Raccolta della giurisprudenza

SENTENZA DELLA CORTE (Grande Sezione)

6 ottobre 2015*

«Rinvio pregiudiziale — Dati personali — Protezione delle persone fisiche con riguardo al trattamento di tali dati — Carta dei diritti fondamentali dell'Unione europea — Articoli 7, 8 e 47 — Direttiva 95/46/CE — Articoli 25 e 28 — Trasferimento di dati personali verso paesi terzi — Decisione 2000/520/CE — Trasferimento di dati personali verso gli Stati Uniti — Livello di protezione inadeguato — Validità — Denuncia di una persona fisica i cui dati sono stati trasferiti dall'Unione europea verso gli Stati Uniti — Poteri delle autorità nazionali di controllo»

Nella causa C-362/14,

avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dalla High Court (Corte d'appello, Irlanda), con decisione del 17 luglio 2014, pervenuta in cancelleria il 25 luglio 2014, nel procedimento

Maximillian Schrems

contro

Data Protection Commissioner,

con l'intervento di:

Digital Rights Ireland Ltd,

LA CORTE (Grande Sezione),

composta da V. Skouris, presidente, K. Lenaerts, vicepresidente, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (relatore) e S. Rodin, K. Jürimäe, presidenti di sezione, A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský, D. Šváby, M. Berger, F. Biltgen e C. Lycourgos, giudici,

avvocato generale: Y. Bot

cancelliere: L. Hewlett, amministratore principale

vista la fase scritta del procedimento e in seguito all'udienza del 24 marzo 2015,

considerate le osservazioni presentate:

— per M. Schrems, da N. Travers, SC, P. O'Shea, BL, e G. Rudden, solicitor, nonché da H. Hofmann, Rechtsanwalt;

* Lingua processuale: l'inglese.

— per il Data Protection Commissioner, da. P. McDermott, BL, S. More O'Ferrall e D. Young, solicitors;

— per la Digital Rights Ireland Ltd, da F. Crehan, BL, nonché da S. McGarr e E. McGarr, solicitors;

— per l'Irlanda, da A. Joyce, B. Counihan e E. Creedon, in qualità di agenti, assistiti da D. Fennelly, BL;

— per il governo belga, da J.-C. Halleux e C. Pochet, in qualità di agenti;

— per il governo ceco, da M. Smolek e J. Vláčil, in qualità di agenti;

— per il governo italiano, da G. Palmieri, in qualità di agente, assistita da P. Gentili, avvocato dello Stato;

— per il governo austriaco, da G. Hesse e G. Kunnert, in qualità di agenti;

— per il governo polacco, da M. Kamejsza, M. Pawlicka e B. Majczyna, in qualità di agenti;

— per il governo sloveno, da A. Grum e V. Klemenc, in qualità di agenti;

— per il governo del Regno Unito, da L. Christie e J. Beeko, in qualità di agenti, assistiti da J. Holmes, barrister;

— per il Parlamento europeo, da D. Moore, A. Caiola e M. Pencheva, in qualità di agenti;

— per la Commissione europea, da B. Schima, B. Martenczuk, B. Smulders e J. Vondung, in qualità di agenti;

— per il Garante europeo della protezione dei dati (GEPD), da C. Docksey, A. Buchta e V. Pérez Asinari, in qualità di agenti,

sentite le conclusioni dell'avvocato generale, presentate all'udienza del 23 settembre 2015,

ha pronunciato la seguente

Sentenza

1 La domanda di pronuncia pregiudiziale verte sull'interpretazione, alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»), degli articoli 25, paragrafo 6, e 28 della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281, pag. 31), come modificata dal regolamento (CE) n. 1882/2003 del Parlamento europeo e del Consiglio, del 29 settembre 2003 (GU L 284, pag. 1; in prosieguo: la «direttiva 95/46»), nonché, in sostanza, sulla validità della decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46 sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti (GU L 215, pag. 7).

2 Tale domanda è stata presentata nell'ambito di una controversia fra il sig. Schrems e il Data Protection Commissioner (commissario per la protezione dei dati; in prosieguo: il «commissario») concernente il rifiuto, da parte di quest'ultimo, di istruire una denuncia presentata dal sig. Schrems per il fatto che Facebook Ireland Ltd (in prosieguo: «Facebook Ireland») trasferisce negli Stati Uniti i dati personali dei propri utenti e li conserva su server ubicati in tale paese.

Contesto normativo

La direttiva 95/46

3 I considerando 2, 10, 56, 57, 60, 62 e 63 della direttiva 95/46 così recitano:

«(2) (...) i sistemi di trattamento dei dati sono al servizio dell'uomo; (…) essi, indipendentemente dalla nazionalità o dalla residenza delle persone fisiche, debbono rispettare le libertà e i diritti fondamentali delle stesse, in particolare la vita privata, e debbono contribuire (…) al benessere degli individui;

(...)

(10) (...) le legislazioni nazionali relative al trattamento dei dati personali hanno lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, riconosciuto anche dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali[, firmata a Roma il 4 novembre 1950,] e dai principi generali del diritto comunitario; (…) pertanto il ravvicinamento di dette legislazioni non deve avere per effetto un indebolimento della tutela da esse assicurata ma deve anzi mirare a garantire un elevato grado di tutela nella Comunità;

(...)

(56) (...) lo sviluppo degli scambi internazionali comporta necessariamente il trasferimento oltre frontiera di dati personali; (…) la tutela delle persone garantita nella Comunità dalla presente direttiva non osta al trasferimento di dati personali verso paesi terzi che garantiscano un livello di protezione adeguato; (…) l'adeguatezza della tutela offerta da un paese terzo deve essere valutata in funzione di tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti;

(57) (...) per contro, (...) deve essere vietato il trasferimento di dati personali verso un paese terzo che non offre un livello di protezione adeguato;

(...)

(60) (...) comunque i trasferimenti di dati verso i paesi terzi possono aver luogo soltanto nel pieno rispetto delle disposizioni prese dagli Stati membri in applicazione della presente direttiva, in particolare dell'articolo 8;

(...)

(62) (...) la designazione di autorità di controllo che agiscano in modo indipendente in ciascuno Stato membro è un elemento essenziale per la tutela delle persone con riguardo al trattamento di dati personali;

(63) (...) tali autorità devono disporre dei mezzi necessari all'adempimento dei loro compiti, siano essi poteri investigativi o di intervento, segnatamente in caso di reclami di singoli individui, nonché poteri di avviare azioni legali; (...)».

4 Gli articoli 1, 2, 25, 26, 28 e 31 della direttiva 95/46 dispongono quanto segue:

«*Articolo 1*

Oggetto della direttiva

1. Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.

(…)

Articolo 2

Definizioni

Ai fini della presente direttiva si intende per:

a) "dati personali": qualsiasi informazione concernente una persona fisica identificata o identificabile ("persona interessata"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale;

b) "trattamento di dati personali" ("trattamento"): qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione;

(...)

d) "responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario;

(...)

Articolo 25

Principi

1. Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva.

2. L'adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate.

3. Gli Stati membri e la Commissione si comunicano a vicenda i casi in cui, a loro parere, un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2.

4. Qualora la Commissione constati, secondo la procedura dell'articolo 31, paragrafo 2, che un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, gli Stati membri adottano le misure necessarie per impedire ogni trasferimento di dati della stessa natura verso il paese terzo in questione.

5. La Commissione avvia, al momento opportuno, negoziati per porre rimedio alla situazione risultante dalla constatazione di cui al paragrafo 4.

6. La Commissione può constatare, secondo la procedura di cui all'articolo 31, paragrafo 2, che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona.

Gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione.

Articolo 26

Deroghe

1. In deroga all'articolo 25 e fatte salve eventuali disposizioni contrarie della legislazione nazionale per casi specifici, gli Stati membri dispongono che un trasferimento di dati personali verso un paese terzo che non garantisce una tutela adeguata ai sensi dell'articolo 25, paragrafo 2 può avvenire a condizione che:

a) la persona interessata abbia manifestato il proprio consenso in maniera inequivocabile al trasferimento previsto, oppure

b) il trasferimento sia necessario per l'esecuzione di un contratto tra la persona interessata ed il responsabile del trattamento o per l'esecuzione di misure precontrattuali prese a richiesta di questa, oppure

c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto, concluso o da concludere nell'interesse della persona interessata, tra il responsabile del trattamento e un terzo, oppure

d) il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, oppure per co[n]statare, esercitare o difendere un diritto per via giudiziaria, oppure

e) il trasferimento sia necessario per la salvaguardia dell'interesse vitale della persona interessata, oppure

f) il trasferimento avvenga a partire da un registro pubblico il quale, in forza di disposizioni legislative o regolamentari, sia predisposto per l'informazione del pubblico e sia aperto alla consultazione del pubblico o di chiunque possa dimostrare un interesse legittimo, nella misura in cui nel caso specifico siano rispettate le condizioni che la legge prevede per la consultazione.

2. Salvo il disposto del paragrafo 1, uno Stato membro può autorizzare un trasferimento o una categoria di trasferimenti di dati personali verso un paese terzo che non garantisca un livello di protezione adeguato ai sensi dell'articolo 25, paragrafo 2, qualora il responsabile del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi; tali garanzie possono segnatamente risultare da clausole contrattuali appropriate.

3. Lo Stato membro informa la Commissione e gli altri Stati membri in merito alle autorizzazioni concesse a norma del paragrafo 2.

In caso di opposizione notificata da un altro Stato membro o dalla Commissione, debitamente motivata sotto l'aspetto della tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, la Commissione adotta le misure appropriate secondo la procedura di cui all'articolo 31, paragrafo 2.

Gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione.

(...)

Articolo 28

Autorità di controllo

1. Ogni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri.

Tali autorità sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite.

2. Ciascuno Stato membro dispone che le autorità di controllo siano consultate al momento dell'elaborazione delle misure regolamentari o amministrative relative alla tutela dei diritti e delle libertà della persona con riguardo al trattamento dei dati personali.

3. Ogni autorità di controllo dispone in particolare:

— di poteri investigativi, come il diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo;

— di poteri effettivi d'intervento, come quello di formulare pareri prima dell'avvio di trattamenti, conformemente all'articolo 20, e di dar loro adeguata pubblicità o quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i Parlamenti o altre istituzioni politiche nazionali;

— del potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva ovvero di adire per dette violazioni le autorità giudiziarie.

