PNR EU-Canada, la Corte di Giustizia blocca l'accordo: tra difesa dei diritti umani e implicazioni istituzionali

di Chiara Graziani

Title: The EU-Canada PNR agreement rejected by the Court of Justice: between human rights protection and institutional implications

Keywords: PNR data; Antiterrorism; Data protection.

1. – Con il parere in commento, la Corte di Giustizia dell'Unione europea si è pronunciata sul progetto di accordo fra il Canada e l'Unione europea in merito al trasferimento e al trattamento dei dati PNR (*Passenger Name Record*) ritenendolo *in parte qua* contrastante con alcune disposizioni della Carta dei diritti fondamentali dell'Unione europea (d'ora in poi "la Carta"). Il parere era stato richiesto dal Parlamento europeo il 30 gennaio 2015, ai sensi dell'art. 218, par. 11, del Trattato sul funzionamento dell'Unione europea (d'ora in poi TFUE), in base al quale il Parlamento è tra i soggetti legittimati a domandare l'*opinion* della Corte di Giustizia sulla compatibilità con i Trattati di accordi negoziati tra l'Unione e paesi terzi. Il parere negativo impedisce l'entrata in vigore dell'accordo, che deve essere pertanto modificato. È esattamente quanto accaduto nella circostanza di specie, poiché, a causa della rilevata incompatibilità di alcune clausole con i parametri invocati – in particolare, gli articoli 7 e 8 della Carta – una rinegoziazione dell'accordo – e probabilmente, come si vedrà, non solo di questo – si renderà indispensabile.

Prima di analizzare il parere, è opportuno fornire alcune nozioni preliminari essenziali. Innanzitutto, come detto, l'accordo oggetto della pronuncia verte sullo scambio di dati PNR tra Europa e Canada. Tali dati sono costituiti da informazioni personali (nome, data di viaggio, itinerario, posti assegnati, modalità di pagamento ecc.), risultanti dal codice di prenotazione, relative a passeggeri di voli aerei, che vengono raccolte e conservate dai vettori. Il trasferimento dei dati può avvenire secondo due criteri alternativi: da un lato, si ha il metodo c.d. *pull*, in base al quale le autorità statali competenti per la raccolta e il trattamento dei dati hanno accesso diretto a questi ultimi, senza nessun coinvolgimento dei vettori aerei; dall'altro, vi è il metodo *push*, il quale non garantisce alle dette autorità un accesso diretto, ma i dati devono essere preventivamente richiesti ai vettori aerei.

Tralasciando i tecnicismi sul metodo di trasferimento – che, tra l'altro, come si vedrà, tende verso l'impiego del metodo *push*, considerato più garantistico – appare necessario sottolineare che, negli ultimi anni, la raccolta e l'analisi dei dati PNR ha giocato un ruolo chiave nell'ambito della lotta al terrorismo e alla criminalità transfrontaliera (v. in generale C.C. Murphy, *EU Counter-Terrorism Law: Pre-Emption and the Rule of Law*, Oxford, 2012, 147 ss.). In effetti, i dati in questione si rivelano particolarmente utili, per le autorità che svolgono azione di contrasto ai detti crimini, ai fini dello svolgimento di un'azione preventiva. Infatti, la raccolta avviene nei confronti di *tutti* i passeggeri, a prescindere da eventuali sospetti di coinvolgimento in attività terroristiche. Questo permette un

monitoraggio indiscriminato di coloro che viaggiano su tratte internazionali e, di conseguenza, tramite uno *screening* che può essere definito "seriale", l'individuazione di soggetti potenzialmente criminali, anche qualora manchino segnalazioni di indizi a loro carico. È evidente che l'adozione di una strategia preventiva di contrasto al terrorismo basata sull'utilizzo dei PNR – a prescindere dalla compatibilità con le garanzie individuali – implica cooperazione tra le autorità dei vari Stati coinvolti (cfr. V. Mitsilegas, *Transatlantic counterterrorism cooperation and European values: the elusive quest for coherence*, in E. Fahey, D. Curtin (eds.), *A Transatlantic Community Law*, Cambridge, 2014, 289).

