Raccolta della giurisprudenza

SENTENZA DELLA CORTE (Grande Sezione)

16 luglio 2020*

«Rinvio pregiudiziale – Tutela delle persone fisiche con riguardo al trattamento dei dati personali – Carta dei diritti fondamentali dell'Unione europea – Articoli 7, 8 e 47 – Regolamento (UE) 2016/679 – Articolo 2, paragrafo 2 – Ambito di applicazione – Trasferimento a fini commerciali di dati personali verso paesi terzi – Articolo 45 – Decisione di adeguatezza della Commissione – Articolo 46 – Trasferimento soggetto a garanzie adeguate – Articolo 58 – Poteri delle autorità di controllo – Trattamento da parte delle pubbliche autorità di un paese terzo, a fini di sicurezza nazionale, dei dati trasferiti – Valutazione dell'adeguatezza del livello di protezione garantito in un paese terzo – Decisione 2010/87/UE – Clausole tipo di protezione per il trasferimento di dati personali verso paesi terzi – Garanzie appropriate offerte dal titolare del trattamento – Validità – Decisione di esecuzione (UE) 2016/1250 – Adeguatezza della protezione garantita dallo scudo Unione europea-Stati Uniti per la privacy – Validità – Denuncia di una persona fisica i cui dati sono stati trasferiti dall'Unione europea verso gli Stati Uniti»

Nella causa C-311/18,

avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dalla High Court (Alta Corte, Irlanda), con decisione del 4 maggio 2018, pervenuta in cancelleria il 9 maggio 2018, nel procedimento

Data Protection Commissioner

contro

Facebook Ireland Ltd,

Maximillian Schrems,

con l'intervento di:

The United States of America,

Electronic Privacy Information Centre,

BSA Business Software Alliance Inc.,

Digitaleurope,

* Lingua processuale: l'inglese.

LA CORTE (Grande Sezione),

composta da K. Lenaerts, presidente, R. Silva de Lapuerta, vicepresidente, A. Arabadjiev, A. Prechal, M. Vilaras, M. Safjan, S. Rodin, P.G. Xuereb, L.S. Rossi e I. Jarukaitis, presidenti di sezione, M. Ilešič, T. von Danwitz (relatore) e D. Šváby, giudici,

avvocato generale: H. Saugmandsgaard Øe

cancelliere: C. Strömholm, amministratrice

vista la fase scritta del procedimento e in seguito all'udienza del 9 luglio 2019,

considerate le osservazioni presentate:

– per il Data Protection Commissioner, da D. Young, solicitor, B. Murray e M. Collins, SC, nonché C. Donnelly, BL;

– per Facebook Ireland Ltd, da P. Gallagher e N. Hyland, SC, A. Mulligan e F. Kieran, BL, nonché P. Nolan, C. Monaghan, C. O'Neill e R. Woulfe, solicitors;

– per M. Schrems, da H. Hofmann, Rechtsanwalt, E. McCullough, J. Doherty e S. O'Sullivan, SC, nonché G. Rudden, solicitor;

– per The United States of America, da E. Barrington, SC, S. Kingston, BL, nonché S. Barton e B. Walsh, solicitors;

– per l'Electronic Privacy Information Centre, da S. Lucey, solicitor, G. Gilmore e A. Butler, BL, nonché C. O'Dwyer, SC;

– per BSA Business Software Alliance Inc., da B. Van Vooren e K. Van Quathem, advocaten;

– per Digitaleurope, da N. Cahill, barrister, J. Cahir, solicitor, e M. Cush, SC;

– per l'Irlanda, da A. Joyce e M. Browne, in qualità di agenti, assistiti da D. Fennelly, BL;

– per il governo belga, da J.-C. Halleux e P. Cottin, in qualità di agenti;

– per il governo ceco, da M. Smolek, J. Vláčil, O. Serdula e A. Kasalická, in qualità di agenti;

– per il governo tedesco, da J. Möller, D. Klebs e T. Henze, in qualità di agenti;

– per il governo francese, da A.-L. Desjonquères, in qualità d'agente;

– per il governo dei Paesi Bassi, da C.S. Schillemans, K. Bulterman e M. Noort, in qualità di agenti;

– per il governo austriaco, da J. Schmoll e G. Kunnert, in qualità di agenti;

– per il governo polacco, da B. Majczyna, in qualità di agente;

– per il governo portoghese, da L. Inez Fernandes, A. Pimenta e C. Vieira Guerra, in qualità di agenti;

– per il governo del Regno Unito, da S. Brandon, in qualità di agente, assistito da J. Holmes, QC, e C. Knight, barrister;

– per il Parlamento europeo, da M.J. Martínez Iglesias e A. Caiola, in qualità di agenti;

– per la Commissione europea, da D. Nardi, H. Krämer e H. Kranenborg, in qualità di agenti;

– per il Comitato europeo per la protezione dei dati (EDPB), da A. Jelinek e K. Behn, in qualità di agenti,

sentite le conclusioni dell'avvocato generale, presentate all'udienza del 19 dicembre 2019,

ha pronunciato la seguente

Sentenza

1 La domanda di pronuncia pregiudiziale in sostanza, verte:

– sull'interpretazione dell'articolo 3, paragrafo 2, primo trattino, degli articoli 25 e 26, nonché dell'articolo 28, paragrafo 3, 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 1995, L 281, pag. 31), letti alla luce dell'articolo 4, paragrafo 2, TUE e degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»),

– sull'interpretazione e la validità della decisione 2010/87/UE della Commissione, del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46 (GU 2010, L 39, pag. 5), come modificata dalla decisione di esecuzione (UE) 2016/2297 della Commissione, del 16 dicembre 2016 (GU 2016, L 344, pag. 100) (in prosieguo: «decisione CPT»), nonché

– sull'interpretazione e la validità della decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy (GU 2016, L 207, pag. 1; in prosieguo: la «decisione "scudo per la privacy"»).

2 Tale domanda è stata presentata nell'ambito di una controversia che vede opposti il Data Protection Commissioner (Commissario per la protezione dei dati; in prosieguo: il «Commissario») a Facebook Ireland Ltd e al sig. Maximillian Schrems relativamente ad una denuncia presentata da quest'ultimo riguardo al trasferimento di dati personali da parte di Facebook Ireland Ltd a Facebook Inc. negli Stati Uniti.

Contesto normativo

Direttiva 95/46

3 L'articolo 3 della direttiva 95/46, intitolato «Campo d'applicazione», al suo paragrafo 2 enunciava quanto segue:

«Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali[:]

– effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale;

(...)».

4 L'articolo 25 di tale direttiva così disponeva:

«1. Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali (...) 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; (...)

(...)

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».

5 L'articolo 26, paragrafi 2 e 4, di detta direttiva prevedeva quanto segue:

«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.

(...)

4. Qualora la Commissione decida, secondo la procedura di cui all'articolo 31, paragrafo 2, che alcune clausole contrattuali tipo offrono le garanzie sufficienti di cui al paragrafo 2, gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione».

6 Ai sensi dell'articolo 28, paragrafo 3, della medesima direttiva:

«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

(…)».

RGPD

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

8 I considerando 6, 10, 101, 103, 104, da 107 a 109, 114, 116 e 141 di detto regolamento così recitano:

«(6) La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

(...)

(10) Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. Per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento. In combinato disposto con la legislazione generale e orizzontale in materia di protezione dei dati che attua la direttiva 95/46/CE gli Stati membri dispongono di varie leggi settoriali in settori che richiedono disposizioni più specifiche. Il presente regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali («dati sensibili»). In tal senso, il presente regolamento non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito.

(...)

(101) I flussi di dati personali verso e da paesi al di fuori dell'Unione e organizzazioni internazionali sono necessari per l'espansione del commercio internazionale e della cooperazione internazionale. L'aumento di tali flussi ha posto nuove sfide e problemi riguardanti la protezione dei dati personali. È opportuno però che, quando i dati personali sono trasferiti

dall'Unione a titolari del trattamento e responsabili del trattamento o altri destinatari in paesi terzi o a organizzazioni internazionali, il livello di tutela delle persone fisiche assicurato nell'Unione dal presente regolamento non sia compromesso, anche nei casi di trasferimenti successivi dei dati personali dal paese terzo o dall'organizzazione internazionale verso titolari del trattamento e responsabili del trattamento nello stesso o in un altro paese terzo o presso un'altra organizzazione internazionale. In ogni caso, i trasferimenti verso paesi terzi e organizzazioni internazionali potrebbero essere effettuati soltanto nel pieno rispetto del presente regolamento. Il trasferimento potrebbe aver luogo soltanto se, fatte salve le altre disposizioni del presente regolamento, il titolare del trattamento o il responsabile del trattamento rispetta le condizioni stabilite dalle disposizioni del presente regolamento in relazione al trasferimento di dati personali verso paesi terzi o organizzazioni internazionali.

(...)

(103) La Commissione può decidere, con effetto nell'intera Unione, che un paese terzo, un territorio o un settore specifico all'interno di un paese terzo, o un'organizzazione internazionale offrono un livello adeguato di protezione dei dati, garantendo in tal modo la certezza del diritto e l'uniformità in tutta l'Unione nei confronti del paese terzo o dell'organizzazione internazionale che si ritiene offra tale livello di protezione. In tali casi, i trasferimenti di dati personali verso tale paese terzo od organizzazione internazionale possono avere luogo senza ulteriori autorizzazioni. La Commissione può inoltre decidere, dopo aver fornito una dichiarazione completa che illustra le motivazioni al paese terzo o all'organizzazione internazionale, di revocare una tale decisione.

(104) In linea con i valori fondamentali su cui è fondata l'Unione, in particolare la tutela dei diritti dell'uomo, è opportuno che la Commissione, nella sua valutazione del paese terzo, o di un territorio o di un settore specifico all'interno di un paese terzo, tenga conto del modo in cui tale paese rispetta lo stato di diritto, l'accesso alla giustizia e le norme e gli standard internazionali in materia di diritti dell'uomo, nonché la legislazione generale e settoriale riguardante segnatamente la sicurezza pubblica, la difesa e la sicurezza nazionale, come pure l'ordine pubblico e il diritto penale. L'adozione di una decisione di adeguatezza nei confronti di un territorio o di un settore specifico all'interno di un paese terzo dovrebbe prendere in considerazione criteri chiari e obiettivi come specifiche attività di trattamento e l'ambito di applicazione delle norme giuridiche e degli atti legislativi applicabili in vigore nel paese terzo. Il paese terzo dovrebbe offrire garanzie di un adeguato livello di protezione sostanzialmente equivalente a quello assicurato all'interno dell'Unione, segnatamente quando i dati personali sono trattati in uno o più settori specifici. In particolare, il paese terzo dovrebbe assicurare un effettivo controllo indipendente della protezione dei dati e dovrebbe prevedere meccanismi di cooperazione con autorità di protezione dei dati degli Stati membri e agli interessati dovrebbero essere riconosciuti diritti effettivi e azionabili e un mezzo di ricorso effettivo in sede amministrativa e giudiziale.

(...)

(107) La Commissione può riconoscere che un paese terzo, un territorio o un settore specifico all'interno di un paese terzo, o un'organizzazione internazionale non garantiscono più un livello adeguato di protezione dei dati. Di conseguenza il trasferimento di dati personali verso tale paese terzo od organizzazione internazionale dovrebbe essere vietato, a meno che non siano soddisfatti i requisiti di cui al presente regolamento relativamente ai trasferimenti sottoposti a garanzie adeguate, comprese norme vincolanti d'impresa, e a deroghe per situazioni particolari. In tal caso è opportuno prevedere consultazioni tra la Commissione e detti paesi terzi o organizzazioni internazionali. La Commissione dovrebbe informare tempestivamente il paese terzo o l'organizzazione internazionale dei motivi e avviare consultazioni con questi al fine di risolvere la situazione.

(108) In mancanza di una decisione di adeguatezza, il titolare del trattamento o il responsabile del trattamento dovrebbe provvedere a compensare la carenza di protezione dei dati in un paese terzo con adeguate garanzie a tutela dell'interessato. Tali adeguate garanzie possono consistere nell'applicazione di norme vincolanti d'impresa, clausole tipo di protezione dei dati adottate dalla Commissione, clausole tipo di protezione dei dati adottate da un'autorità di controllo o clausole contrattuali autorizzate da un'autorità di controllo. Tali garanzie dovrebbero assicurare un rispetto dei requisiti in materia di protezione dei dati e dei diritti degli interessati adeguato ai trattamenti all'interno dell'Unione, compresa la disponibilità di diritti azionabili degli interessati e di mezzi di ricorso effettivi, fra cui il ricorso effettivo in sede amministrativa o giudiziale e la richiesta di risarcimento, nell'Unione o in un paese terzo. Esse dovrebbero riguardare, in particolare, la conformità rispetto ai principi generali in materia di trattamento dei dati personali e ai principi di protezione dei dati fin dalla progettazione e di protezione dei dati di default. (...)

(109) La possibilità che il titolare del trattamento o il responsabile del trattamento utilizzi clausole tipo di protezione dei dati adottate dalla Commissione o da un'autorità di controllo non dovrebbe precludere ai titolari del trattamento o ai responsabili del trattamento la possibilità di includere tali clausole tipo in un contratto più ampio, anche in un contratto tra il responsabile del trattamento e un altro responsabile del trattamento, né di aggiungere altre clausole o garanzie supplementari, purché non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo adottate dalla Commissione o da un'autorità di controllo o ledano i diritti o le libertà fondamentali degli interessati. I titolari del trattamento e i responsabili del trattamento dovrebbero essere incoraggiati a fornire garanzie supplementari attraverso impegni contrattuali che integrino le clausole tipo di protezione.

(...)

(114) In ogni caso, se la Commissione non ha adottato alcuna decisione circa il livello adeguato di protezione dei dati di un paese terzo, il titolare del trattamento o il responsabile del trattamento dovrebbe ricorrere a soluzioni che diano all'interessato diritti effettivi e azionabili in relazione al trattamento dei suoi dati personali nell'Unione, dopo il trasferimento, così da continuare a beneficiare dei diritti fondamentali e delle garanzie.

(...)

(116) Con i trasferimenti transfrontalieri di dati personali al di fuori dell'Unione potrebbe aumentare il rischio che la persona fisica non possa esercitare il proprio diritto alla protezione dei dati, in particolare per tutelarsi da usi o comunicazioni illeciti di tali informazioni. Allo stesso tempo, le autorità di controllo possono concludere di non essere in grado di dar corso ai reclami o svolgere indagini relative ad attività condotte oltre frontiera. I loro sforzi di collaborazione nel contesto transfrontaliero possono anche essere ostacolati dall'insufficienza di poteri per prevenire e correggere, da regimi giuridici incoerenti e da difficoltà pratiche quali la limitatezza delle risorse disponibili. (...)

(...)

(141) Ciascun interessato dovrebbe avere il diritto di proporre reclamo a un'unica autorità di controllo, in particolare nello Stato membro in cui risiede abitualmente, e il diritto a un ricorso giurisdizionale effettivo a norma dell'articolo 47 della Carta qualora ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento o se l'autorità di controllo non dà seguito a un reclamo, lo respinge in tutto o in parte o lo archivia o non agisce quando è necessario intervenire per proteggere i diritti dell'interessato. (...)».

9 L'articolo 2, paragrafi 1 e 2, di tale regolamento così recita:

«1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

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

a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;

b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;

c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;

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

10 L'articolo 4 del citato regolamento stabilisce quanto segue:

«Ai fini del presente regolamento s'intende per:

(...)

2) "trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

(...)

7) "titolare del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) "responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) "destinatario": la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

(...)».

11 L'articolo 23 del medesimo regolamento è così formulato:

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

a) la sicurezza nazionale;

b) la difesa;

c) la sicurezza pubblica;

d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;

(...)

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

a) le finalità del trattamento o le categorie di trattamento;

b) le categorie di dati personali;

c) la portata delle limitazioni introdotte;

d) le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti;

e) l'indicazione precisa del titolare del trattamento o delle categorie di titolari;

f) i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento;

g) i rischi per i diritti e le libertà degli interessati; e

h) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa».