È possibile un ricorso giurisdizionale avverso le decisioni dell'autorità di controllo recanti pregiudizio.

4. Qualsiasi persona, o associazione che la rappresenti, può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali. La persona interessata viene informata del seguito dato alla sua domanda.

Qualsiasi persona può, in particolare, chiedere a un'autorità di controllo di verificare la liceità di un trattamento quando si applicano le disposizioni nazionali adottate a norma dell'articolo 13 della presente direttiva. La persona viene ad ogni modo informata che una verifica ha avuto luogo.

(...)

6. Ciascuna autorità di controllo, indipendentemente dalla legge nazionale applicabile al trattamento in questione, è competente per esercitare, nel territorio del suo Stato membro, i poteri attribuitile a norma del paragrafo 3. Ciascuna autorità può essere invitata ad esercitare i suoi poteri su domanda dell'autorità di un altro Stato membro.

(…)

Articolo 31

(...)

2. Nei casi in cui è fatto riferimento al presente articolo, si applicano gli articoli 4 e 7 della decisione 1999/468/CE [del Consiglio, del 28 giugno 1999, recante modalità per l'esercizio delle competenze di esecuzione conferite alla Commissione (GU L 184, pag. 23)], tenendo conto delle disposizioni dell'articolo 8 della stessa.

(...)».

La decisione 2000/520

5 La decisione 2000/520 è stata adottata dalla Commissione sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46.

6 I considerando 2, 5 e 8 di tale decisione così recitano:

«(2) La Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato. In tal caso è possibile trasferire dati personali dagli Stati membri senza che siano necessarie ulteriori garanzie.

(...)

(5) Per il trasferimento di dati dalla Comunità agli Stati Uniti, il livello adeguato di protezione di cui alla presente decisione sarebbe raggiunto ove le organizzazioni si conformino ai "principi dell'approdo sicuro in materia di riservatezza" ("The Safe Harbor Privacy Principles"), in prosieguo "i principi", nonché alle "domande più frequenti" ("Frequently Asked Questions"), in prosieguo "FAQ", pubblicate dal governo degli Stati Uniti in data 21 luglio 2000, che forniscono indicazioni per l'attuazione dei principi stessi. Le organizzazioni devono inoltre rendere note pubblicamente le loro politiche in materia di riservatezza e sono sottoposte all'autorità della Commissione federale per il commercio [Federal Trade Commission (FTC)] ai sensi della sezione 5 del Federal Trade Commission Act, che vieta attività o pratiche sleali o ingannevoli in materia commerciale o collegata al commercio, oppure di altri organismi istituiti con legge in grado di assicurare efficacemente il rispetto dei principi applicati in conformità alle FAQ.

(...)

(8) Nell'interesse della trasparenza, e per salvaguardare la facoltà delle competenti autorità degli Stati membri di assicurare la protezione degli individui riguardo al trattamento dei dati personali, è necessario che la presente decisione specifichi le circostanze eccezionali in cui può essere giustificata la sospensione di specifici flussi di dati anche in caso di constatazione di adeguata protezione».

7 Ai sensi degli articoli da 1 a 4 della decisione 2000/520:

«*Articolo 1*

1. Ai fini dell'applicazione dell'articolo 25, paragrafo 2, della direttiva 95/46/CE, per tutte le attività che rientrano nel campo di applicazione di detta direttiva, si considera che i "Principi di approdo sicuro in materia di riservatezza", in prosieguo i "principi", di cui all'allegato I della presente decisione, applicati in conformità agli orientamenti forniti dalle "Domande più frequenti" (FAQ) di cui all'allegato II della presente decisione, pubblicate dal Dipartimento del commercio degli Stati Uniti in data 21 luglio 2000, garantiscano un livello adeguato di protezione dei dati personali trasferiti dalla Comunità a organizzazioni aventi sede negli Stati Uniti sulla base della seguente documentazione pubblicata dal Dipartimento del commercio degli Stati Uniti:

a) riepilogo delle modalità di esecuzione dei principi di approdo sicuro, di cui all'allegato III;

b) memorandum sui danni per violazioni della riservatezza ed autorizzazioni esplicite previste dalle leggi degli Stati Uniti, di cui all'allegato IV;

c) lettera della Commissione federale per il commercio (FTC), di cui all'allegato V;

d) lettera del Dipartimento dei trasporti degli Stati Uniti, di cui all'allegato VI.

2. Le seguenti condizioni devono sussistere in relazione a ogni singolo trasferimento di dati:

a) l'organizzazione che riceve i dati si è chiaramente e pubblicamente impegnata a conformarsi ai principi applicati in conformità alle FAQ, e

b) detta organizzazione è sottoposta all'autorità prevista per legge di un ente governativo degli Stati Uniti, compreso nell'elenco di cui all'allegato VII, competente ad esaminare denunce e a imporre la cessazione di prassi sleali e fraudolente nonché a disporre il risarcimento di qualunque soggetto, a prescindere dal paese di residenza o dalla nazionalità, danneggiato a seguito del mancato rispetto dei principi applicati in conformità alle FAQ.

3. Le condizioni di cui al paragrafo 2 sono considerate soddisfatte per ogni organizzazione che autocertifica la sua adesione ai principi applicati in conformità alle FAQ a partire dalla data di notifica al Dipartimento del commercio degli Stati Uniti (o all'ente da esso designato) del pubblico annuncio dell'impegno di cui al paragrafo 2, lettera a), e dell'identità dell'ente governativo di cui al paragrafo 2, lettera b).

Articolo 2

La presente decisione dispone soltanto in merito all'adeguatezza della protezione offerta negli Stati Uniti, in base ai principi applicati in conformità alle FAQ, al fine di quanto prescritto dall'articolo 25, paragrafo 1, della direttiva 95/46/CE. Essa nulla dispone relativamente all'applicazione di altre disposizioni della stessa direttiva, relative al trattamento di dati personali all'interno degli Stati membri e in particolare dell'articolo 4 della stessa.

Articolo 3

1. Fatto salvo il loro potere di adottare misure per garantire l'ottemperanza alle disposizioni nazionali adottate in forza di disposizioni diverse dall'articolo 25 della direttiva 95/46/CE, le autorità competenti degli Stati membri possono avvalersi dei loro poteri, al fine di tutelare gli interessati con riferimento al trattamento dei dati personali che li riguardano, per sospendere flussi di dati diretti a un'organizzazione che ha autocertificato la sua adesione ai principi applicati in conformità alle FAQ nei casi in cui:

a) gli enti governativi degli Stati Uniti di cui all'allegato VII della presente decisione, o un organismo indipendente di ricorso ai sensi della lettera a) del "principio di esecuzione" di cui all'allegato I della presente decisione abbiano accertato che l'organizzazione viola i principi applicati in conformità alle FAQ, oppure

b) sia molto probabile che i principi vengano violati; vi siano ragionevoli motivi per ritenere che l'organismo di esecuzione competente non stia adottando o non adotterà misure adeguate e tempestive per risolvere un caso concreto, la continuazione del trasferimento dei dati potrebbe determinare un rischio imminente di gravi danni per gli interessati e le autorità competenti dello Stato membro abbiano fatto il possibile, date le circostanze, per informare l'organizzazione dandole l'opportunità di replicare.

La sospensione dei flussi deve cessare non appena sia garantito il rispetto dei principi applicati in conformità alle FAQ e ciò sia stato notificato alle competenti autorità dell'UE.

2. Gli Stati membri comunicano immediatamente alla Commissione l'adozione di misure a norma del paragrafo 1.

3. Gli Stati membri e la Commissione s'informano altresì a vicenda in merito ai casi in cui l'azione degli organismi responsabili non garantisca la conformità ai principi applicati in conformità alle FAQ negli Stati Uniti.

4. Ove le informazioni di cui ai paragrafi 1, 2 e 3 del presente articolo provino che uno degli organismi incaricati di garantire la conformità ai principi applicati conformemente alle FAQ negli Stati Uniti non svolge la sua funzione in modo efficace, la Commissione ne informa il Dipartimento del commercio degli Stati Uniti e, se necessario, presenta progetti di misure secondo la procedura istituita dall'articolo 31 della direttiva 95/46/CE, al fine di annullare o sospendere la presente decisione o limitarne il campo d'applicazione.

Articolo 4

1. La presente decisione può essere adattata in qualsiasi momento alla luce dell'esperienza acquisita nella sua attuazione e/o qualora il livello di protezione offerta dai principi e dalle FAQ sia superato dai requisiti della legislazione degli Stati Uniti. La Commissione valuta in ogni caso l'applicazione della presente decisione tre anni dopo la sua notifica agli Stati membri sulla base delle informazioni disponibili e comunica qualsiasi riscontro al comitato istituito dall'articolo 31 della direttiva 95/46/CE, fornendo altresì ogni indicazione che possa influire sulla valutazione relativa all'adeguata salvaguardia offerta dalla disposizione di cui all'articolo 1 della presente decisione, ai sensi dell'articolo 25 della direttiva 95/46/CE, nonché di eventuali applicazioni discriminatorie della decisione stessa.

2. La Commissione, se necessario, presenta progetti di opportuni provvedimenti in conformità alla procedura di cui all'articolo 31 della direttiva 95/46/CE».

8 L'allegato I della decisione 2000/520 così recita:

«Principi di approdo sicuro (safe harbor) del dipartimento del commercio degli Stati Uniti, 21 luglio 2000 (...) (...) il Dipartimento del commercio sta provvedendo a pubblicare sotto la propria autorità statutaria questo documento e le Frequently Asked Questions ("i principi") al fine di incoraggiare, promuovere e sviluppare il commercio internazionale. I principi sono stati messi a punto in consultazione con l'industria e con il grande pubblico per facilitare gli scambi commerciali fra Stati Uniti ed Unione europea. Essi sono destinati unicamente ad organizzazioni americane che ricevono dati personali dall'Unione europea, al fine di permettere a tali organizzazioni di ottemperare al principio di "approdo sicuro" ed alla presunzione di "adeguatezza" che esso comporta. Giacché questi principi sono stati concepiti esclusivamente a tal fine una loro estensione ad altri fini può non risultare opportuna. (...) La decisione di un'organizzazione di qualificarsi per l'approdo sicuro è puramente volontaria, e la qualifica può essere ottenuta in vari modi. (...) L'adesione a tali principi può essere limitata: a) se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia; b) da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione; oppure c) se la direttiva o la legislazione degli Stati membri rendono possibili eccezioni o deroghe, a condizione che tali eccezioni o deroghe si applichino in contesti comparabili. Coerentemente con l'obiettivo di una maggiore tutela della sfera privata le organizzazioni devono fare il possibile per attuare detti principi integralmente ed in modo trasparente, specificando nelle rispettive politiche in materia di tutela della sfera privata in quali casi saranno regolarmente applicate le eccezioni ammesse dal punto b). Per lo stesso motivo, quando i principi e/o la legislazione statunitense consentono tale scelta, le organizzazioni sono tenute a scegliere, per quanto possibile, la protezione più elevata. (...)».

