Processo penale e giustizia n. 1 | 2019

Dibattiti tra norme e prassi

Debates: Law and Praxis

PAOLO TROISI

Ricercatore di Procedura penale – Università degli Studi di Roma "Tor Vergata"

Passenger Name Records, privacy e accertamento penale
Passenger Name Records, privacy *and criminal proceedings*

L'utilizzo, al fine di prevenire e reprimere i reati, dei dati del codice di prenotazione dei passeggeri dei vettori aerei se, da un lato, può rivelarsi valido strumento per fronteggiare il terrorismo ed altre gravi forme di criminalità, dall'altro, dà vita ad un sistema di sorveglianza di massa fondato sulla raccolta indiscriminata e l'analisi sistematica di informazioni personali a prescindere dall'esistenza di elementi indicativi di un qualsiasi nesso con azioni criminose. Nonostante le cautele apprestate, al riguardo, dalla direttiva (UE) 2016/681 e dal d.lgs. 21 maggio 2018, n. 53, resta aperto il dibattito sulla proporzionalità di una misura fortemente invasiva per la vita privata ed idonea ad incidere, negativamente, sulle libertà fondamentali e sulla presunzione di innocenza.

The use of passenger name record data is a valid instrument to prevent, detect, investigate and prosecute terrorist offences and serious crime. Nonetheless it creates a mass surveillance system by the indiscriminate collection and sistematic analysis of personal informations without there being reasons based on individual circumstances that would permit the inference that the persons concerned may be involved in a crime. The debate on the proportionality of a measure strongly invasive for private life and suitable to affect the fundamental freedoms and the presumption of innocence remains open, despite the cautions set by Directive (EU) 2016/681 and by Legislative Decree 21 May 2018, n. 53.

IL CONTESTO DI RIFERIMENTO

Il progetto di un sistema europeo di utilizzo, al fine di prevenire e perseguire reati, dei dati del codice di prenotazione dei passeggeri dei vettori aerei (c.d. PNR, acronimo di *Passenger Name Record*) si è sviluppato in concomitanza con il potenziamento che, a partire dai primi anni duemila, ha interessato, all'interno dell'Unione, lo scambio di informazioni utili per il contrasto alla criminalità transfrontaliera.

È con il Programma dell'Aia (formulato dal Consiglio europeo di Bruxelles del 4 e 5 novembre 2004) che la cooperazione informativa – da intendersi come «la raccolta, l'archiviazione, il trattamento, l'analisi e lo scambio delle pertinenti informazioni» (art. 87, par. 2, lett. *a*, TFUE)[1] – ha subito una svolta decisiva, attraverso l'elaborazione del c.d. *principio di disponibilità*, destinato ad aprire nuove frontiere in un ambito fino ad allora regolato dall'opposto principio del dominio esclusivo, da parte delle autorità statali, sui dati acquisiti nel corso o in funzione delle investigazioni penali.

Nella prospettiva delineata dal principio di disponibilità, le barriere costituite dai confini nazionali non devono più rappresentare un ostacolo. Questo significa – secondo la definizione contenuta nel Pro-

[1] Sul tema v., tra gli altri, F. Boehm, *Information sharing and data protection in the area of freedom, security and justice. Towards harmonized data protection principles for information exchange at EU-level*, Berlino, Heidelberg, 2012; S. Braum-V. Covolo, *From Proven Fragmentation to Guaranteed Data Protection within the Virtual Criminal Law Enforcement Area: a report on Personal Data Protection within the Framework of Police and Judicial Cooperation in Criminal Matters*, in K. Ligeti (a cura di), *Toward a Prosecutor for the European Union*, vol. 1, *A Comparative Analysis*, Oxford, Hart Publishing, 2013, p. 1011 ss.; G. Di Paolo, *La circolazione dei dati personali nello spazio giudiziario europeo dopo Prüm*, in T. Rafaraci (a cura di), *La cooperazione di polizia e giudiziaria in materia penale nell'Unione europea dopo il Trattato di Lisbona*, Milano, Giuffrè, 2011, p. 198 ss.; C. Fanuele, *Lo scambio di informazioni a livello europeo*, in L. Filippi-P. Gualtieri-P. Moscarini-A. Scalfati (a cura di), *La circolazione investigativa nello spazio giuridico europeo: strumenti, soggetti, risultati*, Padova, Cedam, 2010, p. 19 ss.; F. Peroni-M. Gialuz (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, Eut, 2009. Sia consentito anche il rinvio a P. Troisi, *Il potenziamento della cooperazione transfrontaliera. Lo scambio di informazioni*, in L. Kalb (a cura di), *«Spazio europeo di giustizia» e procedimento penale italiano*, Torino, Giappichelli, 2012, p. 195 ss., e Id., *La circolazione di informazioni per le investigazioni penali nello spazio giuridico europeo*, Padova, Cedam, 2012.

gramma dell'Aia [2] – che, in tutta l'Unione, «un ufficiale di un servizio di contrasto di uno Stato membro che ha bisogno di informazioni nell'esercizio delle sue funzioni sia in condizione di ottenerle da un altro Stato membro» e che «il servizio di contrasto nell'altro Stato membro che dispone di tali informazioni sia tenuto a trasmettergliele per i fini dichiarati».

Il salto di qualità è notevole: le singole autorità di *law enforcement* devono essere poste nelle condizioni di individuare il Paese che dispone di informazioni utili e di potervi accedere. Di conseguenza, ciascuno Stato è tenuto a conservare ed a mettere a disposizione dei *partner* europei i dati raccolti per prevenire, individuare ed indagare su reati commessi da soggetti che si muovono liberamente nel territorio dell'Unione [3].

Plurime sono le direttrici lungo le quali si è evoluta la cooperazione informativa.

La previsione di forme innovative di trasferimento di peculiari categorie di dati (genetici, dattiloscopici, automobilistici o relativi ad eventi di rilievo a dimensione transfrontaliera) ha costituito il nucleo centrale del Trattato di Prüm [4], successivamente inglobato nel quadro giuridico dell'Unione attraverso la decisione 2008/615/GAI (c.d. decisione di Prüm) [5].

All'attuazione del principio di disponibilità, sia pure con un approccio meno ambizioso, si è provveduto anche con la decisione quadro 2006/960/GAI, relativa alla «semplificazione dello scambio di informazioni ed *intelligence* tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge», avente l'obiettivo di promuovere un'ampia condivisione di dati riguardanti, in particolare, i reati connessi alla criminalità organizzata ed al terrorismo [6].

Ulteriori iniziative hanno, poi, contribuito ad implementare la cooperazione di polizia e giudiziaria, sia attraverso lo sviluppo dei circuiti di scambio tra gli Stati [7], sia perfezionando i canali di trasmissione facenti capo ad archivi centralizzati a livello europeo [8].

---

[2] Al «principio di disponibilità» è dedicato il punto 2.1 – intitolato «Miglioramento dello scambio di informazioni» – della parte III del Programma dell'Aia.

[3] In argomento, v. S. Ciampi, *Principio di disponibilità e protezione dei dati personali nel "terzo pilastro" dell'Unione europea*, in F. Peroni-M. Gialuz (a cura di), *Cooperazione informativa*, cit., p. 42.

[4] È stato sottoscritto il 27 maggio 2005 da Belgio, Germania, Spagna, Francia, Lussemburgo, Paesi Bassi e Austria ed è entrato in vigore il 1° novembre 2006. Nel nostro ordinamento è stato recepito con la l. 30 giugno 2009, n. 85.

[5] Sul tema v., tra gli altri, E. Calvanese, *Adesione al trattato di Prüm e cooperazione transfrontaliera per il contrasto alla criminalità*, in A. Scarcella (a cura di), *Prelievo del DNA e banca dati nazionale*, Padova, Cedam, 2009, p. 11 ss.; A. Marandola, Information sharing *nella prospettiva del Trattato di Prüm e della decisione di recepimento nel quadro giuridico dell'Unione*, in F. Peroni-M. Gialuz (a cura di), *Cooperazione informativa* cit., p. 164 ss.

[6] La decisione quadro (c.d. decisione «svedese», in quanto adottata su proposta della Svezia) dà vita ad un sistema generale di scambio di informazioni ai fini di *law enforcement*, destinato ad intensificare i rapporti di collaborazione tra le forze di polizia operanti in ambito europeo, in vista di una cooperazione che sfrutti appieno il bagaglio cognitivo acquisito nel corso di operazioni di *intelligence* o di attività investigative. A fronte della circolazione di una maggiore tipologia di dati, la forma di scambio prescelta – l'accesso indiretto su richiesta – è il frutto, però, di un approccio poco ambizioso sul fronte dell'attuazione del principio di disponibilità (cfr. M. Gialuz, *La tutela della* privacy *nell'ambito del trattamento domestico dei dati genetici e della cooperazione informativa*, in L. Marafioti-L. Luparia (a cura di), *Banca dati del DNA e accertamento penale*, Milano, Giuffrè, 2010, p. 183). È stata recepita in Italia con il d.lgs. 23 aprile 2015, n. 54.

[7] Si pensi alle iniziative volte alla realizzazione di canali di scambio delle informazioni estratte dai casellari giudiziari, attraverso la decisione quadro 2009/315/GAI (recepita con il d.lgs. 12 maggio 2016, n. 74) e la decisione 2009/316/GAI (recepita con il d.lgs. 12 maggio 2016, n. 75). Si pensi, ancora, ai plurimi strumenti adottati per la circolazione di informazioni sulla criminalità organizzata e terroristica (tra i quali, le decisioni 2005/671/GAI e 2007/845/GAI). Rilevante, sia pure senza prevedere alcun canale privilegiato di trasmissione transfrontaliera, è, altresì, la c.d. direttiva sulla *data retention*, riguardante «la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazioni» (direttiva 2006/24/CE, attuata con il d.lgs. 30 maggio 2008, n. 109, che ha modificato l'art. 132 del d.lgs. 30 giugno 2003, n. 196). Tale direttiva è stata, tuttavia, invalidata da C. giust. UE, Grande sez., 8 aprile 2014, Digital Rights Ireland e Seitlinger e altri, in *Giur. cost.*, 2014, p. 2946, in quanto ritenuta non compatibile con gli artt. 7, 8 e 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea.

[8] Su questo fronte, la normativa europea si è mossa nella direzione di potenziare il sistema di banche date centrali europee a fini di *law enforcement*. In tale ottica si inscrive l'istituzione del *Sistema informativo Schengen* di seconda generazione (SIS II) (decisione 2007/533/GAI); la riforma del *Sistema informativo doganale* (SID) (decisione 2009/917/GAI); lo sviluppo degli archivi centralizzati di *Europol* ed *Eurojust* (regolamento UE 2016/794 e decisione 2009/426/GAI); il riconoscimento della facoltà di accesso al *Sistema di informazione visti* (VIS) anche a fini di prevenzione e repressione di reati di terrorismo e altri reati gravi (decisione 2008/633/GAI); la regolamentazione della possibilità da parte delle autorità nazionali e di *Europol* di richiedere il confronto di impronte digitali in loro possesso con quelle archiviate nell'unità centrale dell'*European dactylografic system* (EURODAC), a fini

L'esigenza di fronteggiare la crescente minaccia terroristica e di combattere il fenomeno dei c.d. *foreign fighters* [9] ha reso ancor più pressante, in linea con le indicazioni del Programma di Stoccolma [10] e le *strategic guidelines* di Ypres [11], la necessità di migliorare, intensificare e accelerare, anche con la creazione di nuovi strumenti, la circolazione di informazioni tra le autorità nazionali di contrasto, le agenzie dell'UE ed i Paesi terzi [12].

In questo clima è stata adottata la direttiva (UE) 2016/681 del 27 aprile 2016, sull'uso dei dati del codice di prenotazione dei passeggeri dei voli in arrivo o in partenza dal territorio degli Stati membri «a fini di prevenzione, accertamento, indagine e azione penale per reati di terrorismo e altri gravi reati».

È stato, in tal modo, introdotto, nell'ordinamento europeo, un meccanismo che consente l'archiviazione e l'analisi, per le attività di *intelligence* e le investigazioni penali, di dati personali raccolti, ad altri fini, da soggetti privati (le compagnie aeree).

Sullo sfondo si staglia l'intensificarsi, nel *post* 11 settembre, di un'esigenza di sicurezza che, dal territorio nordamericano, si è rapidamente propagata nel "vecchio" continente, nella comune percezione di dover combattere, sinergicamente, una *global war* [13]. In nome della difesa della collettività è progressivamente aumentata la propensione ad accettare limitazioni delle sfere di libertà, al punto da giustificare *counter-terrorism measures* che, se nel sistema statunitense si sono poste al di fuori del sistema penale ed hanno raggiunto livelli di aperta violazione di diritti umani (si pensi, in via meramente esemplificativa, agli omicidi mirati, alle *extraordinary renditions*, ai trattamenti detentivi degradanti) [14], non hanno tardato a fare ingresso, sia pure con intensità diversa, nella legislazione europea [15] ed in quella dei singoli Stati membri [16].

Il potenziamento della cooperazione informativa e la tensione verso l'apprestamento di strumenti di sorveglianza di massa [17], quale indubbiamente è il monitoraggio automatizzato, su scala globale, dei da-

---

di contrasto del terrorismo e di gravi reati (regolamento UE n. 603/2013); la creazione del *Sistema europeo di sorveglianza delle frontiere* (EUROSUR) (regolamento UE n. 1052/2013).

[9] Su tale fenomeno v., per tutti, C. Cipolletti, *La privazione della cittadinanza nel contrasto ai* foreign terrorist *e il diritto internazionale*, in *Riv. dir. internaz.*, 2016, p. 117 ss.

[10] Documento del Consiglio n. 5731/10 del 3 marzo 2010 relativo alle azioni da intraprendere nel quinquennio 2010-2014.

[11] Si tratta del documento del Consiglio europeo n. 79/14 del 27 giugno 2014, contenente le conclusioni del Consiglio di Ypres, che hanno provveduto a delineare i nuovi orientamenti strategici destinati a guidare l'azione dell'Unione durante il quinquennio 2015-2020.

[12] In tal senso si esprime la Risoluzione del Parlamento europeo dell'11 febbraio 2015 «sulle misure antiterrorismo» [2015/2530 (RSP)], punto n. 22.

[13] Sull'idea di *global war*, con riferimento alla lotta al terrore, v., per i diversi approcci, L. Bonanate, *Guernica. 11 settembre (di un qualsiasi anno)*, in A. D'Orsi (a cura di), *Guerre globali. Capire i conflitti del XXI secolo*, Roma, Carocci, 2003, p. 19 ss.; G. De Vergottini, *Guerra e costituzione. Nuovi conflitti e sfide alla democrazia*, Bologna, Il Mulino, 2004, p. 204 ss.; A. Vedaschi, À La guerre comme à la guerre? *La disciplina della guerra nel diritto costituzionale comparato*, Torino, Giappichelli, 2007, p. 75 ss.