12 Il capo V del RGPD, rubricato «Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali», include gli articoli da 44 a 50 di tale regolamento. L'articolo 44 di tale regolamento, intitolato «Principio generale per il trasferimento», è così formulato:

«Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato».

13 L'articolo 45 di tale regolamento, intitolato «Trasferimento sulla base di una decisione di adeguatezza», ai suoi paragrafi da 1 a 3, così prevede:

«1. Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.

2. Nel valutare l'adeguatezza del livello di protezione, la Commissione prende in considerazione in particolare i seguenti elementi:

a) lo [S]tato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza nonché i diritti effettivi e azionabili degli interessati e un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento;

b) l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale, con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati, comprensiva di adeguati poteri di esecuzione, per assistere e fornire consulenza agli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo degli Stati membri; e

c) gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali.

3. La Commissione, previa valutazione dell'adeguatezza del livello di protezione, può decidere, mediante atti di esecuzione, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo. L'atto di esecuzione prevede un meccanismo di riesame periodico, almeno ogni quattro anni, che tenga conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale. L'atto di esecuzione specifica il proprio ambito di applicazione geografico e settoriale e, ove applicabile, identifica la o le autorità di controllo di cui al paragrafo 2, lettera b), del presente articolo. L'atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 93, paragrafo 2».

14 L'articolo 46 del medesimo regolamento, intitolato «Trasferimento soggetto a garanzie adeguate», ai suoi paragrafi da 1 a 3, è formulato nel modo seguente:

«1. In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

2. Possono costituire garanzie adeguate di cui al paragrafo 1 senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo:

a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;

b) le norme vincolanti d'impresa in conformità dell'articolo 47;

c) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;

d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;

e) un codice di condotta approvato a norma dell'articolo 40, unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; o

f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

3. Fatta salva l'autorizzazione dell'autorità di controllo competente, possono altresì costituire in particolare garanzie adeguate di cui al paragrafo 1:

a) le clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale; o

b) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati».

15 L'articolo 49 del medesimo regolamento, intitolato «Deroghe in specifiche situazioni», stabilisce quanto segue:

«1. In mancanza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, o di garanzie adeguate ai sensi dell'articolo 46, comprese le norme vincolanti d'impresa, è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle seguenti condizioni:

a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;

b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;

c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;

d) il trasferimento sia necessario per importanti motivi di interesse pubblico;

e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;

f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.

Se non è possibile basare il trasferimento su una disposizione dell'articolo 45 o 46, comprese le disposizioni sulle norme vincolanti d'impresa, e nessuna delle deroghe in specifiche situazioni a norma del primo comma del presente paragrafo è applicabile, il trasferimento verso un paese terzo o un'organizzazione internazionale sia ammesso soltanto se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare e del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali. Il titolare del trattamento informa del trasferimento l'autorità di controllo. In aggiunta alla fornitura di informazioni di cui agli articoli 13 e 14, il titolare del trattamento informa l'interessato del trasferimento e degli interessi legittimi cogenti perseguiti.

2. Il trasferimento di cui al paragrafo 1, primo comma, lettera g), non può riguardare la totalità dei dati personali o intere categorie di dati personali contenute nel registro. Se il registro è destinato a essere consultato da persone aventi un legittimo interesse, il trasferimento è ammesso soltanto su richiesta di tali persone o qualora tali persone ne siano i destinatari.

3. Il primo comma, lettere a), b) e c), e il secondo comma del paragrafo 1 non si applicano alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri.

4. L'interesse pubblico di cui al paragrafo 1, primo comma, lettera d), è riconosciuto dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento.

5. In mancanza di una decisione di adeguatezza, il diritto dell'Unione o degli Stati membri può, per importanti motivi di interesse pubblico, fissare espressamente limiti al trasferimento di categorie specifiche di dati verso un paese terzo o un'organizzazione internazionale. Gli Stati membri notificano tali disposizioni alla Commissione.

6. Il titolare del trattamento o il responsabile del trattamento attesta nel registro di cui all'articolo 30 la valutazione e le garanzie adeguate di cui al paragrafo 1, secondo comma, del presente articolo».

16 Ai sensi dell'articolo 51, paragrafo 1, del RGPD:

«Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (l'"autorità di controllo")».

17 Ai termini dell'articolo 55, paragrafo 1, di tale regolamento, «[o]gni autorità di controllo è competente a eseguire i compiti assegnati e a esercitare i poteri a essa conferiti a norma del presente regolamento nel territorio del rispettivo Stato membro».

18 L'articolo 57, paragrafo 1, del suddetto regolamento prevede quanto segue:

«Fatti salvi gli altri compiti indicati nel presente regolamento, sul proprio territorio ogni autorità di controllo:

a) sorveglia e assicura l'applicazione del presente regolamento;

(...)

f) tratta i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'articolo 80, e svolge le indagini opportune sull'oggetto del reclamo e informa il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole, in particolare ove siano necessarie ulteriori indagini o un coordinamento con un'altra autorità di controllo;

(...)».

19 Ai sensi dell'articolo 58, paragrafi 2 e 4, dello stesso regolamento:

«2. Ogni autorità di controllo ha tutti i poteri correttivi seguenti:

(...)

f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;

(…)

j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

(...)

4. L'esercizio da parte di un'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie adeguate, inclusi il ricorso giurisdizionale effettivo e il giusto processo, previste dal diritto dell'Unione e degli Stati membri conformemente alla Carta».

20 L'articolo 64, paragrafo 2, del RGPD così dispone:

«Qualsiasi autorità di controllo, il presidente del [comitato europeo per la protezione dei dati (EDPB)] o la Commissione può richiedere che le questioni di applicazione generale o che producono effetti in più di uno Stato membro siano esaminate dal comitato al fine di ottenere un parere, in particolare se un'autorità di controllo competente non si conforma agli obblighi relativi all'assistenza reciproca ai sensi dell'articolo 61 o alle operazioni congiunte ai sensi dell'articolo 62».

21 Ai sensi dell'articolo 65, paragrafo 1, di detto regolamento:

«Al fine di assicurare l'applicazione corretta e coerente del presente regolamento nei singoli casi, il comitato adotta una decisione vincolante nei seguenti casi:

(...)

c) se un'autorità di controllo competente non richiede il parere del comitato nei casi di cui all'articolo 64, paragrafo 1, o non si conforma al parere del comitato emesso a norma dell'articolo 64. In tal caso qualsiasi autorità di controllo interessata o la Commissione può comunicare la questione al comitato».

22 L'articolo 77 di tale regolamento, intitolato «Diritto di proporre reclamo all'autorità di controllo», è così formulato:

«1. Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione.

2. L'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78».

23 L'articolo 78 dello stesso regolamento, intitolato «Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo», ai suoi paragrafi 1 e 2, così prevede:

«1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda.

2. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ciascun interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora l'autorità di controllo che sia competente ai sensi degli articoli 55 e 56 non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto ai sensi dell'articolo 77».

24 L'articolo 94 del RGPD è così formulato:

«1. La direttiva [95/46] è abrogata a decorrere dal 25 maggio 2018.

2. I riferimenti alla direttiva abrogata si intendono fatti al presente regolamento. I riferimenti al gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE si intendono fatti al comitato europeo per la protezione dei dati istituito dal presente regolamento».

25 A tenore dell'articolo 99 di tale regolamento:

«1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

2. Esso si applica a decorrere da 25 maggio 2018».

Decisione CPT

26 Il considerando 11 della decisione CPT così recita:

«Le autorità di controllo degli Stati membri svolgono un ruolo fondamentale in tale ambito contrattuale garantendo che i dati personali siano adeguatamente tutelati in seguito al trasferimento. Nei casi eccezionali in cui gli esportatori si rifiutino o non siano in grado di impartire le istruzioni necessarie agli importatori, e le persone cui si riferiscono i dati siano esposte ad un imminente rischio di gravi danni, le clausole tipo devono consentire alle autorità di controllo di vigilare sugli importatori e sui subincaricati e di adottare, se del caso, decisioni vincolanti nei loro confronti. Le autorità di controllo devono avere la facoltà di vietare o sospendere i trasferimenti di dati effettuati in base alle clausole contrattuali tipo nei casi eccezionali in cui il trasferimento su base contrattuale rischi di pregiudicare le garanzie e gli obblighi destinati a garantire protezione adeguata agli interessati».

27 L'articolo 1 di detta decisione così recita:

«Le clausole contrattuali tipo riportate in allegato costituiscono garanzie sufficienti per la tutela della vita privata e dei diritti e della libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi ai sensi dell'articolo 26, paragrafo 2, della direttiva 95/46/CE».

28 Ai termini dell'articolo 2, secondo comma della suddetta decisione, quest'ultima «si applica al trasferimento dei dati personali effettuato da responsabili del trattamento stabiliti nell'Unione europea a destinatari stabiliti al di fuori dell'Unione europea che agiscano esclusivamente in veste di incaricati del trattamento».

29 L'articolo 3 della stessa decisione così dispone:

«Ai fini della presente decisione si intende per:

(...)

c) "esportatore" il responsabile del trattamento che trasferisce i dati personali;

d) "importatore" l'incaricato del trattamento stabilito in un paese terzo che s'impegni a ricevere dall'esportatore dati personali al fine di trattarli per conto e secondo le istruzioni dell'esportatore stesso, nonché a norma della presente decisione, e che non sia assoggettato dal paese terzo a un sistema che garantisca una protezione adeguata ai sensi dell'articolo 25, paragrafo 1, della direttiva [95/46];

(...)

f) "normativa sulla protezione dei dati" la normativa che protegge i diritti e le libertà fondamentali del singolo, in particolare il diritto al rispetto della vita privata con riguardo al trattamento di dati personali, applicabile ai responsabili del trattamento nello Stato membro in cui è stabilito l'esportatore;

(...)».

30 Nella sua versione iniziale, precedente all'entrata in vigore della decisione di esecuzione 2016/2297, l'articolo 4 della decisione 2010/87 prevedeva quanto segue:

«1. Fatto salvo il potere di provvedere all'osservanza delle disposizioni nazionali adottate in attuazione dei capi II, III, V e VI della direttiva [95/46], le autorità competenti degli Stati membri possono avvalersi dei poteri loro attribuiti per vietare o sospendere i flussi di dati verso paesi terzi allo scopo di proteggere le persone con riguardo al trattamento dei dati personali, qualora:

a) sia accertato che, in base alla legge ad esso applicabile, l'importatore o il subincaricato è tenuto ad applicare deroghe alla normativa sulla protezione dei dati che eccedono le restrizioni ritenute necessarie in una società democratica ai sensi dell'articolo 13 della direttiva [95/46] e pregiudicano significativamente le garanzie previste dalla normativa sulla protezione dei dati e dalle clausole contrattuali tipo;

b) un'autorità competente abbia accertato che l'importatore o il subincaricato non ha rispettato le clausole contrattuali tipo riportate in allegato; oppure

c) sia probabile che le clausole contrattuali tipo in allegato non vengano rispettate e che la prosecuzione del trasferimento determini un imminente rischio di gravi danni per le persone cui i dati si riferiscono.

2. Il divieto o la sospensione ai sensi del paragrafo 1 sono revocati non appena ne vengano meno le ragioni.

3. Quando prende i provvedimenti di cui ai paragrafi 1 e 2, lo Stato membro informa senza indugio la Commissione; questa trasmette l'informazione agli altri Stati membri».

31 Il considerando 5 della decisione di esecuzione 2016/2297, adottata in seguito alla pronuncia della sentenza del 6 ottobre 2015, Schrems (C-362/14, EU:C:2015:650), è così formulato:

«Mutatis mutandis, una decisione della Commissione adottata ai sensi dell'articolo 26, paragrafo 4, della direttiva 95/46/CE è vincolante per tutti gli organi degli Stati membri destinatari, incluse le loro autorità di controllo indipendenti, nella misura in cui ha l'effetto di riconoscere che i trasferimenti effettuati sulla base delle clausole contrattuali tipo in essa contenute offrono garanzie sufficienti come richiesto dall'articolo 26, paragrafo 2, della direttiva. Questo non impedisce ad un'autorità di controllo nazionale di esercitare i propri poteri di controllo dei flussi di dati, compreso il potere di sospendere o vietare il trasferimento di dati personali, qualora stabilisca che esso avviene in violazione della normativa europea o nazionale sulla protezione dei dati, come, ad esempio, quando l'importatore dei dati non rispetta le clausole contrattuali tipo».

32 Nella sua versione attuale, risultante dalla decisione di esecuzione 2016/2297, l'articolo 4 della decisione CPT così dispone:

«Quando le autorità competenti di uno Stato membro esercitano i poteri ad esse conferiti dall'articolo 28, paragrafo 3, della direttiva [95/46] per sospendere o vietare a titolo definitivo i flussi di dati verso paesi terzi ai fini della tutela delle persone per quanto riguarda il trattamento dei dati personali, lo Stato membro interessato informa immediatamente la Commissione, che a sua volta inoltra l'informazione agli altri Stati membri».

33 L'allegato della decisione CPT, intitolato «Clausole contrattuali tipo ("incaricati del trattamento")», contiene dodici clausole tipo. La clausola 3 di tale allegato, a sua volta intitolata «Clausola del terzo beneficiario», prevede quanto segue:

«1. L'interessato può far valere, nei confronti dell'esportatore, la presente clausola, la clausola 4, lettere da b) a i), la clausola 5, lettere da a) ad e) e da g) a j), la clausola 6, paragrafi 1 e 2, la clausola 7, la clausola 8, paragrafo 2, e le clausole da 9 a 12 in qualità di terzo beneficiario.

2. L'interessato può far valere, nei confronti dell'importatore, la presente clausola, la clausola 5, lettere da a) ad e) e g), la clausola 6, la clausola 7, la clausola 8, paragrafo 2, e le clausole da 9 a 12 qualora l'esportatore sia scomparso di fatto o abbia giuridicamente cessato di esistere, a meno che tutti gli obblighi dell'esportatore siano stati trasferiti, per contratto o per legge, all'eventuale successore che di conseguenza assume i diritti e gli obblighi dell'esportatore, nel qual caso l'interessato può far valere le suddette clausole nei confronti del successore.

(...)».

34 La clausola 4 di tale allegato, dal titolo «Obblighi dell'esportatore», è così formulata:

«L'esportatore dichiara e garantisce quanto segue:

a) che il trattamento, compreso il trasferimento, dei dati personali, è e continua ad essere effettuato in conformità di tutte le pertinenti disposizioni della normativa sulla protezione dei dati (e viene comunicato, se del caso, alle competenti autorità dello Stato membro in cui è stabilito l'esportatore) nel pieno rispetto delle leggi vigenti in quello Stato;

b) che ha prescritto all'importatore, e continuerà a farlo per tutta la durata delle operazioni di trattamento, di trattare i dati personali trasferiti soltanto per suo conto e conformemente alla normativa sulla protezione dei dati e alle presenti clausole;

(...)

f) che, qualora il trasferimento riguardi categorie particolari di dati, gli interessati sono stati o saranno informati prima del trasferimento, o immediatamente dopo, che i dati che li riguardano potrebbero essere trasmessi a un paese terzo che non garantisce una protezione adeguata ai sensi della direttiva [95/46];

g) di trasmettere all'autorità di controllo l'eventuale comunicazione presentata dall'importatore o dal subincaricato ai sensi della clausola 5, lettera b), e della clausola 8, paragrafo 3, qualora decida di proseguire il trasferimento o revocare la sospensione;

(...)».