9 L'allegato II della decisione 2000/520 è redatto come segue:

«Domande più frequenti (FAQ)

(...) FAQ 6 – Autocertificazione

D: *Come può un'organizzazione autocertificare la propria adesione ai principi dell'approdo sicuro?*

R: Un'organizzazione usufruisce dei vantaggi dell'approdo sicuro dalla data in cui autocertifica al Dipartimento del commercio o ad una persona (fisica o giuridica) da esso designata l'adesione ai relativi principi, seguendo le indicazioni sotto riportate.

Per autocertificare l'adesione all'approdo sicuro un'organizzazione può fornire al Dipartimento del commercio o ad una persona (fisica o giuridica) da esso designata una lettera, firmata da un proprio funzionario in nome dell'organizzazione che intende aderire all'approdo sicuro, contenente almeno le seguenti informazioni:

1) denominazione dell'organizzazione, indirizzo postale, indirizzo di posta elettronica, numero di telefono e fax;

2) descrizione delle attività dell'organizzazione in rapporto alle informazioni personali pervenute dall'UE;

3) descrizione della politica perseguita dall'organizzazione in merito a dette informazioni personali, che precisi tra l'altro: a) dove il pubblico può prenderne conoscenza; b) la data della loro effettiva applicazione; c) l'ufficio cui rivolgersi per eventuali reclami, richieste di

accesso e qualsiasi altra questione riguardante l'approdo sicuro; d) lo specifico organo statutario competente ad esaminare i ricorsi contro l'organizzazione relativi a possibili pratiche sleali od ingannevoli e a violazioni delle norme legislative e regolamentari che disciplinano la tutela della sfera privata (ed elencati nell'allegato ai principi); e) il nome dei programmi concernenti la tutela della sfera privata cui partecipa l'organizzazione; f) il metodo di verifica (per esempio all'interno della società, effettuata da terzi) (…) e g) il meccanismo di ricorso indipendente disponibile per indagare sui reclami non risolti.

Le organizzazioni che intendono estendere i benefici dell'approdo sicuro alle informazioni riguardanti le risorse umane trasferite dall'UE per usi nel contesto di un rapporto di lavoro possono farlo qualora esista un organo statutario competente ad esaminare i ricorsi contro l'organizzazione relativi ad informazioni riguardanti le risorse umane, elencato nell'allegato "Principi di approdo sicuro". (...)

Il Dipartimento (o la persona da esso designata) conserverà un elenco di tutte le organizzazioni che inviano queste lettere, assicurando così la disponibilità dei vantaggi legati all'approdo sicuro, ed aggiornerà tale elenco in base alle lettere annuali ed alle notifiche ricevute secondo le modalità precisate nella FAQ 11. (...)

(...) FAQ 11 – Risoluzione delle controversie e modalità di controllo dell'applicazione (enforcement)

D: *Come si applicano le norme derivanti dal principio della garanzia di applicazione (enforcement) per la risoluzione delle controversie, e come si procede se un'organizzazione continua a non rispettare i principi?*

R: Il principio della garanzia di applicazione (enforcement) stabilisce le norme per l'applicazione dell'approdo sicuro. Le modalità di applicazione delle norme di cui al punto b) di tale principio sono illustrate nella domanda sulla verifica (FAQ 7). La presente domanda interessa i punti a) e c), che prescrivono l'istituzione di dispositivi indipendenti di ricorso. Tali dispositivi possono assumere forme diverse, ma devono soddisfare le prescrizioni formulate nel contesto delle garanzie d'applicazione. Un'organizzazione può adempiere a tali prescrizioni nei modi seguenti: 1) applicando programmi di riservatezza elaborati dal settore privato nei quali siano integrati i principi dell'approdo sicuro e che contemplino dispositivi di attuazione efficaci, del tipo descritto dal principio delle garanzie d'applicazione; 2) uniformandosi a norme giurisdizionali o regolamentari emanate dalle corrispondenti autorità di controllo, che disciplinino il trattamento di reclami individuali e la soluzione delle controversie; oppure 3) impegnandosi a cooperare con le autorità di tutela dei dati aventi sede nella Comunità europea o loro rappresentanti autorizzati. Quest'elenco è fornito a titolo puramente esemplificativo e non limitativo. Il settore privato può indicare altri meccanismi di applicazione, purché rispettino il principio delle garanzie d'applicazione e le FAQ. Si noti che le citate garanzie d'applicazione si aggiungono a quelle di cui al paragrafo 3 dell'introduzione ai principi, in forza delle quali le iniziative di autoregolamentazione devono avere carattere vincolante in virtù dell'articolo 5 del Federal Trade Commission Act o analogo testo di legge.

Meccanismi di ricorso:

I consumatori dovrebbero essere incoraggiati a presentare gli eventuali reclami all'organizzazione direttamente interessata, prima di rivolgersi ai dispositivi indipendenti di ricorso. (...)

(...)

Attività della Commissione federale per il commercio (Federal Trade Commission, FTC):

La Commissione federale per il commercio (FTC) si è impegnata ad esaminare in via prioritaria i casi trasmessi da organizzazioni di autoregolamentazione in materia di riservatezza (quali BBBOnline e TRUSTe) e dagli Stati membri dell'UE per denunciare la presunta non conformità ai principi dell'approdo sicuro, al fine di stabilire se vi siano state violazioni della sezione 5 del FTC Act, che vieta azioni o pratiche sleali od ingannevoli nel commercio. (...) (...)».

10 Ai sensi dell'allegato IV della decisione 2000/520:

«Tutela della riservatezza e risarcimento danni, autorizzazioni legali, fusioni e acquisizioni secondo la legge degli Stati Uniti

Il presente documento risponde alla richiesta della Commissione europea di chiarimenti sulla legge statunitense per quanto riguarda a) risarcimento dei danni per violazione della sfera privata (privacy), b) le "autorizzazioni esplicite" previste dalla legge degli Stati Uniti per l'uso di dati personali in modo contrastante con i principi "approdo sicuro" (safe harbor), c) l'effetto delle fusioni e acquisizioni sugli obblighi assunti in base a tali principi.

(...)

B. Autorizzazioni legali esplicite I principi "approdo sicuro" contengono un'eccezione qualora atti legislativi, regolamenti o la giurisprudenza "comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione". È ovvio che quando la legge statunitense impone un'obbligazione conflittuale, le organizzazioni statunitensi, che aderiscano o no ai principi "approdo sicuro", devono osservare la legge. Per quanto riguarda le autorizzazioni esplicite, sebbene i principi "approdo sicuro" intendano colmare le differenze tra il sistema americano e quello europeo relativamente alla tutela della privacy, siamo tenuti al rispetto delle prerogative legislative dei legislatori eletti. La limitata eccezione al rigoroso rispetto dei principi "approdo sicuro" cerca di stabilire un equilibrio in grado di conciliare i legittimi interessi delle parti. L'eccezione è limitata ai casi in cui esiste un'autorizzazione esplicita. Tuttavia, come caso limite, la legge, il regolamento o la decisione del tribunale pertinenti devono esplicitamente autorizzare una particolare condotta delle organizzazioni aderenti ai principi "approdo sicuro". In altre parole, l'eccezione non verrà applicata se la legge non prescrive nulla. Inoltre, l'eccezione verrà applicata soltanto se l'esplicita autorizzazione è in conflitto con il rispetto dei principi "approdo sicuro". Anche in questo caso, l'eccezione "si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione". Ad esempio, se la legge si limita ad autorizzare un'azienda a fornire dati personali alle pubbliche autorità, l'eccezione non verrà applicata. Al contrario, se la legge autorizza espressamente l'azienda a fornire dati personali ad organizzazioni governativ[e] senza il consenso dei singoli, ciò costituisce una "autorizzazione esplicita" ad agire in contrasto con i principi "approdo sicuro". In alternativa, le specifiche eccezioni alle disposizioni relative alla notifica al consenso rientrerebbero nell'ambito dell'eccezione (dato che ciò equivarrebbe ad una specifica autorizzazione a rivelare informazioni senza notifica e consenso). Ad esempio, una legge che autorizzi i medici a fornire le cartelle cliniche dei loro pazienti agli ufficiali sanitari senza il previo consenso dei pazienti stessi potrebbe consentire un'eccezione ai principi di notifica e di scelta. Tale autorizzazione non permetterebbe ad un medico di fornire le stesse cartelle cliniche alle casse mutue malattie o ai laboratori di ricerca farmaceutica perché ciò esulerebbe dall'ambito degli usi consentiti dalla legge e dunque dall'ambito dell'eccezione (...). L'autorizzazione in questione può essere un'autorizzazione

"autonoma" a fare determinate cose con i dati personali ma, come illustrato negli esempi di cui sopra, è probabile che si tratti di un'eccezione a una legge generale che proscrive la raccolta, l'uso o la divulgazione dei dati personali. (...)».

La comunicazione COM(2013) 846 final

11 Il 27 novembre 2013 la Commissione ha adottato la comunicazione al Parlamento europeo e al Consiglio, intitolata «Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA» [COM(2013) 846 final; in prosieguo: la «comunicazione COM(2013) 846 final»]. Tale comunicazione era corredata di una relazione, parimenti datata 27 novembre 2013, contenente le «conclusioni dei copresidenti dell'UE del gruppo di lavoro ad hoc UE-USA sulla protezione dei dati personali» («Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection»). Tale relazione era stata elaborata, come indicato dal suo punto 1, in cooperazione con gli Stati Uniti d'America in seguito alle rivelazioni dell'esistenza, in tale paese, di diversi programmi di controllo che comprendevano la raccolta e il trattamento su larga scala di dati personali. Detta relazione conteneva, segnatamente, un'analisi dettagliata dell'ordinamento giuridico statunitense per quanto attiene, in particolare, alle basi giuridiche che autorizzano l'esistenza di programmi di controllo, nonché la raccolta e il trattamento di dati personali da parte delle autorità americane.