[14] Su questi temi, per un'ampia panoramica, cfr., per tutti, T. Groppi, *Democrazia e terrorismo. Diritti fondamentali e sicurezza dopo l'11 settembre*, Napoli, Editoriale Scientifica, 2006, e, più di recente, K. Roach (a cura di), *Comparative Counter-Terrorism Law*, Cambridge University Press, 2015.

[15] Di recente, in materia antiterrorismo, sono state adottate la direttiva 2015/849/UE «relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo» (che ha abrogato la direttiva 2005/60/CE ed è stata, di recente, modificata dalla direttiva 2018/843/UE) e la direttiva 2017/541/UE «sulla lotta contro il terrorismo» (che ha sostituito la decisione quadro 2002/475/GAI). Al riguardo, v. F. Manfredini, *Con la direttiva 2017/541/UE le istituzioni europee rafforzano la lotta contro il terrorismo internazionale*, in *Cass. pen.*, 2017, p. 3384 ss.

[16] Molteplici sono state nel nostro ordinamento le leggi adottate, dopo gli attentati americani del 2001, sulla scia dell'emergenza terroristica (si pensi ai decreti legge 18 ottobre 2001, n. 378; 27 luglio 2005, n. 144; 18 febbraio 2015, n. 7; ed alla l. 28 luglio 2016, n. 153). In dottrina, sui vari interventi succedutisi nel tempo, v., tra gli altri, A.A. Dalia (a cura di), *Le nuove norme di contrasto al terrorismo*, Milano, Giuffrè, 2006; R.E. Kostoris-R. Orlandi (a cura di), *Contrasto al terrorismo interno ed internazionale*, Torino, Giappichelli, 2007; R.E. Kostoris-F. Viganò (a cura di), *Il nuovo "pacchetto" antiterrorismo*, Torino, Giappichelli, 2016; A.P. Viola, *Le nuove misure investigative, processuali e ordinamentali per il contrasto al terrorismo*, in G.M. Baccari-K. La Regina-E.M. Mancuso, *Il nuovo volto della giustizia penale*, Milano, Cedam, 2015, p. 123 ss.

[17] Sul tema della «sorveglianza di massa» cfr., *ex multis*, D. Cole-F. Fabbrini-S. Schulhofer (a cura di), *Surveillance, Privacy and Trans-Atlantic Relations*, Oxford, Hart Publishing, 2017; D. Lyons, *Massima sicurezza. Sorveglianza e «guerra al terrorismo»*, Milano, Cortina, 2004; A. Manna, *Erosione delle garanzie individuali in nome dell'efficienza dell'azione di contrasto al terrorismo: la privacy*, in *Riv. it. dir. proc. pen.*, 2004, p. 1022 ss.; F. Rossi Dal Pozzo, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal* Safe Harbour *al* Privacy Shield*)*, in *Riv. dir. internaz.*, 2016, p. 690 ss.; M. Simoncini,

ti forniti dai passeggeri all'atto della prenotazione di un volo, sono, nient'altro, che la reazione all'accresciuto senso di insicurezza.

Ad essere mutato, in realtà, è proprio il paradigma dei rapporti tra sicurezza e libertà [18]: la «sicurezza pubblica», da fonte di possibili di compressioni, in via eccezionale, delle libertà individuali, sembra essere divenuta, essa stessa, diritto fondamentale, destinato tendenzialmente a prevalere, in un giudizio di bilanciamento, sui valori concorrenti [19].

Di qui, i tentativi di arginare il processo e ristabilire le gerarchie [20], nel contesto di un dibattito tutt'altro che sopito.

L'EVOLUZIONE DEL DIBATTITO

Tortuoso è stato l'*iter* che ha condotto all'approvazione della direttiva (UE) 2016/681. La ricerca di un approccio comune è stata accompagnata da un'accesa discussione sulla necessità e proporzionalità, rispetto alle finalità perseguite, dell'istituzione di un sistema PNR europeo.

La riflessione trae origine dalla circostanza che i dati del codice di prenotazione sono informazioni (comprendenti nome, recapiti, data del viaggio, itinerario, dati sull'emissione del biglietto, agente di viaggio, modalità di pagamento, posto assegnato, tipologia di bagaglio, *etc.*) raccolte e conservate dalle compagnie aeree per meri scopi operativi e commerciali, idonee a rivelare abitudini, relazioni sociali, condizioni finanziarie, preferenze dei passeggeri [21].

La loro archiviazione ed analisi per finalità di *law enforcement* se, da un lato, può rivelarsi valido strumento per fronteggiare il terrorismo ed altre forme di criminalità, dall'altro, realizza una schedatura ed un controllo sistematico di dati personali non motivato né dalla previa commissione di reati, né

Legislazione antiterrorismo e tutela della privacy, in *Riv. trim. dir. pubbl.*, 2007, p. 959 ss.; A. Sperti, *Il Terrorist Surveillance Programme e le sue delicate implicazioni sul piano costituzionale*, in *Quaderni cost.*, 2009, p. 102 ss.; M. Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*, Oxford, Hart Publishing, 2017; A. Vedaschi, *I programmi di sorveglianza di massa nello Stato di diritto. La "*data retention*" al test di legittimità*, in *Dir. pubbl. comp. eur.*, 2014, p. 1224 ss.; M. Vermeulen-R. Bellanova, *European "smart" surveillance: What's at stake for data protection, privacy and non-discrimination?*, in *Security and Human Rights*, 2013, 4, p. 297 ss.

[18] Di «nuovo paradigma del rapporto tra libertà e sicurezza» come risposta all'emergenza del terrorismo internazionale dopo gli attentati dell'11 settembre 2001, discorre P. Ridola, *Libertà e diritti nello sviluppo storico del costituzionalismo*, in R. Nania-P. Ridola (a cura di), *I diritti costituzionali*, vol. I, Torino, Giappichelli, 2006, p. 148.

[19] Il tema è stato approfondito dalla dottrina costituzionalistica. Sulla configurabilità di un diritto alla sicurezza pubblica come diritto individuale v., sia pure con diversi accenti, G. Cerrina Feroni-G. Morbidelli, *La sicurezza: un valore superprimario*, in *Percorsi cost.*, 2008, 1, p. 33 ss.; T.E. Frosini-C. Bassu, *La libertà personale nell'emergenza costituzionale*, in A. Di Giovine (a cura di), *Democrazie protette e protezione della democrazia*, Torino, Giappichelli, 2005, p. 77 ss.; C. Mosca, *La sicurezza come diritto di libertà. Teoria generale delle politiche della sicurezza*, Padova, Cedam, 2012, p. 73 ss.; S. Raimondi, *Per l'affermazione della sicurezza pubblica come diritto*, in *Dir. amm.*, p. 2006, 747 ss.; P. Torretta, *"Diritto alla sicurezza" e altri diritti e libertà della persona: un complesso bilanciamento costituzionale*, in A. D'Aloia (a cura di), *Diritti e Costituzione. Profili evolutivi e dimensioni inedite*, Milano, Giuffrè, 2003, p. 454 ss. In senso critico verso questo approccio, cfr. A. Pace, *La funzione di sicurezza nella legalità costituzionale*, in *Quaderni cost.*, 2014, p. 989, il quale, pur ritenendo indiscutibile che, dopo gli avvenimenti dell'11 settembre 2011, la percezione della sicurezza pubblica sia profondamente cambiata, rimarca come «ciò non legittima la tesi che il diffuso bisogno di sicurezza costituisca ormai il contenuto di un vero e proprio diritto dei cittadini». Nello stesso senso, Id., *Libertà e sicurezza. Cinquant'anni dopo*, in *Diritto e società*, 2013, p. 177 ss.

[20] Degna di nota, in questa direzione, è stata, come si dirà nel prosieguo, la più recente giurisprudenza della Corte di giustizia dell'Unione, che ha assunto un ruolo «ancora una volta determinante nel ricalibrare il delicato equilibrio del binomio libertà-sicurezza» (così A. Vedaschi, *L'accordo internazionale sui dati dei passeggeri aviotrasportati (PNR) alla luce delle indicazioni della Corte di giustizia dell'Unione europea*, in *Giur. cost.*, 2017, p. 1918).

[21] I dati PNR sono definiti dalla direttiva (UE) 2016/681 (art. 3, n. 5) come «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 e di prenotazione interessati per ogni volo prenotato da qualunque persona o per suo conto, siano esse registrate in sistemi di prenotazione, in sistemi di controllo delle partenze utilizzato per la registrazione dei passeggeri sui voli, o in altri sistemi equivalenti con le stesse funzionalità». Comprendono, in particolare, diciannove categorie di informazioni, specificamente individuate dall'allegato I alla direttiva. La Grande sezione della Corte di Giustizia UE, nel parere n. 1/15 del 26 luglio 2017, sull'accordo PNR tra il Canada e l'Unione europea (in *Dir. informaz. e informatica*, 2017, p. 856 ss.), ha espressamente riconosciuto che «se taluni dati PNR, considerati isolatamente, non sembrano poter rivelare informazioni importanti sulla vita privata degli interessati, tuttavia, considerati complessivamente, detti dati possono, tra l'altro, rivelare un itinerario di viaggio completo, abitudini di viaggio, relazioni esistenti tra due o più persone nonché informazioni sulla situazione finanziaria dei passeggeri aerei, sulle loro abitudini alimentari o sul loro stato di salute» (punto n. 128).

dall'emergere di indizi o anche solo sospetti in tal senso [22]. Significativa è l'invasione nella vita privata dei cittadini e inevitabili i riflessi sulle libertà individuali e sulla presunzione di innocenza.

La prassi di adoperare i dati PNR per la lotta al crimine risulta, in realtà, adottata da molti Stati, pur in assenza di normative *ad hoc*, fin dagli anni '50 del secolo scorso [23]. Il dibattito sul tema si è, però, aperto a seguito degli attacchi terroristici dell'11 settembre. Gli Stati Uniti, anche alla luce delle modalità con le quali erano stati portati a termine gli attentati, hanno, per la prima volta, messo a punto un programma volto ad imporre ai vettori di comunicare alle competenti autorità nazionali i dati dei passeggeri risultanti dal codice di prenotazione [24]. Analogamente ha fatto il Canada [25] e, in progresso di tempo, ulteriori Paesi *extra* UE [26].

Tali iniziative hanno, indirettamente, coinvolto l'Unione, dato che la disciplina generale sulla *data protection* già allora vietava il trasferimento di dati personali a Paesi terzi senza che fosse assicurato un livello di protezione valutato «adeguato» dalla Commissione (art. 25 direttiva 95/46/CE). Le compagnie aeree, in caso di voli internazionali in partenza o in arrivo nel territorio dell'Unione, si trovavano, dunque, nell'impossibilità di adempiere all'obbligo di trasmissione senza, nel contempo, violare la normativa europea. Di qui, la necessità di stipulare accordi che consentissero ai vettori di rispondere alle richieste di comunicazione ed assicurassero, contestualmente, una protezione dei dati equivalente a quella garantita dalla legislazione UE.

I primi accordi con gli Stati Uniti risalgono al 2004 ed al 2007 [27]. Analoghe intese sono state raggiunte con il Canada nel 2006 [28] e l'Australia nel 2008 [29]. Dando seguito alle direttive del Piano d'azione per l'attuazione del Programma di Stoccolma, la Commissione, nel 2010, ha predisposto una comunicazione sul trasferimento dei dati PNR verso Paesi terzi [30], volta a fissare i criteri generali per i futuri negoziati. Si è, così, provveduto a rivisitare, sulla base di un'unica serie di principi, i termini delle intese con Stati Uniti [31] e Australia [32]. È stato, nella medesima cornice, siglato un nuovo accordo con il Canada, ritenuto, però, dalla Corte di giustizia, non compatibile con il diritto alla protezione dei dati e, perciò, non ancora approvato dal Parlamento europeo [33]. Colloqui sono stati, inoltre, avviati con altri Paesi [34].

---

[22] Sul tema sia consentito il rinvio a P. Troisi, *La circolazione di informazioni*, cit., p. 119 ss.

[23] Cfr. F. Rossi Dal Pozzo, *Protezione dei dati personali e diritti fondamentali della persona: le nuove norme sui «codici di prenotazione» (PNR)*, in *Riv. dir. internaz. priv. e proc.*, 2016, p. 1022 ss.

[24] Si tratta dello *US Aviation and Transportation Security Act* del 19 novembre 2001. Sulla genesi di tale normativa v., anche per ulteriori indicazioni bibliografiche, G.A. Cannetti, *I* Personal Name Records *tra istanze di sicurezza globale e tutela dei dati personali*, in *I quaderni europei. Scienze giuridiche*, n. 63, *Diritto alla* privacy *e trattamento automatizzato dei dati fra diritto civile, diritto penale e diritto internazionale ed europeo*, 2014, p. 86 ss.

[25] *Custom Act* 2001 e *Immigration and Refugee Act* 2001.

[26] Si tratta, ad esempio, di Australia, Argentina, Brasile, Danimarca, Messico, Giappone, Federazione Russa, Emirati Arabi Uniti, Arabia Saudita, Sud Corea.

[27] Il primo accordo con gli Stati Uniti è del maggio 2004 ed è stato approvato con la decisione del Consiglio 2004/496/CE, preceduta dalla decisione della Commissione 2004/535/CE «relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei» trasferiti agli Stati Uniti. Tali decisioni sono state, però, annullate dalla Corte di giustizia, con sentenza del 30 maggio 2006, nelle cause riunite C-317/04 e C-318/04 (in *G.U.U.E.*, C 178 del 29 luglio 2006), perché fondate su una base giuridica ritenuta non corretta. Un nuovo accordo per il trasferimento dei dati PNR al Dipartimento per la sicurezza interna degli Stati Uniti è stato concluso nel luglio 2007 (in *G.U.U.E.*, L 204 del 4 agosto 2007).

[28] In *G.U.U.E.*, L 82 del 21 marzo 2006.

[29] In *G.U.U.E.*, L 213 dell'8 agosto 2008.

[30] Si tratta del documento COM(2010) 492 del 21 settembre 2010, su cui ha espresso, in data 19 ottobre 2010, un *Parere* tendenzialmente critico il Garante europeo della protezione dei dati (in *G.U.U.E.*, C 357 del 30 dicembre 2010).

[31] L'accordo, firmato il 14 dicembre 2011, è stato approvato con decisione del Consiglio del 26 aprile 2012 (in *G.U.U.E.*, L 215 dell'11 agosto 2012). Osservazioni critiche sono state espresse dal Garante europeo con *Parere* del 9 dicembre 2011 (in *G.U.U.E.*, C 35 del 9 febbraio 2012).

[32] L'accordo è stato concluso con decisione del Consiglio del 13 dicembre 2011 (in *G.U.U.E.*, L 186 del 14 luglio 2012). Cfr. il *Parere* del Garante europeo della protezione dei dati del 15 luglio 2011 (in *G.U.U.E.*, C 322 del 5 novembre 2011).

