Causa C-817/19**Sintesi della domanda di pronuncia pregiudiziale ai sensi dell'articolo 98, paragrafo 1, del regolamento di procedura della Corte di giustizia****Data di deposito:**

31 ottobre 2019

Giudice del rinvio:

Cour constitutionnelle (Belgio)

Data della decisione di rinvio:

17 ottobre 2019

Ricorrente:

ASBL «Ligue des droits humains»

I. Oggetto del ricorso e posizione delle parti

- 1 Il legislatore belga ha adottato la loi du 25 décembre 2016, relative au traitement des données des passagers (legge del 25 dicembre 2016, in materia di trattamento dei dati dei passeggeri) (*Moniteur belge* del 25 gennaio 2017; in prosieguo, anche: la «legge PNR») diretta, essenzialmente, a recepire:
 - la direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi (in prosieguo, anche: la «direttiva PNR»);
 - la direttiva 2004/82/CE del Consiglio, del 29 aprile 2004, concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate (in prosieguo, anche: la «direttiva API»).
- 2 La legge PNR prevede in diversi settori del trasporto internazionale di persone (aereo, ferroviario, stradale internazionale e marittimo) e in capo agli operatori di viaggio l'obbligo di trasmettere i dati dei rispettivi viaggiatori a una banca dati gestita dal Service public fédéral intérieur (Servizio federale pubblico dell'Interno, Belgio; in prosieguo: l'«SPF Intérieur»).

- 3 A tal fine, la legge istituisce, in seno all' SPF Intérieur, un' «unità d'informazione sui passeggeri» (articoli da 12 a 14) composta, in particolare, da membri distaccati dei servizi di polizia, di sicurezza dello Stato, segreti e di sicurezza e delle dogane e incaricata, segnatamente, della conservazione e del trattamento dei dati dei passeggeri trasmessi dai vettori e dagli operatori di viaggio.
- 4 La «banca dati dei passeggeri» contiene, da una parte, i dati relativi alle prenotazioni e, dall'altra, i dati di registrazione e di imbarco [detti «API» (Advance Passenger Information) e «PNR» (Passenger Name Record)] (articolo 9).
- 5 Tali dati sono trattati, segnatamente, a fini di indagine, di azione penale e di esecuzione di pene relative a reati previsti dalla legge, nonché di prevenzione di gravi turbative dell'ordine pubblico nel quadro della radicalizzazione violenta, del monitoraggio delle attività dei servizi segreti e di sicurezza e nell'ottica di un miglioramento dei controlli delle persone alle frontiere esterne, oltre che a fini di contrasto dell'immigrazione irregolare (articolo 8).
- 6 Il trattamento dei dati può avvenire nel quadro del controllo preliminare dei passeggeri (prima della loro partenza o del loro arrivo) (articoli da 24 a 26) o nel quadro di ricerche specifiche (articolo 27).
- 7 La legge prevede che i dati dei passeggeri siano conservati nella banca dati dei passeggeri per un periodo massimo di cinque anni a decorrere dalla loro registrazione (articoli da 18 a 23).
- 8 L'ASBL «Ligue des droits humains» critica la legge nei seguenti sette punti:
 - le modalità di attuazione della legge del 25 dicembre 2016 (articolo 3, paragrafo 2, e articolo 7, paragrafo 3);
 - le nozioni di «documenti d'identità» e di «documenti di viaggio» (articolo 7, paragrafi 1 e 2);
 - i dati interessati (articoli 4, punto 9, e 9);
 - la nozione di «passeggero» (articolo 4, punto 10);
 - le finalità del trattamento dei dati «PNR» (articolo 8);
 - la gestione della banca dati dei passeggeri e il trattamento dei dati nel quadro del controllo preliminare dei passeggeri e delle ricerche specifiche (articoli da 12 a 16, da 24 a 27, 50 e 51);
 - la durata della conservazione dei dati PNR (articolo 18).
- 9 Essa ha denunciato talune irregolarità e presentato alla Cour constitutionnelle (Corte costituzionale, Belgio) un ricorso di annullamento fondato su due motivi.

- 10 Il primo motivo concerne essenzialmente l'articolo 23 del regolamento (UE) 2016/679¹, gli articoli 7, 8 e 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta») e l'articolo 8 della Convenzione europea dei diritti dell'uomo (in prosieguo: la «CEDU»).
- 11 Essa afferma, essenzialmente, che l'ingerenza nel diritto al rispetto della vita privata e nel diritto alla protezione dei dati personali è illecita in quanto non risponde ai criteri di legalità, necessità e proporzionalità.
- 12 Anzitutto, la legge PNR riconoscerebbe un'ampia discrezionalità al potere esecutivo che essa incarica di definire, mediante regio decreto, taluni elementi essenziali in spregio al principio di legalità, in virtù del quale l'ingerenza deve essere prevista ex lege o, in caso di delega al Re, gli elementi essenziali devono essere previsti in modo sufficientemente preciso e dettagliato.
- Inoltre, la legge impugnata non perseguirebbe un obiettivo legittimo. Essa prevede infatti un controllo preliminare, detto «pre-screening», che consiste nel valutare il rischio rappresentato dai passeggeri prima dell'arrivo, del transito o della partenza nazionale.
- 13 La ricorrente contesta poi la necessità delle misure impugate ai fini del raggiungimento dell'obiettivo perseguito.
- A suo avviso, anche una mappatura dei dati - nettamente meno lesiva della vita privata rispetto alla creazione di una banca dati - consentirebbe di realizzare l'obiettivo perseguito.
- 14 Infine, essa afferma che la legge impugnata non rispetterebbe il principio di proporzionalità, poiché i dati sono raccolti in modo indifferenziato e generalizzato dagli operatori e trasmessi alle autorità competenti per essere conservati per cinque anni senza alcuna distinzione, differenziazione, limitazione o eccezione in funzione dell'obiettivo perseguito.
- 15 Più precisamente, la legge viola il principio di proporzionalità in considerazione (a) del suo campo di applicazione e delle categorie di dati interessati, (b) dei trattamenti di dati da essa previsti, (c) delle sue finalità e (d) della durata della conservazione dei dati.
- 16 Anzitutto, la legge impugnata definisce in termini molto ampi i dati raccolti che eccedono evidentemente quanto strettamente necessario.

¹ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati; GU 2016, L 119, pag. 1; in prosieguo, anche: il «RGPD»).

- 17 La ricorrente osserva che sembrerebbe – ma la legge non è chiara – che il pre-screening debba essere compiuto nella banca dati centralizzata dell’UIP con il supporto di criteri prestabiliti che fungono da indicatori della presenza della minaccia. Orbene, la legge PNR non definisce né la natura precisa delle banche dati utilizzate ai fini della correlazione, né le modalità di quest’ultima. Inoltre, la legge PNR non prevede che detta correlazione sia circoscritta alle banche dati utilizzate in relazione alla lotta al terrorismo e ai reati gravi.
- 18 La ricorrente critica altresì le ricerche specifiche che la legge prevede senza precisare i dati effettivamente accessibili.
- 19 La ricorrente contesta inoltre le finalità del trattamento dei dati che sono nettamente più ampie di quelle previste dalla direttiva PNR, come la lotta contro l’immigrazione irregolare, le attività potenzialmente integranti una minaccia per gli interessi fondamentali dello Stato o ancora la lotta alla «radicalizzazione violenta», definita unicamente in una circolare.
- 20 Infine, la ricorrente critica la durata quinquennale della conservazione dei dati. Il legislatore non giustificerebbe in alcun modo la scelta del termine massimo autorizzato dalla direttiva PNR, che rivelerebbe il carattere sproporzionato della misura.
- 21 Il Conseil des ministres (Consiglio dei Ministri, Belgio) (che difende la legge) eccepisce, in via principale, l’irricevibilità del primo motivo nella parte in cui concerne la violazione dell’articolo 23 del RGPD, poiché sia dal considerando 19 di detto regolamento, sia dall’articolo 1 della direttiva PNR emergerebbe chiaramente che il trattamento dei dati «PNR» non ricade nel campo di applicazione del RGPD, bensì della cooperazione giudiziaria e di polizia tra gli Stati membri e della direttiva (UE) 2016/680².
- 22 Inoltre, esso nega che vi sia stata una lesione del principio di legalità, posto che la legge conterrebbe gli elementi essenziali delle misure da essa introdotte e l’autorizzazione concessa al Re sarebbe sufficientemente precisa. Quanto al resto, il requisito della legalità va inteso in senso sostanziale in linea con la Corte europea dei diritti dell’uomo, cosicché gli atti regolamentari soddisfano la nozione di «legge» ai sensi della Convenzione europea dei diritti dell’uomo.

La legge PNR mirerebbe a garantire la sicurezza pubblica consentendo non soltanto il perseguimento dei reati di terrorismo o di talune forme gravi di criminalità, ma anche, grazie a un’analisi preventiva dei dati raccolti, una loro prevenzione. La Corte di giustizia avrebbe riconosciuto che questi obiettivi sono

² Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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 e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU 2016, L 119, pag. 89; in prosieguo: la «direttiva 2016/680»).

legittimi ai sensi dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, sia nella sua sentenza dell'8 aprile 2014, Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238), sia nel suo parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017 (EU:C:2017:592).

- 23 Il Consiglio dei Ministri ritiene che le misure impugnate siano proporzionate.
- 24 Per quanto attiene alla creazione di una banca dati «passeggeri», il Consiglio dei Ministri osserva che la ricorrente si limiterebbe a sostenere, senza dimostrarlo, che una mappatura dei dati avrebbe consentito di realizzare l'obiettivo perseguito e che detta misura avrebbe integrato un'ingerenza meno grave nel diritto al rispetto della vita privata. Esso aggiunge che una semplice mappatura dei dati non sarebbe sufficiente per compiere le valutazioni preliminari nell'ottica di individuare i rischi per la sicurezza. La creazione di una banca dati consentirebbe peraltro di soddisfare il considerando 25 della direttiva PNR, che invita a conservare i dati per il periodo necessario tenendo presenti gli obiettivi perseguiti.

- 25 Per quanto attiene alla correlazione tra le diverse banche dati, il Consiglio dei Ministri ricorda che gli articoli 24 e 25 della legge PNR recepiscono l'articolo 6 della direttiva PNR. Inoltre, dai lavori preparatori emergerebbe che il legislatore non intende compiere una correlazione tra la banca dati «passeggeri» e tutte le banche dati cui le autorità competenti hanno accesso, ma unicamente tra la banca dati «passeggeri» e quelle che corrispondono alle finalità perseguite dalla legge impugnata. Dette misure sarebbero conformi agli insegnamenti del parere 1/15 della Corte di giustizia, posto che l'articolo 6, paragrafo 3, della direttiva PNR non precisa neppure quali banche dati possano essere poste in correlazione. La sussistenza di un potere discrezionale non violerebbe neppure il principio di legalità come interpretato dalla Corte europea dei diritti dell'uomo.

Inoltre, l'obiettivo della legge non potrebbe essere conseguito se i viaggiatori conoscessero a priori i criteri che determinano una corrispondenza positiva dal momento che essi potrebbero, in tal caso, adattare di conseguenza la propria condotta. L'articolo 16 della legge impugnata indica inoltre, chiaramente, che il pre-screening deve essere effettuato all'interno della banca dati «passeggeri», il che sarebbe quindi in linea con il principio di legalità.

- 26 Per quanto attiene alla durata della conservazione dei dati, il Consiglio dei Ministri ritiene che non sia irragionevole prevedere un termine di conservazione di cinque anni, corrispondente peraltro alla durata minima della prescrizione dell'azione penale rispetto ai reati che possono essere puniti con misure correzionali.

La durata della conservazione di detti dati, conforme alla durata prevista dalla direttiva PNR, non sarebbe quindi affatto sproporzionata.

- 27 Il secondo motivo, sollevato in via subordinata, verte essenzialmente sulla violazione del combinato disposto dell'articolo 3, paragrafo 2, TFUE e dell'articolo 45 della Carta.

- 28 La ricorrente afferma che l'articolo 3, paragrafo 1, l'articolo 8, paragrafo 2, e il capo 11, contenente gli articoli da 28 a 31, della legge PNR violerebbe la libera circolazione delle persone, in quanto riguardano non soltanto i trasporti extra-UE, ma anche quelli intra-UE (compresi gli scali). La ricorrente ritiene, in altre parole, che, estendendo il sistema «PNR» ai voli intra-UE, le disposizioni impugnate ripristinino indirettamente controlli alle frontiere lesivi della libera circolazione delle persone.
- 29 A parere del Consiglio dei Ministri, la legge impugnata non reintrorrebbe alcun controllo alle frontiere e non violerebbe in alcun modo la libera circolazione delle persone. La direttiva PNR non si applicherebbe all'immigrazione irregolare e la legge impugnata recepirebbe non soltanto la direttiva PNR, ma anche la direttiva API.

Il motivo, così come formulato, concerne unicamente gli articoli 3, paragrafo 1, e 8, paragrafo 2, e il capo 11 della legge impugnata. Orbene, dalla definizione della nozione di «frontiere esterne» emerge che la legge PNR riguarderebbe unicamente i controlli extra-UE. Inoltre, la legge PNR recepirebbe la direttiva 2004/82/CE, cosicché non potrebbe essere intesa nel senso che ripristini un controllo alle frontiere dell'area Schengen.