12 Al punto 1 della comunicazione COM(2013) 846 final, la Commissione ha precisato che «[g]li scambi commerciali sono oggetto della decisione [2000/520]», aggiungendo che tale decisione «fornisce una base giuridica per il trasferimento dei dati personali dall'UE a società stabilite negli Stati Uniti che hanno aderito ai principi d'Approdo sicuro». Inoltre, sempre al punto 1, la Commissione ha messo in evidenza l'importanza sempre maggiore dei flussi di dati personali, legata segnatamente allo sviluppo dell'economia digitale, il quale ha effettivamente «portato a una crescita esponenziale nella quantità, qualità, diversità e natura delle attività di trattamento dei dati».

13 Al punto 2 di tale comunicazione, la Commissione ha osservato che «le preoccupazioni sul livello di protezione dei dati personali dei cittadini dell'[Unione] trasferiti agli Stati Uniti nell'ambito del principio dell'Approdo sicuro sono aumentate», e che «[l]a natura volontaria e dichiarativa del regime ha difatti attirato grande attenzione sulla sua trasparenza e sulla sua applicazione».

14 Inoltre, essa ha indicato, in questo stesso punto 2, che «[i] dati personali dei cittadini dell'[Unione] inviati negli USA nell'ambito [del] regime [dell'approdo sicuro] possono essere consultati e ulteriormente trattati dalle autorità americane in maniera incompatibile con i motivi per cui erano stati originariamente raccolti nell'[Unione] e con le finalità del loro trasferimento agli Stati Uniti», e che «[l]a maggior parte delle imprese Internet americane che risultano più direttamente interessate [dai] programmi [di controllo], sono certificate nell'ambito del regime Approdo sicuro».

15 Al punto 3.2 della comunicazione COM(2013) 846 final, la Commissione ha rilevato l'esistenza di un certo numero di carenze quanto all'attuazione della decisione 2000/520. Da un lato, essa ha ivi menzionato il fatto che talune imprese americane certificate non rispettavano i principi di cui all'articolo 1, paragrafo 1, della decisione 2000/520 (in prosieguo: i «principi di approdo sicuro») e che dovevano essere apportati miglioramenti a tale decisione concernenti «i punti deboli strutturali relativi alla trasparenza e all'applicazione, i principi sostanziali dell'Approdo sicuro e il funzionamento dell'eccezione per motivi di sicurezza nazionale». Dall'altro, essa ha osservato che l'«Approdo sicuro funge inoltre da interfaccia per il trasferimento di dati personali di cittadini dell'UE dall'[Unione] europea agli Stati Uniti da parte di imprese che sono tenute a consegnare dati ai servizi di intelligence americani nell'ambito dei programmi di raccolta statunitensi».

16 La Commissione ha concluso, a questo stesso punto 3.2, che, se, «[t]enuto conto dei punti deboli individuati, il regime Approdo sicuro non può continuare ad essere applicato secondo le attuali modalità, (…) abrogarlo nuocerebbe [tuttavia] agli interessi delle imprese che ne sono membri, nell'[Unione] e negli USA». Infine, sempre a detto punto 3.2, la Commissione ha aggiunto che essa intendeva cominciare «col discutere con le autorità americane i punti deboli individuati».

La comunicazione COM(2013) 847 final

17 Sempre il 27 novembre 2013, la Commissione ha adottato la comunicazione al Parlamento europeo e al Consiglio sul funzionamento del regime «Approdo sicuro» dal punto di vista dei cittadini dell'UE e delle società ivi stabilite [COM(2013) 847 final; in prosieguo: la «comunicazione COM(2013) 847 final»]. Come risulta dal suo punto 1, tale comunicazione si basava, segnatamente, sulle informazioni ricevute nell'ambito del Gruppo di lavoro ad hoc Unione europea-Stati Uniti e faceva seguito a due relazioni di valutazione della Commissione, pubblicate, rispettivamente, nel 2002 e nel 2004.

18 Il punto 1 di tale comunicazione precisa che il funzionamento della decisione 2000/520 «si basa sugli impegni assunti dalle imprese che vi aderiscono e sulla loro auto-certificazione» e aggiunge che «[l]'adesione è volontaria, ma [che] una volta sottoscritta le norme sono vincolanti».

19 Inoltre, emerge dal punto 2.2 della comunicazione COM(2013) 847 final che, al 26 settembre 2013, 3 246 imprese, facenti parte di numerosi settori dell'economia e dei servizi, erano certificate. Tali imprese fornivano, principalmente, servizi sul mercato interno dell'Unione, in particolare nel settore di Internet, e una parte di esse erano imprese dell'Unione con controllate negli Stati Uniti. Alcune di queste imprese trattavano i dati relativi ai loro dipendenti in Europa e li inviavano in tale paese a fini di gestione delle risorse umane.

20 Sempre al punto 2.2, la Commissione ha sottolineato che «[o]gni insufficienza a livello di trasparenza o di applicazione da parte americana [aveva] l'effetto di far ricadere la responsabilità sulle autorità per la protezione dei dati europee e sulle imprese che si avvalgono del regime in oggetto».

21 Si evince, segnatamente, dai punti da 3 a 5 e 8 della comunicazione COM(2013) 847 final che, nella prassi, un numero considerevole di imprese certificate non rispettava, o rispettava solo in parte, i principi dell'approdo sicuro.

22 Inoltre, al punto 7 di tale comunicazione, la Commissione ha affermato che «tutte le imprese partecipanti al programma PRISM [programma di raccolta di informazioni su larga scala], e che consentono alle autorità americane di avere accesso a dati conservati e trattati negli USA, risultano certificate nel quadro di Approdo sicuro», e che tale sistema «è diventato così una delle piattaforme di accesso delle autorità americane di intelligence alla raccolta di dati personali inizialmente trattati nell'[Unione]». A tal riguardo, la Commissione ha constatato, al punto 7.1 di detta comunicazione, che «un certo numero di basi giuridiche previste dalla legislazione americana consente la raccolta e il trattamento su larga scala di dati personali conservati o altrimenti trattati da società ubicate negli Stati Uniti» e che «[a] causa dell'ampia entità dei programmi, può accadere che dati trasferiti nell'ambito di Approdo sicuro siano accessibili alle autorità americane e vengano ulteriormente trattati da queste al di là di quanto è necessario e proporzionato alla protezione della sicurezza nazionale come previsto dall'eccezione di cui alla decisione [2000/520]».

23 Al punto 7.2 della comunicazione COM(2013) 847 final, intitolata «Limitazioni e rimedi», la Commissione ha sottolineato che «i principali beneficiari delle garanzie previste dal diritto americano sono i cittadini statunitensi o le persone che risiedono legalmente negli USA» e che «[n]on vi è inoltre alcuna possibilità, né per gli interessati [dell'Unione] che per quelli americani, di ottenere

l'accesso, la rettifica o la cancellazione dei dati, o rimedi amministrativi o giurisdizionali in relazione alla raccolta e all'ulteriore trattamento dei loro dati personali nell'ambito dei programmi di controllo statunitensi».

24 Secondo il punto 8 della comunicazione COM(2013) 847 final, fra le imprese certificate figuravano «[l]e imprese del web come Google, Facebook, Microsoft, Apple, Yahoo», le quali contano «[centinaia di] milioni di clienti in Europa» e trasferiscono dati personali negli Stati Uniti a fini del loro trattamento.

25 La Commissione ha concluso, a questo stesso punto 8, che «l'accesso su larga scala, da parte dei servizi di intelligence, ai dati trasferiti negli USA da imprese certificate nell'ambito di Approdo sicuro solleva altri gravi problemi riguardanti la continuità dei diritti dei cittadini europei in materia di protezione in caso di invio dei loro dati negli Stati Uniti».

Procedimento principale e questioni pregiudiziali

26 Il sig. Schrems, cittadino austriaco residente in Austria, è iscritto alla rete sociale Facebook (in prosieguo: «Facebook») dal 2008.

27 Chiunque risieda nel territorio dell'Unione e desideri utilizzare Facebook è tenuto, al momento della sua iscrizione, a sottoscrivere un contratto con Facebook Ireland, una controllata di Facebook Inc., situata, da parte sua, negli Stati Uniti. I dati personali degli utenti di Facebook residenti nel territorio dell'Unione vengono trasferiti, in tutto o in parte, su server di Facebook Inc. ubicati nel territorio degli Stati Uniti, ove essi sono oggetto di un trattamento.

28 Il 25 giugno 2013 il sig. Schrems ha investito il commissario di una denuncia, con la quale lo invitava, in sostanza, ad esercitare le proprie competenze statutarie, vietando a Facebook Ireland di trasferire i suoi dati personali verso gli Stati Uniti. In tale denuncia egli faceva valere che il diritto e la prassi vigenti in tale paese non offrivano una protezione sufficiente dei dati personali conservati nel territorio del medesimo contro le attività di controllo ivi praticate dalle autorità pubbliche. Il sig. Schrems si riferiva, a tal riguardo, alle rivelazioni fatte dal sig. Edward Snowden in merito alle attività dei servizi di intelligence degli Stati Uniti, e in particolare a quelle della National Security Agency (in prosieguo: la «NSA»).

29 Considerando di non essere obbligato a procedere ad un'indagine sui fatti denunciati dal sig. Schrems, il commissario ha respinto la denuncia in quanto priva di fondamento. Egli ha ritenuto, infatti, che non esistessero prove del fatto che la NSA avesse avuto accesso ai dati personali dell'interessato. Il commissario ha aggiunto che le censure formulate dal sig. Schrems nella sua denuncia non potevano essere fatte valere in maniera utile, in quanto ogni questione relativa all'adeguatezza della protezione dei dati personali negli Stati Uniti doveva essere risolta in conformità alla decisione 2000/520 e che, in tale decisione, la Commissione aveva constatato che gli Stati Uniti d'America assicuravano un livello di protezione adeguato.

30 Il sig. Schrems ha proposto un ricorso dinanzi alla High Court (Corte d'appello) avverso la decisione di cui al procedimento principale. Dopo aver esaminato le prove prodotte dalle parti nel procedimento principale, tale giudice ha dichiarato che la sorveglianza elettronica e l'intercettazione dei dati personali trasferiti dall'Unione verso gli Stati Uniti rispondevano a finalità necessarie e indispensabili per l'interesse pubblico. Tuttavia, detto giudice ha aggiunto che le rivelazioni del sig. Snowden avevano dimostrato che la NSA ed altri organi federali avevano commesso «eccessi considerevoli».