[33] Il 18 luglio 2013 la Commissione adottava una proposta di decisione del Consiglio relativa alla conclusione dell'accordo tra il Canada e l'Unione europea sul trasferimento e sul trattamento dei dati PNR [COM(2013) 528], nonché una proposta di decisione del Consiglio relativa alla firma dell'accordo [COM(2013) 529]. Il 30 settembre 2013 il Garante europeo della protezione

La legalizzazione, attraverso i citati accordi, di una *policy* originata altrove [35], le linee guida adottate, in materia, dall'Organizzazione internazionale dell'aviazione civile (ICAO) [36], il progressivo incremento di iniziative di singoli Stati membri volte a sviluppare sistemi PNR nazionali [37], hanno reso indifferibile una politica comune europea, che contemperasse istanze di sicurezza e tutela dei diritti.

Le resistenze politiche, generate, senza dubbio, da una maggiore sensibilità, in area europea, per la tutela della *privacy*, hanno, tuttavia, reso lungo e accidentato il percorso.

Già all'esito delle trattative per il primo accordo con gli Stati Uniti, la Commissione, con una comunicazione del 2003, aveva auspicato un «approccio globale» dell'Unione sull'uso dei dati PNR [38]. La prima proposta di decisione quadro, presentata nel 2007 [39], veniva, però, abbandonata in seguito al trattato di Lisbona, essendo divenuta obsoleta in conseguenza del venir meno della struttura a «pilastri».

All'invito, contenuto nel Programma di Stoccolma, ad istituire un meccanismo di scambio dei dati del codice di prenotazione, faceva seguito una nuova proposta, questa volta di direttiva [40], che teneva conto delle raccomandazioni formulate dal Parlamento europeo e dei pareri del Garante della protezione dei dati, del Gruppo di lavoro «Articolo 29» e dell'Agenzia per i diritti fondamentali [41]. Le reazioni critiche, tuttavia, non si facevano attendere [42] ed inducevano la Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo (LIBE) a respingere (il 29 aprile 2013) il progetto di direttiva. Ad ulteriormente complicare il processo, sopraggiungeva l'annullamento, da parte della Corte

dei dati esprimeva *Parere* critico su tali proposte (in *G.U.U.E.*, C 51 del 2014). Il 5 dicembre 2013 il Consiglio adottava la decisione relativa alla firma dell'accordo. Lo stesso giorno decideva di chiedere l'approvazione del Parlamento che, con risoluzione del 25 novembre 2014, presentava richiesta di parere alla Corte di giustizia circa la compatibilità con i trattati. La Grande sezione della Corte di giustizia si è espressa negativamente su tale compatibilità con il già citato parere n. 1/15 del 26 luglio 2017. Al riguardo in dottrina v., tra gli altri, E. Carpanelli-N. Lazzerini, *PNR: Passenger Name Record, Problems Not Resolved? The EU PNR Conundrum After Opinion 1/15 of the CJEU*, in *Air and Space Law*, 2017, p. 377 ss.; C. Graziani, *PNR EU-Canada, la Corte di Giustizia blocca l'accordo: tra difesa dei diritti umani e implicazioni istituzionali*, in *DPCE Online*, 2017, p. 959 ss.; A. Vedaschi, *The European Court of Justice on the EU-Canada Passenger Name Record Agreement*, in *European Constitutional Law Review*, 2018, p. 410 ss.; Ead., *L'accordo internazionale*, cit., p. 1913 ss.

[34] Sul tema degli accordi PNR tra Unione e Stati terzi v., anche per ulteriori indicazioni bibliografiche, M. Botta-M. De Azevedo, *La protezione dei dati personali nelle relazioni USA-UE*, in *Dir. informaz. e informatica*, 2010, p. 315 ss.; C. Di Stasio, *La lotta multilivello al terrorismo internazionale*, Milano, Giuffrè, 2010, p. 466 ss.; D. Maffei, *«Legislazione dell'emergenza» e tutela dei dati personali dei passeggeri: il conflitto Europa-Usa*, in *Dir. informaz. e informatica*, 2006, p. 778 ss.; V. Papakonstantinou-P. De Hert, *The PNR Agreement and Transatlantic Anti-Terrorism Co-Operation: No Firm Human Rights Framework on Either Side of the Atlantic*, in *Common Market Law Review*, 2009, p. 885 ss.; F. Rossi Dal Pozzo, *Servizi di trasporto aereo e diritti dei singoli nella disciplina comunitaria*, Milano, Giuffrè, 2008, p. 168 ss.; M. Spatti, *Il trasferimento dei dati relativi al* Passenger Name Record*: gli Accordi dell'Unione europea con Australia e Stati Uniti d'America*, in *Dir. commercio internaz.*, 2013, p. 683 ss.; A. Terrasi, *Trasmissione dei dati personali e tutela della riservatezza: l'accordo tra Unione Europea e Stati Uniti del 2007*, in *Riv. dir. internaz.*, 2008, p. 381 ss.; G. Tiberi, *L'accordo tra la Comunità europea e gli Stati Uniti sulla schedatura elettronica dei passeggeri aerei al vaglio della Corte di giustizia*, in *Quaderni cost.*, 2006, p. 824 ss.; M. Tzanou, *The War Against Terror and Transatlantic Information Sharing: Spillovers of Privacy or Spillovers of Security?*, in *Utrecht Journal of International and European Law*, 2015, p. 87 ss.; A. Vedaschi-G. Marino Noberasco, *From DRD to PNR: Looking for a New Balance Between Privacy and Security*, in D. Cole-F. Fabbrini-S. Schulhofer (a cura di), *Surveillance*, cit., p. 67 ss.

[35] Così, testualmente, A. Vedaschi, *L'accordo internazionale*, cit., p. 1922.

[36] Si tratta delle *Guidelines on Passenger Name Record* (doc. 9944), adottate dall'ICAO nel 2010, dirette a fissare misure uniformi per la creazione di sistemi di trasmissione, conservazione e protezione dei dati PNR.

[37] Se già da tempo alcuni Stati membri (come Regno unito e Danimarca) avevano autonomamente introdotto una normativa *ad hoc*, nel 2012 la Commissione europea, nell'ambito del programma *Prevention of and fight against crime* (ISEC), aveva stanziato la somma di cinquanta milioni di euro per la presentazione, da parte degli Stati membri, di progetti per lo sviluppo di sistemi PNR nazionali (*Law enforcement cooperation through measures to set up Passenger Information Units in Member States for the collection, processing, analysis and exchange of Passenger Name Record data*), stimolando, così, iniziative in questa direzione.

[38] Si tratta della Comunicazione su «Trasferimento di dati di identificazione delle pratiche: un approccio globale dell'UE» [COM(2003) 826].

[39] Cfr. COM(2007) 654 del 6 novembre 2007 «sull'uso dei dati del codice di prenotazione nelle attività di contrasto».

[40] È la proposta di direttiva «sull'uso dei dati del codice di prenotazione a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi» [COM(2011) 32 del 2 febbraio 2011].

[41] Si tratta della Risoluzione del Parlamento europeo n. 561 del novembre 2008 e dei pareri del Garante europeo della protezione dei dati (in *G.U.U.E.*, C 110 dell'1° maggio 2008), del Gruppo di lavoro «Articolo 29» per la protezione dei dati (parere n. 145 del 5 dicembre 2007) e dell'Agenzia per i diritti fondamentali del 28 ottobre 2008.

[42] Cfr., per tutti, il *Parere* del Garante europeo della protezione dei dati del 25 marzo 2011 (in *G.U.U.E.*, C 181 del 22 giugno 2011) ed il *Parere* n. 10/11 del 5 aprile 2011 del Gruppo «Articolo 29».

di giustizia, della direttiva sulla *data retention* [43], con argomenti agevolmente estensibili anche al meccanismo di raccolta e scambio ipotizzato dalla proposta.

Lo scenario è, repentinamente, mutato con il ridestarsi dell'emergenza terroristica. Gli attacchi del gennaio 2015 alla redazione di *Charlie Hebdo* hanno spinto il Parlamento europeo, per anni scettico, ad annoverare, tra le priorità, la messa a punto della direttiva PNR [44]. I successivi attentati di Parigi del novembre 2015 hanno impresso una decisiva accelerazione all'*iter* legislativo, portato a termine all'indomani dei tragici eventi di Bruxelles del marzo 2016 [45], lo stesso giorno, non a caso, dell'approvazione del pacchetto UE di riforma della protezione dei dati [46], a riprova della costante ricerca di un ragionevole punto di equilibrio tra aneliti securitari e prerogative individuali.

La regolamentazione europea

Plurime sono le cautele adottate, dalla disciplina approvata, nel consentire alle autorità di contrasto la raccolta ed il trattamento dei dati del codice di prenotazione, in vista dell'obiettivo di «garantire la sicurezza, proteggere la vita e l'incolumità delle persone» e, al contempo, creare un quadro normativo uniforme per la protezione dei dati PNR e la tutela della riservatezza dei passeggeri (*considerando* n. 5).

La direttiva, innanzitutto, esclude l'accesso diretto delle pubbliche autorità agli archivi informatici dei vettori (c.d. metodo *pull*). È, invece, prevista l'istituzione, in ciascuno Stato membro, di un'Unità d'informazione sui passeggeri (UIP), a cui le compagnie aeree sono tenute a trasferire elettronicamente, da 24 a 48 ore prima della partenza e immediatamente dopo la chiusura volo, i dati forniti dai passeggeri (c.d. metodo *push*) [47]. Il trasferimento è disposto a favore dell'Unità dello Stato nel cui territorio atterra o dal cui territorio partano voli *extra*-UE (art. 8). Si prevede, comunque, che le singole normative di recepimento possano estendere l'obbligo anche ai voli *intra*-UE (art. 2) [48].

Ricevuti i dati PNR, l'Unità nazionale provvede ad una prima analisi automatizzata, che si avvale di criteri di rischio prestabiliti e del confronto con le informazioni archiviate in altre banche dati [49]. Lo sco-

[43] C. giust. UE, Grande sez., 8 aprile 2014, Digital Rights Ireland e Seitlinger e altri, cit.

[44] Con la Risoluzione dell'11 febbraio 2015 «sulle misure antiterrorismo», il Parlamento europeo, da un lato, si impegnava a mettere a punto la direttiva PNR, dall'altro auspicava che il relativo *iter* si svolgesse parallelamente a quello del pacchetto sulla protezione dei dati.

[45] Per una sintesi dei vari passaggi che hanno condotto al voto favorevole del Parlamento europeo (il 14 aprile 2016) e del Consiglio (il 21 aprile 2016) e, dunque, all'adozione della direttiva in data 27 aprile 2016 v., tra gli altri, F. Di Matteo, *La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella direttiva PNR?*, in *Dir. umani e dir. internaz.*, 2017, p. 213 ss.; D. Lowe, *The European Union's Passenger Name Record Data Directive 2016/681: Is It Fit For Purpose?*, in *International Criminal Law Review*, 2017, p. 78 ss.; F. Rossi Dal Pozzo, *Protezione dei dati personali*, cit., p. 1032 ss.; G. Tiberi, *La direttiva UE sull'uso dei dati del codice di prenotazione (PNR) nella lotta al terrorismo e ai reati gravi*, in *Quaderni cost.*, 2016, p. 590 ss.

[46] Si tratta, come noto, del Regolamento UE 2016/679 e della direttiva (UE) 2016/680, quest'ultima relativa 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, nonché alla libera circolazione di tali dati». Sull'evoluzione, in ambito europeo, della disciplina sulla protezione dei dati trattati a fini di *law enforcement* v., *ex multis*, G. Buttarelli, *Data protection in the area of freedom, security and justice: challenges for the judiciary*, in H. Hijmans-H. Kranenborg, *Data protection anno 2014: how to restore trust? Contributions in honour of Peter Hustinx, European data protection supervisor 2004-2014*, Cambridge, Intersentia, 2014, p. 49 ss.; S. Ciampi, *Principio di disponibilità e protezione dei dati personali nel "terzo pilastro"*, cit., p. 34 ss.; E. De Busser, *EU data protection in transatlantic cooperation in criminal matters. Will the EU be serving its citizens an American meal?*, in *Utrecht Law Rev*, 2010, 6, p. 86 ss.; P. De Hert-V. Papakonstantinou, *The Police and Criminal Justice Data Protection Directive: comment and analysis*, in *Comput Law Mag SCL*, 2012, 22, p. 21 ss.; T. Marquenie, *The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework*, in *Computer Law & Security Review*, 2017, p. 324 ss.; G. Tiberi, *Protezione dei dati personali e sicurezza dopo il Trattato di Lisbona*, in G. Grasso-L. Picotti-R. Sicurella (a cura di), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, Giuffrè, 2011, p. 524 ss. Sia consentito anche il rinvio a P. Troisi, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, in S. Sica-V. D'Antonio-G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Milano, Cedam, 2016, p. 313 ss.

[47] Si prevede, comunque, la possibilità di richiedere ai vettori aerei la trasmissione dei dati PNR, caso per caso, anche in momenti diversi, per rispondere ad una minaccia specifica e reale connessa a reati di terrorismo o a gravi reati (art. 8, par. 5). I protocolli ed i formati da utilizzare per il trasferimento dei dati sono stati definiti dalla decisione di esecuzione (UE) 2017/759.

[48] Il *considerando* n. 33 chiarisce, inoltre, che la direttiva non pregiudica la possibilità che gli Stati membri istituiscano un sistema di raccolta e trattamento dei dati PNR provenienti da operatori economici diversi dai vettori aerei, come le agenzie di viaggio e gli operatori turistici.

[49] Tale analisi è preceduta da uno *screening* diretto a verificare che i dati trasmessi corrispondano, effettivamente, a quelli

po è controllare i passeggeri prima dell'arrivo o della partenza del volo, per individuare persone che potrebbero essere implicate nella commissione di reati di terrorismo o di altri gravi reati (c.d. *controllo in tempo reale*). Ad un eventuale «riscontro positivo», deve seguire un esame individuale non automatizzato (volto a verificare la necessità di appositi interventi), all'esito del quale l'Unità nazionale trasmette i dati dei passeggeri identificati e i risultati del relativo trattamento alle autorità di *law enforcement* competenti, nonché alle UIP di tutti gli altri Stati membri (per l'inoltro ai rispettivi organi giudiziari, di polizia e di *intelligence*).

L'Unità nazionale provvede alla comunicazione dei dati trasmessi dai vettori aerei e dei risultati del loro trattamento anche per rispondere a richieste debitamente motivate formulate, con riferimento a casi specifici, dalle autorità di contrasto interne e dalle Unità d'informazione (o, in presenza di situazioni di emergenza, direttamente dalle autorità competenti) di altri Stati dell'Unione (c.d. *controllo reattivo*).

Al di fuori di questi casi, il trattamento dei dati PNR da parte dell'Unità nazionale è consentito al solo scopo di definire o aggiornare i criteri di valutazione da utilizzare, in sede di controllo in tempo reale, per individuare persone sospettate di essere coinvolte in attività criminali (c.d. *controllo proattivo*).