In via ulteriormente subordinata, il considerando 10 della direttiva PNR prevederebbe esplicitamente la possibilità di estendere l'utilizzo dei dati «PNR» ai voli intra-UE, il che dimostrerebbe che detta misura non è, di per sé, lesiva né della libera circolazione né del regolamento (CE) n. 562/2006.

II. Contesto normativo

Convenzione europea dei diritti dell'uomo

- 30 L'articolo 8 così dispone:

«1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.

2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

Diritto dell'Unione

Carta dei diritti fondamentali dell'Unione europea

- 31 L'articolo 7 della Carta («Rispetto della vita privata e della vita familiare») prevede quanto segue:

«Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni».

- 32 L'articolo 8 della Carta («Protezione dei dati di carattere personale») è così formulato:

«1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

- 33 L'articolo 52, paragrafo 1, della Carta così prevede:

«Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni 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».

Regolamento generale sulla protezione dei dati (RGPD)

- 34 L'articolo 2, paragrafo 2, lettera d), così dispone:

«2. Il presente regolamento non si applica ai trattamenti di dati personali:

(...)

d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse».

- 35 L'articolo 23 così dispone:

«1. Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:

- a) la sicurezza nazionale;
- b) la difesa;
- c) la sicurezza pubblica;
- d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;
- e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;
- f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;
- g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;
- h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);
- i) la tutela dell'interessato o dei diritti e delle libertà altrui;
- j) l'esecuzione delle azioni civili.

2. In particolare qualsiasi misura legislativa di cui al paragrafo 1 contiene disposizioni specifiche riguardanti almeno, se del caso:

- a) le finalità del trattamento o le categorie di trattamento;
- b) le categorie di dati personali;
- c) la portata delle limitazioni introdotte;
- d) le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti;
- e) l'indicazione precisa del titolare del trattamento o delle categorie di titolari;

- f) i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento;
- g) i rischi per i diritti e le libertà degli interessati; e
- h) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa».

Direttiva PNR

36 L'articolo 3 è così formulato:

Ai fini della presente direttiva si intende per:

«(...)

4) “passeggero”, chiunque, compresi i passeggeri in trasferimento o in transito ed esclusi i membri dell'equipaggio, sia trasportato o da trasportare in un aeromobile con il consenso del vettore aereo, risultante dalla registrazione di tali passeggeri nell'elenco dei passeggeri».

37 L'articolo 4 così dispone:

«Unità d'informazione sui passeggeri

1. Ciascuno Stato membro stabilisce o designa un'autorità competente in materia di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, o una sua sezione, che agisca in qualità di “unità d'informazione sui passeggeri” (UIP).

2. La UIP è incaricata di:

a) raccogliere i dati PNR presso i vettori aerei, conservare, trattare e trasferire tali dati o i risultati del loro trattamento alle autorità competenti di cui all'articolo 7;

b) scambiare sia i dati PNR che i risultati del trattamento di tali dati con le UIP degli altri Stati membri e con Europol conformemente agli articoli 9 e 10.

(...))».

38 L'articolo 6 così dispone:

«1. I dati PNR trasferiti dai vettori aerei sono raccolti dall'UIP dello Stato membro interessato secondo quanto previsto all'articolo 8. Qualora nei dati PNR trasferiti dai vettori aerei siano compresi dati diversi da quelli elencati nell'allegato I, l'UIP li cancella in via definitiva non appena li riceve.

2. L'UIP provvede al trattamento dei dati PNR unicamente per le seguenti finalità:

- a) valutare i passeggeri prima dell'arrivo previsto nello Stato membro o della partenza prevista dallo Stato membro per identificare quelli da sottoporre a ulteriore verifica da parte delle autorità competenti di cui all'articolo 7 e, se del caso, da parte di Europol, a norma dell'articolo 10, in considerazione del fatto che gli stessi potrebbero essere implicati in reati di terrorismo o in reati gravi;
- b) rispondere, caso per caso, a una richiesta debitamente motivata e basata su motivi sufficienti da parte delle autorità competenti di trasmettere e trattare dati PNR in casi specifici a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, e di comunicare i risultati di tale trattamento alle stesse autorità competenti o, se del caso, a Europol; e
- c) analizzare i dati PNR per aggiornare i criteri esistenti o definire nuovi criteri da usare nelle valutazioni effettuate ai sensi del paragrafo 3, lettera b), al fine di identificare le persone che potrebbero essere implicate in reati di terrorismo o in reati gravi.

(...)).

39 L'articolo 12 così dispone:

«1. Gli Stati membri provvedono affinché i dati PNR trasmessi dai vettori aerei all'UIP siano da questa conservati in una banca dati per un periodo di cinque anni dal trasferimento all'UIP dello Stato membro dal cui territorio parte o nel cui territorio atterra il volo.

2. Allo scadere del periodo di sei mesi dal trasferimento dei dati PNR di cui al paragrafo 1, tutti i dati PNR sono resi anonimi mediante mascheratura dei seguenti elementi che potrebbero servire a identificare direttamente il passeggero cui i dati PNR si riferiscono:

- a) il nome o i nomi, compresi i nomi di altri passeggeri figuranti nel PNR e il numero di viaggiatori che viaggiano insieme figurante nel PNR;
- b) l'indirizzo e gli estremi;
- c) informazioni su tutte le modalità di pagamento, compreso l'indirizzo di fatturazione, nella misura in cui contenga informazioni che potrebbero servire a identificare direttamente il passeggero cui si riferiscono i dati PNR o altre persone;
- d) informazioni sui viaggiatori abituali ("Frequent flyer");
- e) osservazioni generali contenenti informazioni che potrebbero servire a identificare direttamente il passeggero cui si riferiscono i dati PNR; e

f) i dati API eventualmente raccolti.

3. Allo scadere del periodo di sei mesi di cui al paragrafo 2, la comunicazione dei dati PNR integrali è consentita solo se:

a) è ragionevolmente ritenuta necessaria ai fini dell'articolo 6, paragrafo 2, lettera b); e

b) è approvata da:

i) un'autorità giudiziaria; o

ii) un'altra autorità nazionale competente ai sensi del diritto nazionale per verificare se sono soddisfatte le condizioni per la comunicazione, fatti salvi l'informazione e l'esame a posteriori del responsabile della protezione dei dati dell'UIP.

4. Gli Stati membri provvedono affinché i dati PNR siano cancellati in via definitiva allo scadere del periodo di cui al paragrafo 1. Questo obbligo non incide sui casi in cui dati PNR specifici sono stati trasferiti a un'autorità competente e sono usati nell'ambito di un caso specifico a fini di prevenzione, accertamento, indagine e azione penale dei reati di terrorismo o reati gravi, nel qual caso la loro conservazione presso l'autorità competente è disciplinata dal diritto nazionale.

5. I risultati del trattamento di cui all'articolo 6, paragrafo 2, lettera a), sono conservati presso l'UIP soltanto per il tempo necessario a informare di un riscontro positivo le autorità competenti e, conformemente all'articolo 9, paragrafo 1, a informare di un riscontro positivo le UIP degli altri Stati membri. Il risultato di un trattamento automatizzato, anche qualora risulti negativo a seguito dell'esame individuale non automatizzato di cui all'articolo 6, paragrafo 5, può comunque essere memorizzato in modo da evitare futuri "falsi" riscontri positivi fino a che i dati di riferimento non sono cancellati a norma del paragrafo 4 del presente articolo».

40 L'allegato I alla direttiva PNR, dal titolo «Dati del codice di prenotazione raccolti dai vettori aerei», menziona, in particolare:

«(...)

12. Osservazioni generali (comprese tutte le informazioni disponibili sui minori non accompagnati di età inferiore a 18 anni, quali nome e sesso del minore, età, lingua o lingue parlate, nome e recapito dell'accompagnatore alla partenza e relazione con il minore, nome e recapito dell'accompagnatore all'arrivo e relazione con il minore, agente alla partenza e all'arrivo)

(...)

18. Informazioni anticipate sui passeggeri (API) eventualmente raccolte (tra cui: tipo, numero, paese di rilascio e data di scadenza del documento, cittadinanza, cognome, nome, sesso, data di nascita, compagnia aerea, numero di volo, data di partenza, data di arrivo, aeroporto di partenza, aeroporto di arrivo, ora di partenza e ora di arrivo)

(...)).

Direttiva API

41 L'articolo 1 così dispone:

«La presente direttiva intende migliorare i controlli alle frontiere e combattere l'immigrazione illegale attraverso la trasmissione anticipata, da parte dei vettori, dei dati relativi alle persone trasportate alle competenti autorità nazionali».

Diritto belga

42 Le disposizioni pertinenti della **legge PNR** (come modificata dalle leggi del 15 e del 30 luglio 2018 e dalla legge del 2 maggio 2019) sono le seguenti:

«CAPO 2. Ambito di applicazione

Articolo 3. § 1 La presente legge stabilisce gli obblighi a carico dei vettori e degli operatori di viaggio in materia di trasmissione dei dati dei passeggeri diretti, provenienti o in transito sul territorio nazionale.

§ 2. Il Re, con decreto adottato in sede di Consiglio dei Ministri per ciascun settore di trasporto e per gli operatori di viaggio, stabilisce i dati dei passeggeri da trasmettere e le loro modalità di trasmissione, previo parere della competente autorità di controllo del trattamento dei dati personali. (...)

CAPO 3. Definizioni

Articolo 4. Ai fini dell'applicazione della presente legge e dei rispettivi decreti esecutivi, si intende con:

(...)

9° “PNR”: le informazioni relative alle modalità di viaggio di ciascun passeggero, comprendenti i dati di cui all'articolo 9 necessari per il trattamento e il controllo delle prenotazioni a cura dei vettori e degli operatori di viaggio 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 (utilizzati per il controllo dei passeggeri all'atto dell'imbarco), o in altri sistemi equivalenti con le stesse funzionalità;

10° “passeggero”: chiunque, compresi i passeggeri in trasferimento o in transito ed esclusi i membri dell’equipaggio, sia trasportato o da trasportare dal vettore con il consenso di quest’ultimo, risultante dalla registrazione di tale persona nell’elenco dei passeggeri;

(...)

CAPO 5. Finalità del trattamento dei dati

Articolo 8. § 1 I dati dei passeggeri sono trattati ai fini:

1° della conduzione di indagini e del perseguimento dei reati, ivi compresa l’esecuzione di pene o di misure restrittive della libertà personale, concernenti i reati previsti [nel] Code d’Instruction criminelle (codice di procedura penale);

2° della conduzione di indagini e del perseguimento dei reati, ivi compresa l’esecuzione di pene o di misure restrittive della libertà personale, concernenti reati previsti [nel] Code pénal (codice penale);

3° della prevenzione di gravi turbative all’ordine pubblico nel quadro della radicalizzazione violenta mediante il controllo dei fenomeni e dei raggruppamenti ai sensi dell’articolo 44/5, § 1, punti 2 e 3, e § 2, della loi du 5 août 1992, sur la fonction de police (legge del 5 agosto 1992, in materia di funzioni di polizia);

4° del controllo delle attività di cui agli articoli 7, punti 1 e 3/1, e 11, § 1, punti da 1 a 3 e 5, della loi du 30 novembre 1998, organique des services de renseignement et de sécurité (legge organica del 30 novembre 1998, che disciplina i servizi segreti e di sicurezza);

5° della conduzione delle indagini e del perseguimento dei reati previsti [in diverse leggi].

§ 2. Nel rispetto delle condizioni previste nel capo 11, i dati dei passeggeri sono inoltre trattati ai fini del miglioramento dei controlli sulle persone alle frontiere esterne e del contrasto all’immigrazione irregolare.

CAPO 6. - Dati dei passeggeri

Articolo 9. § 1 Per quanto attiene ai dati relativi alle prenotazioni, i dati dei passeggeri comprendono al massimo:

1° il codice PNR di identificazione;

2° la data di prenotazione e di emissione del biglietto;

3° le date previste di viaggio;

4° i cognomi, i nomi e le date di nascita;

- 5° l'indirizzo, il recapito telefonico e l'indirizzo di posta elettronica;
- 6° le informazioni sulle modalità di pagamento, compreso l'indirizzo di fatturazione;
- 7° l'itinerario completo per il passeggero interessato;
- 8° le informazioni relative ai “viaggiatori registrati”, vale a dire i viaggiatori abituali;
- 9° l'agenzia di viaggio o l'agente di viaggio;
- 10° lo status di viaggio del passeggero, inclusi conferme, check-in, assenze all'imbarco o passeggero senza prenotazione;
- 11° le indicazioni riguardanti la scissione o la divisione del PNR;
- 12° le osservazioni generali, comprese tutte le informazioni disponibili sui minori non accompagnati di età inferiore a 18 anni, quali nome e sesso del minore, età, lingua o lingue parlate, nome e recapito dell'accompagnatore alla partenza e relazione con il minore, nome e recapito dell'accompagnatore all'arrivo e relazione con il minore, agente presente alla partenza e all'arrivo;
- 13° i dati sull'emissione del biglietto, compresi il numero del biglietto, la data di emissione, i biglietti di sola andata, i campi ATFQ;
- 14° le informazioni sul posto, compreso il numero di posto assegnato;
- 15° le informazioni sul code share (codici comuni);
- 16° tutte le informazioni relative al bagaglio;
- 17° il numero e i nomi degli altri viaggiatori figuranti nel PNR;
- 18° tutti i dati anticipati sui passeggeri (API) raccolti ed elencati sub § 2;
- 19° la cronistoria delle modifiche dei dati di cui ai numeri da 1 a 18;

§ 2. Per quanto attiene ai dati di registrazione e di imbarco, i dati anticipati di cui al § 1, punto 18°, sono:

- 1° il tipo di documento di viaggio;
- 2° il numero di documento;
- 3° la cittadinanza;
- 4° il paese di rilascio del documento;
- 5° la data di scadenza del documento;

- 6° il cognome, il nome, il sesso e la data di nascita;
 - 7° il vettore/operatore di viaggio;
 - 8° il numero del trasporto;
 - 9° la data di partenza e di arrivo;
 - 10° il luogo di partenza e di arrivo;
 - 11° l'ora di partenza e di arrivo;
 - 12° il numero complessivo di persone trasportate;
 - 13° il numero di posto;
 - 14° il codice PNR di identificazione della pratica;
 - 15° il numero, il peso e l'identificazione dei bagagli;
 - 16° il valico di frontiera di ingresso nel territorio nazionale.
- (...)