31 Orbene, secondo questo stesso giudice, i cittadini dell'Unione non avrebbero alcun diritto effettivo ad essere sentiti. La supervisione sull'operato dei servizi di intelligence verrebbe effettuata nell'ambito di un procedimento segreto e non contraddittorio. Una volta che i dati personali sono stati trasferiti

verso gli Stati Uniti, la NSA e altri organi federali, come il Federal Bureau of Investigation (FBI), potrebbero accedere a tali dati nell'ambito della sorveglianza e delle intercettazioni indifferenziate da essi praticate su larga scala.

32 La High Court (Corte d'appello) ha constatato che il diritto irlandese vieta il trasferimento dei dati personali al di fuori del territorio nazionale, fatti salvi i casi in cui il paese terzo in questione assicura un livello di protezione adeguato della vita privata, nonché dei diritti e delle libertà fondamentali. L'importanza dei diritti al rispetto della vita privata e all'inviolabilità del domicilio, garantiti dalla Costituzione irlandese, implicherebbe che qualsiasi ingerenza in tali diritti sia proporzionata e conforme ai requisiti previsti dalla legge.

33 Orbene, l'accesso massiccio e indifferenziato a dati personali sarebbe manifestamente contrario al principio di proporzionalità e ai valori fondamentali protetti dalla Costituzione irlandese. Affinché intercettazioni di comunicazioni elettroniche possano essere considerate conformi a tale Costituzione, occorrerebbe dimostrare che tali intercettazioni sono mirate, che la sorveglianza su talune persone o taluni gruppi di persone è oggettivamente giustificata nell'interesse della sicurezza nazionale o della repressione della criminalità, e che esistono garanzie adeguate e verificabili. Pertanto, secondo la High Court (Corte d'appello), qualora il procedimento principale dovesse essere definito sulla base del solo diritto irlandese, occorrerebbe constatare che, alla luce dell'esistenza di un serio dubbio sul fatto che gli Stati Uniti d'America assicurino un livello di protezione adeguato dei dati personali, il commissario avrebbe dovuto compiere un'indagine sui fatti lamentati dal sig. Schrems nella sua denuncia e che il commissario ha erroneamente respinto quest'ultima.

34 Tuttavia, la High Court (Corte d'appello) considera che tale causa verte sull'attuazione del diritto dell'Unione ai sensi dell'articolo 51 della Carta, cosicché la legittimità della decisione di cui al procedimento principale deve essere valutata sulla scorta del diritto dell'Unione. Orbene, secondo tale giudice, la decisione 2000/520 non soddisfa i requisiti risultanti sia dagli articoli 7 e 8 della Carta sia dai principi enunciati dalla Corte nella sentenza Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238). Il diritto al rispetto della vita privata, garantito dall'articolo 7 della Carta e dai valori fondamentali comuni alle tradizioni degli Stati membri, sarebbe svuotato di significato qualora i pubblici poteri fossero autorizzati ad accedere alle comunicazioni elettroniche su base casuale e generalizzata, senza alcuna giustificazione oggettiva fondata su motivi di sicurezza nazionale o di prevenzione della criminalità, specificamente riguardanti i singoli interessati, e senza che tali pratiche siano accompagnate da garanzie adeguate e verificabili.

35 La High Court (Corte d'appello) osserva, inoltre, che il sig. Schrems, nel suo ricorso, ha contestato in realtà la legittimità del regime dell'approdo sicuro istituito dalla decisione 2000/520 e sul quale poggia la decisione di cui al procedimento principale. Pertanto, anche se il sig. Schrems non ha formalmente contestato la validità né della direttiva 95/46 né della decisione 2000/520, secondo tale giudice occorre chiarire se, avuto riguardo all'articolo 25, paragrafo 6, di tale direttiva, il commissario fosse vincolato dalla constatazione effettuata dalla Commissione in tale decisione, secondo la quale gli Stati Uniti d'America garantiscono un livello di protezione adeguato, oppure se l'articolo 8 della Carta autorizzasse il commissario a discostarsi, se del caso, da una siffatta constatazione.

36 È in tale contesto che la High Court (Corte d'appello) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se, nel decidere in merito a una denuncia presentata a un'autorità indipendente investita per legge delle funzioni di gestione e di applicazione della legislazione sulla protezione dei dati, secondo cui i dati personali sono trasferiti a un paese terzo (nel caso di specie, gli Stati Uniti d'America) il cui diritto e la cui prassi si sostiene non prevedano adeguate tutele per i soggetti interessati, tale autorità sia assolutamente vincolata dalla constatazione in senso contrario dell'Unione contenuta nella decisione 2000/520, tenuto conto degli articoli 7, 8 e 47 della Carta, nonostante le disposizioni dell'articolo 25, paragrafo 6, della direttiva 95/46.

2) Oppure, in alternativa, se detta autorità possa e/o debba condurre una propria indagine sulla questione alla luce degli sviluppi verificatisi nel frattempo, successivamente alla prima pubblicazione della decisione 2000/520».

Sulle questioni pregiudiziali

37 Con le sue questioni pregiudiziali, che occorre esaminare congiuntamente, il giudice del rinvio chiede, in sostanza, se e in che misura l'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce degli articoli 7, 8 e 47 della Carta, debba essere interpretato nel senso che una decisione adottata in forza di tale disposizione, come la decisione 2000/520, con la quale la Commissione constata che un paese terzo assicura un livello di protezione adeguato, osti a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, possa esaminare la domanda di una persona relativa alla tutela dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, allorché tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non assicurano un livello di protezione adeguato.

Sui poteri delle autorità nazionali di controllo ai sensi dell'articolo 28 della direttiva 95/46, in presenza di una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, di tale direttiva

38 Occorre rammentare, in via preliminare, che le disposizioni della direttiva 95/46, disciplinando il trattamento di dati personali che possono arrecare pregiudizio alle libertà fondamentali e, segnatamente, al diritto al rispetto della vita privata, devono essere necessariamente interpretate alla luce dei diritti fondamentali garantiti dalla Carta (v. sentenze Österreichischer Rundfunk e a., C-465/00, C-138/01 e C-139/01, EU:C:2003:294, punto 68; Google Spain e Google, C-131/12, EU:C:2014:317, punto 68, nonché Ryneš, C-212/13, EU:C:2014:2428, punto 29).

39 Risulta dall'articolo 1, nonché dai considerando 2 e 10 della direttiva 95/46, che essa è intesa a garantire non solo una tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche, e segnatamente del diritto fondamentale al rispetto della vita privata con riguardo al trattamento dei dati personali, ma anche un livello elevato di protezione di tali libertà e diritti fondamentali. L'importanza sia del diritto fondamentale al rispetto della vita privata, garantito dall'articolo 7 della Carta, sia del diritto fondamentale alla tutela dei dati personali, garantito dall'articolo 8 della stessa, è inoltre sottolineata nella giurisprudenza della Corte (v. sentenze Rijkeboer, C-553/07, EU:C:2009:293, punto 47; Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 53, nonché Google Spain e Google, C-131/12, EU:C:2014:317, punti 53, 66 e 74 e la giurisprudenza ivi citata).

40 Per quanto attiene ai poteri di cui dispongono le autorità di controllo nazionali quanto al trasferimento di dati personali verso paesi terzi, si deve rilevare che l'articolo 28, paragrafo 1, della direttiva 95/46 obbliga gli Stati membri ad istituire una o più autorità pubbliche incaricate di controllare in piena indipendenza l'osservanza delle norme dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento di tali dati. Detto obbligo risulta altresì dal diritto primario dell'Unione, segnatamente dall'articolo 8, paragrafo 3, della Carta e dall'articolo 16, paragrafo 2, TFUE (v., in tal senso, sentenze Commissione/Austria, C-614/10, EU:C:2012:631, punto 36, e Commissione/Ungheria, C-288/12, EU:C:2014:237, punto 47).

41 La garanzia d'indipendenza delle autorità nazionali di controllo è diretta ad assicurare che il controllo del rispetto delle disposizioni in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali sia efficace e affidabile e deve essere interpretata alla luce di tale finalità. Essa è stata disposta al fine di rafforzare la protezione delle persone e degli organismi interessati dalle decisioni di tali autorità. L'istituzione, negli Stati membri, di autorità di controllo indipendenti,

costituisce quindi, come rilevato dal considerando 62 della direttiva 95/46, un elemento essenziale del rispetto della tutela delle persone con riguardo al trattamento dei dati personali (v. sentenze Commissione/Germania, C-518/07, EU:C:2010:125, punto 25, nonché Commissione/Ungheria C-288/12, EU:C:2014:237, punto 48 e la giurisprudenza ivi citata).

42 Al fine di garantire tale protezione, le autorità nazionali di controllo devono, segnatamente, assicurare un giusto equilibrio fra, da un lato, il rispetto del diritto fondamentale alla vita privata e, dall'altro, gli interessi che impongono una libera circolazione dei dati personali (v., in tal senso, sentenze Commissione/Germania, C-518/07, EU:C:2010:125, punto 24, e Commissione/Ungheria C-288/12, EU:C:2014:237, punto 51).

43 A tal fine, dette autorità dispongono di un'ampia gamma di poteri e questi, elencati in maniera non esaustiva all'articolo 28, paragrafo 3, della direttiva 95/46, costituiscono altrettanti mezzi necessari all'adempimento dei loro compiti, come sottolineato dal considerando 63 di tale direttiva. In tal senso, dette autorità godono, segnatamente, di poteri investigativi, come quello di raccogliere qualsiasi informazione necessaria all'esercizio della loro funzione di controllo, di poteri effettivi d'intervento, come quello di vietare a titolo provvisorio o definitivo un trattamento di dati o, ancora, del potere di promuovere azioni giudiziarie.

44 È vero che si evince dall'articolo 28, paragrafi 1 e 6, della direttiva 95/46 che i poteri delle autorità nazionali di controllo riguardano i trattamenti di dati personali effettuati nel territorio del loro Stato membro, cosicché esse non dispongono di poteri, sulla base di tale articolo 28, con riguardo ai trattamenti di siffatti dati effettuati nel territorio di un paese terzo.