Il trattamento è, in ogni caso, consentito soltanto per finalità di prevenzione e repressione di reati di terrorismo o altri gravi reati specificamente indicati [50]. Solo per tali obiettivi, è possibile che i dati e i risultati del trattamento vengano trasmessi alle autorità di contrasto e alle Unità d'informazione sui passeggeri di altri Stati membri. Sempre e unicamente per questi scopi, le autorità nazionali che li ricevono possono sottoporli ad ulteriori verifiche e analisi, prima di adottare le misure o i provvedimenti ritenuti appropriati.

È sancito, comunque, il divieto di assumere decisioni che comportino conseguenze giuridiche negative per l'interessato o che lo danneggino in modo significativo esclusivamente sulla base del trattamento automatizzato dei dati PNR o per motivi fondati su ragioni discriminatorie (artt. 1, 6, 7 e 9).

I dati pervenuti all'Unità nazionale sono conservati in apposita banca dati per un periodo di cinque anni, per poi essere cancellati in via definitiva. Trascorsi sei mesi dal trasferimento sono, ad ogni modo, resi anonimi mediante mascheramento degli elementi che potrebbero servire per l'identificazione personale del passeggero o di altre persone. La comunicazione dei dati integrali è consentita, scaduti i sei mesi, solo se necessaria per rispondere, in casi specifici, a richieste debitamente motivate degli organi di *law enforcement*, previa autorizzazione di un'autorità giudiziaria o di altra autorità nazionale competente.

Le risultanze del controllo in tempo reale sono, invece, conservate soltanto per il tempo necessario ad informare di un riscontro positivo le autorità deputate alla prevenzione e repressione dei reati e le UIP degli altri Stati membri. I risultati dei trattamenti automatizzati, anche in caso di riscontro negativo a seguito di esame individuale non automatizzato, possono, comunque, essere memorizzati al fine di evitare futuri «falsi riscontri positivi», almeno finché i dati di riferimento non siano definitivamente cancellati (art. 12).

Ulteriori prescrizioni sono dettate per l'accesso di Europol ai dati PNR (art. 10), per il loro trasferimento a Paesi terzi (art. 11), per vietare il trattamento di dati sensibili (art. 13, par. 4), per regolare l'attività di sorveglianza demandata all'autorità nazionale di controllo ed al responsabile della protezione dei dati (artt. 5 e 15), per riconoscere all'interessato diritti di accesso, rettifica, cancellazione e ricorso giurisdizionale, nonché per assicurare la protezione dei dati e la previsione di adeguate sanzioni (artt. 13 e 14).

L'attuazione interna

Con il d.lgs. 21 maggio 2018, n. 53, attraverso un *iter* che, come in sede europea, si è sviluppato parallelamente alla riforma sulla *data protection* [51], il legislatore ha trasposto, nell'ordinamento interno, l'intera di-

elencati nell'allegato I alla direttiva. Eventuali dati diversi devono essere immediatamente cancellati in via definitiva dall'UIP (art. 6, par. 1).

[50] Per quanto riguarda i reati di terrorismo, il riferimento è, oggi, alla direttiva (UE) 2017/541, che ha sostituito la precedente direttiva 2002/475. Gli altri «reati gravi» sono quelli elencati nell'allegato II alla direttiva, purché siano puniti, dal diritto nazionale degli Stati membri, con una pena detentiva o una misura di sicurezza privativa della libertà personale non inferiore a tre anni.

[51] È di pochi giorni antecedente il d.lgs. 18 maggio 2018, n. 51, relativo all'attuazione della direttiva (UE) 2016/680, adottato,

sciplina dettata dalla direttiva PNR [52], integrandola con le necessarie norme attuative ed estendendola, alla luce della facoltà riservata ai Paesi membri, anche ai voli *intra*-UE. È fatto obbligo, dunque, ai vettori aerei di trasferire all'Unità italiana d'informazione sui passeggeri i dati del codice di prenotazione di tutti i voli, di linea e non, in arrivo o in partenza dal territorio dello Stato (art. 1, comma 1, lett. *a*).

L'UIP nazionale – configurata come organo interforze, composto da personale della polizia di Stato, dell'arma dei carabinieri e del corpo della guardia di finanza [53] – è incardinata presso il Dipartimento della pubblica sicurezza del Ministero dell'interno, nell'ambito della Direzione Centrale della Polizia Criminale (art. 2, comma 2, lett. *s*), individuata come articolazione più idonea a svolgere le funzioni di raccolta, analisi, trasmissione e scambio di informazioni assegnate dalla direttiva.

A tali fini, l'Unità utilizza un «Sistema informativo» istituto, anch'esso, presso il Dipartimento della pubblica sicurezza [54], le cui modalità tecniche di funzionamento sono affidate alla fonte ministeriale (art. 4) [55]. Data la mole di informazioni destinate a confluire nel sistema e la conseguente necessità, almeno in fase di prima attuazione, di specifiche competenze tecniche, è prevista la possibilità per l'UIP di avvalersi, nelle operazioni di ricezione dei dati dai vettori aerei, di «un operatore economico qualificato», che, in tal caso, assume il ruolo di responsabile del trattamento (art. 6, comma 2, lett. *a*) [56].

Le «autorità competenti nazionali» a cui l'Unità d'informazione trasmette i dati ricevuti o i risultati del loro trattamento – nei casi di «riscontro positivo» o a seguito di richiesta debitamente motivata (art. 12) – sono individuate: per le forze di polizia, nella direzione investigativa antimafia, nonché nella polizia di Stato, nell'arma dei carabinieri e nel corpo della guardia di finanza; sul fronte giudiziario, nella direzione nazionale antimafia e antiterrorismo e in tutte le autorità giudiziarie legittimate a perseguire i reati di terrorismo o gli altri gravi reati indicati dalla direttiva; per il comparto *intelligence*, negli organismi facenti parte del Sistema di informazione per la sicurezza della Repubblica (art. 2, comma 2, lett. *b*) [57].

Non è chiaro se, a fronte di un riscontro positivo, debbano essere allertate, contestualmente, tutte le «autorità competenti» o si debba tener conto dei concreti elementi di sospetto che l'analisi dei dati faccia emergere. Essendo la comunicazione funzionale a consentire le necessarie verifiche e l'adozione dei «provvedimenti idonei a prevenire e reprimere» i reati (art. 12, comma 1), andrebbe preferita un'esegesi tesa a limitarla, oltre che agli organi centralizzati (direzione investigativa, direzione nazionale e organismi di sicurezza della Repubblica), alle forze di polizia e agli uffici del pubblico ministero in concreto

anch'esso, sulla base della comune legge di delegazione europea 2016-2017 (l. 25 ottobre 2017, n. 163) (per una lettura combinata delle due normative, v. L. Pulito, *Il trattamento dei dati personali in ambito penale e l'uso del* passenger name record *per contrastare il terrorismo e altri reati gravi*, in *questa Rivista*, 2018, 6, p. 1138 ss.). Con il d.lgs. 10 agosto 2018, n. 101, sono state, poi, adottate le disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679.

[52] Va evidenziato che la nuova disciplina ha inglobato anche quella relativa al trasferimento, da parte dei vettori aerei, dei c.d. dati API (*Advance Passenger Information*), regolata dal d.lgs. 2 agosto 2007, n. 144 (che, dunque, è stato abrogato), attuativo della direttiva (UE) 2004/82/CE. Si tratta, principalmente, dei dati anagrafici risultanti dalla banda a lettura ottica del passaporto (comprendenti, nome, luogo di nascita e cittadinanza dell'interessato, numero e data di scadenza del passaporto, *etc.*), che sono raccolti e resi disponibili agli Uffici incaricati dei controlli di polizia di frontiera al fine di migliorare i controlli alle frontiere esterne e prevenire l'immigrazione illegale. Siccome la direttiva 2016/681 include, tra i dati PNR da comunicare alle UIP, anche gli API eventualmente raccolti, il legislatore nazionale, al fine di evitare la coesistenza di due normative nazionali diverse regolanti gli obblighi di trasmissione a carico delle compagnie aeree, ha ritenuto di unificare le discipline in un unico testo (il d.lgs. n. 53 del 2018, appunto), assicurando, comunque, modalità di trattamento differenziate in ragione delle diverse finalità previste per ciascuna delle predette categorie di informazioni (cfr. *Relazione illustrativa allo schema di decreto legislativo*, consultabile sul sito del Governo, p. 1 ss.). In senso critico, rispetto a tale scelta, si era espresso il Garante per la protezione dei dati personali nel *Parere* del 22 febbraio 2018 sullo schema di decreto legislativo (consultabile sul sito internet del Garante).

[53] Organizzazione e pianta organica sono rimessi ad apposito decreto ministeriale (art. 6, comma 1).

[54] Nel contesto della disciplina, il nuovo Sistema informativo sarà destinato a gestire sia i dati PNR, che quelli API (in sostituzione, quanto a questi ultimi, dell'attuale *Border Control Sistem*), garantendone, al contempo, il trattamento differenziato. Sicché i dati API saranno trattati sia dalla UIP, quali componenti dei dati PNR, sia dagli Uffici di frontiera, per le finalità dei controlli sull'immigrazione illegale.

[55] Si tratta del d.m. 17 agosto 2018, recante «modalità tecniche di funzionamento del Sistema Informativo e di trasferimento dei dati del codice di prenotazione (PNR)», in *G.U.*, Serie Generale, n. 235 del 9 ottobre 2018.

[56] Nella *Relazione illustrativa*, cit., p. 7 si precisa che «il recepimento della direttiva implica l'afflusso di informazioni riguardanti oltre 200.000.000 di passeggeri» e che, quindi, «tale rilevante mole di dati può richiedere, soprattutto nella fase di prima attuazione, la necessità di fare ricorso all'intervento di operatori economici in possesso del necessario *know how* ai fini della loro acquisizione, mediante adeguati *software*».

[57] Vale a dire gli organismi previsti dagli artt. 4, 6 e 7 della l. 3 agosto 2007, n. 124.

legittimati con riguardo al luogo di partenza o di arrivo del volo ed alla tipologia di reato in cui si sospetta il passeggero sia implicato.

In relazione all'attività di analisi e trattamento, all'Unità nazionale è assegnato, conformemente a quanto disposto dalla direttiva, il compito di definire ed aggiornare periodicamente i criteri da adoperare nella valutazione in tempo reale dei passeggeri. A ciò provvede, sentite le «autorità competenti nazionali», nel rispetto dei principi di necessità, proporzionalità, specificità e non discriminazione (art. 8, comma 2).

Quanto alle banche dati con cui confrontare, sempre in occasione dei controlli che precedono l'arrivo o la partenza del volo, i dati ricevuti dai vettori, in vista della individuazione di sospetti già "noti" alle forze dell'ordine, è indicato unicamente il Centro elaborazione dati (CED) del Ministero dell'interno. Per il resto, è fatto generico riferimento, in termini analoghi a quelli della direttiva, ad «altre banche dati nazionali, europee ed internazionali contenenti informazioni utili ai fini di prevenzione e repressione dei reati di terrorismo e dei reati gravi» (art. 8, comma 1, lett. *a*).

Si stabilisce, altresì, che all'autorizzazione necessaria per la trasmissione dei dati PNR integrali, a seguito di «pseudonimizzazione» [58] per il decorso del termine di sei mesi dal trasferimento, provveda: l'autorità giudiziaria, in caso di richiesta formulata nell'ambito di un procedimento penale o di un procedimento per l'applicazione di misure di prevenzione; il vice capo della polizia, direttore centrale della polizia criminale, per le richieste aventi finalità di prevenzione dei reati (art. 10, comma 3).

Perplessità suscita, però, l'espressione «autorità giudiziaria», non accompagnata da ulteriori specificazioni. Il riferimento parrebbe essere all'organo giudiziario procedente. L'esegesi, tuttavia, per le richieste avanzate nel corso delle indagini preliminari, indurrebbe ad identificare, in capo all'ufficio del pubblico ministero, la legittimazione sia a richiedere (quale autorità nazionale competente) la comunicazione, sia ad autorizzarla; e ciò in contrasto con la *ratio* della previsione, tesa a pretendere un controllo esterno qualificato dopo che gli elementi identificativi siano stati mascherati. La formula andrebbe, dunque, intesa in senso restrittivo, come «autorità giurisdizionale», con conseguente competenza, nella fase investigativa, del giudice per le indagini preliminari, secondo un modello già in essere nel sistema processuale (si pensi alle intercettazioni ed al prelievo coattivo di materiale biologico).

Sul fronte della protezione dei dati, è fatto rinvio alla nuova disciplina regolante il trattamento a fini di *law enforcement* (d.lgs. n. 51 del 2018) [59] e, per quanto riguarda i dati detenuti dai vettori aerei, alle disposizioni del regolamento generale UE e del codice della *privacy* (art. 22, commi 1 e 2). L'autorità nazionale di controllo è il garante per la protezione dei dati; il responsabile della protezione è nominato con decreto del capo della polizia, nell'ambito della direzione centrale della polizia criminale (artt. 20 e 21) [60]. Per i diritti di accesso, rettifica, cancellazione e ricorso giurisdizionale si fa rinvio, conformemente alla normativa regolante i trattamenti da parte delle forze di polizia (art. 48 d.lgs. n. 51 del 2018), alle prerogative riconosciute in relazione ai dati conservati nel CED del Ministero dell'interno (art. 10, commi 3, 4 e 5, l. n. 121 del 1981) (art. 23).

Specifiche sanzioni amministrative pecuniarie, irrogate dall'Ente nazionale per l'aviazione civile, sono previste, a carico dei vettori, in caso di violazione degli obblighi loro imposti (art. 24).

I RIFLESSI SUL DIRITTO ALLA *PRIVACY* E ALLA PROTEZIONE DEI DATI

Ora, non c'è dubbio che la disciplina, come congegnata a livello europeo e recepita dal legislatore interno, abbia beneficiato del lungo dibattito sviluppatosi in materia. Evidenti sono i miglioramenti ap-

[58] Si tratta della procedura di mascheramento degli elementi identificativi prevista dalla direttiva, denominata dal legislatore interno «pseudonimizzazione» su indicazione del Garante per la protezione dei dati, essendo quest'ultima nozione – già utilizzata dal Regolamento UE 2016/679 – più idonea ad indicare la situazione in cui i dati personali non vengono definitivamente eliminati, ma non sono più attribuibili ad un interessato specifico senza l'utilizzo di informazioni aggiuntive (cfr. *Parere* del 22 febbraio 2018, cit., punto 8).

[59] Per quanto riguarda il trattamento da parte degli organismi di *intelligence*, trova applicazione la relativa disciplina dettata dal Codice della *privacy* (art. 58), come di recente modificata dal d.lgs. n. 101 del 2018, che rinvia al d.lgs. n. 51 del 2018.