CAPO 7. Unità d'informazione sui passeggeri

Articolo 12. All'interno del Servizio federale pubblico dell'Interno è istituita un'Unità d'informazione sui passeggeri (UIP).

Articolo 13. § 1 La UIP è incaricata:

1° della raccolta, della conservazione e del trattamento dei dati dei passeggeri trasmessi dai vettori e dagli operatori di viaggio e della gestione della banca dati dei passeggeri;

2° dello scambio, sia dei dati dei passeggeri che dei risultati del loro trattamento, con le UIP degli altri Stati membri dell'Unione europea, con Europol e con i paesi terzi conformemente al capo 12.

§ 2. Fatte salve altre disposizioni di legge, l'UIP non può utilizzare i dati conservati in forza del capo 9 per finalità diverse da quelle indicate nell'articolo 8.

Articolo 14. § 1 L'UIP è composta:

1° da un funzionario (...) responsabile:

- a) dell'organizzazione e del funzionamento dell'UIP;
- b) del controllo del rispetto da parte dei vettori e degli operatori di viaggio degli obblighi ad essi incombenti, come previsti nel capo 4;

- c) della gestione e dell'uso della banca dati passeggeri;
 - d) del trattamento dei dati dei passeggeri;
 - e) del rispetto della legalità e della regolarità dei trattamenti di cui al capo 10;
- (...).

2° da membri distaccati provenienti dai seguenti servizi (...):

- a) Servizi di polizia (...);
 - b) Sicurezza dello Stato (...);
 - c) Servizio generale segreto e di sicurezza (...);
 - d) Amministrazione (...) delle dogane e delle accise
- (...).

CAPO 8. Banca dati dei passeggeri

Articolo 15. § 1 È creata una banca dati dei passeggeri gestita dal Servizio federale pubblico dell'Interno in cui sono registrati i dati dei passeggeri.

(...).

§ 4. I trattamenti dei dati dei passeggeri compiuti in forza della presente legge sono soggetti alla loi relative à la protection des données (legge in materia di protezione dei dati). L'autorità competente per il controllo del trattamento dei dati personali esercita le competenze previste nella loi relative à la protection de la vie privée (legge in materia di tutela della vita privata). (...)

(...)

CAPO 9. Termini di conservazione

Articolo 18. I dati dei passeggeri sono conservati nella banca dati dei passeggeri per un periodo massimo di cinque anni a decorrere dalla loro registrazione. Decorso detto termine, i dati sono distrutti.

(...)

CAPO 10. Trattamento dei dati

Sezioni I. Trattamento dei dati dei passeggeri nel quadro del controllo preliminare dei passeggeri

Articolo 24. § 1 I dati dei passeggeri sono trattati ai fini dell'effettuazione di un controllo preliminare dei passeggeri prima del loro arrivo, della loro partenza o

del transito previsto sul territorio nazionale al fine di stabilire quali persone debbano essere sottoposte a un controllo più approfondito.

[metodi di controllo preliminare]

Articolo 25 (...)

§ 2. La valutazione dei passeggeri prima del loro arrivo, transito o partenza in ragione dei criteri prestabiliti è compiuta in modo non discriminatorio. Tali criteri non possono riguardare l'identificazione di un individuo e devono essere mirati, proporzionati e specifici.

§ 3. I criteri di cui trattasi non possono essere fondati su dati che rivelano l'origine razziale o etnica di una persona, le sue convinzioni religiose o filosofiche, le sue opinioni politiche, la sua appartenenza a un'organizzazione sindacale, il suo stato di salute, la sua vita sessuale o orientamento sessuale.

(...)

Sezione 2. - Trattamento dei dati nel quadro di ricerche specifiche

Articolo 27. I dati dei passeggeri sono utilizzati al fine di compiere ricerche specifiche per le finalità indicate all'articolo 8, § 1, punti 1°, 2°, 4° e 5°, e alle condizioni di cui all'articolo 46 septies del codice di procedura penale o all'articolo 16/3 della legge organica del 30 novembre 1998, che disciplina i servizi segreti e di sicurezza, o all'articolo 281, § 4, de la loi générale sur les douanes et accises (legge generale in materia di dogane e accise), coordinata il 18 luglio 1977.

CAPO 11. Trattamento dei dati dei passeggeri ai fini del miglioramento dei controlli alle frontiere e del contrasto dell'immigrazione irregolare

Articolo 28. § 1. Il presente capo si applica ai trattamenti dei dati dei passeggeri compiuti dai servizi di polizia incaricati del controllo alle frontiere e dall'Office des étrangers (Ufficio stranieri) in vista del miglioramento dei controlli delle persone alle frontiere esterne e della lotta all'immigrazione irregolare.

(...)

Articolo 29. § 1 (...)

§ 2. Sono trasmessi unicamente i dati [API] concernenti le seguenti categorie di passeggeri:

1° i passeggeri che intendono entrare o che sono entrati sul territorio attraverso le frontiere esterne del Belgio;

2° i passeggeri che intendono lasciare o hanno lasciato il territorio attraverso le frontiere esterne del Belgio;

3° i passeggeri che intendono attraversare, si trovano o hanno attraversato una zona internazionale di transito sita in Belgio.

§ 3. I dati dei passeggeri di cui al § 2 sono trasmessi ai servizi di polizia indicati nell'articolo 14, § 1, punto 2, lettera a), immediatamente dopo la loro registrazione nella banca dati dei passeggeri. Detti servizi conservano i dati in un file provvisorio e li distruggono nelle ventiquattro ore successive alla trasmissione.

§ 4. (...) I dati dei passeggeri di cui al § 2 sono trasmessi all'Ufficio stranieri immediatamente dopo la loro registrazione nella banca dati dei passeggeri. Detto ufficio conserva i dati in un file provvisorio e li distrugge nelle ventiquattro ore successive alla trasmissione.

(...).

Articolo 31. Nelle ventiquattro ore successive al termine del trasporto, di cui all'articolo 4, punti da 3 a 6, i vettori e gli operatori di viaggio distruggono tutti i dati dei passeggeri indicati nell'articolo 9, § 1, punto 18, (...).

(...)

CAPO 15. Disposizioni di modifica

Sezione I. Modifica del codice di procedura penale

Articolo 50. Nel codice di procedura penale, è inserito un articolo 46 septies formulato come segue:

“Articolo 46 septies. Nell'indagare sui crimini e i reati di cui all'articolo 8, § 1, punti 1, 2 e 5, della legge del 25 dicembre 2016, in materia di trattamento dei dati dei passeggeri, il procuratore del Re può, con decisione scritta e motivata, incaricare l'ufficiale di polizia giudiziaria di chiedere all'UIP di comunicare i dati dei passeggeri conformemente all'articolo 27 della legge succitata.

(...)

Sezione 2. Modifica della legge organica del 30 novembre 1998, che disciplina i servizi segreti e di sicurezza

Articolo 51. Nel capo III, sezione I, sottosezione 2, della legge organica del 30 novembre 1998, che disciplina i servizi segreti e di sicurezza, è inserito un articolo 16/3 redatto come segue:

“Articolo 16/3. § 1 I servizi segreti e di sicurezza possono, nell'interesse dell'esercizio dei loro compiti, a fronte di decisione debitamente motivata, accedere ai dati dei passeggeri di cui all'articolo 27 della legge del 25 dicembre 2016, in materia di trattamento dei dati dei passeggeri (...)”».

III. Valutazione della Cour constitutionnelle (Corte costituzionale)

- 43 La Cour constitutionnelle (Corte costituzionale) precisa anzitutto che il suo esame del ricorso tiene conto delle modifiche apportate alla legge del 25 dicembre 2016 dalle leggi del 15 e del 30 luglio 2018 e dalla legge del 2 maggio 2019.
- 44 Inoltre, la Cour constitutionnelle (Corte costituzionale) limita la portata del ricorso di annullamento stabilendo che il primo motivo è diretto unicamente contro l'articolo 3, paragrafo 2, l'articolo 4, punti 9 e 10, gli articoli da 7 a 9, da 12 a 16, 18, da 24 a 27, 50 e 51 della legge, mentre il secondo motivo è volto a contestare l'articolo 3, paragrafo 1, l'articolo 8, paragrafo 2, e gli articoli da 28 a 31 della legge.

1. Sulla ricevibilità del primo motivo: applicabilità dell'articolo 23 del RGPD alla legge PNR

- 45 Il giudice del rinvio ricorda che la tutela offerta dal RGPD si fonda sull'articolo 16, paragrafo 2, TFUE e che, in linea di principio, il trattamento dei dati personali effettuato dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali non ricade nel RGPD, bensì nella direttiva 2016/680. La direttiva in questione stabilisce norme specifiche in materia di protezione delle persone fisiche 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, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, nel rispetto della natura specifica di tali attività.
- 46 La legge PNR disciplina la raccolta e il trasferimento dei dati PNR, la creazione di una banca dati dei passeggeri, gestita dall'UIP, le finalità del trattamento di detta banca dati e l'accesso ad essa. Detta legge recepisce essenzialmente la direttiva PNR, ma il suo contenuto va al di là della sua trasposizione.
- 47 Riferendosi al parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017 (EU:C:2017:592), il giudice del rinvio osserva che disposizioni disciplinanti la raccolta, il trasferimento e il trattamento di dati «PNR» possono ricadere sia nell'ambito della protezione dei dati (articolo 16 TFUE), sia in quello della cooperazione di polizia (articolo 87 TFUE).

Esso osserva altresì che il considerando 5 della direttiva PNR chiarisce che gli obiettivi della direttiva in questione sono «tra l'altro, garantire la sicurezza, proteggere la vita e l'incolumità delle persone, nonché creare un quadro normativo per la tutela dei dati PNR per quanto riguarda il loro trattamento da parte delle autorità competenti». Tuttavia, il considerando 38 della medesima direttiva precisa che gli obiettivi della direttiva sono «il trasferimento dei dati PNR da parte dei vettori aerei e il loro trattamento a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei

reati gravi», il che potrebbe attribuire a detti obiettivi un carattere preponderante rispetto a quelli della protezione dei dati.

Il giudice del rinvio constata inoltre che il diritto nazionale non esclude l'intera legge PNR dall'ambito di applicazione dell'articolo 23 del RGPD.

- 48 La Cour constitutionnelle (Corte costituzionale) conclude quindi che, al fine di stabilire se le prescrizioni di cui all'articolo 23 del RGPD trovino applicazione alla legge PNR, che recepisce, tra l'altro e principalmente, la direttiva PNR, occorre sottoporre alla Corte una prima questione pregiudiziale.

2. *Sul merito del primo motivo*

La Cour constitutionnelle (Corte costituzionale) esamina quindi nel merito il motivo, nelle sue sette parti citate al punto 8 della presente sintesi. Essa stabilisce che le prime due censure dirette contro le «modalità di attuazione» e contro le nozioni di «documenti d'identità» e di «documento di viaggio» sono destituite di fondamento. Essa prosegue il suo esame delle altre cinque censure sollevando dubbi quanto all'interpretazione di talune disposizioni della direttiva PNR e alla loro validità alla luce della Carta.

Sui dati interessati (articoli 4, punto 9, e 9 della legge PNR)

- 49 La ricorrente ritiene che l'ambito di applicazione molto esteso rispetto ai dati dei passeggeri oggetto degli articoli 4, punto 9, e 9, della legge PNR, sia manifestamente sproporzionato rispetto all'obiettivo perseguito. A suo parere, i dati di cui trattasi potrebbero rientrare tra i dati delicati, come l'appartenenza a un'organizzazione sindacale, le affinità personali e le relazioni personali o professionali.
- 50 Il giudice del rinvio ricorda che un'ingerenza dei poteri pubblici nell'esercizio del diritto al rispetto della vita privata deve non solo fondarsi su una disposizione normativa sufficientemente precisa, ma anche rispondere a un bisogno sociale imperativo in una società democratica ed essere proporzionata all'obiettivo legittimo perseguito. Il legislatore dispone al riguardo di un margine di discrezionalità che non è, tuttavia, illimitato: affinché una norma sia compatibile con il diritto al rispetto della vita privata, occorre che il legislatore abbia stabilito un giusto equilibrio tra tutti i diritti e gli interessi in causa.

Nel suo parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017 (EU:C:2017:592), la Corte ha ricordato che un'ingerenza nel diritto alla protezione dei dati personali deve essere limitata allo «stretto necessario» (v. punti 140 e 141).