45 Tuttavia, l'operazione consistente nel far trasferire dati personali da uno Stato membro verso un paese terzo costituisce, di per sé, un trattamento di dati personali ai sensi dell'articolo 2, lettera b), della direttiva 95/46 (v., in tal senso, sentenza Parlamento/Consiglio e Commissione, C-317/04 e C-318/04, EU:C:2006:346, punto 56) effettuato nel territorio di uno Stato membro. Infatti, tale disposizione definisce il «trattamento di dati personali» alla stregua di «qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali» e menziona, a titolo di esempio, «la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione».

46 Il considerando 60 della direttiva 95/46 precisa che i trasferimenti di dati personali verso i paesi terzi possono aver luogo soltanto nel pieno rispetto delle disposizioni prese dagli Stati membri in applicazione di tale direttiva. A tal riguardo, il capo IV di detta direttiva, nel quale figurano gli articoli 25 e 26 della medesima, ha predisposto un regime che mira a garantire un controllo da parte degli Stati membri sui trasferimenti di dati personali verso i paesi terzi. Tale regime è complementare al regime generale attuato dal capo II di questa stessa direttiva, riguardante le condizioni generali di liceità dei trattamenti di dati personali (v., in tal senso, sentenza Lindqvist, C-101/01, EU:C:2003:596, punto 63).

47 Poiché le autorità nazionali di controllo sono incaricate, ai sensi dell'articolo 8, paragrafo 3, della Carta e dell'articolo 28 della direttiva 95/46, di sorvegliare il rispetto delle norme dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, ciascuna di esse è quindi investita della competenza a verificare se un trasferimento di dati personali dal proprio Stato membro verso un paese terzo rispetti i requisiti fissati dalla direttiva 95/46.

48 Riconoscendo al contempo, al suo considerando 56, che i trasferimenti di dati personali dagli Stati membri verso paesi terzi sono necessari allo sviluppo degli scambi internazionali, la direttiva 95/46 pone come principio, al suo articolo 25, paragrafo 1, che siffatti trasferimenti possano avere luogo soltanto se tali paesi terzi garantiscono un livello di protezione adeguato.

49 Inoltre, il considerando 57 di detta direttiva precisa che i trasferimenti di dati personali verso paesi terzi che non offrono un livello di protezione adeguato devono essere vietati.

50 Al fine di controllare i trasferimenti di dati personali verso i paesi terzi in funzione del livello di protezione ad essi accordato in ciascuno di tali paesi, l'articolo 25 della direttiva 95/46 impone una serie di obblighi agli Stati membri e alla Commissione. Risulta, segnatamente, da tale articolo, che la constatazione se un paese terzo assicuri o meno un livello di protezione adeguato può essere effettuata, come rilevato dall'avvocato generale al paragrafo 86 delle sue conclusioni, vuoi dagli Stati membri vuoi dalla Commissione.

51 La Commissione può adottare, sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, una decisione che constata che un paese terzo garantisce un livello di protezione adeguato. Conformemente al secondo comma di tale disposizione, una siffatta decisione ha come destinatari gli Stati membri, i quali devono adottare le misure necessarie per conformarvisi. Ai sensi dell'articolo 288, quarto comma, TFUE, essa ha un carattere vincolante per tutti gli Stati membri destinatari e si impone pertanto a tutti i loro organi (v., in tal senso, sentenze Albako Margarinefabrik, 249/85, EU:C:1987:245, punto 17, e Mediaset, C-69/13, EU:C:2014:71, punto 23), nella parte in cui produce l'effetto di autorizzare trasferimenti di dati personali dagli Stati membri verso il paese terzo da essa interessato.

52 Pertanto, fintantoché la decisione della Commissione non sia stata dichiarata invalida dalla Corte, gli Stati membri e i loro organi, fra i quali figurano le loro autorità di controllo indipendenti, non possono certo adottare misure contrarie a tale decisione, come atti intesi a constatare con effetto vincolante che il paese terzo interessato da detta decisione non garantisce un livello di protezione adeguato. Infatti, gli atti delle istituzioni dell'Unione si presumono, in linea di principio, legittimi e producono pertanto effetti giuridici, finché non siano stati revocati o annullati nel contesto di un ricorso per annullamento ovvero dichiarati invalidi a seguito di un rinvio pregiudiziale o di un'eccezione di illegittimità (sentenza Commissione/Grecia, C-475/01, EU:C:2004:585, punto 18 e la giurisprudenza ivi citata).

53 Tuttavia, una decisione della Commissione adottata sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, come la decisione 2000/520, non può impedire alle persone i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo di investire le autorità nazionali di controllo di una domanda, ai sensi dell'articolo 28, paragrafo 4, di tale direttiva, relativa alla protezione dei loro diritti e delle loro libertà con riguardo al trattamento di tali dati. Analogamente, una decisione di tale natura non può, come rilevato dall'avvocato generale, segnatamente, ai paragrafi 61, 93 e 116 delle sue conclusioni, né elidere né ridurre i poteri espressamente riconosciuti alle autorità nazionali di controllo dall'articolo 8, paragrafo 3, della Carta, nonché dall'articolo 28 di detta direttiva.

54 Né l'articolo 8, paragrafo 3, della Carta né l'articolo 28 della direttiva 95/46 escludono dall'ambito di competenza delle autorità nazionali di controllo il controllo dei trasferimenti di dati personali verso paesi terzi che sono stati oggetto di una decisione della Commissione in forza dell'articolo 25, paragrafo 6, di tale direttiva.

55 In particolare, l'articolo 28, paragrafo 4, primo comma, della direttiva 95/46, il quale dispone che «[q]ualsiasi persona (…) può presentare [alle autorità nazionali di controllo] una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali», non prevede alcuna eccezione a tal riguardo nel caso in cui la Commissione abbia adottato una decisione in forza dell'articolo 25, paragrafo 6, di tale direttiva.

56 Inoltre, sarebbe contrario al sistema predisposto dalla direttiva 95/46, nonché alla finalità degli articoli 25 e 28 della stessa se una decisione della Commissione adottata in applicazione dell'articolo 25, paragrafo 6, di detta direttiva avesse come effetto di impedire ad un'autorità nazionale

di controllo di esaminare la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei suoi dati personali che sono stati o potrebbero essere trasferiti da uno Stato membro verso un paese terzo interessato da tale decisione.

57 Al contrario, l'articolo 28 della direttiva 95/46 si applica, per la sua stessa natura, a ogni trattamento di dati personali. Pertanto, anche in presenza di una decisione della Commissione adottata sulla base dell'articolo 25, paragrafo 6, di tale direttiva, le autorità nazionali di controllo investite da una persona di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei dati personali che la riguardano, devono poter verificare, in piena indipendenza, se il trasferimento di tali dati rispetti i requisiti fissati da detta direttiva.

58 Se così non fosse, le persone i cui dati personali sono stati o potrebbero essere trasferiti verso il paese terzo di cui trattasi sarebbero private del diritto, garantito all'articolo 8, paragrafi 1 e 3, della Carta, di investire le autorità nazionali di controllo di una domanda ai fini della protezione dei loro diritti fondamentali (v., per analogia, sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 68).

59 Una domanda, ai sensi dell'articolo 28, paragrafo 4, della direttiva 95/46, con la quale una persona i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo fa valere, come nel procedimento principale, che il diritto e la prassi di tale paese non assicurano, nonostante quanto constatato dalla Commissione in una decisione adottata in base all'articolo 25, paragrafo 6, di tale direttiva, un livello di protezione adeguato, deve essere intesa nel senso che essa verte, in sostanza, sulla compatibilità di tale decisione con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona.

60 A tal riguardo, occorre richiamare la giurisprudenza costante della Corte secondo la quale l'Unione è un'Unione di diritto, nel senso che tutti gli atti delle sue istituzioni sono soggetti al controllo della conformità, segnatamente, ai Trattati, ai principi generali del diritto nonché ai diritti fondamentali (v., in tal senso, sentenze Commissione e a./Kadi, C-584/10 P, C-593/10 P e C-595/10 P, EU:C:2013:518, punto 66; Inuit Tapiriit Kanatami e a./Parlamento e Consiglio, C-583/11 P, EU:C:2013:625, punto 91, nonché Telefónica/Commissione, C-274/12 P, EU:C:2013:852, punto 56). Le decisioni della Commissione adottate in forza dell'articolo 25, paragrafo 6, della direttiva 95/46 non possono pertanto sfuggire ad un siffatto controllo.

61 Ciò premesso, la Corte è competente in via esclusiva a dichiarare l'invalidità di un atto dell'Unione, quale una decisione della Commissione adottata in applicazione dell'articolo 25, paragrafo 6, della direttiva 95/46; la natura esclusiva di tale competenza ha lo scopo di garantire la certezza del diritto assicurando l'applicazione uniforme del diritto dell'Unione (v. sentenze Melki e Abdeli, C-188/10 e C-189/10, EU:C:2010:363, punto 54, nonché CIVAD, C-533/10, EU:C:2012:347, punto 40).

62 Per quanto i giudici nazionali siano effettivamente legittimati ad esaminare la validità di un atto dell'Unione, come una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, essi non sono tuttavia competenti a constatare essi stessi l'invalidità di un siffatto atto (v., in tal senso, sentenze Foto-Frost, 314/85, EU:C:1987:452, punti da 15 a 20, nonché IATA e ELFAA, C-344/04, EU:C:2006:10, punto 27). A fortiori, in sede di esame di una domanda, ai sensi dell'articolo 28, paragrafo 4, di tale direttiva, avente ad oggetto la compatibilità di una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, di detta direttiva con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona, le autorità nazionali di controllo non sono competenti a constatare esse stesse l'invalidità di una siffatta decisione.

63 Alla luce di tali considerazioni, qualora una persona i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo che è stato oggetto di una decisione della Commissione in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, investa un'autorità nazionale di controllo di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di tali dati e

contesti, in occasione di tale domanda, come nel procedimento principale, la compatibilità di tale decisione con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona, incombe a tale autorità esaminare detta domanda con tutta la diligenza richiesta.