2. – E, in effetti, a livello UE diversi provvedimenti sono stati adottati al fine del miglioramento e rafforzamento della lotta al terrorismo e alla criminalità transfrontaliera tramite l'utilizzo di questi dati. Si pensi solo, da ultimo, alla direttiva 2016/681, approvata nell'aprile 2016 e volta a regolare lo scambio di dati PNR dei passeggeri di voli internazionali che hanno come destinazione o origine un paese UE (si veda sul tema D. Lowe, *The European Union Passenger Name Record Data Directive: Is is Fit for Purpose?*, in 17 *Int'l Crim. L. Rev.* 78 (2017)). In particolare, i vettori aerei vengono obbligati a fornire i dati alle competenti autorità degli Stati membri e sono stabilite, da un lato, una serie di regole relative al loro trattamento e utilizzo e, dall'altro, un novero di garanzie individuali per i passeggeri. La direttiva deve essere recepita entro il 25 maggio 2018.

Quando, invece, si tratta di regolare l'utilizzo di dati PNR non da parte di Stati membri UE, bensì per mano di autorità di paesi terzi, il paese verso il quale i dati verranno trasferiti deve assicurare un "livello di protezione adeguato" dei dati personali, a norma dell'art. 25 della direttiva 95/46/CE. L'adeguatezza del livello di protezione può essere certificata da una decisione della Commissione europea (c.d. decisione di adeguatezza), basata anche sulle garanzie fornite dal diritto interno del paese in questione oppure sull'esistenza di un accordo tra il paese terzo e l'Unione europea. Per questo motivo, l'Unione ha stipulato, nel corso del tempo, vari accordi internazionali con diversi paesi proprio al fine di consentire lo scambio di dati PNR (si veda, per una ricostruzione dettagliata del tema, 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 (eds.), *Surveillance, Privacy and Transatlantic Relations*, Oxford, 2017, 67). Risale al 2004 la firma del primo accordo in tal senso con gli Stati Uniti, in cui, in seguito agli eventi del settembre 2001, era stata approvata una legge che obbligava tutti i vettori aerei a trasferire i dati PNR alla competente autorità statunitense (*US Customs and Border Control*). Tale accordo venne invalidato dalla Corte di Giustizia nel 2006, a seguito della richiesta del Parlamento europeo di annullare la decisione di adeguatezza della Commissione e la decisione del Consiglio sulla conclusione dell'accordo. Di conseguenza, l'accordo fu rinegoziato al fine di giungere, nel 2007, ad una nuova versione (con la quale, tra l'altro, si passava dal metodo *pull* al metodo *push*), anch'essa successivamente sottoposta a rinegoziazione su richiesta del Parlamento europeo. L'attuale testo dell'accordo USA-UE relativo ai PNR è in vigore dal 2012, così come un analogo accordo sul tema con l'Australia (una precedente versione risaliva al 2008). Sono ancora in corso i negoziati per la stipulazione con il Messico, mentre potrebbero iniziare quelli con l'Argentina.

Anche l'accordo con il Canada, oggetto del parere che si commenta, non è il primo a cui l'Unione europea è addivenuta con tale paese terzo: il precedente accordo PNR UE-Canada era datato 2006 e riguardava, oltre allo scambio dei dati PNR, anche quello dei dati API (acronimo di *Advance Passenger Information*, ossia informazioni ulteriori raccolte al momento dell'imbarco). Si trattava di un accordo con un periodo di validità limitato (settembre 2009), per cui, alla sua scadenza, nuovi negoziati dovettero essere intrapresi. A questo punto, la "storia" dell'accordo PNR tra Unione europea e Canada si interseca con quella relativa all'accordo con gli Stati Uniti e con il Messico. Infatti, si è prima detto che l'accordo con gli Stati Uniti risalente al 2007 fu rinegoziato a seguito di richiesta del Parlamento europeo. Ebbene, è proprio con la stessa risoluzione (Parlamento europeo, Risoluzione 5 maggio 2010) che tale richiesta venne estesa anche in relazione al Canada, nel