[60] Sono, altresì, regolate le figure del «titolare del trattamento» (che è il Dipartimento della pubblica sicurezza) e del «responsabile del trattamento» (la Direzione Centrale della Polizia Criminale, per i dati PNR, e la Direzione Centrale dell'Immigrazione e della Polizia delle Frontiere, per i dati API) (art. 4, commi 1 e 2).

portati rispetto alla originaria proposta di direttiva del 2011 [61], a partire dalla elencazione dei «reati gravi», la cui prevenzione e repressione, unitamente a quelli di terrorismo, giustifica il trattamento, fino alle più puntuali previsioni in tema di protezione dei dati: l'obbligo di conservare i registri di tutte le attività di trattamento e di metterli a disposizione dell'autorità nazionale di controllo; il dovere di informare senza indebito ritardo l'interessato e l'autorità garante in caso di violazioni di dati personali suscettibili di arrecare un rilevante pregiudizio alla riservatezza; l'introduzione della figura del responsabile della protezione dei dati, con la funzione di «punto di contatto unico» per gli interessati in merito a tutte le questioni connesse al trattamento; il potenziamento del ruolo dell'autorità nazionale di controllo (artt. 13-15 direttiva e 20-24 d.lgs. n. 53 del 2018) [62].

L'attenzione posta al tema della protezione dei dati è, del resto, pienamente conforme al ruolo decisivo che, in epoca digitale, la *data protection* ha assunto ai fini della tutela dell'identità di ciascun individuo [63]. Si tratta, in una società democratica, di un interesse non solo privato, ma anche pubblico [64].

Nonostante gli indiscussi passi in avanti, restano, però, immutate le potenzialità invasive del sistema.

L'ingerenza nella sfera privata è *in re ipsa*, se si considera che oggetto di archiviazione, analisi e scambio sono informazioni, quand'anche non sensibili, inerenti a persone fisiche identificate o, comunque, identificabili [65]. Ciò avviene, oltretutto, in deroga ad uno dei cardini dell'autodeterminazione informativa, il principio di finalità limitata: dati ottenuti per scopi essenzialmente commerciali vengono, poi, adoperati, senza il consenso dell'interessato, per obiettivi, anch'essi determinati e legittimi (il contrasto al terrorismo ed alla criminalità grave), ma assolutamente diversi e non consequenziali rispetto a quelli della raccolta iniziale. La deroga non è attenuata dall'obbligo, posto in capo ai vettori, di informare adeguatamente i passeggeri (art. 22, comma 2, d.lgs. n. 53 del 2018), in quanto il contesto in cui i dati sono forniti è profondamente differente da quello in cui successivamente vengono riversati e costituisce, per di più, manifestazione, quantomeno con riguardo ai viaggi *intra*-UE, dell'esercizio di una libertà fondamentale, quella di circolazione.

A fronte di un'eccezione di tal portata alla "finalità limitata", stringente diviene la verifica di «necessità» e «proporzionalità» imposta dalle fonti sovranazionali.

La Convenzione europea (Cedu), come noto, riconosce e tutela il diritto al rispetto della vita privata, consentendone limitazioni solo se previste per legge, rispondenti ad obiettivi legittimi e *necessarie* in una società democratica (art. 8). Secondo la giurisprudenza di Strasburgo, dalla Convenzione emerge un'insopprimibile esigenza di bilanciamento tra interessi pubblici e privati, che induce a ritenere conformi alla Cedu interferenze alla *privacy* unicamente nella misura in cui soddisfino *bisogni sociali impellenti*, siano *proporzionate* agli scopi perseguiti e si fondino su *ragioni giustificative pertinenti e sufficienti* [66].

---

[61] Cfr. il *Parere* del Garante europeo della protezione dei dati del 24 settembre 2015 (in *G.U.U.E.*, C 392 del 25 novembre 2015), punto n. 62, che, sia pure critico rispetto allo strumento istituito, ha accolto favorevolmente «i vari miglioramenti apportati alla proposta dal Consiglio e dalla Commissione LIBE, che riguardano, ad esempio, le specifiche disposizioni sulla protezione dei dati, la presenza di un Responsabile della protezione dei dati, o un riferimento specifico al potere delle autorità garanti».

[62] Su questi temi v., per tutti, F. Di Matteo, *La raccolta indiscriminata*, cit., p. 232.

[63] Sul tema, v. S. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. critica dir. priv.*, 1997, p. 583 ss. V., altresì, nel settore penalistico, S. Allegrezza, *Giustizia penale e diritto all'autodeterminazione dei dati personali nella regione Europa*, in D. Negri (a cura di), *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, Roma, Aracne, 2007, p. 61 ss.

[64] Per queste considerazioni v. F. Rossi Dal Pozzo, *Protezione dei dati personali*, cit., p. 1020. Cfr., altresì, S. Ciampi, *Principio di disponibilità*, cit., p. 38. Evidenzia la «duplice dimensione» della protezione dei dati, «di diritto dell'interessato all'autodeterminazione informativa e alla riservatezza, da un lato, e di strumento di tutela oggettiva che consenta il controllo sulla genuinità del dato, dall'altro», A. Marandola, Information sharing *nella prospettiva del Trattato di Prüm*, cit., p. 180.

[65] Lo ha chiarito C. giust. UE, Grande sez., 8 aprile 2014, Digital Rights Ireland e Seitlinger e altri, cit., secondo cui, una normativa che consenta alle autorità pubbliche di accedere in maniera generalizzata ai dati personali, pregiudica i diritti al rispetto della vita privata ed alla protezione dei dati, indipendentemente dal se le informazioni abbiano o meno carattere sensibile o che gli interessati abbiano subito eventuali inconvenienti in seguito a tale ingerenza (punti nn. 33-36).

[66] Così si esprime Corte e.d.u., Grande camera, 4 dicembre 2008, S. e Marper c. Regno Unito, in *Riv. it. dir. proc. pen.*, 2009, p. 346, che ha considerato *sproporzionata*, rispetto agli scopi perseguiti, l'ingerenza nella vita privata che si realizza attraverso la conservazione, senza limiti di tempo, di dati biologici ed impronte digitali di soggetti non perseguiti penalmente o non condannati. Più di recente v. Corte e.d.u., 13 settembre 2018, Big Brother e altri c. Regno Unito, che, in tema di accesso da parte delle autorità pubbliche ai dati esterni delle comunicazioni conservati dai fornitori dei servizi di comunicazione, ha dichiarato incompatibile con l'art. 8 Cedu la normativa inglese in quanto eccedente i limiti imposti dal principio di proporzionalità, non es-

Nella stessa direzione si muove la Carta dei diritti fondamentali dell'Unione nel consacrare il diritto al rispetto della vita privata (art. 7) ed alla protezione dei dati personali, prescrivendo che il trattamento sia improntato al principio di lealtà, avvenga, per *finalità determinate*, in base al consenso della persona o a un altro fondamento legittimo previsto dalla legge, contempli l'accesso dell'interessato e il controllo di una autorità indipendente (art. 8). Eventuali limitazioni, stabilite dalla legge e rispettose del contenuto essenziale dei diritti, possono essere apportate, in conformità al principio di *proporzionalità*, solo laddove siano *necessarie* e rispondano effettivamente a *finalità di interesse generale* riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui (art. 52). Il diritto di ogni persona «alla protezione dei dati di carattere personale che la riguardano» è, peraltro, espressamente sancito dal Trattato sul funzionamento dell'Unione europea (art. 16).

La Corte di giustizia ha, al riguardo, rimarcato che la lotta al terrorismo ed alla criminalità grave costituisce, senza dubbio, interesse generale dell'Unione, idoneo a giustificare restrizioni dei detti diritti. Affinché l'ingerenza possa ritenersi consentita è, tuttavia, indispensabile che *non superi i limiti di quanto è appropriato e necessario al conseguimento dell'obiettivo* e che siano fissate *regole chiare* e *precise* in grado di delimitarne la portata ed il campo di applicazione [67].

È in questa cornice che si collocano le perplessità su una misura idonea a porre sotto sorveglianza, a prescindere dall'esistenza di elementi indicativi di un qualsiasi nesso con azioni criminose, la vita privata di chiunque decida di spostarsi, per via aerea, all'interno dell'Europa o verso Paesi terzi. Il controllo generalizzato di *tutti* i passeggeri rappresenta, del resto, il *proprium* di uno strumento ideato, principalmente, al fine di individuare persone "non note", mai sospettate prima, e consentire, in tempo utile, interventi in funzione preventiva o repressiva [68].

Questa sorta di "capacità predittiva" – tipica delle attività di *intelligence* e delle indagini proattive[69] – costituisce l'aspetto più controverso del sistema, ma anche il *quid pluris* rispetto agli altri circuiti di scambio di informazioni [70], che lo renderebbe *necessario* nella lotta al terrorismo ed alla criminalità transnazionale. Una disciplina comune europea si giustificherebbe, in tale ottica, con l'esigenza di evitare tutele eterogenee dei diritti individuali [71] ed obblighi differenti a carico delle compagnie aeree [72].

Non si è mancato, però, di obiettare che nessun esauriente vaglio sia stato compiuto sull'efficacia di misure meno invasive della profilazione di *default* di milioni di viaggiatori [73]. Sicché, non essendone stati in concreto dimostrati i vantaggi, difetterebbe il carattere *necessario* dell'ingerenza [74]. Né varrebbe in-

sendo confinata allo scopo di combattere forme gravi di crimine e non prevedendo la preventiva autorizzazione di un tribunale o di un organo amministrativo indipendente.

[67] Sono i principi espressi da C. giust. UE, Grande sez., 8 aprile 2014, Digital Rights Ireland e Seitlinger e altri, cit.; C. giust. UE, Grande sez., 6 ottobre 2015, Schrems, in *Giur. cost.*, 2016, p. 273; C. giust. UE, Grande sez., 21 dicembre 2016, Tele2 Sverige e Watson, in *Dir. informaz. e informatica*, 2016, p. 984.

[68] Nella *Relazione di accompagnamento* alla proposta di direttiva del 2011 [COM(2011) 32] si chiariva che, a differenza degli altri strumenti della cooperazione informativa, quali i dati API, il SIS e il VIS, che servono quando l'identità del sospetto è «nota», i dati PNR consentono, invece, di effettuare valutazioni sui passeggeri e, così, contribuiscono ad identificare criminali o terroristi «non noti». Servono, dunque, principalmente, come strumento di *intelligence* criminale. Lo precisa anche il *considerando* n. 7 della direttiva, nel riconoscere che «la valutazione dei dati PNR consente l'identificazione di persone mai sospettate», sicché, attraverso il loro uso, «è possibile far fronte alla minaccia di reati di terrorismo e reati gravi da una prospettiva diversa rispetto al trattamento di altre categorie di dati personali».

[69] Le indagini proattive, in effetti, hanno funzione anticipatoria, in quanto non prendono avvio da un specifica *notitia criminis*, né sono volte semplicemente a cercarla, ma si fondano su un approccio proteso all'assunzione di iniziative dirette ad impedire la commissione di delitti, piuttosto che alla mera reazione agli eventi (cfr., sul tema, la *Risoluzione del XVIII Congresso internazionale di diritto penale*, Istanbul, 20-27 settembre 2009, in *Riv. dir. proc.*, 2010, p. 333 ss.). Sulla tendenza, in epoca di lotta alla criminalità organizzata e al terrorismo, ad una progressiva osmosi tra «prevenzione» e «repressione» attraverso la criminalizzazione di condotte meramente preparatorie e la diretta interconnessione (con conseguenti sovrapposizioni) tra attività di *intelligence* ed indagine penale v., per tutti, D. Curtotti, *Procedimento penale e* intelligence *in Italia: un'osmosi inevitabile, ancora orfana di regole*, in *questa Rivista*, 2018, 3, p. 435 ss.; R. Orlandi, *Inchieste preparatorie nei procedimenti di criminalità organizzata*, in *Riv. it. dir. proc. pen.*, 1996, p. 584 ss.; F. Viganò, *Terrorismo, guerra e diritto penale*, in *Riv. it. dir. proc. pen.*, 2006, p. 694 ss.

[70] Che non esistano sistemi alternativi meno invasivi, ma analogamente efficaci, è evidenziato anche in dottrina (cfr., per tutti, F. Rossi Dal Pozzo, *Protezione dei dati personali*, cit., p. 1057).

[71] Cfr. F. Rossi Dal Pozzo, *Protezione dei dati personali*, cit., p. 1058.

[72] E. Carpanelli-N. Lazzerini, *PNR: Passenger Name Record, Problems Not Resolved?*, cit., p. 379.

[73] È il principale rilievo mosso dal *Parere* del Garante europeo della protezione dei dati del 24 settembre 2015, cit., punti n. 12 e 14.

[74] Per queste considerazioni v., tra i tanti, F. Di Matteo, *La raccolta indiscriminata*, cit., p. 223 ss.; D. Lowe, *The European Union's*

vocare l'obiettivo di armonizzare legislazioni differenti, obiettivo di per sé non sufficiente a legittimare una compressione della riservatezza oltre lo stretto indispensabile [75].

Nel dibattito è entrata anche la Corte di giustizia. L'*occasio* è stata la richiesta di parere del Parlamento europeo sulla compatibilità, con i diritti sanciti dagli artt. 7 e 8 della Carta, dell'accordo PNR tra l'Unione europea ed il Canada [76]. Nel ribadire gli approdi raggiunti con le sentenze *Digital Rights Ireland*, *Schrems* e *Tele2 Sverige* [77], per la prima volta applicati al settore in esame, i giudici del Lussemburgo hanno messo da parte posizioni ideologiche sulla primazia dei diritti individuali o sulla funzionalizzazione di questi ultimi alla «sicurezza pubblica», adottando, al contrario, un approccio realistico, conscio dell'utilità di strumenti di sorveglianza nella lotta al terrorismo, ma pure dei rischi che ne discendono per gli individui [78]. L'impegno è stato, dunque, nella direzione di delineare i confini entro cui i sacrifici alla *privacy* ed all'autodeterminazione informativa, conseguenti al trattamento massivo dei dati PNR, risultino proporzionati al fine di combattere il terrorismo ed i gravi reati di natura transnazionale [79].

Modello di riferimento nell'enucleare le condizioni di legittimità della misura – che la Corte non ha ritenuto del tutto soddisfatte dall'accordo UE-Canada – è stata, senza dubbio, la più evoluta disciplina della direttiva PNR, con particolare riguardo al divieto assoluto di trattamento dei dati sensibili [80] ed alla necessità che i risultati delle analisi automatizzate siano sottoposti a riesame individuale [81]. Ma la disamina è andata ben oltre e consente di ricavare argomenti con cui la normativa interna all'Unione dovrà, necessariamente, confrontarsi.

Tralasciando le questioni, pure non secondarie, relative alla base giuridica [82] ed alla non chiara enun-

Passenger Name Record Data Directive 2016/681, cit., p. 78 ss. Cfr., altresì, G. Tiberi, *La direttiva UE sull'uso dei dati del codice di prenotazione*, cit., p. 593, che ravvisa la violazione del principio di minimizzazione dei dati personali, per «essere un sistema di indiretta raccolta di dati personali che per default deve essere massivo e indiscriminato e che trova proprio nell'abbondanza delle informazioni estraibili la propria ragion d'essere».

[75] Cfr., ancora, il *Parere* del Garante europeo della protezione dei dati del 24 settembre 2015, cit., punti 15 e 19-31.

[76] Si tratta di C. giust. UE, Grande sez., parere n. 1/15 del 26 luglio 2017, cit.