35 La clausola 5 di tale allegato, intitolata «Obblighi dell'importatore (...)», prevede quanto segue:

«L'importatore dichiara e garantisce quanto segue:

a) di trattare i dati personali esclusivamente per conto e secondo le istruzioni dell'esportatore, nonché a norma delle presenti clausole, e di impegnarsi a informare prontamente l'esportatore qualora non possa per qualsiasi ragione ottemperare a tale disposizione, nel qual caso l'esportatore ha facoltà di sospendere il trasferimento e/o risolvere il contratto;

b) di non avere motivo di ritenere che la normativa ad esso applicabile impedisca di seguire le istruzioni dell'esportatore o di adempiere agli obblighi contrattuali, e di comunicare all'esportatore, non appena ne abbia conoscenza, qualsiasi modificazione di tale normativa che possa pregiudicare le garanzie e gli obblighi previsti dalle presenti clausole, nel qual caso l'esportatore ha facoltà di sospendere il trasferimento e/o di risolvere il contratto;

(...)

d) che comunicherà prontamente all'esportatore:
   i) qualsiasi richiesta giuridicamente vincolante presentata da autorità giudiziarie o di polizia ai fini della comunicazione di dati personali, salvo che la comunicazione sia vietata da norme specifiche, ad esempio da norme di diritto penale miranti a tutelare il segreto delle indagini;
   ii) qualsiasi accesso accidentale o non autorizzato; e
   iii) qualsiasi richiesta ricevuta direttamente dagli interessati cui non abbia risposto, salvo che sia stato autorizzato a non rispondere;

(...)».

36 La nota a piè di pagina cui fa rinvio il titolo di tale clausola 5 è formulata nei termini seguenti:

«Disposizioni vincolanti della legislazione nazionale applicabile all'importatore che non vanno oltre quanto è necessario in una società democratica sulla base di uno degli interessi di cui all'articolo 13, paragrafo 1, della direttiva [95/46]; in altri termini, le restrizioni necessarie alla salvaguardia della sicurezza dello Stato, della difesa, della pubblica sicurezza, della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate, di un rilevante interesse economico o finanziario dello Stato, della protezione della persona cui si riferiscono i dati o dei diritti o delle libertà altrui, non sono in contraddizione con le clausole contrattuali tipo. (...)».

37 La clausola 6 dell'allegato della decisione CPT, intitolata «Responsabilità», è così formulata:

«1. Le parti convengono che l'interessato che abbia subito un pregiudizio per violazione degli obblighi di cui alla clausola 3 o alla clausola 11 ad opera di una parte o del subincaricato ha diritto di ottenere dall'esportatore il risarcimento del danno sofferto.

2. Qualora l'interessato non sia in grado di proporre l'azione di risarcimento di cui al paragrafo 1 nei confronti dell'esportatore per violazione di uno degli obblighi di cui alla clausola 3 o alla clausola 11 ad opera dell'importatore o del subincaricato, in quanto l'esportatore sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, l'importatore riconosce all'interessato stesso il diritto di agire nei suoi confronti così come se egli fosse l'esportatore (...).

(...)».

38 La clausola 8 di tale allegato, intitolata «Collaborazione con le autorità di controllo», al paragrafo 2, prevede quanto segue:

«Le parti dichiarano che l'autorità di controllo ha il diritto di sottoporre a controlli l'importatore e i subincaricati nella stessa misura e secondo le stesse modalità previste per l'esportatore dalla normativa sulla protezione dei dati».

39 La clausola 9 del medesimo allegato, intitolata «Legge applicabile», precisa che tali clausole sono soggette alla legge dello Stato membro in cui è stabilito l'esportatore.

40 La clausola 11 di tale allegato, dal titolo «Subcontratto», è del seguente tenore:

«1. L'importatore non può subcontrattare i trattamenti effettuati per conto dell'esportatore ai sensi delle presenti clausole senza il previo consenso scritto dell'esportatore stesso. L'importatore che, con il consenso dell'esportatore, affidi in subcontratto l'esecuzione degli obblighi ai sensi delle presenti clausole stipula, a tal fine, con il subincaricato un accordo scritto che imponga a quest'ultimo gli obblighi cui è egli stesso tenuto in virtù delle clausole (...)

2. Nell'accordo scritto tra l'importatore e il subincaricato è inserita la clausola del terzo beneficiario, di cui alla clausola 3, a favore dell'interessato che non sia in grado di proporre l'azione di risarcimento di cui alla clausola 6, paragrafo 1, nei confronti dell'esportatore o dell'importatore in quanto l'esportatore e l'importatore siano entrambi scomparsi di fatto, abbiano giuridicamente cessato di esistere o siano divenuti insolventi, e nessun successore abbia assunto, per contratto o per legge, l'insieme dei loro obblighi. La responsabilità civile del subincaricato è limitata ai trattamenti da quello effettuati ai sensi delle presenti clausole.

(…)».

41 La clausola 12 dell'allegato della decisione CPT, rubricata «Obblighi al termine dell'attività di trattamento dei dati personali», al paragrafo 1 così prevede:

«Le parti convengono che al termine dell'attività di trattamento l'importatore e il subincaricato provvedono, a scelta dell'esportatore, a restituire a quest'ultimo tutti i dati personali trasferiti e le relative copie ovvero a distruggere tali dati, certificando all'esportatore l'avvenuta distruzione, salvo che gli obblighi di legge impediscano di restituire o distruggere in tutto o in parte i dati personali trasferiti. (...)».

Decisione «scudo per la privacy»

42 Con sentenza del 6 ottobre 2015, Schrems (C-362/14, EU:C:2015:650), la Corte ha annullato 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 (GU 2000, L 215, pag. 7), nella quale la Commissione aveva constatato che tale paese terzo garantiva un livello di protezione adeguato.

43 In seguito alla pronuncia di tale sentenza, la Commissione ha adottato la decisione «scudo per la privacy», dopo aver proceduto, ai fini della sua adozione, ad una valutazione della normativa degli Stati Uniti, come precisato dal punto 65 di detta decisione:

«La Commissione ha valutato le limitazioni e le garanzie cui la normativa statunitense subordina la facoltà delle autorità pubbliche statunitensi di accedere e usare i dati personali trasferiti nell'ambito dello scudo [UE-USA per la privacy] per soddisfare esigenze di sicurezza nazionale, amministrazione della giustizia o altro scopo d'interesse pubblico. Il governo statunitense ha altresì comunicato alla Commissione, tramite l'Ufficio del direttore dell'intelligence nazionale ([Office of the Director of National Intelligence,] ODNI), le dichiarazioni e gli impegni particolareggiati riportati nell'allegato VI della presente decisione. Con lettera firmata dal segretario di Stato, acclusa alla presente decisione come allegato III, il governo degli Stati Uniti si è impegnato altresì a creare un nuovo meccanismo di vigilanza sulle ingerenze per motivi di sicurezza nazionale, indipendente dai servizi di intelligence: il Mediatore dello scudo. Infine, la dichiarazione del Dipartimento della Giustizia degli USA, riportata nell'allegato VII della presente decisione, espone le garanzie e limitazioni relative all'accesso delle autorità pubbliche ai dati per finalità di contrasto e di interesse pubblico. Ai fini della trasparenza e per rispecchiare la natura giuridica di questi impegni, ciascuno dei documenti elencati e allegati alla presente decisione è pubblicato nel Registro federale degli USA».

44 L'analisi effettuata dalla Commissione in merito a tali limiti e garanzie è riassunta ai punti da 67 a 135 della decisione «scudo per la privacy», mentre le conclusioni di tale istituzione relative al livello adeguato di protezione nell'ambito dello scudo Unione europea-Stati Uniti per la privacy figurano ai punti da 136 a 141 di quest'ultima.

45 In particolare, i punti 68, 69, 76, 77, 109, da 112 a 116, 120, 136 e 140 di detta decisione così recitano:

«(68) In virtù della Costituzione degli Stati Uniti, garantire la sicurezza nazionale rientra nei poteri del presidente in qualità di comandante supremo, di capo dell'esecutivo e, per quanto riguarda l'intelligence esterna, di responsabile della conduzione degli affari esteri degli Stati Uniti (…). Sebbene il Congresso abbia il potere d'imporre limitazioni a queste prerogative, e di fatto sia intervenuto in tal senso sotto vari aspetti, il presidente può indirizzare le attività della comunità dell'intelligence statunitense, in particolare mediante decreti o direttive presidenziali. (...) Attualmente i due strumenti giuridici centrali sono il decreto presidenziale 12333 ([Executive Order 12333; in prosieguo: l'"EO 12333"]) (…) e la direttiva presidenziale 28 ([Presidential Policy directive 28; in prosieguo: la "PPD-28"]).

(69) La PPD-28, emanata il 17 gennaio 2014, impone una serie di limitazioni alle operazioni di "intelligence dei segnali" (…). La direttiva presidenziale è vincolante per le autorità di intelligence statunitensi (…) e resta in vigore anche quando cambia l'amministrazione degli Stati Uniti (…). La PPD-28, che riveste particolare importanza per i cittadini stranieri, compresi gli interessati nell'Unione europea (...)

(...)

(76) Sebbene non formulati nei medesimi termini giuridici, nell'essenza [i principi della PPD-28] rispecchiano i principi di necessità e di proporzionalità. (...)

(77) In quanto stabiliti in una direttiva emanata dal presidente nella sua veste di capo dell'esecutivo, detti requisiti sono vincolanti per tutta la comunità dell'intelligence e ad essi è stata data successivamente attuazione con le norme e procedure adottate dai vari enti per tradurre i principi generali in istruzioni specifiche per l'operatività quotidiana. (...)

(...)

(109) Per converso, nell'ambito dell'articolo 702 della [Foreign Intelligence Surveillance Act (FISA)] [l'United States Foreign Intelligence Surveillance Court (FISC) (tribunale per la sorveglianza dell'intelligence esterna degli Stati Uniti); in prosieguo: la «Corte FISA»] non autorizza singole misure di sorveglianza, ma piuttosto programmi di sorveglianza (quali PRISM e UPSTREAM) basandosi sulle certificazioni annuali preparate dal[l'United States Attorney General (Procuratore generale)] e dal [Director of National Intelligence (DNI) (Direttore dell'intelligence nazionale)]. (...) Come indicato in precedenza, le certificazioni che la Corte FISA deve approvare non contengono informazioni sul singolo potenziale obiettivo, ma indicano piuttosto categorie di informazioni di intelligence esterna (…). La Corte FISA non valuta, in base a elementi plausibili né a altro criterio, se la persona costituisca un obiettivo adatto per acquisire informazioni di intelligence esterna (…); il suo controllo verte piuttosto sulla condizione che uno degli scopi rilevanti dell'acquisizione dev'essere quello di ottenere informazioni di intelligence esterna. (...)

(...)

(112) In primo luogo, la legge relativa alla vigilanza sull'intelligence esterna (FISA) prevede una serie di mezzi, a disposizione anche dei cittadini stranieri, per contestare la sorveglianza elettronica illecita (…) offrendo alla persona la possibilità di avviare una causa civile contro gli USA per ottenere un risarcimento pecuniario quando le informazioni che la riguardano sono state usate o divulgate illecitamente e con dolo (…), di adire le vie legali contro agenti del governo statunitense, nella loro capacità personale («abuso di potere») per ottenere un risarcimento pecuniario (…), e di contestare la legalità della sorveglianza (chiedendo anche di sopprimere le informazioni) quando il governo degli Stati Uniti intende usare o divulgare le informazioni raccolte o ricavate dalla sorveglianza elettronica contro la persona in un procedimento giudiziario o amministrativo negli Stati Uniti (…).

(113) In secondo luogo, il governo degli Stati Uniti ha rimandato la Commissione a una serie di ulteriori possibilità di cui l'interessato dell'Unione europea potrebbe valersi per adire le vie legali contro agenti del governo in caso di accesso o uso illecito dei dati personali da parte del governo, anche per asserite finalità di sicurezza nazionale (...).

(114) Infine, il governo statunitense ha indicato nella [Freedom of information Act (FOIA) legge sulla libertà dell'informazione] un mezzo con cui il cittadino straniero può chiedere l'accesso ai dati esistenti degli enti federali, anche quando contengono dati personali che lo riguardano (…). Data la materia trattata, la FOIA non offre una possibilità di ricorso individuale contro l'ingerenza nei dati personali in sé, ma potrebbe in linea di principio permettere alla persona di accedere alle informazioni al riguardo detenute dagli enti d'intelligence nazionali. (...).

(115) Pertanto, sebbene la persona, compreso l'interessato dell'UE, sottoposta a sorveglianza (elettronica) illecita per finalità di sicurezza nazionale disponga di una serie di possibilità di ricorso, altrettanto pacifico è che queste non contemplano almeno alcune delle basi giuridiche di cui possono avvalersi le autorità di intelligence statunitensi (ad esempio l'EO 12333). Inoltre, anche quando la possibilità di ricorso per via giudiziaria è effettivamente offerta, in linea di

principio, anche al cittadino straniero, come ad esempio in caso di sorveglianza ai sensi della FISA, i motivi per cui si possono adire le vie legali sono limitati (…) e l'istanza presentata da una persona (compresi i cittadini statunitensi o residenti negli USA) è dichiarata irricevibile se questa non è in grado di dimostrare la propria legittimazione ad agire (…), il che limita di fatto l'accesso al giudice ordinario (…).

(116) Per offrire a tutti gli interessati dell'UE un'ulteriore via di ricorso, il governo statunitense ha deciso di creare il nuovo meccanismo di mediazione illustrato nella lettera del segretario di Stato degli USA alla Commissione, riportata nell'allegato III della presente decisione. Benché si fondi sulla nomina in seno al Dipartimento di Stato, ai sensi della PPD-28, di un Primo coordinatore (a livello di Sottosegretario) a referente per i governi stranieri che si pongono interrogativi sulle attività di intelligence dei segnali condotte dagli Stati Uniti d'America, il meccanismo si spinge ben oltre quest'idea che ne è all'origine.

(...)

(120) [I]l governo degli Stati Uniti s'impegna a garantire che, nell'esercizio delle sue funzioni, il Mediatore dello scudo possa contare sulla collaborazione di altri meccanismi di vigilanza e di controllo della conformità previsti dalla legge statunitense. (...) Se uno degli organi di vigilanza riscontra un'inosservanza, il servizio della comunità dell'intelligence responsabile (ad esempio un ente di intelligence) deve porvi rimedio, perché solo così il Mediatore può dare alla persona la risposta "positiva" (ossia che l'inosservanza è stata sanata) cui il governo degli Stati Uniti si è impegnato. (...).

(...)

(136) Alla luce delle considerazioni che precedono, la Commissione ritiene che gli Stati Uniti d'America assicurino un livello di protezione adeguato dei dati personali trasferiti nell'ambito dello scudo [Unione europea-Stati Uniti] dall'Unione [europea] alle organizzazioni statunitensi che si sono autocertificate come aderenti al regime.

(...)

(140) In base alle informazioni sull'ordinamento giuridico statunitense disponibili, comprese le dichiarazioni e gli impegni del governo statunitense, la Commissione ritiene che l'ingerenza nei diritti fondamentali della persona i cui dati sono trasferiti dall'Unione verso gli Stati Uniti nell'ambito dello scudo, compiuta dall'autorità pubblica statunitense per esigenze di sicurezza nazionale, amministrazione della giustizia o altro scopo d'interesse pubblico, e le conseguenti limitazioni relative al rispetto dei principi imposte alle organizzazioni che si sono autocertificate come aderenti al regime, si limitino a quanto strettamente necessario per conseguire l'obiettivo legittimo ricercato e che contro le ingerenze di tale natura esiste una tutela giuridica efficace».

46 Ai sensi dell'articolo 1, la decisione «scudo per la privacy»:

«1. Ai fini dell'articolo 25, paragrafo 2, della [direttiva 95/46], gli Stati Uniti d'America assicurano un livello di protezione adeguato dei dati personali trasferiti nell'ambito dello scudo dall'Unione alle organizzazioni statunitensi.

2. Lo scudo [Unione europea-Stati Uniti] per la privacy («scudo») è costituito dai principi emanati dal Dipartimento del Commercio degli Stati Uniti il 7 luglio 2016, riportati nell'allegato II, e dalle dichiarazioni e impegni ufficiali riportati nei documenti di cui agli allegati I e da III a VII.

3. Ai fini del paragrafo 1, sono trasferiti nell'ambito dello scudo i dati personali trasferiti dall'Unione a organizzazioni presenti negli Stati Uniti che figurano nell'elenco degli aderenti allo scudo tenuto e pubblicato dal Dipartimento del Commercio degli Stati Uniti in conformità delle parti I e III dei principi enunciati nell'allegato II».