cui ordinamento giuridico la comunicazione dei dati PNR alla competente autorità è imposta dal *Customs Act* e dall'*Immigration and Refugee Protection Act*, e all'Australia. Nel dicembre 2010 il Consiglio, tramite una propria decisione, autorizzò la Commissione all'apertura dei negoziati tra l'Unione europea e il Canada per la stipulazione dell'accordo. Tale fase giunse a termine nel maggio 2013, mentre è del luglio 2013 la proposta, presentata dalla Commissione, per una decisione del Consiglio sulla conclusione dell'accordo, conformemente alla procedura per l'adozione di accordi internazionali tra l'Unione e Stati terzi, poi adottata nel dicembre dello stesso anno. Seguì la firma dell'accordo il 25 giugno 2014. Nel tempo intercorrente tra la presentazione della proposta di decisione e la relativa adozione da parte del Consiglio, il Garante europeo della protezione dei dati aveva espresso il proprio parere sulla proposta stessa. In tale circostanza, il Garante aveva sollevato molti dei rilievi poi riproposti dal Parlamento europeo. In particolare, il parere si soffermava, da un punto di vista formale, sulla scelta della base giuridica per la decisione del Consiglio (su cui v. *infra*), mentre, da una prospettiva sostanzialistica, metteva in dubbio la necessità e la proporzionalità dell'accordo. Tra i rilievi fatti emergere si segnalano, in quanto coincidono con quelli presentati dal Parlamento europeo, su cui, quindi, si è pronunciata la Corte: la vaghezza nella definizione di alcuni concetti; la mancanza di un sistema di notifica individuale; la parziale inadeguatezza dei meccanismi di vigilanza.

3. – È quindi in questo complesso scenario che si inserisce la richiesta di parere del Parlamento europeo (al quale, a sua volta, il Consiglio aveva richiesto l'approvazione dell'accordo), presentata a gennaio 2015. Nello specifico, si rinvengono due profili: da un lato, viene chiesto di determinare l'appropriatezza della base giuridica della decisione del Consiglio relativa all'adozione dell'accordo; dall'altro, si interroga la Corte sulla compatibilità delle misure previste dall'accordo con gli artt. 16 TFUE (protezione dei dati personali), 7, 8 e 52 della Carta (rispettivamente: diritto alla *privacy*, diritto alla protezione dei dati personali, principio di proporzionalità).

Prima di ricostruire il ragionamento che ha portato la Corte di Giustizia a rilevare il contrasto fra alcune clausole dell'accordo e i parametri invocati, è il caso di ricordare che, l'8 settembre 2016, l'Avvocato Generale Paolo Mengozzi aveva presentato le proprie conclusioni relativamente al caso. In tale circostanza, l'Avvocato Generale aveva sconsigliato l'adozione dell'accordo nella forma in cui era stato presentato all'esame della Corte. Infatti, pur non escludendo la possibilità di rendere l'accordo compatibile con le disposizioni della Carta, Mengozzi rilevava che, per far ciò, sarebbe stato necessario intervenire in senso modificativo su varie clausole. Per molti aspetti, la decisione della Corte ha aderito alle conclusioni dell'Avvocato Generale.

Concentrandosi sul parere, esso può essere suddiviso in due parti. A prescindere dall'attenta ricostruzione del *background* fattuale e giuridico, la Corte si è concentrata anzitutto sulla risoluzione della questione relativa alla base giuridica, per poi passare – e si tratta della sezione più ampia ed articolata della decisione – alla compatibilità delle clausole dell'accordo con i diritti fondamentali.

In via preliminare, la Corte di Giustizia ha ribadito la piena idoneità degli accordi internazionali fra l'Unione e i paesi terzi ad integrare il diritto dell'Unione e, pertanto, la necessità che anch'essi rispettino i parametri fissati dai Trattati e dalla Carta, che ne ha acquisito lo stesso valore giuridico. A tal proposito, si osserva che è la prima volta che la Corte di Giustizia si pronuncia sulla compatibilità di un accordo internazionale con le disposizioni della Carta.