[77] Tale giurisprudenza ha attratto l'attenzione della dottrina. Tra i tanti contributi, v. L. Azoulai-M. Van der Sluis, *Institutionalizing personal data protection in times of global institutional distrust*, in *Common Market Law Review*, 2016, p. 1343 ss.; R. Bifulco, *La sentenza Schrems e la costruzione del diritto europeo della privacy*, in *Giur. cost.*, 2016, p. 289 ss.; F. Fabbrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.*, in *Harvard Human Rights Journal*, 2015, p. 65 ss.; R. Flor, *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. pen. cont.*, 2014, 2, p. 178 ss.; A. Giattini, *La tutela dei dati personali davanti alla Corte di giustizia dell'UE: il caso Schrems e l'invalidità del sistema di "approdo sicuro"*, in *Dir. umani e dir. internaz.*, 2016, p. 247 ss.; M. Granger-K. Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection*, in *European Law Review*, 2014, p. 835 ss.; O. Linskey, *The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland*, in *Common Market Law Review*, 2014, p. 1789 ss.; T. Ojanen, *Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter: ECJ 6 October 2015, Case C-362/14, Maximillian Schrems v Data Protection Commissioner*, in *European Constitutional Law Review*, 2016, p. 318 ss.; O. Pollicino, *Diritto all'oblio e conservazione di dati. La Corte di giustizia a piedi uniti: verso un digital right to privacy*, in *Giur. cost.*, 2014, p. 2949 ss.; G. Tiberi, *Il caso Tele2 Sverige/Watson: una iconica sentenza della Corte di Giustizia nella saga sulla data retention*, in *Quaderni cost.*, 2017, p. 434 ss.; A. Vedaschi-V. Lubello, *Data Retention and Its Implications for the Fundamental Right to Privacy: A European Perspective*, in *Tilburg Law Review*, 2015, 20, p. 14 ss.

[78] Per queste considerazioni, v. C. Graziani, *PNR EU-Canada*, cit., p. 964; A. Vedaschi, *The European Court of Justice*, cit., p. 427 ss.

[79] Ad avviso di A. Vedaschi, *L'accordo internazionale*, cit., p. 1937, la Corte di giustizia «sembra aprire al *contemperamento* piuttosto che al *bilanciamento* fra sicurezza e libertà», al fine di «chiarire *in quale misura* la limitazione della libertà può essere tollerata in ragione di indubbie esigenze di sicurezza».

[80] Cfr. i punti nn. 164-167 del parere, in cui la Corte ha rilevato che il trasferimento ed il trattamento di dati sensibili non apparirebbe giustificato dalla sola finalità di lotta al terrorismo ed ai gravi reati di natura transnazionale, stante il rischio di violazione del principio di non discriminazione (art. 21 della Carta), attraverso, ad esempio, una profilazione fondata su dati (quali la razza o la religione) capaci di indurre le autorità pubbliche ad adibire misure contro specifici gruppi di persone.

[81] Si tratta del punto n. 173 del parere.

[82] La Corte ha censurato l'accordo UE/Canada nella parte in cui è fondato, oltre che sull'art. 87 TFUE (inerente alla cooperazione di polizia), anche sull'art. 82 del TFUE (relativo alla cooperazione giudiziaria, quando invece alcuna previsione dell'accordo è intesa a facilitare tale forma di cooperazione) e non, al contrario, sull'art. 16 TFUE (pur rientrando, tra le finalità, la protezione dei dati personali). Le considerazioni svolte sono estensibili anche alla direttiva PNR, non tanto, però, con riguardo all'inclusione nella base giuridica dell'art. 82 TFUE (essendo previsto, dalla direttiva, lo scambio di informazioni anche tra autorità giudiziarie), quanto, piuttosto, sotto il profilo della mancata indicazione dell'art. 16 TFUE.

ciazione delle informazioni che i vettori aerei devono trasmettere [83], meritano riflessione le considerazioni svolte in merito al trattamento automatizzato dei dati.

L'organo giurisdizionale dell'Unione ha, innanzitutto, preso posizione sulla fissazione dei criteri predeterminati di rischio, pretendendo non solo che siano specifici e non discriminatori (in linea con quanto stabilito dalla direttiva), ma anche «affidabili», idonei, cioè, a condurre a risultati che abbiano come obiettivo unicamente «gli individui sui quali potrebbe gravare un sospetto ragionevole di partecipazione a reati di terrorismo o a reati gravi di natura transnazionale» [84].

Si tratta, certamente, come si avrà modo di dire più avanti, di uno dei nodi cruciali del sistema, da cui finirà per dipendere la sua stessa "validità". Deve registrarsi, tuttavia, nel disegno tracciato dal legislatore europeo, la totale assenza di meccanismi di definizione dei criteri a livello dell'Unione ed il mancato apprestamento di strumenti di controllo. Il tutto è rimesso alla discrezionalità della singola UIP, in cooperazione con le competenti autorità nazionali, con la prospettiva di una tutela non uniforme dei diritti individuali.

Oggetto di interesse sono state, in secondo luogo, le banche dati con cui effettuare il confronto, che, ad avviso della Corte, devono essere «affidabili», «aggiornate» e «limitate» a quelle «gestite in relazione alla lotta al terrorismo e ai reati gravi di natura transnazionale» [85]. L'approccio pare indicativo della necessità di una preventiva selezione degli archivi da utilizzare, archivi che andrebbero individuati esclusivamente in quelli relativi a persone condannate, imputate o indiziate di terrorismo o di altri gravi reati.

Sul punto, però, la disciplina europea pare deficitaria, facendo riferimento a banche dati semplicemente «*pertinenti*» allo scopo. Ad analoghe censure si espone la legge interna che, per un verso, adopera una formula altrettanto generica («altre banche dati nazionali, europee ed internazionali» contenenti informazioni «*utili*» agli obiettivi perseguiti), per l'altro, indica specificamente il Centro elaborazione dati del Ministero dell'interno, che è sì *database* «*pertinente*» o «*utile*», ma sicuramente non circoscritto alla prevenzione e repressione del terrorismo o di reati di grave allarme sociale.

I decreti attuativi, nel regolare le modalità tecniche di funzionamento del Sistema informativo di cui si avvale l'UIP nazionale (art. 4, comma 4, d.lgs. n. 53 del 2018), dovrebbero aver cura di precisare che il raffronto automatizzato avvenga con le sole informazioni del CED classificate come attinenti «alla lotta contro la criminalità comune ed organizzata nonché alla lotta contro il terrorismo e l'eversione» (art. 3, comma 1, lett. *b*, d.P.R. 3 maggio 1982, n. 378) [86]. Ma, in ogni caso, l'utilizzo di banche dati (come, appunto, il CED) aventi funzioni più ampie o parzialmente diverse pone un concreto rischio di *function creep*, vale a dire di graduale allargamento dei confini di operatività del sistema oltre lo scopo per il quale è istituito. La conseguenza è che un eventuale *macht* non sarebbe affatto indicativo di un sospetto di commissione di atti di terrorismo o di gravi reati, con chiara violazione del principio di finalità limitata.

Il pericolo è, peraltro, confermato, nella normativa nazionale, dalla riconosciuta possibilità che i dati PNR siano «riversati» nel CED e sottoposti alla relativa disciplina (art. 10, comma 7, d.lgs. n. 53 del 2018). Il che lascia intravedere futuri trattamenti per fini che esulano da quelli ammessi a livello europeo.

Degni di nota sono, altresì, i rilievi formulati con riguardo al controllo reattivo ed alla conservazione dei dati.

I giudici sovranazionali hanno osservato che un uso dei dati PNR successivo all'analisi compiuta, in tempo reale, prima dell'arrivo del volo dovrebbe fondarsi su «nuove circostanze che lo giustifichino» e avvenire in presenza di specifiche «condizioni sostanziali e procedurali», quali: l'esistenza di «elementi obiettivi che consentano di ritenere che i dati PNR di uno o più passeggeri aerei possano fornire un contributo effettivo di lotta contro i reati di terrorismo e i reati gravi di natura transnazionale»; il controllo

[83] Cfr. i punti n. 155-163. Anche l'elenco dei dati contenuto nell'allegato I alla direttiva presenta, in taluni casi (si pensi al punto n. 12, relativo alle «Osservazioni generali»), profili di indeterminatezza analoghi a quelli rilevati dalla Corte.

[84] Punti n. 172 e 174.

[85] V. il punto n. 172.

[86] Le procedure di raffronto informatico dei dati PNR con quelli conservati nel CED e in altre banche dati sono regolate dall'allegato B al citato d.m. 17 agosto 2018 del Ministero dell'interno, assistito, tuttavia, da «classifica di segretezza». Va, comunque, evidenziato che, nell'introdurre un meccanismo di trattamento automatizzato – a soli fini di «prevenzione» del terrorismo e con un periodo limitato di conservazione di sette giorni – dei dati identificativi dei soggetti che richiedono il noleggio di un autoveicolo, il legislatore nazionale ha previsto che il raffronto avvenga con le sole informazioni conservate nel CED concernenti provvedimenti dell'autorità giudiziaria o dell'autorità di pubblica sicurezza o segnalazioni inserite dalle forze di polizia «per finalità di prevenzione e repressione del terrorismo» (art. 17 d.l. 4 ottobre 2018, n. 113).

preventivo, al di fuori dei casi d'urgenza, di un giudice o di un ente amministrativo indipendente [87]. La Corte ha, inoltre, ritenuto contrastante con il principio di proporzionalità la conservazione dei dati anche dopo la ripartenza dei passeggeri, salvo situazioni particolari in cui si possa concretamente sostenere che il singolo passeggero, nonostante abbia lasciato il Paese, presenti ancora profili di rischio [88].

Entrambi gli aspetti evidenziano lacune della regolamentazione europea. Lungi dal tipizzare i casi in cui le autorità di contrasto, nel corso del periodo di soggiorno dei viaggiatori nel territorio UE, possano domandare (ed ottenere) la trasmissione dei dati PNR, se ne consente l'accesso a seguito di una mera richiesta basata su (imprecisati) «motivi sufficienti», senza alcuna previsione di preventive autorizzazioni, se non, come più sopra detto, qualora si tratti di comunicare i dati integrali a seguito di «pseudonimizzazione». Alcun collegamento è, tra l'altro, operato tra conservazione dei dati e permanenza del passeggero nell'Unione, prevedendosi, al contrario, come nell'accordo con il Canada, un'archiviazione continuativa per cinque anni, anche dopo la partenza verso Paesi terzi ed a prescindere dall'emergere di rischi qualificati [89].

Ulteriori considerazioni sono state spese a proposito del diritto del passeggero ad essere informato dell'uso dei propri dati in casi specifici, non appena, ovviamente, l'informazione non sia più suscettibile di compromettere le indagini [90]. Di questa «notifica individuale», funzionale all'esercizio dei diritti di accesso, rettifica e ricorso giurisdizionale, non v'è traccia alcuna né nella direttiva, né nella disciplina attuativa interna. Ben vero che, nella misura in cui i dati tratti dal codice di prenotazione confluiscano in procedimenti penali o di prevenzione, l'interessato potrà avere conoscenza del loro utilizzo attraverso la consultazione dei relativi fascicoli. Manca, tuttavia, l'obbligo generale di una comunicazione *ad hoc*.

Le conclusioni della Corte di giustizia gettano, dunque, importanti ombre sulla «proporzionalità» del sistema realizzato, ma, al contempo, permettono di individuare gli anticorpi idonei a frenare il cammino verso una «*surveillance society*» [91].

Le ricadute sul sistema processuale

La "vita privata" non è l'unico polo con cui la nuova disciplina interagisce. Nell'arricchire l'armamentario a disposizione delle autorità di *intelligence* e di *law enforcement*, è stata, in effetti, istituzionalizzata una specifica metodologia investigativa, fondata sull'analisi dei dati del codice di prenotazione e suscettibile di sfociare nell'adozione di misure incidenti sulle libertà individuali.

La peculiarità, lo si è detto, è che oggetto di *screening* sono informazioni raccolte e conservate, a scopi di prevenzione e repressione dei reati, a prescindere dall'emergere di elementi indizianti. L'obiettivo principale, lo si è rimarcato, è proprio l'individuazione di soggetti "non noti", ossia di persone che, fino a quel momento, non sono mai state sospettate di essere coinvolte in reati terroristici o in altri gravi reati.

All'orizzonte si profila una potenziale interferenza con la presunzione di innocenza: ogni passeggero è trattato con un pre-giudizio di pericolosità [92], che induce a confrontare i suoi dati personali con quelli contenuti in altri *database* utilizzati in ambito criminalistico ed a valutarli alla luce di predeterminati (ma sconosciuti) criteri di rischio. Ciascuna persona, per la sola ragione di spostarsi per via aerea in ambito europeo o al di fuori dell'Unione, diviene potenziale sospetto di reati (passati o futuri).

Noti sono i rischi di un'archiviazione di massa di tal fatta. L'utilizzo, in funzione delle investigazioni

[87] Cfr. i punti n. 199-202. Nello stesso senso si era espresso il *Parere* del Garante europeo della protezione dei dati del 24 settembre 2015, cit., punti nn. 42-46, nell'osservare che, in caso di richiesta di accesso ai dati da parte di un'autorità competente, si dovrebbe sempre ottenere un'autorizzazione preventiva di un tribunale o di un organo amministrativo indipendente, e che i casi legittimanti l'accesso dovrebbero essere tassativamente definiti.

[88] V. i punti n. 204-211.

[89] Cfr. E. Carpanelli-N. Lazzerini, *PNR: Passenger Name Record, Problems Not Resolved?*, cit., p. 395, secondo cui, tuttavia, sarebbe nella pratica complesso garantire che la conservazione sia limitata alla durata della permanenza nell'UE. Ciò richiederebbe un monitoraggio generale dei movimenti di cittadini e, dunque, l'interoperabilità tra il regime PNR e altri meccanismi che realizzano tale monitoraggio.

[90] Cfr. i punti n. 218-225.

[91] Il rischio in tal senso è ben evidenziato dal *Parere* del Garante europeo della protezione dei dati del 24 settembre 2015, cit., secondo cui «the development of such a system raises serious transparency and proportionality issues» and «it might lead to a move towards a surveillance society» (punto n. 30).

[92] Cfr. F. Rossi Dal Pozzo, *Protezione dei dati personali*, cit., p. 1054.

penali, di dati personali raccolti in maniera indiscriminata e riversati in schedari pubblici accresce la possibilità, per gli individui, di incappare, per sbaglio, nelle maglie della giustizia, di subire rilevanti restrizioni di libertà fondamentali (si pensi alle ricadute sulla libertà di circolazione derivanti dai sistematici controlli a cui dovessero essere sottoposti i cittadini europei nei voli *intra*-UE), di essere ingiustamente accusati di reati.