- 51 La Cour constitutionnelle (Corte costituzionale) osserva che la legge PNR ha l'obiettivo di garantire la sicurezza pubblica, prevedendo un trasferimento dei dati dei passeggeri e il loro utilizzo nel quadro della lotta contro i reati di terrorismo e

la criminalità grave di natura transnazionale. Tali obiettivi costituiscono obiettivi di interesse generale idonei a giustificare ingerenze nel diritto al rispetto della vita privata e nel diritto alla protezione dei dati personali (sentenza dell'8 aprile 2014, Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 42). Inoltre, la Corte di giustizia ha confermato che detti obiettivi di interesse generale potevano giustificare il trasferimento e il trattamento dei dati del codice di prenotazione [parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punti 148 e 149].

- 52 Il giudice del rinvio esamina poi se dette ingerenze siano sufficientemente precise, proporzionate e limitate allo «stretto necessario», tenendo conto della portata dei dati oggetto della legge PNR.

La raccolta dei dati dei passeggeri considerati dalla legge PNR è accompagnata da una serie di garanzie quanto al contenuto di detti dati. I dati di cui trattasi sono infatti individuati in maniera tassativa dall'articolo 9 della legge PNR. Si tratta di informazioni direttamente legate al viaggio che dà luogo al trasporto rientranti nel campo di applicazione della legge PNR di cui, in linea di principio, i vettori e gli operatori di viaggio già dispongono. Inoltre, tali dati corrispondono all'allegato I agli orientamenti dell'Organizzazione per l'aviazione civile internazionale (ICAO). Essi sono quindi pertinenti alla luce degli obiettivi perseguiti dalla legge PNR.

Inoltre, gli articoli 10 e 11, non impugnati, della legge PNR prevedono che i dati dei passeggeri non possano riguardare l'origine razziale o etnica di una persona, le sue convinzioni religiose o filosofiche, le sue opinioni politiche, la sua appartenenza a un'organizzazione sindacale, o i dati riguardanti il suo stato di salute, la sua vita sessuale o il suo orientamento sessuale. Quando i dati dei passeggeri trasferiti dai vettori e dagli operatori di viaggio contengono dati diversi da quelli elencati nell'articolo 9 o nell'articolo 10, l'UIP cancella detti dati aggiuntivi non appena ricevuti e in maniera definitiva. Le disposizioni di cui trattasi garantiscono che dati delicati non possano, in linea di principio, essere raccolti o conservati quali «dati dei passeggeri».

- 53 Nel suo summenzionato parere 1/15 del 26 luglio 2017, con riferimento ai dati delicati, la Corte di giustizia ha altresì osservato che *«gli articoli 7, 8 e 21 nonché l'articolo 52, paragrafo 1, della Carta ostano sia al trasferimento dei dati sensibili verso il Canada sia alla disciplina negoziata dall'Unione con tale Stato terzo delle condizioni relative all'uso e alla conservazione di siffatti dati da parte delle autorità del medesimo Stato terzo»* (punto 167).

Tale osservazione può essere applicata al caso di specie. Benché esistano garanzie che accompagnano i dati dei passeggeri considerati dalla legge PNR, occorre tuttavia chiedersi se tali garanzie siano sufficienti tenuto conto della portata dei dati interessati. I dati di cui all'articolo 9, paragrafo 1, della legge PNR, che riprende i dati presenti nell'allegato I alla direttiva PNR, comprendono in effetti una gamma molto ampia di dati, oltre ai dati di registrazione e di imbarco,

segnatamente: l'itinerario completo per il passeggero, l'agenzia di viaggio, il numero di posto, tutte le informazioni relative al bagaglio, le informazioni sulle modalità di pagamento, compreso l'indirizzo di fatturazione, le osservazioni generali, «comprese tutte le informazioni disponibili sui minori non accompagnati di età inferiore a 18 anni».

Nel suo succitato parere 1/15 del 26 luglio 2017, la Corte ha inoltre osservato che, *«anche 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, e potrebbero persino fornire informazioni sensibili su tali passeggeri, come definite all'articolo 2, lettera e), dell'accordo previsto»* (punto 128).

Nel suo parere del 19 agosto 2016 sulle implicazioni per la protezione dei dati del trattamento delle pratiche passeggeri (in prosieguo: il «parere del 19 agosto 2016»), il Comitato consultivo della convenzione n. 108 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato dei dati personali (in prosieguo: il «comitato consultivo della Convenzione n. 108») ha altresì osservato che *«[i] PNR contengono informazioni finalizzate ad agevolare il viaggio di un passeggero e possono comprendere un certo numero di dati sensibili (dati che possono servire a indicare l'origine razziale, le opinioni politiche, le convinzioni religiose e di altra natura, lo stato di salute o l'orientamento sessuale di una persona), non soltanto tra determinati dati "codificati" ma anche nel campo aperto contenente osservazioni generali (quali richieste di carattere alimentare o medico, o il fatto che un'associazione politica o religiosa abbia beneficiato di biglietti a prezzo ridotto per il viaggio dei suoi membri), il che potrebbe comportare una discriminazione diretta»* (Consiglio d'Europa, parere del 19 agosto 2016, T-PD(2016)18rev, pag. 7).

Anche l'Agenzia dell'Unione europea per i diritti fondamentali ha osservato che i dati PNR *«possono comprendere dati sensibili o particolari alla voce "osservazioni generali"»* [parere 1/2011 dell'Agenzia dell'Unione europea per i diritti fondamentali sulla proposta di direttiva sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi (COM(2011) 32 definitivo), 14 giugno 2011, pag. 8; v. anche, ibid., pag. 13].

- 54 Alla luce del loro ambito di applicazione oltremodo esteso, i dati di cui all'articolo 9 della legge PNR, pur non potendo contenere direttamente dati delicati, possono però rivelare, indirettamente, elementi delicati rientranti nella protezione dei dati personali e del rispetto della vita privata. Tenuto conto del parere 1/15 della Corte di giustizia, la Cour constitutionnelle (Corte costituzionale) si chiede se tali dati, che comprendono i dati indicati nell'allegato I alla direttiva PNR, eccedano lo «stretto necessario» per raggiungere gli obiettivi

perseguiti da detta medesima direttiva. Essa ha quindi deciso di sottoporre alla Corte una seconda questione pregiudiziale.

- 55 Nel suo succitato parere 1/15, del 26 luglio 2017, la Corte ha inoltre svolto le seguenti osservazioni concernenti l'esigenza di una definizione chiara e precisa dei dati oggetto del progetto di accordo tra il Canada e l'Unione europea sul trasferimento e il trattamento dei dati del codice di prenotazione:

«156. A tale riguardo, sebbene le 19 rubriche dei dati PNR che figurano in allegato all'accordo previsto corrispondano, secondo le osservazioni della Commissione, all'allegato I alle linee guida dell'Organizzazione per l'aviazione civile internazionale (OACI) relative ai dati PNR, occorre tuttavia sottolineare, come rilevato dall'avvocato generale al paragrafo 217 delle sue conclusioni, che la rubrica 5, che fa riferimento alle "informazioni sui viaggiatori abituali "frequent flyer" e benefici vari (biglietti gratuiti, passaggi di classe, ecc.)"; e la rubrica 7, che comprende "tutte le informazioni di contatto disponibili (incluse quelle sull'originatore)", non definiscono in modo sufficientemente chiaro e preciso i dati PNR da trasferire.

157. Infatti, per quanto riguarda la rubrica 5, l'uso del termine "ecc." non determina a sufficienza la portata dei dati da trasferire. Inoltre, i termini di tale rubrica non consentono di sapere se la stessa riguardi le informazioni concernenti soltanto lo status dei passeggeri aerei in programmi di fidelizzazione oppure se, al contrario, essa faccia riferimento all'insieme delle informazioni relative ai viaggi aerei e alle operazioni negoziali effettuate nell'ambito di siffatti programmi.

158. Parimenti, la rubrica 7, utilizzando i termini "tutte le informazioni di contatto disponibili", non determina in maniera sufficiente la portata dei dati da trasferire. In particolare, essa non precisa quale sia il tipo delle informazioni di contatto considerate, né se tali informazioni comprendano altresì, come si può dedurre dalla risposta scritta della Commissione ai quesiti posti dalla Corte, quelle dei terzi che abbiano effettuato la prenotazione del volo per il passeggero aereo, dei terzi tramite i quali un passeggero aereo può essere aggiunto, o ancora dei terzi che debbano essere informati in caso di urgenza.

159. Per quanto concerne la rubrica 8, essa riguarda "tutte le informazioni disponibili su pagamento/fatturazione (esclusi altri dettagli relativi alla transazione connessi a una carta di credito o a un conto e non riconducibili alla transazione stessa)". Certamente, tale rubrica potrebbe sembrare particolarmente ampia in quanto impiega l'espressione "tutte le informazioni disponibili". Tuttavia, come risulta dalla risposta della Commissione ai quesiti posti dalla Corte, si deve ritenere che detta rubrica faccia riferimento soltanto alle informazioni relative alle modalità di pagamento e alla fatturazione del biglietto aereo, ad esclusione di qualsiasi altra informazione che non sia direttamente connessa al volo. Interpretata in tal senso, la medesima rubrica può, quindi, essere considerata rispondente ai requisiti di chiarezza e di precisione.

160. Per quanto riguarda la rubrica 17, essa riguarda le “osservazioni generali, comprese le informazioni OSI (Other Supplementary Information), SSI (Special Service Information) e SSR (Special Service Request)”. Secondo le spiegazioni fornite, in particolare, dalla Commissione, tale rubrica costituisce una rubrica detta “testo libero” (free text), volta a includere “tutte le informazioni supplementari”, oltre a quelle elencate nell’allegato all’accordo previsto. Pertanto, una siffatta rubrica non fornisce alcuna indicazione sulla natura e sulla portata delle informazioni che devono essere trasmesse, e sembra persino che possa includere informazioni prive di qualsiasi connessione con la finalità del trasferimento dei dati PNR. Inoltre, poiché le informazioni considerate in tale rubrica sono fornite soltanto a titolo esemplificativo, come testimoniato dall’uso dei termini “comprese”, tale medesima rubrica non fissa alcun limite riguardo alla natura e alla portata delle informazioni che possono figurarvi. In tali circostanze, non si può ritenere che la rubrica 17 sia delimitata con sufficiente chiarezza e precisione.

161. Per quanto riguarda, infine, la rubrica 18, essa riguarda “informazioni API (Advance Passenger Information-informazion[i] anticipat[e] sui passeggeri) eventualmente assunte a fini di prenotazione”. Secondo le precisazioni fornite dal Consiglio e dalla Commissione, tali informazioni corrispondono a quelle di cui all’articolo 3, paragrafo 2, della direttiva 2004/82, ossia il numero e il tipo di documento di viaggio utilizzato, la cittadinanza, il nome completo, la data di nascita, il valico di frontiera di ingresso nel territorio degli Stati membri, il numero del trasporto, l’ora di partenza e di arrivo del mezzo di trasporto, il numero complessivo di passeggeri trasportati con tale mezzo nonché il primo punto di imbarco. Nei limiti in cui tale rubrica è interpretata come comprendente soltanto le informazioni espressamente contemplate in quest’ultima disposizione, si può ritenere che essa soddisfi i requisiti di chiarezza e di precisione.

162. Le disposizioni dell’articolo 4, paragrafo 3, dell’accordo previsto, che prevedono l’obbligo del Canada di cancellare qualsiasi dato PNR che sia stato ad esso trasferito se non figura nell’elenco dell’allegato a tale accordo, non consentono di ovviare alla mancanza di precisione che inficia le rubriche 5, 7 e 17 di tale allegato. Infatti, nei limiti in cui detto elenco non delimita, in quanto tale, con sufficiente chiarezza e precisione, i dati PNR da trasferire, tali disposizioni non sono idonee a rimediare alle incertezze riguardanti i dati PNR che devono essere oggetto del trasferimento.

163. In tali circostanze, per quanto riguarda i dati PNR da trasferire verso il Canada, le rubriche 5, 7 e 17 dell’allegato all’accordo previsto non disciplinano in modo sufficientemente chiaro e preciso la portata dell’ingerenza nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta».

- 56 Dal momento che talune di queste osservazioni potrebbero essere valide anche per il caso di specie, visto il carattere esemplificativo e non tassativo di taluni dati contenuti nell’allegato I alla direttiva PNR, che l’articolo 9 della legge PNR

recepisce, il giudice del rinvio decide di sollevare una terza questione pregiudiziale.