Per quanto riguarda la base giuridica, il Consiglio aveva fondato la propria decisione sugli artt. 82, par.1, lett. d) e 87, par. 2, lett. a) TFUE, rispettivamente relativi alla facilitazione della cooperazione tra autorità giudiziarie, o ad esse equivalenti, nelle materie penali con implicazioni sovranazionali e cooperazione di polizia tramite la raccolta, l'archiviazione e lo scambio di informazioni. A giudizio della Corte, che ha accolto sul punto la prospettazione del Parlamento europeo, combinandola con quanto suggerito dall'Avvocato Generale, la base giuridica corretta va rinvenuta nell'art. 16 TFUE (protezione dei dati

personali) e, al contempo, nell'art. 87 TFUE. L'esclusione dell'art. 82 TFUE è stata motivata sulla base del fatto che non si ravvisano, nel testo dell'accordo, disposizioni volte a facilitare la cooperazione giudiziaria, né, d'altra parte, l'autorità canadese competente è un'autorità giudiziaria o ad essa equivalente. Conformemente alla propria giurisprudenza pregressa, al fine di individuare la base giuridica dell'accordo, la Corte ha proceduto ad un'attenta analisi della finalità dell'accordo, utilizzando quindi uno schema di ragionamento teleologico. Nel caso di specie, ha chiarito come la finalità sia duplice, ossia il progetto di accordo miri, da un lato, al mantenimento della sicurezza pubblica, dall'altro alla protezione dei dati personali. Pur se presentata in sede di disquisizione sulla base giuridica, questa osservazione resta sullo sfondo dell'argomentazione successiva, anche in relazione agli altri punti, presentandosi come cruciale per chiarire da subito la necessità di bilanciare interessi opposti.

Soffermandosi sul secondo grande snodo argomentativo del parere, relativo alla compatibilità con i diritti fondamentali, si sottolinea che la Corte ha ritenuto di utilizzare come parametri solamente le disposizioni della Carta, escludendo, in relazione al diritto alla protezione dei dati personali, l'art. 16 TFUE, in quanto ha affermato il carattere maggiormente specifico dell'art. 8 della Carta, che si configura quindi come *lex specialis*. Anche in questo caso, si tratta di un passaggio importante, poiché fa sì che la decisione si inserisca nel contesto di quella giurisprudenza che utilizza la Carta come parametro a sé (v. *infra*), incrementandone il valore non solo formale – già datole dal Trattato di Lisbona, che la ha equiparata ai Trattati sotto il profilo del valore giuridico – ma anche sostanziale e pratico.

Lo schema seguito dalla Corte di Giustizia è quello classico utilizzato in casi in cui vengano in rilievo limitazioni dei diritti fondamentali: dapprima, viene determinata l'esistenza di un'interferenza delle misure sottoposte ad esame con i diritti in questione; in secondo luogo, ci si sofferma sull'appropriatezza dei mezzi a raggiungere il fine (che deve essere, chiaramente, legittimo e di interesse generale); da ultimo, si decide se le misure adottate si limitano a quanto strettamente necessario per raggiungere la finalità dichiarata (c.d. scrutinio di proporzionalità in senso stretto). Gli ultimi due punti sono strumentali, pertanto, a valutare se l'interferenza è giustificata o meno. Va sin da subito detto che, nel caso che si commenta, la Corte di Giustizia ha rilevato sia l'interferenza con i diritti fondamentali – è tale, infatti, un trasferimento sistematico di dati che possono «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, e potrebbero persino fornire informazioni sensibili su tali passeggeri» (p.to 128) – sia l'appropriatezza dei mezzi per raggiungere il fine. Sotto quest'ultimo profilo, la Corte ha utilizzato dati concreti: sono citate sia alcune informazioni fornite dalle autorità canadesi, sia documenti della Commissione (Comunicazione COM(2010) 492) in cui sono valutati i benefici prodotti dall'analisi dei PNR. Si tratta di un approccio che dimostra una certa "fiducia" della Corte di Giustizia nei confronti di altre istituzioni, europee e non. Si sottolinea, inoltre, il passaggio (p.to 149) nel quale la Corte ha esplicitamente enucleato la dialettica libertà-sicurezza, tramite il riferimento all'art. 6 della Carta. In proposito, si è rilevato che la sicurezza pubblica «costituisce, come risulta dalla giurisprudenza della Corte, una finalità d'interesse generale dell'Unione che può giustificare ingerenze, anche gravi, nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta. Del resto, la protezione della sicurezza pubblica contribuisce altresì alla tutela dei diritti e delle libertà altrui». Perciò, pur se nella sostanza della decisione la Grande Camera è apparsa propendere in favore dei diritti fondamentali, le premesse del bilanciamento appaiono segnate da forte carattere di realismo.