64 Nel caso in cui detta autorità pervenga alla conclusione che gli elementi addotti a sostegno di una siffatta domanda sono privi di fondamento e, per questo motivo, la respinga, la persona che ha proposto detta domanda deve avere accesso, come si evince dall'articolo 28, paragrafo 3, secondo comma, della direttiva 95/46, in combinato con l'articolo 47 della Carta, ai mezzi di ricorso giurisdizionali che le consentono di contestare una siffatta decisione impugnandola dinanzi ai giudici nazionali. Alla luce della giurisprudenza citata ai punti 61 e 62 della presente sentenza, tali giudici devono sospendere la decisione e investire la Corte di un procedimento pregiudiziale per accertamento di validità, allorché essi ritengono che uno o più motivi di invalidità formulati dalle parti o, eventualmente, sollevati d'ufficio siano fondati (v., in tal senso, sentenza T & L Sugars e Sidul Açúcares/Commissione, C-456/13 P, EU:C:2015:284, punto 48 e la giurisprudenza ivi citata).

65 Nell'ipotesi contraria, in cui detta autorità reputi fondate le censure sollevate dalla persona che l'ha investita di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei suoi dati personali, questa stessa autorità, ai sensi dell'articolo 28, paragrafo 3, primo comma, terzo trattino, della direttiva 95/46, in combinato, segnatamente, con l'articolo 8, paragrafo 3, della Carta, deve poter promuovere azioni giudiziarie. A tal riguardo, incombe al legislatore nazionale prevedere mezzi di ricorso che consentano all'autorità nazionale di controllo di cui trattasi di far valere le censure che essa reputa fondate dinanzi ai giudici nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di tale autorità in ordine alla validità della decisione della Commissione, ad un rinvio pregiudiziale inteso all'esame della validità di tale decisione.

66 In virtù delle considerazioni che precedono, si deve rispondere alle questioni sollevate che l'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce degli articoli 7, 8 e 47 della Carta, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, quale la decisione 2000/520, con la quale la Commissione constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, esamini la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato.

Sulla validità della decisione 2000/520

67 Come si evince dalle spiegazioni del giudice del rinvio relative alle questioni sollevate, il sig. Schrems fa valere, nel procedimento principale, che il diritto e la prassi degli Stati Uniti non assicurano un livello di protezione adeguato ai sensi dell'articolo 25 della direttiva 95/46. Come rilevato dall'avvocato generale ai paragrafi 123 e 124 delle sue conclusioni, il sig. Schrems esprime dubbi, che tale giudice sembra peraltro condividere nella sostanza, concernenti la validità della decisione 2000/520. In tali circostanze, in virtù delle constatazioni effettuate ai punti da 60 a 63 della presente sentenza, e al fine di fornire una risposta completa a detto giudice, occorre verificare se tale decisione sia conforme ai requisiti risultanti da detta direttiva, letta alla luce della Carta.

Sui requisiti risultanti dall'articolo 25, paragrafo 6, della direttiva 95/46

68 Come è già stato rilevato ai punti 48 e 49 della presente sentenza, l'articolo 25, paragrafo 1, della direttiva 95/46 vieta i trasferimenti di dati personali verso un paese terzo che non garantisce un livello di protezione adeguato.

69 Tuttavia, ai fini del controllo di tali trasferimenti, l'articolo 25, paragrafo 6, primo comma, di tale direttiva, dispone che la Commissione «può constatare (…) che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 [di tale articolo], in considerazione della sua legislazione nazionale o dei suoi impegni internazionali (…), ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona».

70 È vero che né l'articolo 25, paragrafo 2, della direttiva 95/46 né nessun'altra disposizione della medesima contengono una definizione della nozione di livello di protezione adeguato. In particolare, l'articolo 25, paragrafo 2, di detta direttiva si limita ad enunciare che l'adeguatezza del livello di protezione garantito da un paese terzo «è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati» ed elenca, in maniera non esaustiva, le circostanze che devono essere prese in considerazione in occasione di una siffatta valutazione.

71 Tuttavia, da un lato, come si evince dalla lettera stessa dell'articolo 25, paragrafo 6, della direttiva 95/46, tale disposizione esige che un paese terzo «garantisc[a]» un livello di protezione adeguato in considerazione della sua legislazione nazionale o dei suoi impegni internazionali. Dall'altro, sempre secondo tale disposizione, l'adeguatezza della protezione assicurata dal paese terzo viene valutata «ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona».

72 In tal modo, l'articolo 25, paragrafo 6, della direttiva 95/46 attua l'obbligo esplicito di protezione dei dati personali previsto all'articolo 8, paragrafo 1, della Carta e mira ad assicurare, come rilevato dall'avvocato generale al paragrafo 139 delle sue conclusioni, la continuità del livello elevato di tale protezione in caso di trasferimento di dati personali verso un paese terzo.

73 È vero che il termine «adeguato» figurante all'articolo 25, paragrafo 6, della direttiva 95/46 implica che non possa esigersi che un paese terzo assicuri un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione. Tuttavia, come rilevato dall'avvocato generale al paragrafo 141 delle sue conclusioni, l'espressione «livello di protezione adeguato» deve essere intesa nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza della direttiva 95/46, letta alla luce della Carta. Infatti, in assenza di un siffatto requisito, l'obiettivo menzionato al punto precedente della presente sentenza sarebbe disatteso. Inoltre, il livello elevato di protezione garantito dalla direttiva 95/46, letta alla luce della Carta, potrebbe essere facilmente eluso da trasferimenti di dati personali dall'Unione verso paesi terzi ai fini del loro trattamento in tali paesi.

74 Si evince dalla formulazione espressa dell'articolo 25, paragrafo 6, della direttiva 95/46 che è l'ordinamento giuridico del paese terzo interessato dalla decisione della Commissione che deve garantire un livello di protezione adeguato. Anche se gli strumenti dei quali tale paese terzo si avvale, al riguardo, per assicurare un siffatto livello di protezione, possono essere diversi da quelli attuati all'interno dell'Unione al fine di garantire il rispetto dei requisiti risultanti da tale direttiva, letta alla luce della Carta, tali strumenti devono cionondimeno rivelarsi efficaci, nella prassi, al fine di assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione.

75 In tali condizioni, in sede di esame del livello di protezione offerto da un paese terzo, la Commissione è tenuta a valutare il contenuto delle norme applicabili in tale paese risultanti dalla legislazione nazionale o dagli impegni internazionali di quest'ultimo, nonché la prassi intesa ad assicurare il rispetto di tali norme; al riguardo, tale istituzione deve prendere in considerazione, in conformità all'articolo 25, paragrafo 2, della direttiva 95/46, tutte le circostanze relative ad un trasferimento di dati personali verso un paese terzo.

76 Analogamente, alla luce del fatto che il livello di protezione assicurato da un paese terzo può evolversi, incombe alla Commissione, successivamente all'adozione di una decisione in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, verificare periodicamente se la constatazione relativa al livello di

protezione adeguato assicurato dal paese terzo in questione continui ad essere giustificata in fatto e in diritto. Una siffatta verifica è in ogni caso obbligatoria quando taluni indizi facciano sorgere un dubbio al riguardo.

77 Inoltre, come rilevato dall'avvocato generale ai paragrafi 134 e 135 delle sue conclusioni, in sede di esame della validità di una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, occorre anche tenere conto delle circostanze intervenute successivamente all'adozione di tale decisione.

78 A tal riguardo, occorre constatare che, alla luce, da un lato, del ruolo importante svolto dalla protezione dei dati personali sotto il profilo del diritto fondamentale al rispetto della vita privata e, dall'altro, del numero significativo di persone i cui diritti fondamentali possono essere violati in caso di trasferimento di dati personali verso un paese terzo che non assicura un livello di protezione adeguato, il potere discrezionale della Commissione in ordine all'adeguatezza del livello di protezione assicurato da un paese terzo risulta ridotto, cosicché è necessario procedere ad un controllo stretto dei requisiti risultanti dall'articolo 25 della direttiva 95/46, letto alla luce della Carta (v., per analogia, sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punti 47 e 48).

Sull'articolo 1 della decisione 2000/520

79 La Commissione ha considerato, all'articolo 1, paragrafo 1, della decisione 2000/520, che i principi di cui all'allegato I della medesima, applicati in conformità agli orientamenti forniti dalle FAQ di cui all'allegato II di detta decisione, garantiscono un livello adeguato di protezione dei dati personali trasferiti dall'Unione a organizzazioni aventi sede negli Stati Uniti. Risulta da tale disposizione che sia tali principi sia tali FAQ sono stati pubblicati dal Dipartimento del commercio degli Stati Uniti.

80 L'adesione di un'organizzazione ai principi dell'approdo sicuro avviene sulla base di un sistema di autocertificazione, come si evince dall'articolo 1, paragrafi 2 e 3, di tale decisione, in combinato disposto con la FAQ 6 figurante all'allegato II a detta decisione.

81 Sebbene il ricorso, da parte di un paese terzo, ad un sistema di autocertificazione non sia di per sé contrario al requisito previsto dall'articolo 25, paragrafo 6, della direttiva 95/46, secondo il quale il paese terzo di cui trattasi deve garantire un livello di protezione adeguato «in considerazione della (…) legislazione nazionale o [degli] impegni internazionali» di tale paese, l'affidabilità di un siffatto sistema, con riferimento a tale requisito, poggia essenzialmente sulla predisposizione di meccanismi efficaci di accertamento e di controllo che consentano di individuare e sanzionare, nella prassi, eventuali violazioni delle norme che assicurano la protezione dei diritti fondamentali, e segnatamente del diritto al rispetto della vita privata, nonché del diritto alla protezione dei dati personali.

82 Nella specie, in forza dell'allegato I, secondo comma, della decisione 2000/520, i principi dell'approdo sicuro sono «destinati unicamente ad organizzazioni americane che ricevono dati personali dall'Unione europea, al fine di permettere a tali organizzazioni di ottemperare al principio di "approdo sicuro" ed alla presunzione di "adeguatezza" che esso comporta». Tali principi sono dunque applicabili soltanto alle organizzazioni americane autocertificate che ricevono dati personali dall'Unione, mentre dalle autorità pubbliche americane non si esige il rispetto di detti principi.

83 Inoltre, ai sensi dell'articolo 2 della decisione 2000/520, quest'ultima «dispone soltanto in merito all'adeguatezza della protezione offerta negli Stati Uniti, in base ai principi [dell'approdo sicuro] applicati in conformità alle FAQ, al fine di quanto prescritto dall'articolo 25, paragrafo 1, della direttiva [95/46]», senza tuttavia contenere le constatazioni sufficienti quanto alle misure tramite le quali gli Stati Uniti d'America assicurano un livello di protezione adeguato, ai sensi dell'articolo 25, paragrafo 6, di tale direttiva, in considerazione della loro legislazione nazionale o dei loro impegni internazionali.