47 L'allegato II della decisione «scudo per la privacy», intitolato «Principi del regime dello scudo [Unione europea-Stati Uniti] per la privacy emananti dal Dipartimento del commercio degli Stati Uniti d'America», prevede al punto I.5 che l'adesione ai principi può essere limitata, in particolare, per «esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia».

48 L'allegato III di tale decisione, contiene una lettera, datata 7 luglio 2016, di John Kerry, all'epoca Secretary of State (Segretario di Stato, Stati Uniti), alla Commissaria per la Giustizia, i consumatori e la parità di genere alla quale è unito, quale allegato A, un memorandum, dal titolo «Meccanismo di mediazione dello scudo [Unione europea-Stati Uniti] per la privacy in materia di intelligence dei segnali», che contiene il seguente passaggio:

«In considerazione dell'importanza del regime dello scudo [Unione europea-Stati Uniti] per la privacy («scudo» o «regime»), il presente memorandum stabilisce l'iter di attuazione di un nuovo meccanismo sull'intelligence dei segnali in conformità alla direttiva presidenziale 28 (PPD-28).

(...) Contestualmente il presidente Obama ha annunciato l'emanazione di una nuova direttiva presidenziale, la PPD-28, per precisare che cosa gli USA fanno, e che cosa invece non fanno, nelle attività di sorveglianza all'estero.

L'articolo 4, lettera d), della PPD-28 incarica il segretario di Stato di nominare un Primo coordinatore della diplomazia internazionale per le tecnologie dell'informazione ("Primo coordinatore" o "Prima coordinatrice") che funga da referente per i governi stranieri che si pongono interrogativi sulle attività di intelligence dei segnali condotte dagli Stati Uniti d'America.

(...)

1) [Il Primo coordinatore] svolge la funzione di Mediatore e (...) opera in stretta collaborazione con i funzionari di altri ministeri e enti cui la legge e la politica degli Stati Uniti conferiscono competenze di trattamento delle domande. Il Mediatore è indipendente dalla comunità dell'intelligence statunitense e riferisce direttamente al segretario di Stato, il quale assicura che svolga la sua funzione con obiettività e senza indebite ingerenze che possano influire sulla risposta apportata.

(...)».

49 L'allegato VI della decisione «scudo per la privacy» contiene una lettera dell'Ufficio del direttore dell'intelligence nazionale (Office of the Director of National Intelligence) al Dipartimento del commercio degli Stati Uniti nonché all'amministrazione del commercio internazionale, in data 21 giugno 2016, nella quale si precisa che la PPD-28 consente di procedere ad una «raccolta in blocco (...) di un volume relativamente consistente di informazioni o dati nell'ambito dell'intelligence dei segnali in circostanze in cui la comunità dell'intelligence non può rendere mirata la raccolta ricorrendo a un identificatore associato a un obiettivo specifico».

Procedimento principale e questioni pregiudiziali

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

51 Chiunque risieda nel territorio dell'Unione e desideri utilizzare Facebook è tenuto a sottoscrivere, al momento della sua iscrizione, un contratto con Facebook Ireland, una controllata di Facebook Inc., quest'ultima stabilita 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.

52 Il 25 giugno 2013 il sig. Schrems ha presentato al Commissario una denuncia con la quale chiedeva, in sostanza, a quest'ultimo di vietare a Facebook Ireland di trasferire i suoi dati personali verso gli Stati Uniti, sostenendo che il diritto e le prassi vigenti in tale paese non offrivano una protezione sufficiente dei dati personali conservati nel territorio del medesimo paese contro le attività di sorveglianza ivi praticate dalle autorità pubbliche. Tale denuncia è stata respinta segnatamente sulla base del rilievo che la Commissione aveva constatato, nella sua decisione 2000/520, che gli Stati Uniti garantivano un livello adeguato di protezione.

53 La High Court (Alta Corte, Irlanda), dinanzi alla quale il sig. Schrems aveva presentato ricorso contro il rigetto della sua denuncia, ha sottoposto alla Corte una domanda di pronuncia pregiudiziale vertente sull'interpretazione e la validità della decisione 2000/520. Con sentenza del 6 ottobre 2015, Schrems (C-362/14, EU:C:2015:650), la Corte ha dichiarato non valida tale decisione.

54 In seguito alla suddetta sentenza il giudice del rinvio ha annullato il rigetto della denuncia del sig. Schrems e l'ha rinviata al Commissario. Nell'ambito dell'indagine aperta da quest'ultimo, Facebook Ireland ha spiegato che una gran parte dei dati personali era trasferita a Facebook Inc. sulla base delle clausole tipo di protezione dei dati contenute nell'allegato della decisione CPT. Tenuto conto di tali elementi il Commissario ha invitato il sig. Schrems a riformulare la sua denuncia.

55 Nella denuncia così riformulata, presentata il 1° dicembre 2015, il sig. Schrems ha fatto valere, in particolare, che il diritto statunitense impone a Facebook Inc. di mettere a disposizione delle autorità statunitensi, quali la National Security Agency (NSA) e le Federal Bureau of Investigation (FBI), i dati personali che le sono trasferiti. Egli ha sostenuto che, poiché tali dati sono utilizzati nell'ambito di diversi programmi di sorveglianza in modo incompatibile con gli articoli 7, 8, e 47 della Carta, la decisione CPT non può giustificare il trasferimento dei suddetti dati verso gli Stati Uniti. Il sig. Schrems ha pertanto chiesto al Commissario di vietare o di sospendere il trasferimento dei suoi dati personali verso Facebook Inc.

56 Il 24 maggio 2016 il Commissario ha pubblicato una «bozza di decisione» che riassumeva le conclusioni provvisorie della sua indagine. In tale bozza egli ha provvisoriamente considerato che i dati personali dei cittadini dell'Unione trasferiti verso gli Stati Uniti rischiano di essere consultati e trattati dalle autorità statunitensi in modo incompatibile con gli articoli 7 e 8 della Carta e che il diritto degli Stati Uniti non offre a tali cittadini mezzi di ricorso compatibili con l'articolo 47 della Carta. Il Commissario ha considerato che le clausole tipo di protezione dei dati contenute nell'allegato della decisione CPT non sono idonee a porre rimedio a tale carenza, in quanto esse conferiscono agli interessati unicamente diritti contrattuali nei confronti dell'esportatore e dell'importatore dei dati, senza tuttavia vincolare le autorità statunitensi.

57 Ritenendo che, in tali circostanze, la denuncia riformulata del sig. Schrems sollevasse la questione della validità della decisione CPT, il 31 maggio 2016 il Commissario ha adito la High Court (Alta Corte), fondandosi sulla giurisprudenza risultante dalla sentenza del 6 ottobre 2015, Schrems (C-362/14, EU:C:2015:650, punto 65), affinché la High Court si rivolgesse alla Corte su tale questione. Con decisione del 4 maggio 2018 la High Court (Alta Corte) ha sottoposto alla Corte il presente rinvio pregiudiziale.

58 La High Court (Alta Corte) ha allegato a tale rinvio pregiudiziale una sentenza pronunciata il 3 ottobre 2017 nella quale aveva registrato il risultato dell'esame delle prove dinanzi ad essa prodotte nell'ambito del procedimento nazionale, procedimento al quale aveva partecipato il governo statunitense.

59 In tale sentenza, alla quale si fa riferimento numerose volte nell'ambito della domanda di pronuncia pregiudiziale, il giudice del rinvio ha rilevato di avere, a priori, non solo il diritto ma anche l'obbligo di esaminare tutti i fatti e gli argomenti addotti dinanzi ad esso al fine di decidere, in base ad essi, se sia necessario o meno un rinvio pregiudiziale. In ogni caso tale giudice sarebbe tenuto a prendere in considerazione le eventuali modifiche del diritto verificatesi tra la presentazione del ricorso e l'udienza organizzata dinanzi ad esso. Il giudice del rinvio ha precisato che, nell'ambito del procedimento principale, la sua valutazione non è limitata ai motivi di invalidità dedotti dal Commissario, cosicché può anche rilevare d'ufficio altri motivi di invalidità e, in base ad essi, procedere ad un rinvio pregiudiziale.

60 Secondo le constatazioni che compaiono in tale sentenza, le attività di intelligence delle autorità statunitensi per quanto riguarda i dati personali trasferiti verso gli Stati Uniti si fondano, in particolare, sull'articolo 702 del FISA e sull'E.O. 12333.

61 Per quanto riguarda l'articolo 702 del FISA, il giudice del rinvio precisa, nella medesima sentenza, che, al fine di procurarsi «informazioni in materia di intelligence esterna», tale articolo consente al procuratore generale e al direttore dell'intelligence nazionale di autorizzare congiuntamente, previa approvazione della Corte FISA, la sorveglianza di cittadini stranieri che si trovano al di fuori del territorio degli Stati Uniti e serve, in particolare, quale fondamento dei programmi di sorveglianza PRISM e UPSTREAM. Nell'ambito del programma PRISM, i fornitori di servizi Internet sono tenuti, secondo le constatazioni di tale giudice, a fornire alla NSA tutte le comunicazioni inviate e ricevute da un «selettore», e parte di esse è trasmessa anche allo FBI e alla Central Intelligence Agency (CIA) (agenzia centrale per l'intelligence).

62 Per quanto riguarda il programma UPSTREAM, detto giudice ha constatato che, nell'ambito di tale programma, le imprese di telecomunicazioni che gestiscono la «dorsale» di Internet – vale a dire la rete di cavi, commutatori e router – sono costrette a consentire alla NSA di copiare e filtrare i flussi di traffico Internet al fine di raccogliere comunicazioni inviate da, dirette a o riguardanti il cittadino straniero interessato da un «selettore». Nell'ambito di tale programma, la NSA, secondo le constatazioni del medesimo giudice, ha accesso tanto ai metadati quanto al contenuto delle comunicazioni interessate.

63 Per quanto riguarda l'E.O. 12333, il giudice del rinvio constata che esso consente alla NSA di accedere a dati «in transito» verso gli Stati Uniti, accedendo ai cavi sottomarini posti sul fondale dell'Atlantico, nonché di raccogliere e conservare tali dati prima che essi giungano negli Stati Uniti e siano ivi soggetti alle disposizioni del FISA. Esso precisa che le attività fondate sull'E.O. 12333 non sono disciplinate dalla legge.

64 Relativamente ai limiti posti alle attività di intelligence, il giudice del rinvio sottolinea che i cittadini stranieri rientrano unicamente nell'ambito della PPD-28 e che quest'ultima si limita ad indicare che le attività di intelligence dovrebbero essere «il più possibile mirate possibile» (as tailored as feasible). In base a tali constatazioni, detto giudice considera che gli Stati Uniti procedono a massicci trattamenti dei dati, senza garantire una protezione sostanzialmente equivalente a quella garantita dagli articoli 7 e 8 della Carta.

65 Riguardo alla tutela giurisdizionale, detto giudice osserva che i cittadini dell'Unione non hanno accesso agli stessi mezzi di ricorso di cui dispongono i cittadini statunitensi contro i trattamenti di dati personali da parte delle autorità degli Stati Uniti, poiché il quarto emendamento della Constitution of the United States (Costituzione degli Stati Uniti), che, nel diritto statunitense, costituisce la tutela più importante contro la sorveglianza illegale, è inapplicabile ai cittadini dell'Unione. A tal riguardo, il giudice del rinvio precisa che i mezzi di ricorso che restano a disposizione di questi ultimi incontrano notevoli ostacoli, in particolare l'obbligo – a suo avviso eccessivamente difficile da soddisfare – di dimostrare la loro legittimazione ad agire. Inoltre secondo quanto constatato da tale giudice, le attività della NSA basate sull'EO 12333 non sono soggette a controllo giurisdizionale e non possono essere

oggetto di ricorsi giurisdizionali. Infine, detto giudice ritiene che, poiché, a suo avviso, il Mediatore dello scudo per la privacy non è un organo giurisdizionale ai sensi dell'articolo 47 della Carta, il diritto statunitense non garantisca ai cittadini dell'Unione un livello di protezione sostanzialmente equivalente a quello garantito dal diritto fondamentale sancito da tale articolo.

66 Nella sua domanda di pronuncia pregiudiziale, il giudice del rinvio precisa altresì che le parti del procedimento principale hanno posizioni divergenti, in particolare, quanto alla questione dell'applicabilità del diritto dell'Unione a trasferimenti, verso un paese terzo, di dati personali che possono essere trattati dalle autorità di tale paese segnatamente a fini di sicurezza nazionale, nonché quanto agli elementi da prendere in considerazione ai fini della valutazione del livello di protezione adeguato garantito da detto paese. In particolare, tale giudice rileva che, secondo Facebook Ireland, le constatazioni della Commissione riguardanti l'adeguatezza del livello di protezione garantito da un paese terzo, come quelle contenute nella decisione «scudo per la privacy», vincolano le autorità di controllo anche nel contesto di un trasferimento di dati personali fondato sulle clausole tipo di protezione dei dati contenute nell'allegato della decisione CPT.

67 Per quanto riguarda tali clausole tipo di protezione dei dati, detto giudice si chiede se la decisione CPT possa essere considerata valida, sebbene, secondo lo stesso giudice, dette clausole non abbiano carattere vincolante nei confronti delle autorità statali del paese terzo interessato e, pertanto, non siano idonee a porre rimedio ad un'eventuale assenza di un livello adeguato di protezione in tale paese. A tal proposito, detto giudice ritiene che la possibilità, riconosciuta alle autorità competenti degli Stati membri dall'articolo 4, paragrafo 1, lettera a), della decisione 2010/87, nella sua versione anteriore all'entrata in vigore della decisione di esecuzione 2016/2297, di vietare i trasferimenti di dati personali verso un paese terzo che imponga all'importatore obblighi incompatibili con le garanzie contenute nelle medesime clausole, dimostri che lo stato del diritto del paese terzo può giustificare il divieto di un trasferimento di dati, pur se effettuato sulla base delle clausole tipo di protezione dei dati contenute nell'allegato della decisione CPT, e sottolinea pertanto che queste ultime possono essere insufficienti a garantire una protezione adeguata. Ciò premesso, il giudice del rinvio si interroga sulla portata del potere del Commissario di vietare un trasferimento di dati fondato su tali clausole, pur ritenendo che un potere discrezionale non possa essere sufficiente per garantire un'adeguata tutela.

68 In tale contesto, la High Court (Alta Corte) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se, nel caso in cui dati personali sono trasferiti da una società privata di uno Stato membro dell'[Unione] a una società privata in un paese terzo per scopi commerciali ai sensi della [decisione CPT] e possono essere ulteriormente trattati nel paese terzo dalle sue autorità ai fini della sicurezza nazionale ma anche ai fini dell'applicazione della legge e della gestione della politica estera del paese terzo, il diritto dell'Unione, compresa la Carta, sia applicabile al trasferimento dei dati, nonostante le disposizioni di cui all'articolo 4, paragrafo 2, TUE relative alla sicurezza nazionale e le disposizioni di cui al primo trattino dell'articolo 3, paragrafo 2, della [direttiva 95/46] relative alla pubblica sicurezza, alla difesa e alla sicurezza dello Stato.

2) a) Se, per determinare se vi sia una violazione dei diritti di un individuo a causa del trasferimento di dati, ai sensi della decisione [CPT], dall'Unione verso un paese terzo nel quale possono essere ulteriormente trattati per finalità di sicurezza nazionale, l'elemento di paragone rilevante ai fini dell'applicazione della direttiva [95/46] sia:
   i) la Carta, il TUE, il TFUE, la direttiva [95/46], la [Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950] (o qualsiasi altra disposizione del diritto dell'Unione); oppure
   ii) le leggi nazionali di uno o più Stati Membri.
   b) Qualora l'elemento di paragone rilevante sia quello sub ii), se siano da includere nel raffronto anche le prassi in materia di sicurezza nazionale in uno o più Stati membri.