Il giudizio sulla necessità (quindi, sulla proporzionalità in senso stretto) delle misure, appare complesso e articolato, risultante di una sommatoria di vari fattori. La Corte ha analizzato se esistono regole chiare e precise, nel progetto di accordo ad essa sottoposto, rispetto ai seguenti elementi: categorie di dati PNR rientranti nell'ambito di applicazione dell'accordo; automatizzazione del trattamento; definizione di "reati di terrorismo" e di "reati gravi di natura transnazionale"; autorità canadesi competenti; passeggeri cui l'accordo si applica; conservazione dei dati; comunicazione degli stessi.

In prima battuta, è stata rilevata la mancanza di definizione quanto alle categorie di dati cui l'accordo si applica (v. p.to 157 ss.), non sanata dalla previsione, meramente

tautologica, secondo cui l'accordo non riguarda le categorie non elencate. Inoltre, la potenziale inclusione dei dati sensibili nelle categorie di dati trasferibili costituisce una forte criticità: come ricordato nel parere, essi non possono essere trasferiti se non in base ad una giustificazione particolarmente solida: nell'opinione della Corte, neanche l'esigenza di prevenzione del terrorismo può definirsi tale.

Si è sottolineato, poi, come il meccanismo di trattamento automatizzato dei dati PNR implichi un margine di errore, ma si è osservato anche che ciò ha correttamente indotto le parti dell'accordo a prevedere un riesame non automatizzato prima di adottare in concreto di misure individuali (p.to 173). Inoltre, ai fini dell'adozione di tali misure, questi dati vanno confrontati, stando all'accordo, con dati contenuti in *databases* canadesi relativi a persone sospettate di terrorismo, i quali dovrebbero essere, secondo la Corte di Giustizia, particolarmente affidabili, aggiornati e specifici. In questo passaggio, pertanto, la Corte si addentra in considerazioni piuttosto tecniche, confermando il carattere attento e approfondito dell'analisi.

Rispetto alle finalità di trattamento dei dati, ossia prevenzione dei reati di terrorismo e di altri gravi reati di natura transnazionale e altre finalità correlate alla salvaguardia di interessi vitali della persona, la definizione di queste ultime non è stata ritenuta sufficientemente chiara e precisa, facendo sì che, sotto questo profilo, le misure non siano limitate a quanto strettamente necessario (p.to 181).

I due punti la cui analisi risulta più interessante appaiono essere quelli legati alla conservazione dei dati (o *data retention*) e alla loro comunicazione.

Per quanto riguarda il primo aspetto, in via generale l'accordo prevede un periodo di conservazione massimo di cinque anni, ma già dopo trenta giorni dal momento della raccolta, i dati devono essere resi anonimi (con possibilità di de-anonimizzazione in caso di necessità). Inoltre, la conservazione e uso dei dati dei passeggeri viene messa in atto al loro arrivo in Canada, durante la loro permanenza sul territorio canadese, al momento della partenza e successivamente ad essa. Per quanto concerne i primi tre casi, la Corte ha ritenuto che la conservazione e uso dei dati PNR costituiscano mezzi idonei e non eccedenti i limiti di stretta necessità, con l'unica accortezza, nel caso dell'utilizzo durante il soggiorno in Canada, di garantire che esso sia giustificato da nuove circostanze (p.to 200), su cui un giudice o un'autorità amministrativa svolgano un controllo (p.to 202). Maggiori criticità, invece, sono legate all'uso dei dati dopo la partenza dei passeggeri dal Canada: è apparso superfluo archiviarli in maniera seriale e sistematica (in quanto si tratta di dati già controllati all'arrivo), a meno che non sussista un dimostrato rischio in termini di reati terroristici e di natura transnazionale (p.to 207). Hanno passato il vaglio di legittimità, invece, il periodo di conservazione e l'ambito territoriale, poiché quest'ultimo è esplicitamente delimitato dall'accordo al territorio canadese.