Sulla nozione di «passeggero» (articolo 4, punto 10, della legge PNR)

- 57 La ricorrente critica l'ampiezza della nozione di «passeggero» che comporta un trattamento automatizzato, sistematico e non mirato, dei dati di tutti i passeggeri.
- 58 La definizione della nozione di «passeggero» (articolo 4, punto 10, della legge PNR) fa sì che la raccolta, il trasferimento e il trattamento dei dati PNR dei «passeggeri» rappresentino obblighi generali e indifferenziati che si applicano a tutte le persone trasportate o da trasportare e inserite nell'elenco dei passeggeri. Gli obblighi imposti dalla legge PNR si applicano così a prescindere dall'esistenza di fondati motivi per ritenere che gli interessati abbiano commesso, siano sul punto di commettere o siano stati ritenuti colpevoli di un'infrazione.
- 59 Nel suo parere del 19 agosto 2016, il comitato consultivo della Convenzione n. 108 ha osservato, a questo riguardo, che *«[i]l trattamento dei dati PNR - che ha l'unico vantaggio di consentire l'identificazione delle persone sospette - costituisce un filtraggio generale e non selettivo di tutti i passeggeri, compresi quelli che non sono sospettati di aver commesso un qualche reato, da parte delle autorità competenti e concerne dati inizialmente raccolti a fini commerciali da parte di soggetti privati. Alla luce della portata della violazione dei diritti alla vita privata e alla protezione dei dati derivante dal trattamento dei dati PNR, dev'essere stabilito con chiarezza che detto trattamento costituisce una misura necessaria in una società democratica per una finalità legittima; occorre inoltre che siano state adottate garanzie appropriate. È necessario dimostrare espressamente la necessità della raccolta e dell'ulteriore uso dei dati PNR»* (parere del 19 agosto 2016, T-PD(2016)18rev, pag. 5).
- 60 Nel settore delle comunicazioni elettroniche, la Corte si è pronunciata su una normativa nazionale, che prevedeva una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica e l'obbligo, per i fornitori di servizi di comunicazione elettronica, di conservare tali dati in maniera sistematica e continua, e ciò senza alcuna eccezione (sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a., C-203/15 e C-698/15, EU:C:2016:970).

Essa ha considerato che, *«anche se l'efficacia della lotta contro la criminalità grave, e in particolare contro la criminalità organizzata e il terrorismo, può dipendere in larga misura dall'utilizzo delle moderne tecniche di indagine, un siffatto obiettivo di interesse generale, per quanto fondamentale esso sia, non vale di per sé solo a giustificare che una normativa nazionale che prevede la conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione venga considerata necessaria ai fini della lotta suddetta»* (punto 103).

La Corte ha dichiarato, da un lato, che una normativa siffatta porta alla conseguenza che la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione costituisce la regola, laddove il sistema istituito dalla direttiva 2002/58 esige che tale conservazione dei dati sia l'eccezione e, dall'altro, che «una normativa nazionale (...) la quale riguarda in maniera generalizzata tutti gli abbonati ed utenti iscritti e ha ad oggetto tutti i mezzi di comunicazione elettronica nonché l'insieme dei dati relativi al traffico, non prevede alcuna differenziazione, limitazione o eccezione in funzione dell'obiettivo perseguito. Essa concerne in maniera globale l'insieme delle persone che si avvalgono di servizi di comunicazione elettronica, senza che tali persone si trovino, anche solo indirettamente, in una situazione suscettibile di dar luogo ad azioni penali. Essa si applica dunque finanche a persone per le quali non esiste alcun indizio di natura tale da far credere che il loro comportamento possa avere un nesso, sia pur indiretto o remoto, con violazioni penali gravi. Inoltre, essa non prevede alcuna eccezione, di modo che essa si applica anche a persone le cui comunicazioni sono sottoposte, secondo le norme del diritto nazionale, al segreto professionale (v., per analogia, per quanto riguarda la direttiva 2006/24, sentenza Digital Rights, punti 57 e 58).

106. Una normativa siffatta non richiede alcuna correlazione tra i dati di cui si prevede la conservazione e una minaccia per la sicurezza pubblica. In particolare, essa non è limitata ad una conservazione avente ad oggetto dati relativi ad un periodo di tempo e/o a una zona geografica e/o una cerchia di persone suscettibili di essere implicate in una maniera o in un'altra in una violazione grave, oppure persone che potrebbero, per altri motivi, contribuire, mediante la conservazione dei loro dati, alla lotta contro la criminalità (v., per analogia, per quanto riguarda la direttiva 2006/24, sentenza Digital Rights, punto 59).

107. Una normativa nazionale come quella in discussione nei procedimenti principali travalica dunque i limiti dello stretto necessario e non può essere considerata giustificata, in una società democratica, così come richiede l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta.

108. Per contro, l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, non osta a che uno Stato membro adotti una normativa la quale consenta, a titolo preventivo, la conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione, per finalità di lotta contro la criminalità grave, a condizione che la conservazione dei dati sia, per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone riguardate, nonché la durata di conservazione prevista, limitata allo stretto necessario.

109. Per soddisfare i requisiti enunciati al punto precedente della presente sentenza, la suddetta normativa nazionale deve, in primo luogo, prevedere norme chiare e precise che disciplinino la portata e l'applicazione di una siffatta misura

di conservazione dei dati e fissino un minimo di requisiti, di modo che le persone i cui dati sono stati conservati dispongano di garanzie sufficienti tali da permettere di proteggere efficacemente i loro dati personali contro i rischi di abuso. Essa deve in particolare indicare in quali circostanze e a quali condizioni una misura di conservazione dei dati può, a titolo preventivo, essere adottata, garantendo così che una misura siffatta sia limitata allo stretto necessario (v., per analogia, a proposito della direttiva 2006/24, sentenza Digital Rights, punto 54 e la giurisprudenza ivi citata).

110. In secondo luogo, per quanto riguarda le condizioni sostanziali che devono essere soddisfatte da una normativa nazionale che permetta, nel contesto della lotta contro la criminalità, la conservazione, a titolo preventivo, dei dati relativi al traffico e dei dati relativi all'ubicazione, al fine di garantire che essa sia limitata allo stretto necessario, occorre rilevare che, se certo tali condizioni possono variare in funzione delle misure adottate ai fini della prevenzione, della ricerca, dell'accertamento e del perseguimento della criminalità grave, la conservazione dei dati deve comunque rispondere sempre a criteri oggettivi, istituendo un rapporto tra i dati da conservare e l'obiettivo perseguito. In particolare, tali condizioni devono risultare, in pratica, idonee a delimitare effettivamente la portata della misura e, di conseguenza, il pubblico interessato.

111. Per quanto riguarda la delimitazione di una misura siffatta sotto il profilo del pubblico e delle situazioni potenzialmente riguardati, la normativa nazionale deve essere fondata su elementi oggettivi, che permettano di prendere in considerazione un pubblico i cui dati sono idonei a rivelare una connessione, almeno indiretta, con atti di criminalità grave, a contribuire in un modo o in un altro alla lotta contro la criminalità grave, o a prevenire un grave rischio per la sicurezza pubblica. Una siffatta delimitazione può essere ottenuta mediante un criterio geografico qualora le autorità nazionali competenti considerino, sulla base di elementi oggettivi, che esiste, in una o più zone geografiche, un rischio elevato di preparazione o di commissione di atti di questo tipo.

112. Alla luce dell'insieme delle considerazioni che precedono, occorre rispondere alla prima questione nella causa C-203/15 dichiarando che l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, deve essere interpretato nel senso che esso osta ad una normativa nazionale la quale preveda, per finalità di lotta contro la criminalità, una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica».

La Corte risponde alla seconda questione pregiudiziale sollevata nella causa C-203/15 e alla prima questione pregiudiziale nella causa C-698/15 che l'articolo 15, paragrafo 1, della direttiva 2002/58/CE, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta, deve essere interpretato «nel senso che esso osta ad una normativa nazionale, la quale disciplini la protezione e la sicurezza dei dati relativi al traffico e dei dati relativi all'ubicazione, e

segnatamente l'accesso delle autorità nazionali competenti ai dati conservati, senza limitare, nell'ambito della lotta contro la criminalità, tale accesso alle sole finalità di lotta contro la criminalità grave, senza sottoporre detto accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente, e senza esigere che i dati di cui trattasi siano conservati nel territorio dell'Unione» (punto 125).

- 61 Da parte sua, nella sentenza del 19 giugno 2018, *Centrum for Rättvisa c. Svezia*, la Corte EDU ha, nel frattempo, stabilito la conformità all'articolo 8 della Convenzione europea dei diritti dell'uomo della normativa svedese sull'intercettazione su ampia scala di comunicazioni elettroniche. Essa ha osservato, in particolare, quanto segue:

*«La Corte ha espressamente riconosciuto che le autorità nazionali dispongono di un'ampia discrezionalità nella scelta degli strumenti di tutela della sicurezza nazionale (...). Nelle cause Weber e Saravia e Liberty e a., la Corte ha ammesso che i regimi di intercettazione su ampia scala non oltrepassano di per sé detta discrezionalità. Alla luce della motivazione della Corte nelle decisioni succitate e tenuto conto delle minacce che numerosi Stati contraenti sono chiamati a fronteggiare (tra cui la piaga del terrorismo internazionale e di altre forme gravi di criminalità, come il traffico di stupefacenti, la tratta di esseri umani, lo sfruttamento sessuale dei minori e la criminalità informatica), dei progressi tecnologici che rendono più difficile l'individuazione dei terroristi e dei criminali online e dell'impossibilità di prevedere le modalità di trasmissione delle comunicazioni elettroniche, la Corte ritiene che la decisione di ricorrere a un regime di intercettazioni su vasta scala per individuare minacce sino a quel momento sconosciute per la sicurezza nazionale ricada nella discrezionalità degli Stati» (Corte EDU, 19 giugno 2018, *Centrum for Rättvisa c. Svezia*, § 112).*

Per contro, lo stesso giudice ha statuito che la legge inglese sulle intercettazioni delle comunicazioni violava l'articolo 8 della CEDU in quanto irrispettosa dei criteri enunciati nella sua giurisprudenza. La Corte EDU ha altresì rilevato che *«il funzionamento dei regimi di intercettazione di massa rientra, in linea di principio, nella discrezionalità dello Stato. Per definizione, l'intercettazione di massa non è mirata e una sua subordinazione alla presenza di un "sospetto ragionevole" ne renderebbe impossibile l'attuazione» (Corte EDU, 13 settembre 2018, *Big Brother Watch e a. c. Regno Unito*, § 317).*

- 62 Si pone la questione di stabilire in che misura la succitata giurisprudenza, vertente sulla conservazione generalizzata e indifferenziata di dati in materia di comunicazioni elettroniche, sia applicabile alla raccolta, al trasferimento e al trattamento generalizzato e indifferenziato dei dati dei passeggeri, come organizzati dalla legge del 25 dicembre 2016.
- 63 Nel suo succitato parere 1/15, del 26 luglio 2017, la Corte si è pronunciata su un sistema PNR analogo, ma dal campo di applicazione più circoscritto, posto che il progetto di accordo tra il Canada e l'Unione europea sul trasferimento e sul

trattamento dei dati del codice di prenotazione prevedeva «*il trasferimento sistematico e continuo dei dati PNR di tutti i passeggeri aerei dei voli tra l'Unione e il Canada*» (punto 127). Essa ha considerato che «*il trasferimento dei dati PNR verso il Canada e i trattamenti ulteriori degli stessi possono essere considerati idonei a garantire la realizzazione dell'obiettivo, relativo alla protezione della sicurezza e dell'incolumità pubbliche, perseguito dall'accordo previsto*» (punto 153).

Per quanto attiene ai passeggeri interessati, la Corte ha considerato quanto segue:

«186. *L'accordo previsto comprende i dati PNR di tutti i passeggeri aerei dei voli tra l'Unione e il Canada. Il trasferimento di tali dati verso il Canada avviene indipendentemente da qualsiasi elemento obiettivo che consenta di ritenere che i passeggeri possano presentare un rischio per la sicurezza pubblica in Canada.*

187. *A tale riguardo va rilevato che, com'è stato ricordato ai punti 152 e 169 del presente parere, i dati PNR sono destinati, in particolare, ad essere sottoposti a un trattamento automatizzato. Orbene, com'è stato affermato da più intervenienti, tale trattamento mira a identificare il rischio per la sicurezza pubblica che potrebbero eventualmente presentare persone che non sono, in tale fase, conosciute dai servizi competenti e che potrebbero essere, a motivo di tale rischio, soggette a un esame approfondito. A tale riguardo, il trattamento automatizzato di detti dati, prima dell'arrivo dei passeggeri in Canada, facilita e accelera i controlli di sicurezza, in particolare alle frontiere. Inoltre, l'esclusione di talune categorie di persone, o di alcune zone di origine, sarebbe tale da ostacolare la realizzazione dell'obiettivo del trattamento automatizzato dei dati PNR, ossia l'identificazione, per mezzo di una verifica di tali dati, delle persone che possano presentare un rischio per la sicurezza pubblica tra tutti i passeggeri aerei, e a consentire che tale verifica possa essere aggirata.*

188. *Del resto, conformemente all'articolo 13 della convenzione di Chicago, al quale si sono riferiti in particolare il Consiglio e la Commissione nelle loro risposte ai quesiti posti dalla Corte, tutti i passeggeri aerei, all'entrata, all'interno nonché all'uscita dal territorio di uno Stato contraente, devono osservare le leggi ed i regolamenti di tale Stato che disciplinano l'entrata o l'uscita dei passeggeri aerei dal suo territorio. Tutti i passeggeri aerei che intendono entrare in Canada o uscire da tale paese sono, quindi, sottoposti, in base a detto articolo, ai controlli alle frontiere e tenuti a rispettare le condizioni di entrata e di uscita prescritte dal diritto canadese in vigore. Inoltre, come risulta dai punti 152 e 187 del presente parere, l'identificazione, tramite i dati PNR, di passeggeri che possono presentare un rischio per la sicurezza pubblica fa parte dei controlli alle frontiere. Di conseguenza, poiché sono oggetto di tali controlli, i passeggeri aerei che intendono entrare e soggiornare in Canada, a causa della natura stessa di tale misura, sono soggetti alla verifica dei loro dati PNR.*

189. In tali circostanze, non sembra che l'accordo previsto ecceda i limiti dello stretto necessario in quanto consente il trasferimento dei dati PNR di tutti i passeggeri aerei verso il Canada».