Il pericolo potrebbe essere generato da errori contenuti nelle banche dati adoperate per il raffronto, mai del tutto eliminabili per quante cautele si vogliano apprestare, così come potrebbe derivare dal controllo *ex ante* di tutti i passeggeri sulla scorta dei criteri elaborati attraverso l'uso proattivo dei dati [93]. L'analisi fondata su modelli e profili prefissati (funzionali, almeno in tesi, a svelare sospetti criminali o terroristi ancora ignoti) presenta, in effetti, significativi margini di errore [94], ampiamente riconosciuti anche dalla direttiva che, con riferimento ai criteri "predittivi", auspica che siano «definiti in maniera da ridurre al minimo il numero di *persone innocenti* erroneamente identificate dal sistema» (*considerando* n. 7). È, quindi, espressamente presa in considerazione ed accettata la possibilità di «falsi riscontri positivi» (art. 12, par. 5, direttiva e art. 10, comma 6, d.lgs. n. 53 del 2018).

Il sistema può, insomma, essere fallace. Certo, l'obbligo di un esame individuale dei risultati del trattamento ed il divieto di «decisioni automatizzate» sono diretti a ridimensionare il rischio. Ma, sicuramente, non permettono di escludere che persone vengano sottoposte a misure in qualche modo incidenti sui diritti di libertà per l'unico motivo di aver viaggiato a bordo di un aeromobile [95].

La possibilità che l'analisi delle "prenotazioni aeree" conduca all'adozione di provvedimenti con finalità preventiva o repressiva e determini l'avvio di procedimenti penali o di prevenzione induce, inoltre, ad interrogarsi sul regime di utilizzabilità delle informazioni trasmesse dai vettori e dei risultati del relativo trattamento.

Pare, invero, difficilmente contestabile che i dati PNR, per la loro capacità rappresentativa (di fatti, persone o cose) e per essere formati al di fuori di qualsivoglia contesto procedimentale, rientrino nella categoria della prova documentale, *sub specie* di «documenti informatici» [96]. Come tali sono pienamente utilizzabili, quanto ai procedimenti penali, sia nella fase delle indagini, che in dibattimento.

Il sistema PNR sembra funzionare, da questo punto di vista, come vero e proprio meccanismo di acquisizione e circolazione probatoria in ambito europeo [97]. Per un verso, l'Unità nazionale, a seguito di riscontri positivi, trasmette alle autorità competenti i dati ricevuti dalle compagnie aeree (o dalle UIP di altri Stati). Per altro verso, le autorità nazionali di contrasto possono richiedere i dati, nel corso di specifiche attività preventive o repressive, all'Unità nazionale o a quelle degli altri Paesi dell'Unione; in tale ul-

[93] Così G. Tiberi, *La direttiva UE sull'uso dei dati del codice di prenotazione*, cit., p. 592.

[94] Lo ha evidenziato, nel citato parere, la Corte di giustizia, riconoscendo che le analisi automatizzate dei passeggeri, nei limiti in cui sono effettuate a partire da dati personali non verificati e si fondano su modelli e criteri prestabiliti, presentano necessariamente un tasso d'errore che può essere «significativo» (punti n. 169 e 170).

[95] È ben noto che l'individuazione di un soggetto quale possibile autore del reato attraverso l'utilizzo della profilazione può provocare un «fenomeno di distorta interpretazione di ogni fonte di prova in senso convergente con l'avvenuta identificazione su base criminologica del soggetto», in un'ottica di «raccolta degli elementi probatori selettiva, ossia volta a corroborare una sola posizione, negando le altre». In questi termini e, più in generale, sui limiti epistemici del *criminal profiling* v., anche per ulteriori indicazioni bibliografiche, L. Lupària, *Il* profiling *dell'autore del reato*, in A. Scalfati (a cura di), *Le indagini atipiche*, Torino, Giappichelli, 2014, p. 340.

[96] Viene in rilievo, al riguardo, l'art. 1 della Convenzione di Budapest del 23 novembre 2001 sulla criminalità informatica (recepita con l. 18 marzo 2008, n. 48), che definisce il documento informatico come «qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione». Definizione analoga è contenuta nell'art. 1, comma 1, lett. *p*, d.lgs. 7 marzo 2005, n. 82 (codice dell'amministrazione digitale), secondo cui documento informatico è il «documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti». Il tema è oggetto di significativa attenzione da parte della dottrina. V., *ex multis*, M. Daniele, *La prova digitale nel processo penale*, in *Riv. dir. processuale*, 2011, p. 283 ss.; R. Del Coco, *L'utilizzo probatorio dei dati* whatsapp *tra lacune normative e avanguardie giurisprudenziali*, in *questa Rivista*, 2018, 3, p. 532 ss.; G. Di Paolo, voce *Prova informatica (diritto processuale penale)*, in *Enc. dir.*, Annali VI, Milano, Giuffrè, 2013, p. 736 ss.; L. Marafioti, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, p. 4509 ss.; M. Pittiruti, Digital evidence *e procedimento penale*, Torino, Giappichelli, 2017, p. 23 ss.; P. Tonini, *Documento informatico e giusto processo*, in *Dir. pen. proc.*, 2009, p. 401 ss.; F. Zacché, *La prova documentale*, Milano, Giuffrè, 2012, p. 26 ss.

[97] La finalità della trasmissione dei dati PNR dai vettori alle UIP e da queste alle autorità competenti comprende, del resto, non solo la «prevenzione», ma anche l'«indagine», l'«azione penale» e l'«accertamento», fini che connotano, inevitabilmente, di valore probatorio il meccanismo di acquisizione e scambio dei dati.

tima evenienza, la richiesta, di regola inoltrata tramite l'UIP nazionale, può essere formulata, in situazioni di emergenza, direttamente all'Unità d'informazione estera (artt. 12-16 d.lgs. n. 53 del 2018).

Anche quando il dato informatico è detenuto dall'autorità straniera, non è, pertanto, necessario ricorrere agli ordinari strumenti di acquisizione transnazionale della «prova» [98]. Il riferimento a «qualsiasi canale esistente di cooperazione internazionale di polizia» (art. 17 d.lgs. n. 53 del 2018) vale, in tale scenario, unicamente ad indicare i circuiti adoperabili per lo scambio dei dati.

La particolarità è che si tratta di un meccanismo acquisitivo "chiuso": solo le autorità individuate dalla legge come «competenti» possono richiedere ed ottenere la trasmissione dei dati; l'unica finalità per la quale sono comunicati è il contrasto al terrorismo e ai gravi reati tassativamente indicati. Deve escludersi che, al di fuori dei confini così tracciati, sia possibile, per altri soggetti o in procedimenti relativi a reati diversi, acquisire le informazioni del codice di prenotazione detenute dai vettori o dalle Unità d'informazione sui passeggeri[99].

Va osservato, però, che, nella misura in cui i dati PNR, adoperati in singole vicende, confluiscano in fascicoli processuali o in altri archivi nazionali (come il CED) o sovranazionali (si pensi all'archivio centralizzato di Europol), non sembrano esservi ostacoli a successivi utilizzi oltre i limiti rigorosamente tracciati dalla normativa [100]. Il che amplifica i rischi per le prerogative individuali coinvolte.

Più complesso è il discorso in ordine ai risultati del trattamento effettuato, in tempo reale, dall'Unità nazionale. Si tratta, in tal caso, di una complessa attività di analisi – tipizzata, con riguardo al trattamento automatizzato, ed atipica, per il successivo esame individuale (art. 8, commi 1 e 4, d.lgs. n. 53 del 2018) – compiuta da un organo che, per composizione e collocazione, è posto al vertice dell'apparato statale della pubblica sicurezza.

Alcuna natura documentale può essere riconosciuta alle relative risultanze, che sono, invece, il frutto di verifiche aventi carattere *lato sensu* investigativo, precipuamente rivolte ad «individuare i passeggeri sospettati di essere implicati in reati di terrorismo o in reati gravi» (art. 6, comma 2, lett. *b*, d.lgs. n. 53 del 2018). Non si configurano, dunque, in termini meramente amministrativi, quanto, piuttosto, come operazioni propedeutiche ad allertare gli organi competenti, in vista dell'accertamento di reati o, comunque, della neutralizzazione di possibili fonti di pericolo [101].

Ciò è reso palese dalla stessa normativa interna, che prevede la conservazione dei risultati del trattamento solo «per il tempo strettamente necessario a comunicare gli esiti di eventuali riscontri positivi alle autorità competenti nazionali». Sicché, eseguita l'informazione, vanno definitivamente cancellati (art. 10, comma 6, d.lgs. n. 53 del 2018) [102].

I «riscontri positivi», secondo la terminologia, certamente più pregnante, adoperata dal legislatore nazionale, hanno la valenza di meri elementi di «sospetto» [103], di per sé inidonei sia a legittimare inizia-

[98] La tendenza a superare, in materia di dati informatici, i tradizionali meccanismi della cooperazione europea ed internazionale pare confermata dall'art. 234-*bis* c.p.p. (introdotto dal d.l. n. 43 del 2015) che, sia pure con una formulazione non del tutto chiara, sembra instituire uno strumento derogatorio rispetto agli ordinari circuiti di circolazione della prova. Sul tema v., *ex multis*, S. Aterno, *L'acquisizione di dati personali tra misure antiterrorismo e intromissioni nella privacy*, in *Arch. pen.*, 2016, 1, p. 165 ss.

[99] La nuova normativa, in quanto *lex specialis*, induce a ritenere precluso agli organi investigativi disporre perquisizioni e sequestri informatici, nei confronti delle compagnie aeree, volti a reperire ed apprendere dati PNR. In giurisprudenza, in ogni caso, è stata esclusa la legittimità del provvedimento di perquisizione e sequestro delle credenziali di accesso al sistema informatico di prenotazione dei voli *on line* di una compagnia aerea finalizzato ad identificare per tempo i passeggeri sospettabili di fungere da corrieri internazionali di stupefacenti, trattandosi di provvedimento preordinato non già ad acquisire elementi di conoscenza in ordine ad una o più *notitiae criminis*, quanto a monitorare in modo illimitato, preventivo e permanente il contenuto di un sistema informatico onde pervenire all'accertamento di reati non ancora commessi (cfr. Cass., sez. IV, 17 aprile 2012, n. 19618, in *Cass. pen.*, 2013, p. 1148 ss. In dottrina v. G. Bono, *Il divieto di indagini* ad explorandum *include i mezzi informatici di ricerca della prova*, in *Cass. pen.*, 2013, p. 1525 ss.).

[100] Lo si ricava dal disposto dell'art. 10, commi 5 e 7, d.lgs. n. 53 del 2018, che, da un lato, prevede, per i dati utilizzati «nell'ambito di un caso specifico», la conservazione nel rispetto delle disposizioni del c.p.p. o di quelle riguardanti i trattamenti per finalità di polizia o di *intelligence* e, dall'altro, con riferimento a quelli riversati nel CED, l'applicazione delle relativa disciplina.

[101] L'attività di trattamento dei dati PNR, prima dell'emergere di una notizia di reato, difficilmente potrebbe essere qualificata come «ispettiva e di vigilanza» *ex* art. 220 norme att. c.p.p. (alle cui risultanze viene, generalmente, riconosciuta natura documentale), essendo istituzionalmente compiuta nella prospettiva di un'indagine penale. In dottrina si è efficacemente osservato che, quando un'attività preventiva venga «*sistematicamente* posta in essere in vista di indagini penali, quella stessa attività preventiva si salda funzionalmente all'attività repressiva mutando così la propria natura» (R. Orlandi, *Inchieste preparatorie*, cit., p. 583, nota 47).

[102] Salva la necessità di conservarli al solo fine di «assicurare l'esattezza di futuri riscontri» (art. 10, comma 6).

[103] La disciplina interna, a differenza della direttiva, contiene la puntuale definizione di «riscontro positivo» («l'individuazio-

tive di pubblica sicurezza, sia, soprattutto, a perfezionare una notizia di reato [104]. Dalla legge di attuazione traspare, in maniera più netta rispetto al tenore della direttiva, la necessità che i dati trasmessi siano sottoposti, dalle autorità di polizia e giudiziarie che li ricevono, ad «ulteriore trattamento», quale *condicio sine qua non* per adottare «provvedimenti idonei a prevenire e reprimere reati di terrorismo o reati gravi» (art. 12, comma 1, d.lgs. n. 53 del 2018).

In cosa debba (o possa) consistere tale ulteriore trattamento non è specificato. Parrebbe trattarsi di attività atipica di analisi, valutazione e indagine, avente ad oggetto le informazioni comunicate dall'Unità nazionale e tesa a verificare la fondatezza dei sospetti emersi.

Sbocchi potrebbero essere: interventi di pubblica sicurezza (che, tuttavia, per espresso dettato legislativo, non possono pregiudicare il diritto di entrare nel territorio dello Stato delle persone che godono del diritto di libera circolazione all'interno dell'Unione) [105]; la raccolta di indizi idonei ad avviare un procedimento di prevenzione o ad integrare una vera e propria notizia di reato, con conseguente formale inizio delle indagini preliminari.

Nel meccanismo congegnato, l'acquisizione della *notitia criminis* si presenta, dunque, come fattispecie a formazione progressiva, in cui si saldano le analisi in tempo reale compiute dall'UIP e l'ulteriore trattamento effettuato dalle autorità di *law enforcement*.

Le prime, nell'ottica dell'accertamento penale, hanno il carattere di operazioni di «*intelligence* criminale», collocandosi nella «fase procedurale precedente all'indagine penale, nella quale un'autorità competente incaricata dell'applicazione della legge, ai sensi della legislazione nazionale, ha facoltà di raccogliere, elaborare e analizzare informazioni su reati o attività criminali al fine di stabilire se sono stati commessi o possono essere commessi in futuro atti criminali concreti» [106]. L'esito positivo dell'incrocio informatizzato dei dati e dell'applicazione di criteri di rischio prefissati è indicativo, come detto, di un «sospetto», da avvalorare attraverso successive verifiche non automatizzate. Il riscontro fornito da queste ultime funge da fonte informativa per gli organi inquirenti, che permette di avviare le attività preprocedimentali (di valutazione dei dati e di indagine) dirette ad appurare se possa ravvisarsi una notizia di reato [107].

Gli atti di «ulteriore trattamento», compiuti da polizia giudiziaria o uffici del pubblico ministero, sono assimilabili, in tale schema, a quelli della pre-inchiesta volta alla ricerca della *notitia criminis* [108]. Nulla impedisce, al di fuori di espressi divieti di legge, che la relativa documentazione confluisca nel fascicolo delle indagini e sia utilizzata, non solo a fini investigativi, ma anche per le decisioni da assumere nei procedimenti cautelari, in udienza preliminare e nei riti alternativi.

Riflessioni specifiche s'impongono, tuttavia, con riguardo alle informazioni estratte dagli archivi nazionali o esteri adoperati per il raffronto. Potrebbe trattarsi di dati della più svariata natura, acquisiti nel

---

ne di un passeggero sospettato di essere implicato in un reato di terrorismo o in reati gravi, all'esito dell'attività di analisi dei dati PNR effettuata dall'UIP nazionale») e di «riscontro negativo» («l'esito dell'attività di analisi dei dati PNR effettuata dall'UIP nazionale in base alla quale un passeggero non è sospettato di essere implicato in un reato di terrorismo o in reati gravi») (art. 2, comma 2, lett. *o* e *p*).