84 A ciò si aggiunge che, in conformità all'allegato I, quarto comma, della decisione 2000/520, l'applicabilità di detti principi può essere limitata, segnatamente, «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]», nonché da «disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione».

85 A tal riguardo, al titolo B del suo allegato IV, la decisione 2000/520 sottolinea, per quanto attiene ai limiti ai quali è assoggettata l'applicabilità dei principi dell'approdo sicuro, che «[è] ovvio che quando la legge statunitense impone un'obbligazione conflittuale, le organizzazioni statunitensi, che aderiscano o no ai principi "approdo sicuro", devono osservare la legge».

86 In tal modo, la decisione 2000/520 sancisce il primato delle «esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]» sui principi dell'approdo sicuro, primato in forza del quale le organizzazioni americane autocertificate che ricevono dati personali dall'Unione sono tenute a disapplicare senza limiti tali principi allorché questi ultimi interferiscono con tali esigenze e risultano dunque incompatibili con le medesime.

87 Alla luce del carattere generale della deroga figurante all'allegato I, quarto comma, della decisione 2000/520, essa rende pertanto possibili ingerenze, fondate su esigenze connesse alla sicurezza nazionale e all'interesse pubblico o alla legislazione interna degli Stati Uniti, nei diritti fondamentali delle persone i cui dati personali sono o potrebbero essere trasferiti dall'Unione verso gli Stati Uniti. A tal riguardo, poco importa, per accertare l'esistenza di un'ingerenza nel diritto fondamentale al rispetto della vita privata, che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a tale ingerenza (sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 33 e la giurisprudenza ivi citata).

88 Inoltre, la decisione 2000/520 non contiene alcuna dichiarazione quanto all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione verso gli Stati Uniti, ingerenze che entità statali di tale paese sarebbero autorizzate a compiere laddove perseguano obiettivi legittimi, come la sicurezza nazionale.

89 A ciò si aggiunge il fatto che la decisione 2000/520 non menziona l'esistenza di una tutela giuridica efficace nei confronti delle ingerenze di tale natura. Come rilevato dall'avvocato generale ai paragrafi da 204 a 206 delle sue conclusioni, i meccanismi di arbitrato privato e i procedimenti dinanzi alla Commissione federale per il commercio, i cui poteri, descritti segnatamente nelle FAQ 11 figuranti all'allegato II a tale decisione, sono limitati alle controversie in materia commerciale, riguardano il rispetto, da parte delle imprese americane, dei principi dell'approdo sicuro, e non possono essere applicati nell'ambito delle controversie concernenti la legittimità di ingerenze nei diritti fondamentali risultanti da misure di origine statale.

90 Inoltre, la suesposta analisi della decisione 2000/520 è corroborata dalla valutazione della stessa Commissione quanto alla situazione risultante dall'esecuzione di tale decisione. Infatti, in particolare ai punti 2 e 3.2 della comunicazione COM(2013) 846 final, nonché ai punti 7.1, 7.2 e 8 della comunicazione COM(2013) 847 final, il cui contenuto viene illustrato rispettivamente ai punti da 13 a 16, nonché ai punti 22, 23 e 25 della presente sentenza, tale istituzione ha constatato che le autorità americane potevano accedere ai dati personali trasferiti dagli Stati membri verso gli Stati Uniti e trattarli in maniera incompatibile, segnatamente, con le finalità del loro trasferimento, e al di là di quanto era strettamente necessario e proporzionato per la protezione della sicurezza nazionale.

Analogamente, la Commissione ha constatato che non esistevano, per le persone di cui trattasi, rimedi amministrativi o giurisdizionali che consentissero, segnatamente, di accedere ai dati che le riguardavano e, se del caso, di ottenerne la rettifica o la soppressione.

91 Quanto al livello di protezione delle libertà e dei diritti fondamentali garantito all'interno dell'Unione, una normativa della medesima che comporta un'ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta deve prevedere, secondo la giurisprudenza costante della Corte, regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati. La necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi (sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punti 54 e 55, nonché la giurisprudenza ivi citata).

92 Inoltre, e soprattutto, la protezione del diritto fondamentale al rispetto della vita privata a livello dell'Unione richiede che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario (sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 52 e la giurisprudenza ivi citata).

93 In tal senso, non è limitata allo stretto necessario una normativa che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta [v. in tal senso, in relazione alla direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, (GU L 105, pag. 54), sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punti da 57 a 61].

94 In particolare, si deve ritenere che una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta (v., in tal senso, sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 39).

95 Analogamente, una normativa che non prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati, non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all'articolo 47 della Carta. Infatti, l'articolo 47, primo comma, della Carta esige che ogni individuo i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati abbia diritto ad un ricorso effettivo dinanzi ad un giudice, nel rispetto delle condizioni previste in tale articolo. A tal riguardo, l'esistenza stessa di un controllo giurisdizionale effettivo, destinato ad assicurare il rispetto delle disposizioni del diritto dell'Unione, è inerente all'esistenza di uno Stato di diritto (v., in tal senso, sentenze Les Verts/Parlamento, 294/83, EU:C:1986:166, punto 23; Johnston, 222/84, EU:C:1986:206, punti 18 e 19; Heylens e a., 222/86, EU:C:1987:442, punto 14, nonché, UGT-Rioja e a., da C-428/06 a C-434/06, EU:C:2008:488, punto 80).

96 Come è stato rilevato segnatamente ai punti 71, 73 e 74 della presente sentenza, l'adozione, da parte della Commissione, di una decisione in forza dell'articolo 25, paragrafo 6, della direttiva 95/46 richiede la constatazione, debitamente motivata, da parte di tale istituzione, che il paese terzo di cui trattasi garantisce effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni

internazionali, un livello di protezione dei diritti fondamentali sostanzialmente equivalente a quello garantito nell'ordinamento giuridico dell'Unione, come emerge segnatamente dai punti precedenti della presente sentenza.

97 Orbene, occorre rilevare che la Commissione, nella decisione 2000/520, non ha affermato che gli Stati Uniti d'America «garantiscono» effettivamente un livello di protezione adeguato in considerazione della loro legislazione nazionale o dei loro impegni internazionali.

98 Di conseguenza, e senza che occorra esaminare i principi dell'approdo sicuro sotto il profilo del loro contenuto, si deve concludere che l'articolo 1 di tale decisione viola i requisiti fissati all'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce della Carta, e che esso è, per tale motivo, invalido.

Sull'articolo 3 della decisione 2000/520

99 Si evince dalle considerazioni svolte ai punti 53, 57 e 63 della presente sentenza che, considerato l'articolo 28 della direttiva 95/46, letto alla luce, segnatamente, dell'articolo 8 della Carta, le autorità nazionali di controllo devono poter esaminare, in piena indipendenza, ogni domanda relativa alla protezione dei diritti e delle libertà di una persona con riguardo al trattamento di dati personali che la riguardano. Ciò vale in particolare allorché, in occasione di una siffatta domanda, tale persona sollevi questioni attinenti alla compatibilità di una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, di tale direttiva, con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona.

100 Tuttavia, l'articolo 3, paragrafo 1, primo comma, della decisione 2000/520 contiene una disciplina specifica quanto ai poteri di cui dispongono le autorità nazionali di controllo con riferimento ad una constatazione effettuata dalla Commissione in relazione al livello di protezione adeguato, ai sensi dell'articolo 25 della direttiva 95/46.

101 Così, ai sensi di tale disposizione, tali autorità possono, «[f]atto salvo il loro potere di adottare misure per garantire l'ottemperanza alle disposizioni nazionali adottate in forza di disposizioni diverse dall'articolo 25 della direttiva [95/46], (…) sospendere flussi di dati diretti a un'organizzazione che ha autocertificato la sua adesione ai principi [della decisione 2000/520]», a condizioni restrittive che fissano una soglia elevata di intervento. Per quanto tale disposizione non pregiudichi i poteri di dette autorità di adottare misure intese ad assicurare il rispetto delle disposizioni nazionali adottate in applicazione di questa direttiva, cionondimeno essa esclude che le medesime possano adottare misure intese a garantire il rispetto dell'articolo 25 della direttiva medesima.

102 L'articolo 3, paragrafo 1, primo comma, della decisione 2000/520 deve pertanto essere inteso nel senso che esso priva le autorità nazionali di controllo dei poteri che esse traggono dall'articolo 28 della direttiva 95/46, nel caso in cui una persona, in occasione di una domanda basata su tale disposizione, adduca elementi idonei a rimettere in discussione il fatto che una decisione della Commissione che ha constatato, sul fondamento dell'articolo 25, paragrafo 6, di tale direttiva, che un paese terzo garantisce un livello di protezione adeguato, sia compatibile con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona.

103 Orbene, il potere di esecuzione che il legislatore dell'Unione ha attribuito alla Commissione con l'articolo 25, paragrafo 6, della direttiva 95/46 non conferisce a tale istituzione la competenza di limitare i poteri delle autorità nazionali di controllo previsti al punto precedente della presente sentenza.

104 Ciò premesso, occorre constatare che, adottando l'articolo 3 della decisione 2000/520, la Commissione ha ecceduto la competenza attribuitale all'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce della Carta, e che, per questo motivo, esso è invalido.

105 Poiché gli articoli 1 e 3 della decisione 2000/520 non possono essere separati dagli articoli 2 e 4, nonché dagli allegati alla medesima, la loro invalidità inficia la validità di tale decisione nel suo complesso.

106 Alla luce di tutte le considerazioni che precedono, si deve concludere che la decisione 2000/520 è invalida.

Sulle spese

107 Nei confronti delle parti nel procedimento principale, la presente causa costituisce un incidente sollevato dinanzi al giudice nazionale, cui spetta quindi statuire sulle spese. Le spese sostenute da altri soggetti per presentare osservazioni alla Corte non possono dar luogo a rifusione.

Per questi motivi, la Corte (Grande Sezione) dichiara:

1) **L'articolo 25, paragrafo 6, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, come modificata dal regolamento (CE) n. 1882/2003 del Parlamento europeo e del Consiglio, del 29 settembre 2003, letto alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, come la decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46 sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti, con la quale la Commissione europea constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, come modificata, esamini la domanda di una persona relativa alla protezione dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato.**

2) **La decisione 2000/520 è invalida.**

Firma