3) Se, nel valutare se un paese terzo garantisca il livello di protezione richiesto dal diritto dell'Unione ai dati personali trasferiti in tale paese ai fini dell'articolo 26 della direttiva [95/46], il livello di protezione nel paese terzo debba essere valutato con riferimento:
   a) alle norme vigenti nel paese terzo derivanti dalla sua legislazione nazionale o dagli impegni internazionali e la prassi intesa ad assicurare il rispetto di tali norme, comprese le norme professionali e le misure di sicurezza osservate nel paese terzo;

      oppure
   b) alle norme di cui alla lettera a) congiuntamente alle prassi amministrative, regolamentari e di conformità e alle misure di salvaguardia, alle procedure, ai protocolli, ai meccanismi di controllo e ai mezzi di ricorso extragiudiziali che sono in vigore nel paese terzo.

4) Se, tenuto conto dei fatti accertati dalla High Court (Alta Corte) in relazione al diritto degli Stati Uniti, il trasferimento dei dati personali dall'Unione verso gli Stati Uniti ai sensi della decisione [CPT] violi i diritti degli individui garantiti dagli articoli 7 e/o 8 della Carta.

5) Se, tenuto conto dei fatti accertati dalla High Court (Alta Corte) in relazione al diritto degli Stati Uniti, in caso di trasferimento dei dati personali dall'[Unione] verso gli Stati Uniti ai sensi della decisione [CPT]:
   a) il livello di protezione garantito dagli Stati Uniti rispetti il contenuto essenziale del diritto di un individuo a un ricorso giurisdizionale in caso di violazione dei suoi diritti in materia di tutela dei dati personali garantiti dall'articolo 47 della Carta.

      In caso di risposta affermativa alla quinta questione, lettera a):
   b) se le restrizioni imposte dalla legge statunitense al diritto di un individuo a un ricorso giurisdizionale nell'ambito della sicurezza nazionale degli Stati Uniti siano proporzionate ai sensi dell'articolo 52 della Carta e non vadano al di là di quanto necessario in una società democratica ai fini della sicurezza nazionale.

6) a) Alla luce delle disposizioni [della direttiva 95/46], e in particolare degli articoli 25 e 26, letti alla luce della Carta, quale sia il livello di protezione richiesto che deve essere garantito ai dati personali trasferiti verso un paese terzo a norma delle clausole contrattuali tipo adottate conformemente a una decisione della Commissione a norma dell'articolo 26, paragrafo 4, della direttiva [95/46].
   b) Quali siano i fattori da prendere in considerazione per valutare se il livello di protezione garantito ai dati trasferiti verso un paese terzo ai sensi della decisione [CPT] soddisfi i requisiti della direttiva [95/46] e della Carta.

7) Se il fatto che le clausole contrattuali tipo si applicano tra l'esportatore e l'importatore dei dati e non vincolano le autorità nazionali di un paese terzo, le quali possono esigere che l'importatore dei dati metta a disposizione dei loro servizi di sicurezza, per ulteriore trattamento, i dati personali trasferiti ai sensi delle clausole di cui alla decisione [CPT], escluda che le suddette clausole offrano garanzie sufficienti, come richiesto dall'articolo 26, paragrafo 2, della direttiva [95/46].

8) Se, qualora un importatore di dati di un paese terzo sia soggetto a norme di sorveglianza che, secondo un'autorità garante della protezione dei dati, sono in contrasto con le clausole tipo di protezione o con gli articoli 25 e 26 della direttiva [95/46] e/o con la Carta, un'autorità garante della protezione dei dati sia tenuta a utilizzare i propri poteri esecutivi ai sensi dell'articolo 28, paragrafo 3, della direttiva [95/46] al fine di sospendere i flussi di dati, o se l'esercizio di tali poteri sia limitato solo ai casi eccezionali, alla luce del considerando 11 della decisione [CPT], oppure se un'autorità garante della protezione dei dati possa utilizzare il suo potere discrezionale per non sospendere i flussi di dati.

9) a) Se, ai fini dell'articolo 25, paragrafo 6, della direttiva [95/46], la decisione ["scudo per la privacy"] costituisca una constatazione di applicazione generale che vincola le autorità garanti della protezione dei dati e i giudici degli Stati membri, in base alla quale gli Stati Uniti assicurano un livello di protezione adeguato ai sensi dell'articolo 25, paragrafo 2, della direttiva [95/46], a motivo della loro legislazione nazionale o degli impegni internazionali che hanno assunto.

b) In caso contrario, quale eventuale rilevanza abbia la decisione ["scudo per la privacy"] nella valutazione sull'adeguatezza delle garanzie offerte ai dati trasferiti verso gli Stati Uniti ai sensi della decisione [CPT].

10) Se, considerate le conclusioni della High Court (Alta Corte) in relazione al diritto degli Stati Uniti, l'aver istituito il Mediatore dello "scudo per la privacy", ai sensi dell'allegato A dell'allegato III della decisione ["scudo per la privacy"], congiuntamente al regime in vigore negli Stati Uniti, garantisca che gli Stati Uniti offrano un mezzo di ricorso in favore degli interessati i cui dati personali sono trasferiti negli Stati Uniti ai sensi della decisione [CPT] che sia compatibile con l'articolo 47 della Carta.

11) Se la decisione [CPT] violi gli articoli 7, 8 e/o 47 della Carta».

Sulla ricevibilità della domanda di pronuncia pregiudiziale

69 Facebook Ireland nonché i governi tedesco e del Regno Unito sostengono che la domanda di pronuncia pregiudiziale è irricevibile.

70 Per quanto riguarda l'eccezione sollevata da Facebook Ireland, tale società osserva che le disposizioni della direttiva 95/46 sulle quali si fondano le questioni pregiudiziali sono state abrogate dal RGPD.

71 A tal riguardo, pur se è vero che, in forza dell'articolo 94, paragrafo 1, del RGPD, la direttiva 95/46 è stata abrogata con effetto dal 25 maggio 2018, essa era ancora in vigore al momento della formulazione, il 4 maggio 2018, della presente domanda di pronuncia pregiudiziale pervenuta alla Corte il 9 maggio 2018. Inoltre, l'articolo 3, paragrafo 2, primo trattino, gli articoli 25 e 26 nonché l'articolo 28, paragrafo 3, della direttiva 95/46, ai quali fanno riferimento le questioni pregiudiziali, sono stati sostanzialmente ripresi, rispettivamente, all'articolo 2, paragrafo 2, nonché agli articoli 45, 46 e 58 del RGPD. Occorre, inoltre, ricordare che la Corte ha il compito di interpretare tutte le disposizioni del diritto dell'Unione che possano essere necessarie ai giudici nazionali al fine di dirimere le controversie per le quali sono stati aditi, anche qualora tali disposizioni non siano espressamente indicate nelle questioni ad essa sottoposte da detti giudici (sentenza del 2 aprile 2020, Ruska Federacija, C-897/19 PPU, EU:C:2020:262, punto 43 e giurisprudenza ivi citata). Per questi diversi motivi, la circostanza che il giudice del rinvio abbia formulato le questioni pregiudiziali facendo riferimento unicamente alle disposizioni della direttiva 95/46 non può comportare l'irricevibilità della presente domanda di pronuncia pregiudiziale.

72 Dal canto suo, il governo tedesco fonda la sua eccezione di irricevibilità sulla circostanza, da un lato, che il Commissario ha espresso solo dubbi, e non un'opinione definitiva, quanto alla questione della validità della decisione CPT e, dall'altro, che il giudice del rinvio si è astenuto dal verificare se il sig. Schrems avesse prestato inequivocabilmente il suo consenso ai trasferimenti di dati di cui trattasi nel procedimento principale, circostanza che, ove così fosse, avrebbe l'effetto di rendere inutile una risposta a tale questione. Infine, secondo il governo del Regno Unito, le questioni pregiudiziali hanno carattere ipotetico, dal momento che tale giudice non ha constatato che i suddetti dati erano stati effettivamente trasferiti in base a detta decisione.

73 Da costante giurisprudenza della Corte risulta che spetta esclusivamente al giudice nazionale, cui è stata sottoposta la controversia e che deve assumersi la responsabilità dell'emananda decisione giurisdizionale, valutare, alla luce delle particolari circostanze di ciascuna causa, tanto la necessità di una pronuncia pregiudiziale per essere in grado di pronunciare la propria sentenza, quanto la rilevanza delle questioni che sottopone alla Corte. Di conseguenza, se le questioni sollevate vertono sull'interpretazione o sulla validità di una norma giuridica dell'Unione, la Corte, in linea di principio, è tenuta a statuire. Ne consegue che le questioni vertenti sul diritto dell'Unione godono di una presunzione di rilevanza. Il rifiuto della Corte di pronunciarsi su una questione pregiudiziale sollevata da un giudice nazionale è possibile solo qualora risulti che l'interpretazione richiesta non ha alcuna relazione con la realtà o con l'oggetto del procedimento principale, qualora il problema sia di natura ipotetica oppure quando la Corte non disponga degli elementi di fatto o di diritto necessari per fornire una soluzione utile a tali questioni (sentenze del 16 giugno 2015, Gauweiler e a., C-62/14, EU:C:2015:400, punti 24 e 25; del 2 ottobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, punto 45, nonché del 19 dicembre 2019, Dobersberger, C-16/18, EU:C:2019:1110, punti 18 e 19).

74 Nella fattispecie, la decisione di rinvio contiene elementi di fatto e di diritto sufficienti a comprendere la portata delle questioni pregiudiziali. Inoltre, e soprattutto, nessun elemento del fascicolo di cui dispone la Corte consente di ritenere che l'interpretazione del diritto dell'Unione richiesta non abbia alcun rapporto con la realtà effettiva o con l'oggetto della controversia di cui al procedimento principale o sia di natura ipotetica, in particolare per il fatto che il trasferimento di dati personali di cui trattasi nel procedimento principale sarebbe fondato sul consenso esplicito dell'interessato a tale trasferimento, e non sulla decisione CPT. Infatti, secondo le indicazioni contenute in tale domanda, Facebook Ireland ha riconosciuto che trasferisce a Facebook Inc. i dati personali dei suoi abbonati residenti nell'Unione e che gran parte di tali trasferimenti, di cui il sig. Schrems contesta la liceità, avviene sulla base delle clausole tipo di protezione dei dati contenute nell'allegato della decisione CPT.

75 Peraltro, ai fini della ricevibilità della presente domanda di pronuncia pregiudiziale è irrilevante il fatto che il Commissario non abbia espresso un'opinione definitiva sulla validità di tale decisione, poiché il giudice del rinvio ritiene che per la soluzione della controversia principale sia necessaria la risposta alle questioni pregiudiziali vertenti sull'interpretazione e sulla validità di norme del diritto dell'Unione.

76 Ne consegue che la domanda di pronuncia pregiudiziale è ricevibile.

Sulle questioni pregiudiziali

77 Occorre preliminarmente ricordare che la presente domanda di pronuncia pregiudiziale trae origine da una denuncia del sig. Schrems diretta a far sì che il Commissario disponga la sospensione o il divieto, in futuro, del trasferimento dei suoi dati personali da parte di Facebook Ireland a Facebook Inc. Orbene, sebbene le questioni pregiudiziali facciano riferimento alle disposizioni della direttiva 95/46, è pacifico che il Commissario non aveva ancora adottato una decisione definitiva su tale denuncia allorché tale direttiva è stata abrogata e sostituita dal RGPD, con effetto dal 25 maggio 2018.

78 Tale mancanza di una decisione nazionale distingue la situazione oggetto del procedimento principale da quelle che hanno dato luogo alle sentenze del 24 settembre 2019, Google (Portata territoriale della deindicizzazione) (C-507/17, EU:C:2019:772), e del 1º ottobre 2019, Planet49 (C-673/17, EU:C:2019:801), nelle quali erano in discussione decisioni adottate prima dell'abrogazione di detta direttiva.

79 Occorre, pertanto, rispondere alle questioni pregiudiziali alla luce delle disposizioni del RGPD, e non di quelle della direttiva 95/46.

Sulla prima questione

80 Con la sua prima questione, il giudice del rinvio chiede, in sostanza, se l'articolo 2, paragrafo 1, e l'articolo 2, paragrafo 2, lettere a), b) e d), del RGPD, in combinato disposto con l'articolo 4, paragrafo 2, TUE, debbano essere interpretati nel senso che rientra nell'ambito di applicazione di tale regolamento un trasferimento di dati personali effettuato da un operatore economico stabilito in uno Stato membro verso un altro operatore economico stabilito in un paese terzo, qualora, durante o in seguito a tale trasferimento, detti dati possano essere trattati dalle autorità del suddetto paese terzo a fini di sicurezza pubblica, di difesa e di sicurezza dello Stato.

81 A tal riguardo, occorre anzitutto rilevare che la disposizione contenuta nell'articolo 4, paragrafo 2, TUE, secondo la quale all'interno dell'Unione la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro, riguarda esclusivamente gli Stati membri dell'Unione. Di conseguenza, tale disposizione non è pertinente, nel caso di specie, ai fini dell'interpretazione dell'articolo 2, paragrafo 1, e dell'articolo 2, paragrafo 2, lettere a), b) e d), del RGPD.

82 Ai sensi dell'articolo 2, paragrafo 1, il RGPD si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi. L'articolo 4, punto 2, di tale regolamento definisce la nozione di «trattamento» come «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali» e menziona, a titolo esemplificativo, «la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione», senza distinguere a seconda che tali operazioni siano realizzate all'interno dell'Unione o presentino un nesso con un paese terzo. Inoltre, detto regolamento assoggetta i trasferimenti di dati personali verso paesi terzi a norme specifiche contenute nel suo capo V, intitolato «Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali», e a tal fine, peraltro, conferisce alle autorità di controllo poteri specifici, di cui all'articolo 58, paragrafo 2, lettera j), del medesimo regolamento.

83 Ne consegue che l'operazione consistente nel far trasferire dati personali da uno Stato membro verso un paese terzo costituisce, in quanto tale, un trattamento di dati personali, ai sensi dell'articolo 4, punto 2, del RGPD, effettuato nel territorio di uno Stato membro, trattamento al quale il suddetto regolamento si applica in forza del suo articolo 2, paragrafo 1 [v., per analogia, per quanto riguarda l'articolo 2, lettera b), e l'articolo 3, paragrafo 1, della direttiva 95/46, sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 45 e giurisprudenza ivi citata].

84 Per quanto riguarda la questione se una operazione siffatta possa essere considerata esclusa dall'ambito di applicazione del RGPD in forza dell'articolo 2, paragrafo 2, di quest'ultimo, occorre ricordare che tale disposizione prevede eccezioni all'ambito di applicazione di tale regolamento, quale definito al suo articolo 2, paragrafo 1, e che tali eccezioni devono essere interpretate restrittivamente (v., per analogia, per quanto riguarda l'articolo 3, paragrafo 2, della direttiva 95/46, sentenza del 10 luglio 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, punto 37 e giurisprudenza ivi citata).

85 Nel caso di specie, poiché il trasferimento di dati personali di cui trattasi nel procedimento principale è effettuato da Facebook Ireland verso Facebook Inc., ossia tra due persone giuridiche, tale trasferimento non rientra nell'ambito di applicazione dell'articolo 2, paragrafo 2, lettera c), del RGPD, che riguarda il trattamento di dati effettuato da una persona fisica nell'ambito di un'attività strettamente personale o domestica. Tale trasferimento non rientra neppure nelle eccezioni che compaiono all'articolo 2, paragrafo 2, lettere a), b) e d), di detto regolamento, poiché le attività ivi menzionate a titolo esemplificativo sono, in tutti i casi, attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei privati (v., per analogia, per quanto riguarda l'articolo 3, paragrafo 2, della direttiva 95/46, sentenza del 10 luglio 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, punto 38 e giurisprudenza ivi citata).

86 Orbene, la possibilità che i dati personali trasferiti tra due operatori economici a fini commerciali subiscano, durante o in seguito al trasferimento, un trattamento a fini di pubblica sicurezza, di difesa e di sicurezza dello Stato da parte delle autorità del paese terzo interessato non può escludere detto trasferimento dall'ambito di applicazione del RGPD.

87 Peraltro, imponendo esplicitamente alla Commissione, allorché quest'ultima valuta l'adeguatezza del livello di protezione offerto da un paese terzo, l'obbligo di prendere in considerazione, segnatamente, «la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione», la formulazione stessa dell'articolo 45, paragrafo 2, lettera a), di tale regolamento mette in evidenza il fatto che l'eventuale trattamento, da parte di un paese terzo, dei dati di cui trattasi a fini di sicurezza pubblica, di difesa e di sicurezza dello Stato non rimette in discussione l'applicabilità del suddetto regolamento al trasferimento di cui trattasi.