Rispetto al tema della comunicazione, la disciplina dell'accordo è tripartita: l'autorità canadese responsabile dei dati può comunicarli ad altra autorità canadese, ad autorità di paesi terzi, oppure, in circostanze particolari, a individui. In nessuno dei tre casi la disciplina è stata ritenuta limitata allo stretto necessario. Infatti, in caso di comunicazione ad autorità canadesi, si tratta pur sempre di un utilizzo dei dati, che deve essere posto in essere in coerenza con quanto detto rispetto al punto precedente al momento di analizzare l'aspetto della conservazione (p.to 212). La comunicazione ad autorità di paesi terzi costituirebbe un vero e proprio aggiramento delle garanzie poste dal diritto UE: essa viene prevista a prescindere dall'esistenza di qualsiasi accordo o decisione di adeguatezza della Commissione rispetto a tali paesi terzi, con palese violazione dell'art. 25 della direttiva 95/46/CE (p.to 214). Per quanto attiene, poi, alla comunicazione a individui – che, in effetti, costituisce *ictu oculi* l'aspetto più problematico della questione – essa è stata, di nuovo, censurata rispetto al canone della precisione e chiarezza: risulterebbero troppo vaghi e indefiniti il novero dei potenziali destinatari della comunicazione, le informazioni comunicabili, nonché i limiti e requisiti affinché si possa procedere. Infatti, l'accordo si limita a menzionare, piuttosto apoditticamente, «condizioni e limitazioni giuridiche ragionevoli» (p.to 216).

Altri due aspetti problematici sono stati rinvenuti nella mancanza di un sistema di notificazione individuale quando i dati PNR vengono utilizzati (p.to 225) e nel metodo di vigilanza sul rispetto delle garanzie sulla protezione dei dati. Quest'ultima attività dovrebbe

essere posta in essere, stando all'accordo, da un'autorità indipendente oppure che eserciti i propri compiti in modo imparziale. Tale formulazione linguistica alternativa fa sì che il meccanismo sia giudicato dalla Corte potenzialmente a rischio di mancanza di totale indipendenza da parte dell'autorità di vigilanza (p.to 230), poiché all'esercizio dei compiti in maniera imparziale potrebbe non corrispondere una piena autonomia effettiva.

4. – Ripercorsi i tratti essenziali del parere in esame, è opportuno soffermarsi su come esso si inserisca nella linea giurisprudenziale della Corte di Giustizia sul binomio *privacy*-sicurezza nazionale (tra le decisioni più importanti, sentenza 8 aprile 2014, *Digital Rights Ireland Ltd c. Ministro per le Comunicazioni e al.*, C-293/12 e C-594/12; sentenza 6 ottobre 2015, *Schrems c. Data Protection Commissioner*, C-362/14; sentenza 21 dicembre 2016, *Tele2 Sverige AB e al.*, C-203/15 e C-698/15).

La decisione si introduce a pieno titolo, da un punto di vista sostanziale, nel filone giurisprudenziale richiamato, in cui la Corte ha mostrato una chiara attitudine a far prevalere i diritti individuali (quelli alla *privacy* e alla protezione dei dati in particolare) sulle esigenze di sicurezza nazionale, purtuttavia senza mettere totalmente da parte queste ultime, anzi valorizzandole in un quadro di mantenimento delle garanzie democratiche (per un'analisi approfondita di come il parere in commento si inserisce nella dialettica libertà-sicurezza, da sempre oggetto di interesse degli studi costituzionalistici, si rinvia ad A. Vedaschi, *L'accordo internazionale sui dati dei passeggeri aviotrasportati (PNR) alla luce delle indicazioni della Corte di giustizia dell'Unione europea*, in corso di pubblicazione in *Giurisprudenza costituzionale*, 2017, n. 4). Ciò ha permesso alla CGUE di non indulgere ad un approccio eccessivamente utopistico, mantenendo ferma una visione pragmatica e concreta.