[104] Evidenziano come non possa integrare una notizia di reato «il sospetto» o «il "teorema investigativo"», A.A. Dalia-M. Ferraioli, *Manuale di diritto processuale penale*, Milano, Cedam, 2018, p. 481. Sul concetto di sospetto quale «anello più "lontano" di quello indiziario nella catena che può condurre alla verifica dell'affermazione probatoria», assimilabile «ad una vera e propria ipotesi di ricerca», v. G. Ubertis, *Fatto e valore nel sistema probatorio penale*, Milano, Giuffrè, 1979, p. 118.

[105] Si tal senso si esprimono gli artt. 6, par. 9, direttiva, e 8, comma 5, d.lgs. n. 53 del 2018.

[106] È la definizione di «operazione di *intelligence* criminale» contenuta nell'art. 2, comma 1, lett. *c*, del d.lgs. n. 54 del 2015, attuativo della decisione quadro 2006/960/GAI.

[107] È ampiamente riconosciuta la possibilità di svolgere inchieste preparatorie finalizzate alla formazione della notizia di reato, che possono trarre spunto da «qualsiasi motivo di sospetto, non importa se ricavato da un documento anonimo, da un incrocio di dati, da un'indagine statistica o se altrimenti partorito da una fertile fantasia investigativa» (R. Orlandi, *Inchieste preparatorie*, cit., p. 587).

[108] Sul tema della c.d. pre-inchiesta per la ricerca della notizia di reato v., *ex multis*, R. Aprati, *La notizia di reato nella dinamica del procedimento penale*, Napoli, Jovene, 2010, p. 45 ss.; Ead. *Notizia di reato*, in G. Garuti (a cura di), *Indagini preliminari e udienza preliminari*, vol. 3, *Trattato di procedura penale*, diretto da G. Spangher, Torino, Utet, 2009, p. 33 ss.; F. Falato, *Sulla natura degli atti precedenti alla iscrizione della* notitia criminis *e sull'estensibilità del divieto previsto dall'art. 62 c.p.p.*, in *Cass. pen.*, 2005, p. 1626 ss.; G. Fumu, *L'attività preprocedimentale del pubblico ministero*, in A. Gaito (a cura di), *Accusa penale e ruolo del pubblico ministero*, Napoli, Jovene, 1991, p. 135 ss.; A. Marandola, *I registri del pubblico ministero tra notizia di reato ed effetti procedimentali*, Padova, Cedam, 2001, p. 89 ss.; P.P. Paulesu, *Notizia di reato e scenari investigativi complessi: contrasto alla criminalità organizzata, operazioni «sotto copertura», captazione di dati digitali*, in *Riv. dir. processuale*, 2010, p. 787 ss.; D. Potetti, *Attività del p.m. diretta all'acquisizione della notizia di reato e ricerca della prova*, in *Cass. pen.*, 1995, p. 139 ss.; A. Zappulla, *La formazione della notizia di reato*, Torino, Giappichelli, 2012, p. 24 ss.

corso di attività di *intelligence*, di inchieste preventive, di indagini penali o risultanti da provvedimenti giudiziari. Se alcun ostacolo si frappone al loro impiego per orientare l'azione investigativa, disporre il compimento di atti tipici d'indagine, adottare mezzi di ricerca della prova, ne andrebbe, invece, esclusa la diretta rilevanza negli incidenti cautelari e nei riti alternativi, in cui il giudice è chiamato a rendere una decisione che ingloba un giudizio sulla responsabilità dell'indagato o dell'imputato. In questi casi, il convincimento deve fondarsi su atti che, pur non formati in contraddittorio, richiedono il rispetto di ben precise formalità. Ciò impone, da un lato, di acquisire la documentazione dell'attività da cui è scaturita l'informazione inserita nel *database*, attraverso il ricorso, qualora in possesso di autorità estera, agli strumenti di assistenza giudiziaria; dall'altro, di appurarne, caso per caso, natura e regime di utilizzabilità [109].

Indicazioni in tal senso si ricavano anche dalla normativa regolante il Centro di elaborazione dati del Ministero dell'interno: è espressamente stabilito che i dati e le informazioni ivi conservate «possono essere utilizzati in procedimenti giudiziari o amministrativi soltanto attraverso l'acquisizione delle fonti originarie» (art. 10, comma 2, l. n. 121 del 1981). La norma ha la portata di principio generale e, come tale, è agevolmente estensibile a tutte le informazioni riversate in banche dati e trattate in modo automatizzato [110].

Per quanto attiene all'utilizzabilità dibattimentale, la regola del contraddittorio nella formazione della prova non consente di attribuire valenza probatoria né alle risultanze del «trattamento» dei dati PNR (che, dunque, potrebbero entrare nella sfera cognitiva del giudice solo attraverso l'assunzione degli ordinari mezzi di prova) [111], né alle informazioni ricavate dagli archivi nazionali o stranieri, salvo i casi in cui la legge – alla luce delle deroghe contemplate dall'art. 111, comma 5, Cost. o del carattere *stricto sensu* documentale dell'atto – ne permetta l'acquisizione e sempreché, in caso di elementi ottenuti oltre confine, siano rispettate le forme previste dai meccanismi deputati alla circolazione delle prove [112].

I dati PNR, invece, stante la loro natura di «documenti», hanno, lo si è detto, pieno valore di «prova»: una volta acquisiti nel procedimento penale, «sono conservati nel rispetto delle disposizioni del codice» e, dunque, in deroga alla regola generale che ne prevede il mascheramento dopo sei mesi e la cancellazione trascorsi cinque anni (art. 10, comma 5, d.lgs. n. 53 del 2018).

Né divieti di utilizzo derivano dal principio di finalità limitata. Ben vero è che l'«ulteriore trattamento» va effettuato «unicamente al fine specifico di prevenire, accertare, indagare o perseguire reati di terrorismo o reati gravi» (art. 7, par. 4, direttiva), sicché le analisi e le investigazioni, conseguenti al riscontro positivo dell'Unità nazionale, devono essere orientate verso tale, unico obiettivo. Ciò, però, non limita l'impiego processuale dei dati del codice di prenotazione qualora dagli esiti di queste attività emergano indizi di reati ulteriori e diversi [113].

---

[109] In giurisprudenza se, da un lato, si afferma che, ai fini dell'adozione di provvedimenti cautelari nella fase delle indagini preliminari, possono essere utilizzati, anche al di fuori dei limiti stabiliti dagli artt. 238 c.p.p. e 78 norme att. c.p.p., atti compiuti autonomamente da autorità straniere in un diverso procedimento penale all'estero (Cass., sez. I, 22 gennaio 2009, n. 21673, in *Cass. pen.*, 2010, p. 1072), dall'altro, si è rimarcato come non sia consentita l'utilizzabilità di una documentazione che si risolva in una relazione riassuntiva degli atti compiuti e dei risultati acquisiti e non in una copia legale di essi, venendo meno, in tal caso, «la possibilità della verifica della compatibilità della procedura con i principi basilari dell'ordinamento nazionale» e «rimanendo sostanzialmente preclusa la doverosa valutazione degli elementi probatori acquisiti» (così Cass., sez. I, 25 giugno 1990, n. 2006, in *Cass. pen.*, 1991, p. 260). Ad ogni modo, la prassi interpretativa tende a riconoscere che siano pienamente utilizzabili le informative redatte dalla polizia estera e da questa consegnate direttamente ad autorità di polizia italiane, al di fuori di procedure formali di rogatoria (Cass., sez. II, 28 novembre 2013, n. 51127, in *CED Cass.*, n. 258221), purché si tratti di atti compiuti nel rispetto dei valori fondamentali del nostro ordinamento (Cass., sez. I, 20 febbraio 2014, n. 37250, in *CED Cass.*, n. 260588).

[110] Cfr., sul tema, M. Gialuz, *Banche dati europee e procedimento penale italiano*, in F. Peroni-M. Gialuz (a cura di), *Cooperazione informativa*, cit., p. 258, il quale riconduce la regola al «diritto al controllo della fonte di informazione» e, dunque, al «principio generale che esclude l'utilizzazione di elementi di prova di fonte ignota».

[111] Cfr. R. Aprati, *Notizia di reato*, cit., p. 41, che, in relazione alla pre-inchiesta volta alla ricerca della notizia di reato, chiarisce che «la documentazione di tali attività non potrà rifluire di per sé fra gli atti probatori processuali».

[112] Per quanto riguarda gli atti compiuti nel corso di inchieste amministrative all'estero, si ritiene, generalmente, che la loro acquisizione non sia soggetta al regime delle rogatorie e che siano pienamente utilizzabili in dibattimento (cfr., da ultimo, Cass., sez. VI, 2 luglio 2012, n. 30068, in *CED Cass.*, n. 253273). In dottrina, tuttavia, con particolare riferimento ai dati provenienti da attività di polizia amministrativa o da inchieste di *intelligence* criminali, trattandosi di elementi destinati *ab origine* all'accertamento penale, si ritiene che possano essere acquisiti come documenti solo se costituiscono veicolo di conoscenze non altrimenti acquisibili al processo per l'impossibilità di assumere oralmente la fonte in dibattimento (così si esprime M. Gialuz, *Banche dati europee*, cit., p. 256; v., anche, R. Orlandi, *Atti e informazioni dell'autorità amministrativa nel processo penale*, Milano, Giuffrè, 1992, p. 146).

[113] In tal senso pare doversi interpretare l'art. 7, par. 5, della direttiva, a tenore del quale l'ulteriore trattamento operato dalle autorità competenti «non pregiudica le competenze delle autorità di contrasto e giudiziarie nazionali qualora siano individuati

Non è, comunque, possibile adottare decisioni che determinino conseguenze giuridiche negative per l'interessato sulla base di un mero trattamento automatizzato (art. 12, comma 2, d.lgs. n. 53 del 2018). La previsione, che pare istituire una regola di valutazione della prova, più che di esclusione, si pone, chiaramente, a tutela dei diritti di libertà e di difesa e mira ad evitare che il convincimento sia fondato, in via esclusiva, sul *profiling* [114]. Il concetto di «decisione» andrebbe, qui, inteso in senso ampio, comprensivo non solo dell'attività giurisdizionale, ma anche delle determinazioni degli organi inquirenti inerenti al compimento di atti incidenti su prerogative individuali (si pensi ai mezzi di ricerca della prova) o all'esercizio dell'azione penale.

Considerazioni in parte differenti sollecita l'evenienza in cui, durante un procedimento in corso, avente ad oggetto reati di terrorismo o altri gravi reati, le autorità di polizia o giudiziarie richiedano la trasmissione ed il trattamento di dati PNR (art. 6, par. 2, lett. *b*, direttiva e artt. 6, comma 2, lett. *c*, e 12, comma 1, d.lgs. n. 53 del 2018). L'iniziativa, in tal caso, si inscrive nel pieno dell'attività d'indagine preliminare ed ha il valore, quanto ai dati PNR, di acquisizione documentale, quanto invece al trattamento (compiuto dall'Unità nazionale e dall'organo ricevente), di atto di indagine, sia pure atipico nei contenuti [115].

Certo, per i diritti che vi sono implicati, la richiesta rivolta all'UIP dovrebbe essere contornata, come anticipato, da maggiori garanzie sostanziali e procedurali, attraverso la puntuale tipizzazione dei presupposti che la legittimano (quali, i gravi indizi di reato e la necessità ai fini delle indagini) e la preventiva autorizzazione del giudice [116]. Ma non c'è dubbio che si tratti di modalità più ragionevole di utilizzo delle informazioni tratte dalle prenotazioni dei voli, che ne limita l'accesso a situazioni specifiche, in cui siano già emersi indizi di reato, evitando, così, le analisi sistematiche e l'elaborazione di profili, proprie di una logica "preventiva" fortemente invasiva per i diritti fondamentali e che, rivolta nei confronti di soggetti mai sospettati, potrebbe risultare sproporzionata anche rispetto all'obiettivo della lotta al terrorismo.

altri reati o indizi di reato durante l'azione di contrasto determinata da tale trattamento». La previsione non è stata oggetto di specifica trasposizione nel decreto legislativo attuativo della direttiva «in virtù del generale principio del nostro sistema processuale per il quale, in assenza di specifici divieti, le informazioni possono essere utilizzate per le finalità, alle condizioni e con le modalità previste dalle pertinenti disposizioni in vigore» (così si esprime la *Relazione illustrativa*, cit., p. 10). La possibilità che i dati PNR, una volta trasmessi alle autorità competenti, possano essere utilizzati anche per reati diversi da quelli di terrorismo o di altri gravi reati era stata oggetto di specifica critica nel *Parere* del Garante europeo della protezione dei dati del 24 settembre 2015, cit., punto n. 43.

[114] Cfr., al riguardo, A. Vedaschi, *The European Court of Justice*, cit., p. 14. Evidenzia la necessità di vietare qualsiasi utilizzo probatorio dei risultati del trattamento automatizzato, «dal momento che la sua scientificità non appare validabile», L. Pulito, *Il trattamento dei dati personali in ambito penale*, cit., p. 1148.

[115] È da evidenziare che, con riguardo al trattamento compiuto dall'UIP su richiesta dell'autorità competente, non sono richiamate le modalità tipiche di trattamento previste in sede di controllo in tempo reale dall'art. 8 d.lgs. n. 53 del 2018, né è previsto il limite alla conservazione dei risultati per il tempo strettamente necessario ad informare gli organi competenti.

[116] Occorre rilevare come non appaia in linea con le indicazioni provenienti dalla giurisprudenza sovranazionale e con la valenza che, in un'epoca digitale e interconnessa, assume la tutela della *privacy* e della protezione dei dati, l'orientamento della giurisprudenza interna teso ad affermare che la riservatezza sarebbe «tutelata costituzionalmente soltanto in via mediata», quale componente della libertà personale, della libertà di domicilio e della libertà e segretezza della corrispondenza e di ogni forma di comunicazione (Cass., sez. un., 24 settembre 2003, n. 36747, in *CED Cass.*, n. 225466), o che il diritto alla riservatezza, per quanto riconducibile nell'alveo dell'art. 2 Cost., non godrebbe di una tutela analoga a quella apprestata per gli altri diritti fondamentali (Cass., sez. un., 28 marzo 2006, n. 26795, in *Cass. pen.*, 2006, p. 3037). Su questa scia si ritiene sufficiente il decreto motivato del magistrato del pubblico ministero (anziché l'autorizzazione del giudice), ad esempio, in tema di acquisizione dei tabulati telefonici (C. cost., sent. 11 marzo 1993, n. 81, in *Giur. cost.*, 1993, p. 731), di registrazioni clandestine ad iniziativa della polizia giudiziaria (*ex multis*, Cass., sez. IV, 11 luglio 2017, n. 48084, in *Cass. pen.*, 2018, p. 598) o di videoriprese investigative in luoghi riservati, ancorché non costituenti domicilio (Cass., sez. un., 28 marzo 2006, n. 26795, cit.).