88 Ne consegue che un trasferimento siffatto non può esulare dall'ambito di applicazione del RGPD per il motivo che i dati in questione possono essere trattati, durante o in seguito a tale trasferimento, dalle autorità del paese terzo interessato a fini di pubblica sicurezza, di difesa e di sicurezza dello Stato.

89 Occorre, pertanto, rispondere alla prima questione dichiarando che l'articolo 2, paragrafi 1 e 2, del RGPD deve essere interpretato nel senso che rientra nell'ambito di applicazione di tale regolamento un trasferimento di dati personali effettuato a fini commerciali da un operatore economico stabilito in uno Stato membro verso un altro operatore economico stabilito in un paese terzo, nonostante il fatto che, durante o in seguito a tale trasferimento, i suddetti dati possano essere sottoposti a trattamento da parte delle autorità del paese terzo considerato a fini di sicurezza pubblica, di difesa e sicurezza dello Stato.

Sulle questioni seconda, terza e sesta

90 Con le questioni seconda, terza e sesta, il giudice del rinvio interroga, in sostanza, la Corte sul livello di protezione richiesto dall'articolo 46, paragrafo 1, e dall'articolo 46, paragrafo 2, lettera c), del RGPD nell'ambito di un trasferimento di dati personali verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati. In particolare, tale giudice chiede alla Corte di precisare gli elementi da prendere in considerazione al fine di determinare se tale livello di protezione sia garantito nel contesto di un trasferimento siffatto.

91 Per quanto riguarda il livello di protezione richiesto, dal combinato disposto di tali disposizioni risulta che, in assenza di una decisione di adeguatezza adottata ai sensi dell'articolo 45, paragrafo 3, di tale regolamento, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo solo se ha previsto «garanzie adeguate» e a condizione che gli interessati dispongano di «diritti azionabili e mezzi di ricorso effettivi», potendo tali garanzie adeguate essere fornite, segnatamente, mediante clausole tipo di protezione dei dati adottate dalla Commissione.

92 Sebbene l'articolo 46 del RGPD non precisi la natura dei requisiti che derivano da tale riferimento a «garanzie adeguate», «diritti azionabili» e «mezzi di ricorso effettivi», occorre rilevare che tale articolo è contenuto nel capo V del suddetto regolamento e deve essere pertanto letto alla luce dell'articolo 44 di detto regolamento, rubricato «Principio generale per il trasferimento», il quale dispone che «[t]utte le disposizioni [di detto capo] sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal [medesimo] regolamento non sia pregiudicato». Tale livello di protezione deve, di conseguenza, essere garantito indipendentemente da quale sia la disposizione di detto capo sul cui fondamento viene effettuato un trasferimento di dati personali verso un paese terzo.

93 Come rilevato, infatti, dall'avvocato generale al paragrafo 117 delle sue conclusioni, le disposizioni del capo V del RGPD mirano a garantire la continuità del livello elevato di tale protezione in caso di trasferimento di dati personali verso un paese terzo, conformemente all'obiettivo precisato al considerando 6 di tale regolamento.

94 L'articolo 45, paragrafo 1, prima frase, del RGPD prevede che un trasferimento di dati personali verso un paese terzo può essere autorizzato mediante una decisione adottata dalla Commissione secondo la quale tale paese terzo, un territorio o uno o più settori specifici all'interno dello stesso garantiscono un livello di protezione adeguato. A tal riguardo, senza esigere che il paese terzo considerato garantisca un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione, l'espressione «livello di protezione adeguato» deve essere intesa, come confermato dal considerando 104 dello stesso regolamento, 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 di tale regolamento, letto alla luce della Carta. In assenza di un requisito siffatto, sarebbe, infatti, disatteso l'obiettivo menzionato al punto precedente (v., per analogia, per quanto riguarda l'articolo 25, paragrafo 6, della direttiva 95/46, sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 73).

95 In tale contesto, il considerando 107 del RGPD enuncia che, allorché «un paese terzo, un territorio o un settore specifico all'interno di un paese terzo (...) non garantiscono più un livello adeguato di protezione dei dati (...)[,] il trasferimento di dati personali verso tale paese terzo (...) dovrebbe essere vietato, a meno che non siano soddisfatti i requisiti di cui [a tale regolamento] relativamente ai trasferimenti sottoposti a garanzie adeguate». A tal fine, il considerando 108 di detto regolamento precisa che, in mancanza di una decisione di adeguatezza, le adeguate garanzie che il titolare del trattamento o il responsabile del trattamento deve adottare conformemente all'articolo 46, paragrafo 1, del medesimo regolamento devono «compensare la carenza di protezione dei dati in un paese terzo» per «assicurare un rispetto dei requisiti in materia di protezione dei dati e dei diritti degli interessati adeguato ai trattamenti all'interno dell'Unione».

96 Ne consegue, come rilevato dall'avvocato generale al paragrafo 115 delle sue conclusioni, che tali garanzie adeguate devono essere idonee a garantire che le persone i cui dati personali sono trasferiti verso un paese terzo sulla base di clausole tipo di protezione dei dati godano, come nell'ambito di un trasferimento fondato su una decisione di adeguatezza, di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione.

97 Il giudice del rinvio chiede altresì se tale livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione debba essere determinato alla luce del diritto dell'Unione, in particolare dei diritti garantiti dalla Carta, e/o alla luce dei diritti fondamentali sanciti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (in prosieguo: la «CEDU») oppure alla luce del diritto nazionale degli Stati membri.

98 A tal proposito, occorre ricordare che pur se, come confermato dall'articolo 6, paragrafo 3, TUE, i diritti fondamentali riconosciuti dalla CEDU fanno parte del diritto dell'Unione in quanto principi generali e pur se l'articolo 52, paragrafo 3, della Carta impone di dare ai diritti in essa contemplati e corrispondenti a quelli garantiti dalla CEDU lo stesso significato e la stessa portata di quelli conferiti dalla suddetta Convenzione, quest'ultima non costituisce, finché l'Unione non vi abbia aderito, un atto giuridico formalmente integrato nell'ordinamento giuridico dell'Unione (v. sentenze del 26 febbraio 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, punto 44 e giurisprudenza ivi citata, nonché del 20 marzo 2018, Menci, C-524/15, EU:C:2018:197, punto 22).

99 La Corte ha pertanto dichiarato che l'interpretazione del diritto dell'Unione e l'esame della validità degli atti dell'Unione devono essere effettuati alla luce di diritti fondamentali garantiti dalla Carta (v., per analogia, sentenza del 20 marzo 2018, Menci, C-524/15, EU:C:2018:197, punto 24).

100 Secondo costante giurisprudenza, inoltre, la validità delle disposizioni del diritto dell'Unione e, in mancanza di un espresso richiamo al diritto nazionale degli Stati membri, la loro interpretazione non possono essere valutate alla luce di tale diritto nazionale, neppure di rango costituzionale, in particolare dei diritti fondamentali quali formulati nella loro Costituzione nazionale (v., in tal senso, sentenze del 17 dicembre 1970, Internationale Handelsgesellschaft, 11/70, EU:C:1970:114, punto 3; del 13 dicembre 1979, Hauer, 44/79, EU:C:1979:290, punto 14, nonché del 18 ottobre 2016, Nikiforidis, C-135/15, EU:C:2016:774, punto 28 e giurisprudenza ivi citata).

101 Ne consegue che, nei limiti in cui, da un lato, un trasferimento di dati personali, come quello oggetto del procedimento principale, effettuato a fini commerciali da un operatore economico stabilito in uno Stato membro, verso un altro operatore economico stabilito in un paese terzo, rientra – come risulta dalla risposta alla prima questione – nell'ambito di applicazione del RGPD e nei limiti in cui, d'altro lato, tale regolamento mira in particolare – come emerge dal suo considerando 10 – ad assicurare un livello coerente ed elevato di protezione delle persone fisiche all'interno dell'Unione e, a tal fine, ad assicurare un'applicazione coerente e omogenea delle norme a protezione delle libertà e dei diritti fondamentali di tali persone con riguardo al trattamento dei dati personali in tutta l'Unione, il livello di protezione dei diritti fondamentali richiesto all'articolo 46, paragrafo 1, di tale regolamento deve essere determinato in base alle disposizioni dello stesso regolamento, lette alla luce dei diritti fondamentali garantiti dalla Carta.

102 Il giudice del rinvio chiede inoltre quali elementi debbano essere presi in considerazione al fine di determinare l'adeguatezza del livello di protezione nel contesto di un trasferimento di dati personali verso un paese terzo sul fondamento di clausole tipo di protezione dei dati adottate ai sensi dell'articolo 46, paragrafo 2, lettera c), del RGPD.

103 A tal proposito, sebbene tale disposizione non enumeri i diversi elementi di cui occorre tener conto al fine di valutare l'adeguatezza del livello di protezione che va rispettato nell'ambito di un trasferimento siffatto, l'articolo 46, paragrafo 1, di detto regolamento precisa che gli interessati devono godere di garanzie adeguate e disporre di diritti azionabili e mezzi di ricorso effettivi.

104 La valutazione richiesta, a tal fine, nel contesto di un trasferimento siffatto deve, in particolare, prendere in considerazione tanto le clausole contrattuali convenute tra il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione e il destinatario del trasferimento stabilito nel paese terzo considerato quanto, per quel che riguarda un eventuale accesso delle autorità pubbliche di tale paese terzo ai dati personali trasferiti, gli elementi rilevanti del sistema giuridico di quest'ultimo. Relativamente a quest'ultimo aspetto, gli elementi che occorre prendere in considerazione nel contesto dell'articolo 46 di tale regolamento corrispondono a quelli enunciati, in modo non esaustivo, all'articolo 45, paragrafo 2, di detto regolamento.

105 Occorre pertanto rispondere alle questioni seconda, terza e sesta dichiarando che l'articolo 46, paragrafo 1, e l'articolo 46, paragrafo 2, lettera c), del RGPD devono essere interpretati nel senso che le garanzie adeguate, i diritti azionabili e i mezzi di ricorso effettivi richiesti da tali disposizioni devono garantire che i diritti delle persone i cui dati personali sono trasferiti verso un paese terzo sul fondamento di clausole tipo di protezione dei dati godano di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione da tale regolamento, letto alla luce della Carta. A tal fine, la valutazione del livello di protezione garantito nel contesto di un trasferimento siffatto deve, in particolare, prendere in considerazione tanto le clausole contrattuali convenute tra il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione e il destinatario del trasferimento stabilito nel paese terzo interessato quanto, per quel che riguarda un eventuale accesso delle autorità pubbliche di tale paese terzo ai dati personali così trasferiti, gli elementi rilevanti del sistema giuridico di quest'ultimo, in particolare quelli enunciati all'articolo 45, paragrafo 2, di detto regolamento.

Sull'ottava questione

106 Con l'ottava questione il giudice del rinvio chiede, in sostanza, se l'articolo 58, paragrafo 2, lettere f) e j), del RGPD debba essere interpretato nel senso che l'autorità di controllo competente è tenuta a sospendere o a vietare un trasferimento di dati personali verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati adottate dalla Commissione, allorché la suddetta autorità di controllo ritenga che tali clausole non sono o non possono essere rispettate in detto paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione, in particolare dagli articoli 45 e 46 del RGDP nonché dalla Carta, non possa essere garantita, oppure nel senso che l'esercizio di tali poteri è limitato ad ipotesi eccezionali.

107 Conformemente all'articolo 8, paragrafo 3, della Carta nonché all'articolo 51, paragrafo 1, e all'articolo 57, paragrafo 1, lettera a), del RGPD, le autorità nazionali di controllo sono incaricate di vigilare sul rispetto delle norme dell'Unione relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. Pertanto, ciascuna di esse è investita della competenza di verificare se un trasferimento di dati personali dallo Stato membro a cui essa appartiene verso un paese terzo rispetti i requisiti stabiliti da tale regolamento (v., per analogia, per quanto riguarda l'articolo 28 della direttiva 95/46, sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 47).

108 Da tali disposizioni discende che le autorità di controllo hanno come compito principale quello di sorvegliare l'applicazione del RGDP e di vigilare sul rispetto di quest'ultimo. L'esercizio di tale funzione riveste un'importanza particolare nel contesto di un trasferimento di dati personali verso un paese terzo, in quanto, come risulta dallo stesso tenore letterale del considerando 116 di tale regolamento, «[c]on i trasferimenti transfrontalieri di dati personali al di fuori dell'Unione potrebbe aumentare il rischio che la persona fisica non possa esercitare il proprio diritto alla protezione dei dati, in particolare per tutelarsi da usi o comunicazioni illeciti di tali informazioni». In tale ipotesi, come precisato al medesimo considerando, «le autorità di controllo possono concludere di non essere in grado di dar corso ai reclami o svolgere indagini relative ad attività condotte oltre frontiera».

109 Inoltre, a norma dell'articolo 57, paragrafo 1, lettera f), del RGDP, ogni autorità di controllo è tenuta, nel suo territorio, a trattare i reclami che qualsiasi persona, ai sensi dell'articolo 77, paragrafo 1, di tale regolamento, ha il diritto di proporre quando considera che un trattamento di dati personali che la riguardano costituisca una violazione di tale regolamento, e ad esaminarne l'oggetto nella misura necessaria. L'autorità di controllo deve procedere al trattamento di un reclamo siffatto con tutta la diligenza richiesta (v., per analogia, per quanto riguarda l'articolo 25, paragrafo 6, della direttiva 95/46, sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 63).

110 L'articolo 78, paragrafi 1 e 2, del RGDP riconosce a chiunque il diritto di proporre un ricorso giurisdizionale effettivo, in particolare, nel caso in cui l'autorità di controllo ometta di trattare il suo reclamo. Il considerando 141 di tale regolamento fa del pari riferimento a tale «diritto a un ricorso giurisdizionale effettivo a norma dell'articolo 47 della Carta» nel caso in cui la suddetta autorità di controllo «non agisce quando è necessario intervenire per proteggere i diritti dell'interessato».

111 Ai fini della trattazione dei reclami presentati, l'articolo 58, paragrafo 1, del RGDP conferisce a ciascuna autorità di controllo significativi poteri di indagine. Siffatta autorità, ove, al termine della sua indagine, ritenga che l'interessato, i cui dati personali sono stati trasferiti verso un paese terzo, non goda in quest'ultimo di un livello di protezione adeguato, è tenuta, in applicazione del diritto dell'Unione, a reagire in modo appropriato al fine di porre rimedio all'inadeguatezza constatata, e ciò indipendentemente dall'origine o dalla natura di tale inadeguatezza. A tal fine, l'articolo 58, paragrafo 2, di tale regolamento elenca le diverse misure correttive che l'autorità di controllo può adottare.

112 Benché la scelta del mezzo appropriato e necessario spetti all'autorità di controllo e questa debba fare tale scelta prendendo in considerazione tutte le circostanze del trasferimento di dati personali di cui trattasi, detta autorità è comunque tenuta ad assolvere al suo compito di vigilare sul pieno rispetto del RGPD con tutta la diligenza richiesta.

113 A tal riguardo e come rilevato anche dall'avvocato generale al paragrafo 148 delle sue conclusioni, in forza dell'articolo 58, paragrafo 2, lettere f) e j), di tale regolamento, tale autorità è tenuta a sospendere o a vietare un trasferimento di dati personali verso un paese terzo qualora ritenga, alla luce del complesso delle circostanze proprie di tale trasferimento, che le clausole tipo di protezione dei dati non siano o non possano essere rispettate in tale paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione non possa essere garantita con altri mezzi, ove il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione non abbiano essi stessi sospeso il trasferimento o messo fine a quest'ultimo.