- 64 La Cour constitutionnelle (Corte costituzionale) si chiede se queste considerazioni possano essere applicate con riferimento alla direttiva PNR e a una normativa nazionale, come la legge PNR, che, recependo detta direttiva, prevede la raccolta, il trasferimento e l'uso generalizzati e indifferenziati di dati «PNR» per tutti i passeggeri che viaggiano servendosi del trasporto aereo e ferroviario o mediante autobus, a prescindere da un passaggio attraverso le frontiere esterne dell'Unione. Questo sistema si applica, in effetti, a persone per le quali non esiste alcun indizio tale da far credere che il loro comportamento possa avere un nesso, ancorché indiretto o lontano, con reati gravi ed è più ampio di quello previsto dall'accordo «PNR» con il Canada. Tenuto conto della portata dei dati considerati, si pone la questione se detta misura rispetti i limiti dello «stretto necessario». Prima di pronunciarsi nel merito, la Cour constitutionnelle (Corte costituzionale) ha deciso di sottoporre alla Corte una quarta questione pregiudiziale.

Sulle finalità del trattamento dei dati «PNR» (articolo 8 della legge PNR)

- 65 La ricorrente critica la definizione delle finalità del trattamento dei dati «PNR» contenuta nell'articolo 8 della legge PNR, che sarebbe molto più ampia delle «finalità specifiche», limitate - queste ultime - ai soli reati di terrorismo e reati gravi di cui alla direttiva PNR. Essa ritiene che dette finalità eccedano i limiti dello «stretto necessario».

Le finalità del trattamento dei dati «PNR», come previste agli articoli 1, paragrafo 2, e 6, paragrafo 2, della direttiva PNR, costituiscono unicamente obiettivi di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi (v. anche considerando 7 della direttiva PNR).

Talune delle finalità di trattamento di cui all'articolo 8 della legge PNR corrispondono alle infrazioni oggetto dell'allegato II alla direttiva PNR, conformemente agli obiettivi di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi previsti da detta direttiva. Per contro, alle finalità del trattamento dei dati «PNR» previste dalla direttiva di cui trattasi, se ne aggiungono altre. Lo stesso vale in particolare per il «controllo delle attività di cui agli articoli 7, punto 1 e 3/1, e 11, § 1, punti da 1 a 3 e 5, della legge organica del 30 novembre 1998, che disciplina i servizi segreti e di sicurezza» (articolo 8, paragrafo 1, punto 4°).

Il giudice del rinvio esamina se tali altre finalità siano espresse attraverso regole chiare, precise e limitate allo stretto necessario e nutre dubbi quanto alla finalità di cui all'articolo 8, paragrafo 1, punto 4°, della legge PNR.

La motivazione contenuta nella legge PNR precisa che detta «finalità riguarda le competenze dei servizi segreti, vale a dire la Sicurezza dello Stato e il Servizio

generale segreto e di sicurezza (SGRS). Al fine di assolvere i propri compiti di ricerca, analisi e trattamento delle informazioni relative alle attività che possono costituire una minaccia per gli interessi fondamentali dello Stato, detti servizi devono essere in grado di analizzare i dati dei passeggeri per individuare al più presto eventuali minacce concrete, seguire gli spostamenti di specifiche persone o analizzare fenomeni o tendenze più ampie. I compiti concernenti la ricerca, l'analisi e il trattamento delle informazioni relative alle attività dei servizi segreti stranieri sul territorio belga rientrano in detta finalità» (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, pagg. 19 e 20).

Benché i compiti dei servizi segreti e di sicurezza rientrino, in termini generali, nella sicurezza nazionale e internazionale, il trattamento dei dati «PNR» alla luce della finalità indicata dall'articolo 8, paragrafo 1, punto 4, della legge PNR sembra molto vago e generico.

Inoltre, detta finalità è oggetto, per quanto attiene al controllo preliminare dei passeggeri, dello stesso trattamento delle finalità di cui all'articolo 8, paragrafo 1, punti 1, 2 e 5, della legge PNR (articoli 24, paragrafo 2, e 26, paragrafo 2).

In tale contesto, la Cour constitutionnelle (Corte costituzionale) decide di sottoporre alla Corte una quinta questione pregiudiziale diretta a stabilire se detta finalità sia sufficientemente chiara, precisa e limitata allo stretto necessario.

Sulla gestione della banca dati dei passeggeri e sul trattamento dei dati nel quadro del controllo preliminare dei passeggeri e delle ricerche specifiche (articoli 16, da 24 a 27, 50 e 51 della legge PNR)

- 66 La ricorrente ritiene che i diversi trattamenti e il flusso di dati personali siano manifestamente sproporzionati.
- 67 L'articolo 16 della legge PNR prevede che, nel quadro delle finalità indicate all'articolo 8, paragrafo 1, i dati dei passeggeri siano oggetto dei trattamenti previsti agli articoli da 24 a 27.

– *Sul controllo preliminare dei passeggeri (articoli da 24 a 26)*

- 68 I dati dei passeggeri sono trattati ai fini dell'effettuazione di un controllo preliminare (pre-screening) dei passeggeri prima del loro arrivo, della loro partenza o transito previsto sul territorio nazionale al fine di stabilire quali persone debbano essere sottoposte a un controllo più approfondito. «Si tratta di valutare la potenziale minaccia e di stabilire quali passeggeri siano rilevanti ai fini dell'esercizio dei compiti loro affidati o impongano, ad esempio, l'adozione di una determinata misura (esecuzione di un mandato di arresto, ispezione, ...)». (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, pag. 28).

Il controllo preliminare si fonda su due linee direttrici: da una parte, la correlazione dei dati dei passeggeri con le banche dati e, dall'altra, la correlazione dei dati con criteri prestabiliti.

- 69 Per quanto attiene alla correlazione con le banche dati, i lavori preparatori della legge PNR chiariscono che «[l]a prima linea direttrice consiste nella ricerca di corrispondenze positive correlando i dati dei passeggeri con i dati trattati nelle banche dati gestite dai servizi competenti. Ciò consente, ad esempio, di valutare se una persona presenti un elevato livello di pericolosità in quanto inserita in una banca dati della polizia nel quadro di un fascicolo in materia di terrorismo e poiché, dall'analisi dei suoi dati passeggero, risulta recarsi abitualmente in paesi che ospitano campi di addestramento per terroristi o in paesi di transito verso tali luoghi. Può trattarsi, ad esempio, anche di una persona che, in base alle informazioni disponibili presso i servizi segreti, sta preparando un rapimento e che, secondo i dati di trasporto, intende recarsi in un paese in cui detti servizi, grazie alle informazioni ricevute, sanno che potrà reclutare terzi per attuare i suoi piani. Inoltre, quanto più numerose sono le corrispondenze positive riscontrate da più servizi per una stessa persona, tanto più reale è la minaccia.

La corrispondenza positiva può anche imporre l'adozione di una misura su ordine delle autorità giudiziarie, come l'esecuzione di un mandato d'arresto di una persona che si appresta a lasciare il Belgio.

Inoltre, la corrispondenza positiva può derivare da una correlazione con banche dati internazionali come SIS II, Interpol (SLTD).

L'obiettivo non è naturalmente quello di collegare tutte le banche dati dei servizi con la banca dati passeggeri ma di limitare tecnicamente la correlazione con le banche dati in rapporto diretto con le finalità come stabilite dalla legge.

(...)

Detta correlazione potrà anche essere compiuta attraverso elenchi di persone elaborati specificamente a tal fine dai servizi competenti. In conformità alla legge sulla tutela della vita privata e, più in particolare, al suo articolo 4, paragrafo 1, punto 4, detti elenchi devono essere aggiornati a cadenza regolare» (Doc. Parl, Chambre, 2015-2016, DOC 54-2069/001, pagg. 28 e 29).

- 70 Per quanto attiene alla correlazione con criteri prestabiliti, i lavori preparatori della legge PNR precisano quanto segue:

«La seconda linea direttrice consiste nella ricerca di corrispondenze positive attraverso (uno o più) criteri prestabiliti dall'UIP applicati ai dati dei passeggeri. Detti criteri sono composti di uno o più indicatori oggettivi sulla cui base è possibile dedurre che le persone che ne sono oggetto presentano un comportamento a rischio specifico che può costituire una minaccia rispetto alle finalità di cui all'articolo 8, paragrafo 1, punti 1, 4 e 5, della legge.

Detti criteri possono integrare, ad esempio, determinati comportamenti specifici in materia di prenotazione o di viaggio.

Il loro impiego presenta il vantaggio di poter far emergere profili di passeggeri a rischio che non sono necessariamente noti o menzionati nelle banche dati dei servizi.

Detti criteri possono riguardare, ad esempio, un paese di destinazione o di partenza, combinato a determinate informazioni sul viaggio come le modalità di pagamento e la data di prenotazione» (Doc. Parl, Chambre, 2018-2019, DOC 54-3652/001, pagg. 29 e 30).

«Il controllo preliminare realizzato nel quadro della finalità relativa al controllo dei fenomeni di vigilanza amministrativa e dei gruppi legati alla radicalizzazione violenta è soggetto a condizioni molto più restrittive rispetto alle altre finalità (...)

In sede di controllo preliminare realizzato nel quadro di altre finalità è autorizzato l'accesso ai dati dei passeggeri elencati all'articolo 9» (ibid., pag. 31).

«La corrispondenza positiva deve, in ogni caso, essere convalidata dall'UIP. Infatti, al fine di garantire il pieno rispetto del diritto alla protezione dei dati personali, (...) nessuna decisione implicante conseguenze giuridiche per una determinata persona o idonea a danneggiarla gravemente può essere adottata sulla semplice base del trattamento automatizzato dei dati dei file contenenti informazioni sul suo viaggio. Ecco perché la valutazione effettuata da una persona precederà sempre ogni decisione vincolante per l'interessato.

Detta validazione deve intervenire entro le 24 ore al fine di consentire l'accesso alla banca dati dei passeggeri.

A seguito della validazione della corrispondenza positiva, i servizi alla base di detta corrispondenza garantiscono che ad essa sia dato utilmente seguito entro un termine adeguato. Dare utilmente seguito potrebbe significare l'adozione di una misura attiva (perquisizione, arresto...), ma anche, in via provvisoria, una sua mancata adozione. Tale valutazione operativa spetta pienamente ai servizi competenti» (ibid., pagg. 30 e 31).

- 71 Quanto ai criteri di valutazione prestabiliti dall'UIP, essi non possono essere fondati su dati che rivelano l'origine razziale o etnica di una persona, le sue convinzioni religiose o filosofiche, le sue opinioni politiche, la sua appartenenza a un'organizzazione sindacale, il suo stato di salute, la sua vita sessuale o il suo orientamento sessuale. La valutazione dei passeggeri prima del loro arrivo, transito o partenza in ragione di criteri prestabiliti non è compiuta in modo discriminatorio. Tali criteri non possono riguardare l'identificazione di un individuo e devono essere mirati, proporzionati e specifici.
- 72 Nel suo parere del 19 agosto 2016, il comitato consultivo della Convenzione n. 108 ha osservato quanto segue:

«Il trattamento dei dati personali può riguardare tutti i passeggeri e non soltanto specifici individui sospettati di essere coinvolti in un reato o di rappresentare una minaccia immediata alla sicurezza nazionale o all'ordine pubblico.

(...)

La valutazione dei passeggeri mediante l'abbinamento dei dati può sollevare la questione della prevedibilità, in particolare quando è compiuta sulla base di algoritmi predittivi utilizzando criteri dinamici che possono evolvere in continuazione in base alle capacità di autoapprendimento.

Lo sviluppo di algoritmi per l'esplorazione dei dati dovrebbe fondarsi sui risultati di valutazioni regolari del probabile impatto del trattamento dei dati sui diritti e sulle libertà fondamentali delle persone interessate.

La struttura di base delle analisi dovrebbe fondarsi su indicatori di rischio predefiniti chiaramente stabiliti in anticipo.

La pertinenza dei risultati individuali di dette evoluzioni automatiche dovrebbe essere esaminata con cura caso per caso da una persona e non in maniera automatizzata» (parere del 19 agosto 2016, T-PD(2016)18rev, pag. 8).

- 73 Nella fattispecie, le banche dati indicate all'articolo 24 sono definite con precisione e si trovano in rapporto diretto con le finalità indicate all'articolo 8 della legge PNR. Si tratta, infatti, di banche dati dei «servizi competenti», vale a dire dei servizi di polizia, della Sicurezza dello Stato, del Servizio generale segreto e di sicurezza e delle dogane.

Inoltre, l'articolo 24, paragrafi 4 e 5, della legge PNR garantisce che, in caso di riscontro positivo, il trattamento sistematico automatizzato sia oggetto di una verifica individuale mediante strumenti non automatizzati al fine di valutare se l'autorità competente debba adottare misure in forza del diritto nazionale, come richiesto dall'articolo 6, paragrafo 5, della direttiva PNR.

- 74 Nel suo parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017 (EU:C:2017:592), la Corte di giustizia aveva anche insistito sulla necessità di un riesame individuale mediante mezzi non automatizzati prima dell'adozione di una misura individuale (punto 173).

L'esigenza di un intervento umano, a seguito di una corrispondenza positiva, rappresenta una garanzia idonea ad assicurare che il controllo preliminare non si fondi unicamente su strumenti automatizzati e contribuisca così all'efficacia del sistema.