Sicuramente, il fatto che il parere in commento faccia perno, da un punto di vista logico e giuridico, sulla giurisprudenza pregressa, non è stato tenuto celato dalla Corte, che ha anzi ampiamente richiamato, in numerosi passaggi, i propri precedenti. Tuttavia, il parere è ben lungi dall'essere una decisione meramente confermativa o ricostruttiva di questi ultimi, in quanto, pur nella coincidenza delle affermazioni di principio, si possono scorgere rilevanti profili di novità.

Anzitutto, come già accennato, è la prima volta che la Corte ha dovuto pronunciarsi sulla compatibilità di un accordo internazionale fra l'Unione e uno Stato terzo con i parametri della Carta: ciò, se da un lato consolida l'utilizzo parametrico di quest'ultima (già osservato nei citati casi *Digital Rights*, *Schrems*, *Tele2 Sverige*, ma anche nella sentenza 13 maggio 2014, *Google Spain e al. c. AEPD e Costeja González*, C-131/12, relativa al diritto all'oblio; si veda sul tema O. Pollicino, M. Bassini, *La Carta dei diritti fondamentali dell'Unione europea nel* reasoning *dei giudici di Lussemburgo*, in G. Resta, V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali*, Roma, 2016) dall'altro pone enfasi sulla piena idoneità degli accordi internazionali ad essere considerati diritto UE. Ne risulta, chiaramente, un rafforzamento, non solo dogmatico, ma anche pratico, delle garanzie *lato sensu* costituzionali di matrice europea e del concetto dell'Unione come entità che garantisce la *rule of law*.

Quanto all'utilizzo dei precedenti in tema, la giurisprudenza sulla *data retention* (in primo luogo, la sentenza *Digital Rights*, con la quale la Corte aveva invalidato la direttiva 2006/24/CE, poi confermata, quanto alle affermazioni di principio, dalla decisione *Tele2 Sverige AB*) viene richiamata e applicata in maniera piuttosto puntuale. Infatti, se nella pronuncia *Digital Rights* si erano fissati i canoni generali in base ai quali la conservazione dei dati avrebbe potuto essere legittima, in questo parere sono stati analizzati snodi molto tecnici del progetto di accordo – si veda, ad esempio, la differenziazione fra conservazione prima dell'arrivo, durante la permanenza, al momento della partenza e dopo di essa. Pertanto, è come se venisse "data forma" ai principi enunciati in *Digital Rights* (per un'analisi dettagliata di quest'ultima decisione, si rimanda ad A. Vedaschi, V. Lubello, *Data Retention and its Implications for the Fundamental Right to Privacy: A European Perspective*, in *Tilburg Law Review* 14 (2015); v. anche A. Vedaschi, *I programmi di sorveglianza di massa nello Stato di diritto. La "*data retention*" al test di legittimità*, in *Diritto Pubblico Comparato ed Europeo*, 2014,

n. 3, 1224). Ciò deriva, probabilmente, anche dal diverso tipo di pronuncia. Nel caso in esame, infatti, si tratta di un parere ai sensi dell'art. 218 TFUE, il quale deve direttamente e concretamente orientare le istituzioni europee (in questo caso, alla rinegoziazione dell'accordo: sussiste perciò una *pars costruens* come diretta conseguenza). In *Digital Rights*, invece, si trattava di una questione pregiudiziale, che ha condotto a dichiarare l'invalidità direttiva sulla *data retention*, senza dover immediatamente e necessariamente orientare le istituzioni europee ad una celere approvazione di una nuova direttiva – tanto che, allo stato, non esiste una "nuova" direttiva *data retention*, per quanto vi siano riflessi della giurisprudenza *Digital Rights* nei successivi atti legislativi dell'Unione. Inoltre, ricorre spesso il tema dell'"adeguato livello di protezione", presupposto per il trasferimento di dati personali verso un paese non facente parte dell'Unione, sottoposto a stretto scrutinio nella sentenza *Schrems* (si veda, a commento, 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 12 *Eur. Const. L. Rev.* 318 (2016)). In questo parere, è stato rimarcato il carattere sostanziale di tale garanzia, che non può essere aggirata in maniera surrettizia: come sottolineato in sede di ricostruzione della decisione, non è legittima la comunicazione di dati PNR ad autorità di paesi terzi a prescindere da qualsiasi tipo di controllo sull'esistenza di un adeguato livello di garanzie. Perciò, l'eventuale accordo UE-Canada, sembra dire la Corte, non può funzionare da *passepartout* per permettere uno scambio indiscriminato di dati.