114 L'interpretazione esposta al punto precedente non è inficiata dall'argomento del Commissario secondo cui l'articolo 4 della decisione 2010/87, nella versione precedente all'entrata in vigore della decisione di esecuzione 2016/2297, letto alla luce del considerando 11 di tale decisione, limitava a talune ipotesi eccezionali il potere delle autorità di controllo di sospendere o vietare un trasferimento di dati personali verso un paese terzo. Nella versione risultante dalla decisione di esecuzione 2016/2297, l'articolo 4 della decisione CPT menziona, infatti, il potere di cui dispongono dette autorità, attualmente in forza dell'articolo 58, paragrafo 2, lettere f) e j), del RGPD, di sospendere o di vietare tale trasferimento, senza limitare in alcun modo l'esercizio di tale potere a circostanze eccezionali.

115 In ogni caso, il potere di esecuzione che l'articolo 46, paragrafo 2, lettera c), del RGPD riconosce alla Commissione ai fini dell'adozione di clausole tipo di protezione dei dati non le conferisce la competenza a limitare i poteri di cui dispongono le autorità di controllo ai sensi dell'articolo 58, paragrafo 2, di tale regolamento (v., per analogia, per quanto riguarda l'articolo 25, paragrafo 6, e l'articolo 28 della direttiva 95/46, sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punti 102 e 103). Per di più, il considerando 5 della decisione di esecuzione 2016/2297 conferma che la decisione CPT «non impedisce ad [un'autorità di controllo] di esercitare i propri poteri di controllo dei flussi di dati, compreso il potere di sospendere o vietare il trasferimento di dati personali, qualora stabilisca che esso avviene in violazione della normativa europea o nazionale sulla protezione dei dati».

116 Occorre tuttavia precisare che i poteri dell'autorità di controllo competente sono soggetti al pieno rispetto della decisione con la quale la Commissione, eventualmente, constata, in applicazione dell'articolo 45, paragrafo 1, prima frase, del RGPD, che un determinato paese terzo garantisce un livello di protezione adeguato. In tal caso, infatti, dall'articolo 45, paragrafo 1, seconda frase, di tale regolamento, letto in combinato disposto con il considerando 103 di quest'ultimo, risulta che i trasferimenti di dati personali verso il paese terzo interessato possono aver luogo senza che sia necessario ottenere un'autorizzazione specifica.

117 Ai sensi dell'articolo 288, quarto comma, TFUE, una decisione di adeguatezza della Commissione ha carattere vincolante, in tutti i suoi elementi, per tutti gli Stati membri destinatari e si impone quindi a tutti i loro organi, in quanto constata che il paese terzo interessato garantisce un livello di protezione adeguato e produce l'effetto di autorizzare tali trasferimenti di dati (v., per analogia, per quanto riguarda l'articolo 25, paragrafo 6, della direttiva 95/46, sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 51 e giurisprudenza ivi citata).

118 Pertanto, finché la decisione di adeguatezza 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 adottare misure contrarie a tale decisione, quali atti intesi a constatare con effetto vincolante che il

paese terzo interessato da detta decisione non garantisce un livello di protezione adeguato (v. sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 52 e giurisprudenza ivi citata) e, di conseguenza, a sospendere o vietare trasferimenti di dati personali verso tale paese terzo.

119 Tuttavia, una decisione di adeguatezza della Commissione adottata sulla base dell'articolo 45, paragrafo 3, del RGPD, non può impedire alle persone i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo di investire, in applicazione dell'articolo 77, paragrafo 1, del RGDP, l'autorità nazionale di controllo competente di un reclamo relativo alla protezione dei loro diritti e delle loro libertà con riguardo al trattamento di tali dati. Analogamente, una decisione di tal genere non può né annullare né ridurre i poteri espressamente riconosciuti alle autorità nazionali di controllo dall'articolo 8, paragrafo 3, della Carta nonché dall'articolo 51, paragrafo 1, e dall'articolo 57, paragrafo 1, lettera a), di detto regolamento (v., per analogia, per quanto riguarda l'articolo 25, paragrafo 6, e l'articolo 28 della direttiva 95/46, sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 53).

120 Pertanto, anche in presenza di una decisione di adeguatezza della Commissione, l'autorità nazionale di controllo competente, investita da una persona di un reclamo relativo alla protezione dei suoi diritti e delle sue libertà rispetto ad un trattamento di dati personali che la riguardano, deve poter esaminare, in piena indipendenza, se il trasferimento di tali dati rispetti i requisiti posti dal RGPD e, se del caso, proporre un ricorso dinanzi ai giudici nazionali affinché questi ultimi procedano, se condividono i dubbi di tale autorità quanto alla validità della decisione di adeguatezza, ad un rinvio pregiudiziale diretto all'esame della suddetta validità (v., per analogia, per quanto riguarda l'articolo 25, paragrafo 6, e l'articolo 28 della direttiva 95/46, sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punti 57 e 65).

121 Alla luce delle considerazioni che precedono, occorre rispondere all'ottava questione dichiarando che l'articolo 58, paragrafo 2, lettere f) e j), del RGPD deve essere interpretato nel senso che, a meno che esista una decisione di adeguatezza validamente adottata dalla Commissione, l'autorità di controllo competente è tenuta a sospendere o a vietare un trasferimento di dati verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati adottate dalla Commissione, qualora detta autorità di controllo ritenga, alla luce del complesso delle circostanze proprie di tale trasferimento, che le suddette clausole non siano o non possano essere rispettate in tale paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione, segnatamente dagli articoli 45 e 46 del RGDP e dalla Carta, non possa essere garantita con altri mezzi, ove il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione non abbiano essi stessi sospeso il trasferimento o messo fine a quest'ultimo.

Sulle questioni settima e undicesima

122 Con la settima e l'undicesima questione, che è opportuno esaminare congiuntamente, il giudice del rinvio interpella, in sostanza, la Corte sulla validità della decisione CPT alla luce degli articoli 7, 8 e 47 della Carta.

123 In particolare, come risulta dalla formulazione stessa della settima questione e dalle relative spiegazioni contenute nella domanda di pronuncia pregiudiziale, il giudice del rinvio si chiede se la decisione CPT sia idonea a garantire un livello di protezione adeguato dei dati personali trasferiti verso paesi terzi, considerato che le clausole tipo di protezione dei dati da essa previste non vincolano le autorità di tali paesi terzi.

124 L'articolo 1 della decisione CPT dispone che le clausole tipo di protezione dei dati contenute nell'allegato della stessa decisione costituiscono garanzie sufficienti per la tutela della vita privata e della libertà e dei diritti fondamentali delle persone ai sensi dell'articolo 26, paragrafo 2, della direttiva 95/46. Quest'ultima disposizione è stata ripresa, in sostanza, all'articolo 46, paragrafo 1, e all'articolo 46, paragrafo 2, lettera c), del RGPD.

125 Tuttavia, benché tali clausole siano vincolanti per il titolare del trattamento stabilito nell'Unione e per il destinatario del trasferimento di dati personali stabilito in un paese terzo, nel caso in cui abbiano concluso un contratto con riferimento a tali clausole, è pacifico che esse non possono vincolare le autorità di tale paese terzo, poiché queste ultime non sono parti del contratto.

126 Pur se esistono, pertanto, situazioni in cui, a seconda dello stato del diritto e delle prassi vigenti nel paese terzo interessato, il destinatario di un trasferimento siffatto è in grado di garantire la protezione dei dati necessaria sulla base delle sole clausole tipo di protezione dei dati, sussistono altre situazioni in cui quanto pattuito in tali clausole potrebbe non costituire un mezzo sufficiente che consenta di garantire, in pratica, la protezione effettiva dei dati personali trasferiti nel paese terzo interessato. Ciò si verifica, in particolare, qualora il diritto di tale paese terzo permetta alle autorità pubbliche di quest'ultimo ingerenze nei diritti delle persone interessate relativi a tali dati.

127 Pertanto, si pone la questione se una decisione della Commissione vertente su clausole tipo di protezione dei dati, adottata sulla base dell'articolo 46, paragrafo 2, lettera c), del RGPD, sia invalida, mancando, in tale decisione, garanzie opponibili alle autorità pubbliche dei paesi terzi verso i quali i dati personali sono o potrebbero essere trasferiti sulla base di tali clausole.

128 L'articolo 46, paragrafo 1, del RGPD prevede che, in mancanza di una decisione di adeguatezza, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. Ai sensi dell'articolo 46, paragrafo 2, lettera c), di detto regolamento, tali garanzie possono essere fornite mediante clausole tipo di protezione adottate dalla Commissione. Orbene, tali disposizioni non enunciano che tutte le suddette garanzie debbano essere necessariamente previste da una decisione della Commissione quale la decisione CPT.

129 È importante, in proposito, sottolineare che una decisione del genere si distingue da una decisione di adeguatezza adottata ai sensi dell'articolo 45, paragrafo 3, del RGPD, la quale mira, in esito ad un esame della normativa del paese terzo interessato che tenga conto, in particolare, della legislazione pertinente in materia di sicurezza nazionale e di accesso delle autorità pubbliche ai dati personali, a constatare con effetto vincolante che un paese terzo, un territorio o uno o più settori determinati in quest'ultimo, garantisce un livello di protezione adeguato e che, pertanto, l'accesso a tali dati da parte delle autorità pubbliche del suddetto paese non osta ai trasferimenti di dati verso lo stesso paese terzo. Una decisione di adeguatezza siffatta può essere quindi adottata dalla Commissione solo a condizione che quest'ultima abbia constatato che la normativa pertinente di tale paese terzo in materia presenta effettivamente tutte le garanzie richieste che consentano di ritenere che essa garantisca un livello di protezione adeguato.

130 Per contro, nel caso di una decisione della Commissione che adotta clausole tipo di protezione dei dati, come la decisione CPT, nei limiti in cui una decisione siffatta non riguarda un paese terzo, un territorio o uno o più settori determinati in quest'ultimo, non si può dedurre dall'articolo 46, paragrafo 1, e dall'articolo 46, paragrafo 2, lettera c), del RGPD che la Commissione sia tenuta a procedere, prima dell'adozione di una decisione del genere, a una valutazione dell'adeguatezza del livello di protezione garantito dai paesi terzi verso i quali potrebbero essere trasferiti dati personali in base a tali clausole.

131 A tal riguardo, occorre ricordare che, ai sensi dell'articolo 46, paragrafo 1, di tale regolamento, in mancanza di una decisione di adeguatezza della Commissione, spetta al titolare del trattamento o al responsabile del trattamento stabiliti nell'Unione prevedere segnatamente garanzie adeguate. I considerando 108 e 114 di tale regolamento confermano che, se la Commissione non ha adottato alcuna decisione circa il livello adeguato di protezione dei dati di un paese terzo, il titolare del trattamento o, eventualmente, il responsabile del trattamento «dovrebbe provvedere a compensare la carenza di protezione dei dati in un paese terzo con adeguate garanzie a tutela dell'interessato» e che «[t]ali garanzie dovrebbero assicurare un rispetto dei requisiti in materia di protezione dei dati e dei diritti degli interessati adeguato ai trattamenti all'interno dell'Unione, compresa la disponibilità di diritti azionabili degli interessati e di mezzi di ricorso effettivi (...) nell'Unione o in un paese terzo».

132 Poiché, come risulta dal punto 125 della presente sentenza, è intrinseco al carattere contrattuale delle clausole tipo di protezione dei dati che queste ultime non possano vincolare le autorità pubbliche dei paesi terzi, e poiché tuttavia l'articolo 44, l'articolo 46, paragrafo 1, e l'articolo 46, paragrafo 2, lettera c), del RGPD, interpretati alla luce degli articoli 7, 8 e 47 della Carta, esigono che il livello di protezione delle persone fisiche garantito da tale regolamento non sia compromesso, può rivelarsi necessario completare le garanzie contenute in tali clausole tipo di protezione dei dati. A tal riguardo, il considerando 109 di tale regolamento enuncia che «[l]a possibilità che il titolare del trattamento (...) utilizzi clausole tipo di protezione dei dati adottate dalla Commissione (...) non dovrebbe precludere ai titolari del trattamento (...) di aggiungere altre clausole o garanzie supplementari» e precisa, in particolare, che questi ultimi «dovrebbero essere incoraggiati a fornire garanzie supplementari (...) che integrino le clausole tipo di protezione [dei dati]».

133 Appare quindi che le clausole tipo di protezione dei dati adottate dalla Commissione ai sensi dell'articolo 46, paragrafo 2, lettera c), dello stesso regolamento mirano unicamente a fornire ai titolari del trattamento o ai responsabili del trattamento stabiliti nell'Unione garanzie contrattuali che si applicano in modo uniforme in tutti i paesi terzi e, pertanto, indipendentemente dal livello di protezione garantito in ciascuno di essi. Poiché tali clausole tipo di protezione dei dati non possono, tenuto conto della loro natura, fornire garanzie che vadano al di là di un obbligo contrattuale di vegliare a che sia rispettato il livello di protezione richiesto dal diritto dell'Unione, esse possono richiedere, in funzione della situazione esistente nell'uno o nell'altro paese terzo, l'adozione di misure supplementari da parte del titolare del trattamento al fine di garantire il rispetto di tale livello di protezione.

134 A tal proposito, come rilevato dall'avvocato generale al paragrafo 126 delle sue conclusioni, il meccanismo contrattuale previsto dall'articolo 46, paragrafo 2, lettera c), del RGPD si basa sull'attribuzione della responsabilità al titolare del trattamento o al responsabile del trattamento stabiliti nell'Unione e, in subordine, all'autorità di controllo competente. Incombe pertanto, anzitutto, a tale titolare del trattamento o al responsabile del trattamento verificare, caso per caso, e, eventualmente, in collaborazione con il destinatario del trasferimento, se il diritto del paese terzo di destinazione garantisca una protezione adeguata, alla luce del diritto dell'Unione, dei dati personali trasferiti sulla base di clausole tipo di protezione dei dati, fornendo, se necessario, garanzie supplementari rispetto a quelle offerte da tali clausole.

135 Qualora il titolare del trattamento o il responsabile del trattamento, stabiliti nell'Unione, non possano adottare misure supplementari sufficienti a garantire tale protezione, essi o, in subordine, l'autorità di controllo competente, sono tenuti a sospendere o mettere fine al trasferimento di dati personali verso il paese terzo interessato. Tale ipotesi ricorre in particolare nel caso in cui il diritto di tale paese terzo imponga al destinatario di un trasferimento di dati personali proveniente dall'Unione obblighi in contrasto con dette clausole e, pertanto, atti a rimettere in discussione la garanzia contrattuale di un livello di protezione adeguato contro l'accesso delle autorità pubbliche di detto paese terzo a tali dati.

136 Pertanto, il solo fatto che clausole tipo di protezione dei dati contenute in una decisione della Commissione adottata in applicazione dell'articolo 46, paragrafo 2, lettera c), del RGPD, come quelle contenute nell'allegato della decisione CPT, non vincolino le autorità dei paesi terzi verso i quali dati personali possono essere trasferiti non può inficiare la validità di tale decisione.

137 Tale validità dipende, per contro, dalla questione se, conformemente al requisito risultante dall'articolo 46, paragrafo 1, e dall'articolo 46, paragrafo 2, lettera c), del RGPD, interpretati alla luce degli articoli 7, 8 e 47 della Carta, siffatta decisione contenga meccanismi efficaci che consentano, in pratica, di garantire che sia rispettato il livello di protezione richiesto dal diritto dell'Unione e che i trasferimenti di dati personali, fondati su siffatte clausole, siano sospesi o vietati in caso di violazione di tali clausole o di impossibilità di rispettarle.

138 Per quanto riguarda le garanzie contenute nelle clausole tipo di protezione dei dati contenute nell'allegato della decisione CPT, dalla clausola 4, lettere a) e b), dalla clausola 5, lettera a), dalla clausola 9 nonché dalla clausola 11, paragrafo 1, della stessa risulta che il titolare del trattamento stabilito nell'Unione, il destinatario del trasferimento di dati personali, nonché l'eventuale subincaricato di quest'ultimo, si impegnano reciprocamente a far sì che il trattamento di tali dati, compreso il loro trasferimento, sia effettuato e continuerà ad essere effettuato conformemente alla «normativa sulla protezione dei dati», ossia, secondo la definizione che compare all'articolo 3, lettera f), di tale decisione, «la normativa che protegge i diritti e le libertà fondamentali del singolo, in particolare il diritto al rispetto della vita privata con riguardo al trattamento di dati personali, applicabile ai responsabili del trattamento nello Stato membro in cui è stabilito l'esportatore». Orbene, le disposizioni del RGPD, lette alla luce della Carta, fanno parte di tale normativa.