Un controllo preliminare sistematico dei passeggeri rappresenta quindi, in linea di principio, una misura pertinente alla luce dell'obiettivo che consiste nell'individuare e prevenire minacce per la sicurezza pubblica.

Tuttavia, come già osservato dalla Corte di giustizia nel suo succitato parere 1/15 del 26 luglio 2017, i trattamenti originati dal controllo preliminare «*possono fornire informazioni supplementari sulla vita privata dei passeggeri aerei*» (punto 131); inoltre, «*dette analisi sono effettuate senza che esistano motivi fondati su circostanze individuali che consentano di ritenere che gli interessati potrebbero presentare un rischio per la sicurezza pubblica*» (*ibid.*, punto 132).

Constatando che il trattamento automatizzato dei dati «PNR», fondato su modelli e criteri prestabiliti, presenta un tasso di errore significativo (*ibid.*, punti 169 e 170), la Corte ha tuttavia considerato che «*i modelli e i criteri prestabiliti dovrebbero essere, da un lato, specifici e affidabili, consentendo di raggiungere (...) risultati che abbiano come obiettivo gli individui sui quali potrebbe gravare un sospetto ragionevole di partecipazione a reati di terrorismo o a reati gravi di natura transnazionale e, dall'altro, non discriminatori*» e che «*le banche dati con le quali i dati PNR sono confrontati devono essere affidabili, aggiornate e limitate a banche dati gestite dal Canada in relazione alla lotta al terrorismo e ai reati gravi di natura transnazionale*» (*ibid.*, punto 172). Infine, per garantire che detta valutazione non abbia natura discriminatoria e sia limitata allo stretto necessario, la Corte ha ritenuto che «*l'affidabilità e l'aggiornamento di tali modelli e criteri prestabiliti nonché delle banche dati utilizzate dovrebbero essere oggetto, tenendo conto di dati statistici e dei risultati della ricerca internazionale, del riesame congiunto dell'attuazione dell'accordo previsto*», un anno dopo l'entrata in vigore e in seguito periodicamente (*ibid.*, punto 174).

- 75 Quanto al resto, sembrerebbe tecnicamente impossibile definire ulteriormente i criteri prestabiliti che possano servire ai fini della determinazione di profili di rischio. Come detto prima, i criteri di cui trattasi devono essere specifici, affidabili e non discriminatori.
- 76 Benché la direttiva PNR e la legge PNR non forniscano alcuna indicazione sulla modalità con cui i criteri alla base del controllo preliminare siano prestabiliti dall'UIP, le garanzie che circondano l'elaborazione di detti criteri sembrano sufficienti per non giudicare sproporzionata la misura impugnata. Tuttavia, per stabilire se detto controllo preliminare sistematico sia sufficientemente chiaro, preciso e limitato allo stretto necessario, occorre sottoporre alla Corte una sesta questione pregiudiziale.

– *Sulle ricerche specifiche (articoli 27, 50 e 51)*

- 77 L'articolo 27 della legge PNR autorizza il trattamento dei dati dei passeggeri per compiere ricerche specifiche per le finalità indicate nell'articolo 8, paragrafo 1, punti 1, 2, 4 e 5, e alle condizioni previste all'articolo 46 *septies* del codice di procedura penale o all'articolo 16/3 della legge del 30 novembre 1998, introdotti, rispettivamente, dagli articoli 50 e 51 della legge PNR. Conformemente all'articolo 20 della legge PNR, le condizioni di applicazione dell'articolo 27 valgono anche per le richieste di accesso alla scadenza del termine di sei mesi previsto all'articolo 19.

- 78 L'articolo 46 *septies* del codice di procedura penale riguarda ricerche specifiche nel quadro della finalità di cui all'articolo 8, paragrafo 1, punti 1, 2 e 5, della legge PNR. Detta misura è accompagnata da varie garanzie, tra cui l'autorizzazione preliminare da parte del procureur du Roi (pubblico ministero belga).
- 79 L'articolo 16/3 della legge del 30 novembre 1998 riguarda, dal canto suo, ricerche specifiche nel quadro della finalità indicata nell'articolo 8, paragrafo 1, punto 4, della legge PNR. Detta misura è accompagnata da varie garanzie, tra cui l'informazione e il controllo da parte del Comité permanent R (Comitato permanente R.).
- 80 La ricorrente ritiene che i membri distaccati dei servizi di polizia appartenenti all'UIP non siano sufficientemente indipendenti per rispondere alle domande di accesso nel quadro di ricerche specifiche.
- 81 L'articolo 14, paragrafo 1, della legge PNR stabilisce la composizione dell'UIP. Al riguardo, i lavori preparatori chiariscono quanto segue: *«Il modello belga si fonda su un'idea di unità multidisciplinare composta da un funzionario a livello dirigenziale che esplica funzioni di direzione, membri amministrativi e membri distaccati provenienti dai servizi competenti.*

L'UIP sarà composta:

- *da un funzionario a livello dirigenziale assistito da un servizio di supporto che, in seno al SPF dell'Interno, sarà responsabile in particolare della gestione della banca dati, del rispetto degli obblighi dei vettori e degli operatori di viaggio, dell'attività di rendicontazione, della stipula di protocolli con i servizi competenti e del rispetto delle condizioni di trattamento. Il servizio di supporto sarà composto, segnatamente, da analisti, giuristi, esperti ICT e dal delegato alla protezione dei dati, che disporranno delle necessarie autorizzazioni di sicurezza;*
- *da membri distaccati provenienti dai servizi competenti tassativamente indicati nel punto 2 del paragrafo 1, vale a dire: i servizi di polizia, i servizi segreti e la Dogana. Le precise finalità rappresentano, di per sé, la prima limitazione. Ad esempio, a livello dei servizi della polizia integrata, è evidente che un agente di quartiere all'interno della polizia locale non potrà mai venire a conoscenza dei dati dei passeggeri posto che le finalità non rientrano nei suoi compiti.*

Il distaccamento dei servizi competenti mira a garantire un certo livello di competenze ma non esclude assolutamente accordi tra di essi al fine di condividere i distacchi» (Doc. Parl, Chambre, 2015-2016, DOC 54-2069/001, pag. 22).

Il ministre de la Sécurité et de l'Intérieur (Ministro della Sicurezza e degli Interni) ha aggiunto che *«[s]arà nominato anche un data protection officer incaricato di relazionare alla Commission de la protection de la vie privée (Commissione per*

la tutela della vita privata)» (Doc. parl, Chambre, 2015-2016, DOC 54-2069/003, pag. 24).

L'arrêté royal du 21 décembre 2017, relatif à l'exécution de la loi PNR (regio decreto del 21 dicembre 2017, rcante esecuzione della legge PNR) stabilisce le modalità di composizione e organizzazione dell'UIP. La relazione al Re che introduce detto regio decreto precisa che *«[L]a banca dati può (...) essere consultata solo in seno all'UIP e unicamente da parte dei suoi membri, nel quadro dell'espletamento delle loro mansioni, e dal delegato alla protezione dei dati»³.*

La procedura di distacco è prevista dagli articoli da 12 a 21 di detto regio decreto. Il coinvolgimento dei membri distaccati dei servizi competenti nel funzionamento dell'UIP mira a garantire che detto ufficio sia composto da persone che godono di una certa esperienza al fine di rafforzare l'efficacia della sua azione. Tale possibilità di distacco è peraltro espressamente prevista dall'articolo 4, paragrafo 3, della direttiva PNR.

Nulla consente di ritenere che queste persone, pur mantenendo il loro status nel rispettivo servizio di origine, non esercitino le loro funzioni in maniera indipendente all'interno dell'UIP. Inoltre, i membri dell'UIP sono soggetti a sanzioni penali in caso di mancato rispetto del segreto professionale o laddove omettano, consapevolmente e volontariamente, di fornire informazioni, dati e notizie ostacolando le finalità di cui all'articolo 8 (articoli 48 e 49).

- 82 Per quanto attiene all'accesso ai dati «PNR» nel quadro di ricerche specifiche decorso un termine di sei mesi, nel suo parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017 (EU:C:2017:592), la Corte ha rilevato che l'uso dei dati PNR così archiviati dovrebbe *«essere fondato su criteri oggettivi per definire le circostanze e le condizioni alle quali le autorità canadesi contemplate dall'accordo previsto possano avere accesso a tali dati ai fini del loro uso»* e che *«tale uso dovrebbe essere subordinato, salvo casi di urgenza debitamente giustificati, a un controllo preventivo effettuato o da un giudice, o da un ente amministrativo indipendente la cui decisione che autorizzi l'uso intervenga a seguito di una richiesta motivata di tali autorità presentata, in particolare, nell'ambito di procedure di prevenzione, di accertamento o di esercizio dell'azione penale»* (punto 208).
- 83 Al fine di verificare se l'UIP possa essere considerata come detta «altra autorità nazionale competente» ai sensi dell'articolo 12, paragrafo 3, della direttiva PNR, occorre, prima di pronunciarsi, sottoporre alla Corte di giustizia una settima questione pregiudiziale.

³ *Moniteur belge* del 29 dicembre 2017, seconda edizione, pag. 116833.

Sulla durata della conservazione dei dati «PNR» (articolo 18 della legge PNR)

- 84 La ricorrente ritiene che il termine di conservazione di cinque anni previsto per i dati «PNR» sia sproporzionato.
- 85 Il considerando 25 della direttiva PNR enuncia quanto segue:
- «Il periodo di conservazione dei dati PNR dovrebbe essere lungo quanto necessario e proporzionato agli obiettivi di prevenire, accertare, indagare e promuovere un'azione penale nei confronti dei reati di terrorismo e dei reati gravi. Tenuto conto della loro natura e del loro uso, occorre che i dati PNR siano conservati per un periodo sufficientemente lungo per poter effettuare analisi e utilizzarli nelle indagini. Per evitare un uso sproporzionato, è opportuno che dopo il periodo iniziale i dati PNR siano resi anonimi mediante mascheratura degli elementi dei dati. Per garantire il massimo livello di protezione dei dati, è opportuno che l'accesso alla serie integrale di dati PNR, che consenta l'identificazione diretta dell'interessato, sia concesso soltanto a condizioni molto rigorose e limitate dopo detto periodo iniziale».
- 86 Secondo la giurisprudenza della Corte di giustizia, la durata della conservazione dei dati deve «sempre rispondere (...) a criteri oggettivi, che pongano un rapporto tra i dati personali da conservare e l'obiettivo perseguito» (sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 93; ordinanza del 16 marzo 2017, Tele2 Sverige e Watson e a., C-203/15 REC e C-698/15 REC, EU:C:2017:222, punto 110; parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punto 191).
- 87 Per quanto riguarda, più nello specifico, i dati «PNR», nel succitato parere 1/15 del 26 luglio 2017, la Corte di giustizia ha ritenuto che la durata di cinque anni *«non sembra eccedere i limiti di quanto è strettamente necessario ai fini della lotta al terrorismo e ai reati gravi di natura transnazionale»* (punto 209), fermo restando che *«per quanto riguarda i passeggeri aerei per i quali un siffatto rischio non è stato individuato al loro arrivo in Canada e fino alla loro partenza da tale paese terzo, non sembra che esista, una volta ripartiti, alcun rapporto, sia pure indiretto, tra i loro dati PNR e l'obiettivo perseguito dall'accordo previsto, che giustifichi (...) un'archiviazione continua dei dati PNR di tutti i passeggeri aerei dopo la loro partenza dal Canada ai fini di un eventuale accesso a detti dati, indipendentemente da un qualsivoglia collegamento con la lotta al terrorismo e ai reati gravi di natura transnazionale (v., per analogia, sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a., C-203/15 e C-698/15, EU:C:2016:970, punto 119)»* (punto 205).
- 88 L'articolo 18 della legge PNR prevede che i dati dei passeggeri siano conservati nella banca dati passeggeri per un periodo massimo di cinque anni a decorrere dalla loro registrazione e che, decorso detto termine, siano distrutti. Conformemente all'articolo 21, paragrafo 1, di detta legge, l'UIP vigila affinché i

dati dei passeggeri siano cancellati dalla sua banca dati in maniera definitiva decorso il periodo di cui all'articolo 18.

Tuttavia, il termine di cinque anni deve essere letto in combinato disposto con gli articoli 19 e seguenti della medesima legge, che disciplinano anche le modalità di conservazione dei dati. L'articolo 19 di detta legge deve esso stesso essere letto in combinato disposto con l'articolo 4, punto 14, che definisce la «personalizzazione mediante mascheramento di elementi di dati» come «l'operazione volta a rendere invisibili per un utente elementi di dati che potrebbero servire a identificare direttamente la persona interessata, di cui all'articolo 19».

L'articolo 20 della legge PNR prevede che alla scadenza del periodo di sei mesi di cui all'articolo 19, la comunicazione della totalità dei dati passeggeri è autorizzata unicamente ai fini del trattamento dei dati prescritto all'articolo 27 e soltanto in conformità alle disposizioni ivi contenute.

Inoltre, il risultato del trattamento di cui all'articolo 24 è conservato dall'UIP soltanto per il tempo necessario per informare le autorità competenti e le UIP degli altri Stati membri dell'esistenza di una corrispondenza positiva (articolo 21, paragrafo 3, primo comma).

L'articolo 22 della legge PNR garantisce che il funzionario a livello dirigenziale e il delegato alla protezione dei dati abbiano accesso a tutti i dati rilevanti solo nel quadro dell'espletamento dei loro compiti.