Da ultimo, si rileva che il parere in commento costituisce il primo caso in cui la Corte di Giustizia si è pronunciata negativamente in relazione ad un accordo sullo scambio di PNR adducendo motivazioni di carattere sostanziale e correlate ai diritti individuali. Infatti, anche nel 2006, nell'invalidare la decisione del Consiglio sull'accordo del 2004 con gli Stati Uniti, la Corte non aveva deciso sul merito, che pure era stato contestato da parte del Parlamento europeo nella richiesta di annullamento, preferendo invalidare l'accordo sulla base dei rilievi meramente formali – in particolare, mancanza di base giuridica – formulati dall'Avvocato Generale.

5. – In conclusione, può ritenersi che il parere in commento rivesta un'importanza fondamentale per due articolati ordini di ragioni.

Da un punto di vista teorico-generale, come visto, numerosi principi, elaborati nelle decisioni precedenti in materia di privacy e protezione dei dati personali, vengono applicati al particolare settore dei dati PNR e agli accordi internazionali tra l'Unione europea e gli Stati terzi. Pertanto, la Corte di Giustizia ha colto l'occasione, presentatasi con la richiesta di parere proveniente dal Parlamento europeo, di rafforzare la propria autorevolezza in materia di diritti. Ciò è stato fatto, peraltro, seguendo un approccio molto tecnicistico, se si pensa che dalla lettura della decisione emerge come la Corte, nell'analizzare la chiarezza e la precisione delle disposizioni dell'accordo, abbia sindacato anche la scelta di singoli termini e locuzioni.

Da un punto di vista più pragmatico, poi, si deve dire che la decisione avrà, probabilmente, rilevanti implicazioni che potrebbero essere definite "sistemiche". Innanzitutto, il fatto che la Corte abbia ritenuto l'art. 82 TFUE inadatto a formare la base giuridica per l'accordo potrebbe gettare dubbi sulla legittimità degli accordi per il trasferimento dei dati PNR, al momento in vigore, con l'Australia e gli Stati Uniti. Essi, inoltre, potrebbero dover essere rinegoziati anche da un punto di vista sostanziale, perché appaiono caratterizzati da molte delle criticità rilevate dalla Corte. Anche le negoziazioni degli accordi con il Messico, chiaramente, subiranno l'influenza di questa decisione, di cui dovranno tenere conto. Ciò era stato, in effetti, sottolineato anche dalle istituzioni europee, che nel 2015 avevano chiarito che i negoziati con il Messico non potevano essere finalizzati fino alla pronuncia che qui si commenta. Vieppiù, il fatto che la Corte abbia censurato i meccanismi di vigilanza sull'implementazione delle garanzie relative alla protezione dei dati potrebbe porre a rischio il c.d. *Privacy Shield*, ossia l'accordo, approvato nel 2016, che regolamenta il trasferimento di dati tra USA e Unione europea, criticato proprio in relazione

a questo aspetto (Article 29 Data Protection Working Party, Opinion 01/2016). Infine, altro tema rilevante lasciato aperto dal parere riguarda i rapporti tra il *decisum* esaminato e la direttiva PNR, da recepire entro il 2018. Infatti, se, da un lato, sembrerebbero non esserci rilevanti problemi di coordinamento, dato che la direttiva è anzi stata spesso citata come "modello" di una corretta gestione dello scambio dei dati PNR da parte della Corte (ad esempio, in relazione alla questione legata ai dati sensibili, si veda p.to 166), dall'altro alcune criticità rilevate dalla Corte appaiono essere proprie anche della direttiva (ad esempio, in tema di *data retention*, anche nella direttiva manca la differenziazione tra passeggeri in arrivo e passeggeri in uscita).

La decisione analizzata, pertanto, apre interessanti scenari e sarà rilevante osservare quali posizioni verranno fatte proprie in seguito dalle istituzioni dell'Unione.