopo sei mesi dal relativo trasferimento, gli stessi vengono "pseudonimizzati" mediante mascheramento di una serie di elementi, tra cui i nominativi personali, il numero dei passeggeri, gli indirizzi e le informazioni idonee ai possibili contatti con le persone, le modalità di pagamento, i dati dei frequent flyer e ogni altra indicazione idonea a consentire l'identificazione della persona.

Nel contesto generale della salvaguardia dell'intero impianto normativo, è istituita quale autorità nazionale di controllo il "Garante per la protezione dei dati personali", chiamato ad esercitare le proprie funzioni conformemente alle modalità contemplate dal relativo Codice (d. lgs. n 196/2003) e con compiti consultivi, potendo esprimere pareri su richiesta delle persone interessate.

Sul piano della protezione dei dati emerge la figura del "responsabile" ad hoc (profilo che trova fondamento giuridico ex art. 24 del Regolamento 2016/679) nominato dal Capo della Polizia - Direttore Generale della Pubblica Sicurezza e individuato all'interno della su richiamata Direzione Centrale della Polizia Criminale, il quale ha il precipuo compito di vigilare sulla corretta gestione del sistema PNR, attuando le misure tecniche e di sicurezza e informando il Garante sulle anomalie riscontrate, relative a eventuali illeciti sul trattamento dei dati.

Spiccano ancora ulteriori, specifiche norme riguardanti giustappunto il trattamento dei dati esercitato dai vettori ed esclusivamente

improntato al rispetto del citato Codice anche per ciò che concerne l'obbligo di informazione verso i passeggeri e l'adozione di ogni opportuna procedura organizzativa a presidio della riservatezza personale, in ispecie tenendo presente che è fatto divieto di rivelare 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 degli interessati.

Vero quel che precede, ci accorgiamo che in seno alla struttura UIP sono affidati i compiti di conservazione, raccolta, consultazione, comunicazione e cancellazione dei dati, nonché di sicurezza onde evitare la distruzione o la perdita delle informazioni registrate e di accesso non autorizzato o di trattamento non consentito o non conforme agli scopi previsti dal decreto.

Particolare attenzione è altresì dedicata alla tutela dell'utenza del trasporto aereo atteso il formale riconoscimento dei diritti di cui all'art. 10, commi 3 e 4 e 5 della legge 121 del 1981, che attiene alla utilizzazione nei processi giudiziari e amministrativi delle informazioni conservate negli archivi del CED (Centro elaborazione dati del Ministero dell'Interno), in relazione ai trattamenti dei dati personali in applicazione del decreto in parola.

Del resto, a ben vedere, dinanzi al mancato rispetto delle regole del sistema PNR sono comminate severe sanzioni amministrative - di competenza dell'ENAC - da 5 mila fino a 100 mila euro per ogni viaggio a cui si riferisce la condotta irregolare - ove i fatti illeciti peraltro non costituiscano reato, come clausola di riserva - nei confronti dei vettori che omettono di trasmettere i dati ovvero li trasmettono in modo difforme da quanto previsto dalla novella o in maniera incompleta o errata.

Ebbene, se tali comportamenti risultassero reiterati secondo i dettami della legge 689/81 art. 8 bis, detto ente potrebbe disporre la sospensione da uno a dodici mesi ovvero la revoca della licenza, dell'autorizzazione o della concessione rilasciate dall'autorità nazionale inerenti alla attività professionale oggetto di permesso e al mezzo di trasporto utilizzato.

Riportando il discorso nell'alveo dell' Advanced Passenger

Information, annotiamo che il vettore aereo è obbligato a cancellare, entro ventiquattrore dall'arrivo del volo, i dati API trasmessi all'autorità nazionale e la violazione di siffatto obbligo, ferma restando l'applicazione dell'art. 12 comma 6 del t.u. 286/1998 (disposizioni contro le immigrazioni clandestine), comporterebbe l'applicazione da parte del Garante per la protezione dei dati personali della sanzione amministrativa pecuniaria da 5 mila a 50 mila euro (vale a dire la stessa del d. lgs. N.144/2007).

Rimaniamo, infine, convintamente certi di poter riconoscere al sistema PNR un autentico valore aggiunto in favore di ciascuno Stato membro, sia, per un verso, in termini di potenziamento circa l'abilità di risposta repressiva da parte dell'*intelligence* - che, invero, ben integrando gli strumenti già esistenti per il contrasto dei reati transfrontalieri sarà in grado di discernere meglio il panorama delle minacce esterne - e sia, per altro verso, quale mezzo di prevenzione delle azioni delittuose contro gli obiettivi maggiormente sensibili come, *in primis*, aeroporti e aviazione civile in generale.