Infine, il trattamento dei dati è oggetto di registrazione ed è in correlazione diretta con le finalità previste all'articolo 8 (articolo 23, paragrafo 1). L'UIP vigila sulla registrazione conservando, sotto la propria responsabilità, per cinque anni traccia documentale di tutti i sistemi e le procedure di trattamento (articolo 23, paragrafo 2, primo comma).

- 89 La durata della conservazione dei dati dei passeggeri deve essere stabilita tenendo conto delle finalità del trattamento di detti dati, in legame diretto con gli obiettivi della prevenzione, della ricerca e del perseguimento dei reati di terrorismo e dei reati gravi.
- 90 Tuttavia, la Commissione per la tutela della vita privata aveva osservato che, in presenza di un termine di conservazione di lunga durata e di una conservazione di ampia portata dei dati, «il rischio di profilazione degli interessati aumenta, al pari del rischio di sviamento della finalità (*fonction creep*), vale a dire il potenziale sviamento dell'utilizzo dei dati per infrazioni diverse rispetto alle quali non vi era inizialmente accordo (politico) sullo scambio dei dati» [Commissione per la tutela della vita privata, parere di iniziativa n. 01/2010 del 13 gennaio 2010, relativo al progetto di legge sull'approvazione dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e sul trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) da parte dei vettori aerei al Dipartimento per la sicurezza interna degli Stati Uniti (DHS) (Accordo PNR del

2007), fatto a Bruxelles il 23 luglio 2007 e a Washington il 26 luglio 2007, punto 3.3, pagg. 17 e 18).

Nel suo parere n. 55/2015, del 16 dicembre 2015, sul progetto di legge divenuto la legge PNR, la Commissione per la tutela della vita privata riteneva altresì che la necessità di un termine quinquennale di conservazione dei dati dovesse essere giustificata in maniera più precisa e fondata.

Nel suo parere del 19 agosto 2016, il comitato consultivo della Convenzione n. 108 aveva altresì osservato che «i dati mascherati consentono ancora di identificare le persone e mantengono per tale ragione il carattere di dati personali e anche la loro conservazione deve essere limitata nel tempo per prevenire un controllo permanente generalizzato» (parere del 19 agosto 2016, T-PD(2016)18rev, pag. 9).

- 91 La Cour constitutionnelle (Corte costituzionale) ritiene che si renda necessario sottoporre alla Corte un’ottava questione pregiudiziale al fine di stabilire se - tenuto conto di quanto precede e delle diverse garanzie elencate al precedente punto 88 - detto termine quinquennale di conservazione autorizzato dalla direttiva PNR sia compatibile con le osservazioni della Corte di giustizia citate al precedente punto 87, nella parte in cui non opera alcuna distinzione tra i passeggeri interessati a seconda che, nel quadro del controllo preliminare, risulti o meno che essi rappresentano una minaccia per la sicurezza pubblica.

3. *Sul secondo motivo*

- 92 La ricorrente ritiene che, estendendo il sistema «PNR» ai voli intra-UE, le disposizioni impugnate ripristinino indirettamente controlli alle frontiere lesivi della libera circolazione delle persone.
- 93 Per quanto attiene all’ambito di applicazione della legge PNR, i lavori preparatori precisano quanto segue:

«L’inclusione dei trasferimenti intra-UE nella raccolta dei dati consentirà di ottenere un quadro più completo degli spostamenti dei passeggeri che rappresentano una potenziale minaccia per la sicurezza intracomunitaria e nazionale. La prassi ha già dimostrato che taluni “returnees” (chiamati anche *foreign fighter* che rientrano in Europa) si imbarcano su diversi voli prima di raggiungere la loro destinazione finale.

La direttiva UE PNR prevede esplicitamente la possibilità per gli Stati membri di trattare i dati dei passeggeri dell’UE per il traffico internazionale all’interno dell’Unione europea. Inoltre, il 21 aprile 2016, tutti gli Stati membri hanno approvato, in seno al Consiglio dei Ministri degli Interni e della Giustizia, una dichiarazione diretta a recepire la direttiva UE PNR nei diritti nazionali anche per il traffico interno all’Unione europea» (Doc. Parl., Chambre, 2015-2016, DOC 54-2069/001, pag. 7).

- 94 La Cour constitutionnelle (Corte costituzionale) osserva che i passeggeri di cui al capo 11 della legge PNR, come i dati indicati e il termine di conservazione, sono limitati.

Infatti, nei lavori preparatori si osserva che «(...) sono interessati soltanto i passeggeri che intendono attraversare o che hanno attraversato le frontiere esterne del Belgio per entrarvi o uscirne, indipendentemente dal tipo di trasporto utilizzato (marittimo, ferroviario, terrestre, aereo). Pertanto, unicamente i dati di detti passeggeri saranno utilizzati dai servizi di polizia incaricati del controllo alle frontiere e dall'Ufficio stranieri.

Anche i passeggeri che intendono transitare per la zona internazionale di transito, ad esempio, di un aeroporto situato in Belgio sono interessati nella misura in cui sono soggetti alle norme in materia di accesso al territorio, soggiorno, stabilimento e allontanamento degli stranieri. Queste persone devono quindi disporre dei documenti di viaggio richiesti. Determinate persone sono soggette ad obbligo di visto di transito aeroportuale; in tali aree sono ammessi controlli che possono, in taluni casi, portare all'adozione di una misura di respingimento.

(...) Solo i dati dei passeggeri detti "API" saranno trasmessi ai servizi di polizia e all'Ufficio stranieri in forza del presente capo. Tali dati sono elencati nell'articolo 9, paragrafo 2, del disegno di legge.

Essi corrispondono essenzialmente a quelli che i vettori aerei devono già trasmettere in forza del regio decreto dell'11 dicembre 2006.

(...)

Inoltre, l'utilizzo dei dati è limitato a ventiquattro ore. Al di là di tale termine, se l'accesso ai dati dei passeggeri si rende necessario nel quadro dell'esercizio dei suoi compiti di legge, l'Ufficio stranieri invia all'UIP una richiesta motivata» (*ibid.*, pagg. 34 e 35).

- 95 Come detto prima, il considerando 10 della direttiva PNR autorizza l'estensione del sistema «PNR» ai voli intra-UE. L'articolo 2 della direttiva PNR disciplina la procedura diretta a estendere il campo di applicazione.

La finalità della lotta contro l'immigrazione irregolare e del miglioramento del controllo alle frontiere riguarda unicamente le categorie di passeggeri elencate all'articolo 29, paragrafo 2, della legge PNR, ed è circoscritta ai dati «API» di cui all'articolo 9, paragrafo 1, punto 18°, di detta legge. I trattamenti compiuti nel quadro di tale finalità sono parimenti circoscritti. Le disposizioni impugnate si inseriscono nel quadro del recepimento della direttiva «API» che ha, anch'essa, come obiettivi la lotta contro l'immigrazione irregolare e il miglioramento del controllo alle frontiere.

- 96 Tuttavia, nel suo parere n. 55/2015, del 16 dicembre 2015, sul progetto di legge divenuto la legge del 25 dicembre 2016, la Commissione per la tutela della vita

privata s'interroga sulla compatibilità con il principio della libera circolazione delle persone dell'istituito sistema «PNR» che riguarda «sia i trasporti da e verso l'area Schengen (extra-Schengen) che i trasporti in entrata e in uscita all'interno di essa (intra-Schengen)», il che potrebbe sfociare «indirettamente in una reintroduzione dei controlli alle frontiere interne» (punti da 21 a 25).

- 97 Nutrendo dubbi quanto all'interpretazione e alla validità della direttiva 2004/82 «API», alla luce della Carta e del TUE, la Cour constitutionnelle (Corte costituzionale) decide di sottoporre alla Corte una nona questione pregiudiziale.
- 98 La Cour constitutionnelle (Corte costituzionale) pone un'ultima questione concernente l'eventuale gestione degli effetti della sua sentenza nel tempo.

IV. Questioni pregiudiziali

La Cour constitutionnelle (Corte costituzionale) solleva quindi le seguenti questioni pregiudiziali:

1. Se l'articolo 23 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati - RGPD), in combinato disposto con l'articolo 2, paragrafo 2, lettera d), di detto regolamento, debba essere interpretato nel senso che esso si applica a una normativa nazionale come la legge del 25 dicembre 2016, in materia di trattamento dei dati dei passeggeri, che recepisce la direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, la direttiva 2004/82/CE del Consiglio, del 29 aprile 2004, concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate e la direttiva 2010/65/UE del Parlamento europeo e del Consiglio, del 20 ottobre 2010, relativa alle formalità di dichiarazione delle navi in arrivo o in partenza da porti degli Stati membri e che abroga la direttiva 2002/6/CE.

2. Se l'allegato I alla direttiva (UE) 2016/681 sia compatibile con gli articoli 7, 8 e 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, nella misura in cui i dati ivi enumerati sono molto ampi - in particolare, i dati di cui al punto 18 dell'allegato I alla direttiva (UE) 2016/681, che eccedono i dati di cui all'articolo 3, paragrafo 2, della direttiva 2004/82/CE - e nella misura in cui, considerati complessivamente, detti dati potrebbero rivelare dati delicati e violare così i limiti dello «stretto necessario».

3. Se i punti 12 e 18 dell'allegato I alla direttiva (UE) 2016/681 siano compatibili con gli articoli 7, 8 e 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, nella misura in cui, tenuto conto dei termini «comprese» e «tra cui», i dati ivi indicati sono menzionati a titolo esemplificativo

e non tassativo, con conseguente violazione eventuale del requisito di precisione e chiarezza delle disposizioni che comportano un'ingerenza nel diritto al rispetto della vita privata e nel diritto alla protezione dei dati personali.

4. Se l'articolo 3, punto 4, della direttiva (UE) 2016/681 e l'allegato I a detta stessa direttiva siano compatibili con gli articoli 7, 8 e 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, nella misura in cui il sistema di raccolta, trasferimento e trattamento generalizzato dei dati dei passeggeri introdotto da dette disposizioni riguarda tutte le persone che si servono di un determinato mezzo di trasporto, a prescindere da ogni elemento obiettivo che consenta di ritenere che detta persona possa presentare un rischio per la sicurezza pubblica.

5. Se l'articolo 6 della direttiva (UE) 2016/681, in combinato disposto con gli articoli 7, 8 e 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, debba essere interpretato nel senso che esso osta a una normativa nazionale, come la legge impugnata, che ammette, quale finalità del trattamento dei dati «PNR», il controllo delle attività oggetto dei servizi segreti e di sicurezza, includendo così detta finalità nella prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

6. Se l'articolo 6 della direttiva (UE) 2016/681 sia compatibile con gli articoli 7, 8 e 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, nella misura in cui il controllo preliminare da esso introdotto, mediante correlazione con banche dati e criteri prestabiliti, si applica in maniera sistematica e generalizzata ai dati dei passeggeri, a prescindere da qualsiasi elemento obiettivo che consenta di ritenere che essi possano presentare un rischio per la sicurezza pubblica.

7. Se la nozione di «altra autorità nazionale competente» di cui all'articolo 12, paragrafo 3, della direttiva (UE) 2016/681 possa essere interpretata come indicante l'UIP istituita dalla legge del 25 dicembre 2016, che potrebbe quindi autorizzare, nel quadro di ricerche specifiche, l'accesso ai dati «PNR», decorso un termine di sei mesi.

8. Se l'articolo 12 della direttiva (UE) 2016/681, in combinato disposto con gli articoli 7, 8 e 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, debba essere interpretato nel senso che esso osta a una normativa nazionale come la legge impugnata che prevede un termine generale di conservazione dei dati di cinque anni, senza differenziare a seconda che i passeggeri interessati si rivelino, nel quadro del controllo preliminare, idonei o meno a presentare una minaccia per la sicurezza pubblica.

9. a) Se la direttiva 2004/82/CE sia compatibile con l'articolo 3, paragrafo 2, del Trattato sull'Unione europea e con l'articolo 45 della Carta dei diritti fondamentali dell'Unione europea, nella misura in cui gli obblighi ivi previsti si applicano ai voli interni all'Unione europea.

b) Se la direttiva 2004/82/CE, in combinato disposto con l'articolo 3, paragrafo 2, del Trattato sull'Unione europea e con l'articolo 45 della Carta dei diritti fondamentali dell'Unione europea, debba essere interpretata nel senso che essa osta a una disciplina nazionale come quella della legge impugnata che, ai fini del contrasto all'immigrazione irregolare e del rafforzamento dei controlli alle frontiere, autorizza un sistema di raccolta e trattamento dei dati dei passeggeri «diretti, provenienti o in transito sul territorio nazionale», il che potrebbe comportare indirettamente una reintroduzione dei controlli alle frontiere interne.

10. Qualora, sulla base delle risposte fornite alle questioni pregiudiziali che precedono, la Cour constitutionnelle (Corte costituzionale belga) dovesse giungere alla conclusione che la legge impugnata, che recepisce in particolare la direttiva (UE) 2016/681, viola uno o più degli obblighi derivanti dalle disposizioni citate in tali questioni, se detto giudice possa mantenere provvisoriamente gli effetti della legge del 25 dicembre 2016, in materia di trattamento dei dati dei passeggeri, per evitare una situazione di incertezza del diritto e consentire che i dati raccolti e conservati in precedenza possano ancora essere utilizzati per le finalità previste dalla legge.