139 Inoltre, il destinatario del trasferimento di dati personali stabilito in un paese terzo si impegna, in forza della suddetta clausola 5, lettera a), ad informare prontamente il titolare del trattamento stabilito nell'Unione della sua eventuale impossibilità di conformarsi agli obblighi che gli incombono in forza del contratto concluso. In particolare, secondo la suddetta clausola 5, lettera b), tale destinatario certifica di non avere motivo di ritenere che la normativa ad esso applicabile gli impedisca di adempiere agli obblighi che gli incombono in forza del contratto concluso e si impegna a comunicare al titolare del trattamento, non appena ne abbia conoscenza, qualsiasi modificazione della normativa nazionale ad esso applicabile che possa pregiudicare le garanzie e gli obblighi previsti dalle clausole tipo di protezione dei dati contenute nell'allegato della decisione CPT. Peraltro, se è vero che la stessa clausola 5, lettera d), i), consente al destinatario del trasferimento di dati personali, in presenza di legislazione che gliene faccia divieto, ad esempio norme di diritto penale miranti a tutelare il segreto delle indagini, di non comunicare al titolare del trattamento stabilito nell'Unione una richiesta giuridicamente vincolante presentata da autorità giudiziarie o di polizia ai fini della comunicazione di dati personali, egli è tuttavia tenuto, conformemente alla clausola 5, lettera a), dell'allegato della decisione CPT, ad informare il titolare del trattamento dell'impossibilità di conformarsi alle clausole tipo di protezione dei dati.

140 Nelle due ipotesi in essa previste, tale clausola 5, lettere a) e b), conferisce al titolare del trattamento stabilito nell'Unione il diritto di sospendere il trasferimento di dati e/o di risolvere il contratto. Alla luce dei requisiti risultanti dall'articolo 46, paragrafo 1, e paragrafo 2, lettera c), del RGPD, letto alla luce degli articoli 7 e 8 della Carta, la sospensione del trasferimento di dati e/o la risoluzione del contratto hanno natura obbligatoria per il titolare del trattamento qualora il destinatario del trasferimento non sia, o non sia più, in grado di rispettare le clausole tipo di protezione dei dati. In caso contrario, il titolare del trattamento violerebbe gli obblighi ad esso incombenti ai sensi della clausola 4, lettera a), dell'allegato della decisione CPT, interpretata alla luce delle disposizioni del RGPD e della Carta.

141 Appare quindi che la clausola 4, lettera a), e la clausola 5, lettere a) e b), di detto allegato impongono al titolare del trattamento stabilito nell'Unione e al destinatario del trasferimento di dati personali di assicurarsi che la legislazione del paese terzo di destinazione consenta a detto destinatario di

conformarsi alle clausole tipo di protezione dei dati contenute nell'allegato della decisione CPT, prima di procedere ad un trasferimento di dati personali verso tale paese terzo. Per quanto riguarda tale verifica, la nota a piè di pagina relativa alla suddetta clausola 5 precisa che non sono in contraddizione con tali clausole tipo di protezione dei dati disposizioni vincolanti di siffatta legislazione nazionale che non vanno oltre quanto è necessario in una società democratica per salvaguardare, in particolare, la sicurezza dello Stato, la difesa e la sicurezza pubblica. Per contro, come sottolineato dall'avvocato generale al paragrafo 131, delle sue conclusioni, il fatto di conformarsi ad un obbligo dettato dal diritto del paese terzo di destinazione che vada oltre quanto è necessario a tal fine deve essere considerato una violazione di dette clausole. La valutazione, da parte di tali operatori, del carattere necessario di un obbligo siffatto deve, se del caso, tener conto della constatazione dell'adeguatezza del livello di protezione garantito dal paese terzo interessato contenuta in una decisione di adeguatezza della Commissione, adottata ai sensi dell'articolo 45, paragrafo 3, del RGPD.

142 Ne consegue che il titolare del trattamento stabilito nell'Unione e il destinatario del trasferimento di dati personali sono tenuti a verificare, preliminarmente, il rispetto, nel paese terzo interessato, del livello di protezione richiesto dal diritto dell'Unione. Il destinatario di tale trasferimento ha, se del caso, l'obbligo, in forza della stessa clausola 5, lettera b), di informare il titolare del trattamento della sua eventuale impossibilità di conformarsi a tali clausole, in tal caso incombe a quest'ultimo di sospendere il trasferimento di dati e/o di risolvere il contratto.

143 Qualora il titolare del trasferimento dei dati personali verso un paese terzo abbia comunicato al responsabile del trattamento, ai sensi della clausola 5, lettera b), dell'allegato della decisione CPT, che la legislazione del paese terzo interessato non gli consente di conformarsi alle clausole tipo di protezione dei dati contenute nell'allegato della decisione CPT, dalla clausola 12 di tale allegato discende che tutti i dati che sono già stati trasferiti verso tale paese terzo e le relative copie devono essere restituiti o distrutti. In ogni caso, la clausola 6 dello stesso allegato sanziona l'inosservanza di tali clausole tipo, conferendo all'interessato il diritto di ottenere il risarcimento del danno subito.

144 Occorre aggiungere che, ai sensi della clausola 4, lettera f), dell'allegato della decisione CPT il titolare del trattamento stabilito nell'Unione si impegna, allorché categorie particolari di dati potrebbero essere trasferite verso un paese terzo che non offra un livello di protezione adeguato, ad informarne l'interessato prima del trasferimento o appena possibile dopo quest'ultimo. Tale informazione può mettere tale interessato in condizione di esercitare il diritto di ricorso riconosciutogli dalla clausola 3, paragrafo 1, dello stesso allegato contro il titolare del trattamento, affinché quest'ultimo sospenda il trasferimento previsto, risolva il contratto concluso con il destinatario del trasferimento di dati personali o, eventualmente, chieda a quest'ultimo la restituzione o la distruzione dei dati trasferiti.

145 Infine, ai sensi della clausola 4, lettera g), dell'allegato della decisione CPT, il titolare del trattamento stabilito nell'Unione è tenuto – allorché il destinatario del trasferimento di dati personali gli notifica, in applicazione della clausola 5, lettera b), del medesimo allegato che la normativa ad esso applicabile è oggetto di una modifica che può avere conseguenze negative per le garanzie e gli obblighi previsti dalle clausole tipo di protezione dei dati – a trasmettere tale comunicazione all'autorità di controllo competente qualora decida, malgrado detta comunicazione, di proseguire il trasferimento o revocarne la sospensione. La trasmissione di siffatta comunicazione a tale autorità di controllo e il diritto di quest'ultima di procedere a verifiche presso il destinatario del trasferimento di dati personali in applicazione della clausola 8, paragrafo 2, dello stesso allegato consentono a detta autorità di controllo di verificare se occorra procedere alla sospensione o al divieto del trasferimento previsto al fine di garantire un livello di protezione adeguato.

146 In tale contesto, l'articolo 4 della decisione CPT, letto alla luce del considerando 5 della decisione di esecuzione 2016/2297, conferma che la decisione CPT non impedisce in alcun modo all'autorità di controllo competente di sospendere o, se del caso, vietare un trasferimento di dati personali verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati contenute nell'allegato di tale decisione. A tale riguardo, come risulta dalla risposta all'ottava questione, a meno che esista una

decisione di adeguatezza validamente adottata dalla Commissione, l'autorità di controllo competente è tenuta, a norma dell'articolo 58, paragrafo 2, lettere f) e j), del RGPD, a sospendere o a vietare un trasferimento siffatto, qualora detta autorità ritenga, alla luce di tutte le circostanze proprie di tale trasferimento, che le suddette clausole non siano o non possano essere rispettate in tale paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione non possa essere garantita con altri mezzi, ove il titolare del trattamento del trattamento o il responsabile del trattamento stabiliti nell'Unione non abbiano essi stessi sospeso il trasferimento o messo fine a quest'ultimo.

147 Per quanto riguarda la circostanza, menzionata dal Commissario, che trasferimenti di dati personali verso siffatto paese terzo potrebbero eventualmente essere oggetto di decisioni divergenti delle autorità di controllo in Stati membri diversi, occorre aggiungere che, come risulta dall'articolo 55, paragrafo 1, e dall'articolo 57, paragrafo 1, lettera a), del RGPD, il compito di vigilare sul rispetto di tale regolamento è affidato, in linea di principio, a ciascuna autorità di controllo nel territorio dello Stato membro cui essa appartiene. Inoltre, al fine di evitare decisioni divergenti, l'articolo 64, paragrafo 2, di tale regolamento prevede la possibilità, per l'autorità di controllo che ritenga che i trasferimenti di dati verso un paese terzo debbano, in generale, essere vietati, di adire il Comitato europeo per la protezione dei dati (EDPB), il quale può, in applicazione dell'articolo 65, paragrafo 1, lettera c), dello stesso regolamento, adottare una decisione vincolante, in particolare quando un'autorità di controllo non si conforma al parere emesso.

148 Ne consegue che la decisione CPT prevede meccanismi efficaci che consentono, in pratica, di garantire che il trasferimento verso un paese terzo di dati personali sulla base delle clausole tipo di protezione dei dati contenute nell'allegato di tale decisione sia sospeso o vietato qualora il destinatario del trasferimento non rispetti dette clausole o si trovi nell'impossibilità di rispettarle.

149 Alla luce di tutte le considerazioni che precedono, occorre rispondere alle questioni settima e undicesima dichiarando che dall'esame della decisione CPT alla luce degli articoli 7, 8 e 47 della Carta non è emerso alcun elemento idoneo ad inficiarne la validità.

Sulle questioni quarta, quinta, nona e decima

150 Con la nona questione, il giudice del rinvio chiede, in sostanza, se e in che limiti l'autorità di controllo di uno Stato membro sia vincolata dalle constatazioni contenute nella decisione «scudo per la privacy» secondo le quali gli Stati Uniti assicurano un livello di protezione adeguato. Con le sue questioni quarta, quinta e decima, detto giudice chiede, in sostanza, se, tenuto conto delle sue constatazioni riguardo al diritto degli Stati Uniti, il trasferimento verso tale paese terzo di dati personali sul fondamento delle clausole tipo di protezione dei dati contenute nell'allegato della decisione CPT violi i diritti garantiti dagli articoli 7, 8 e 47 della Carta e chiede, segnatamente, alla Corte se l'aver istituito il Mediatore menzionato nell'allegato III della decisione «scudo per la privacy» sia compatibile con il suddetto articolo 47.

151 Occorre anzitutto rilevare che, sebbene il ricorso del Commissario nel procedimento principale metta in dubbio la validità della sola decisione CPT, tale ricorso è stato proposto dinanzi al giudice del rinvio prima dell'adozione della decisione «scudo per la privacy». Nei limiti in cui, con la quarta e la quinta questione, detto giudice interroga la Corte, in via generale, sulla tutela che deve essere garantita, in forza degli articoli 7, 8 e 47 della Carta, nel contesto di un siffatto trasferimento, l'esame della Corte deve prendere in considerazione le conseguenze derivanti dall'adozione della decisione «scudo per la privacy», occorsa nel frattempo. Ciò vale a maggior ragione in quanto detto giudice chiede esplicitamente, con la sua decima questione, se con il Mediatore menzionato in quest'ultima decisione sia garantita la protezione richiesta da detto articolo 47.

152 Inoltre, dalle indicazioni contenute nella domanda di pronuncia pregiudiziale emerge che, nell'ambito del procedimento principale, Facebook Ireland ha sostenuto che la decisione «scudo per la privacy» produceva, per il Commissario, effetti vincolanti per quanto riguarda la constatazione dell'adeguatezza del livello di protezione garantito dagli Stati Uniti e, di conseguenza, quanto alla liceità di un trasferimento di dati personali verso tale paese terzo effettuato sulla base di clausole tipo di protezione dei dati contenute nell'allegato della decisione CPT.

153 Orbene, come risulta dal punto 59 della presente sentenza, nella sua sentenza del 3 ottobre 2017, allegata alla domanda di pronuncia pregiudiziale, il giudice del rinvio ha sottolineato di essere tenuto a prendere in considerazione le modifiche della normativa intercorse tra la proposizione del ricorso e l'udienza tenutasi dinanzi ad esso. Appare, pertanto, che tale giudice abbia l'obbligo di prendere in considerazione, per dirimere la controversia di cui al procedimento principale, il mutamento di circostanze risultante dall'adozione della decisione «scudo per la privacy» nonché dagli eventuali effetti vincolanti di quest'ultima.

154 In particolare, l'esistenza degli effetti vincolanti connessi alla constatazione, da parte della decisione «scudo per la privacy», di un livello di protezione adeguato negli Stati Uniti è rilevante ai fini della valutazione tanto degli obblighi, ricordati ai punti 141 e 142 della presente sentenza, che incombono al titolare del trattamento e al destinatario di un trasferimento di dati personali verso un paese terzo effettuato sulla base delle clausole tipo di protezione dei dati contenute nell'allegato della decisione CPT, quanto degli obblighi che gravano, eventualmente, sull'autorità di controllo di sospendere o vietare un trasferimento siffatto.

155 Per quanto riguarda, infatti, gli effetti vincolanti della decisione «scudo per la privacy», l'articolo 1, paragrafo 1, di tale decisione dispone che, ai fini dell'articolo 45, paragrafo 1, del RGDP, «gli Stati Uniti d'America assicurano un livello di protezione adeguato dei dati personali trasferiti nell'ambito dello scudo [Unione europea-Stati Uniti] dall'Unione alle organizzazioni statunitensi». Ai sensi dell'articolo 1, paragrafo 3, della stessa decisione si considera che i dati personali sono trasferiti nell'ambito di siffatto scudo allorché sono trasferiti dall'Unione a organizzazioni stabilite negli Stati Uniti che compaiono nell'elenco degli aderenti a detto scudo tenuto e pubblicato dal Dipartimento del Commercio degli Stati Uniti in conformità delle parti I e III dei principi enunciati nell'allegato II della medesima decisione.

156 Come risulta dalla giurisprudenza ricordata ai punti 117 e 118 della presente sentenza, la decisione «scudo per la privacy» ha carattere vincolante per le autorità di controllo nella parte in cui constata che gli Stati Uniti garantiscono un livello di protezione adeguato e, pertanto, ha l'effetto di autorizzare trasferimenti di dati personali effettuati nell'ambito dello scudo per la privacy Unione europea-Stati Uniti. Pertanto, fino a che tale decisione non sia stata dichiarata invalida dalla Corte, l'autorità di controllo competente non può sospendere o vietare un trasferimento di dati personali verso un'organizzazione aderente a tale scudo in base al rilievo che essa considera, contrariamente a quanto ritenuto dalla Commissione in detta decisione, che la normativa statunitense che disciplina l'accesso ai dati personali trasferiti nell'ambito di detto scudo e l'utilizzo di tali dati da parte delle autorità pubbliche di tale paese terzo a fini di sicurezza nazionale, di amministrazione della giustizia o di interesse pubblico non garantisca un livello di protezione adeguato.

157 Ciò non toglie che, conformemente alla giurisprudenza ricordata ai punti 119 e 120 della presente sentenza, quando una persona le presenta un reclamo, l'autorità di controllo competente deve esaminare, in piena indipendenza, se il trasferimento di dati personali di cui trattasi rispetti i requisiti posti dal RGPD e, laddove ritenga fondate le censure dedotte da tale persona al fine di contestare la validità di una decisione di adeguatezza, proporre un ricorso dinanzi ai giudici nazionali affinché questi ultimi sottopongano alla Corte un rinvio pregiudiziale ai fini della valutazione della validità della suddetta decisione.

158 Un reclamo proposto ai sensi dell'articolo 77, paragrafo 1, del RGDP, con il quale una persona, i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo, fa valere che il diritto e la prassi di tale paese non garantiscono, nonostante quanto constatato dalla Commissione in una decisione adottata in base all'articolo 45, paragrafo 3, di tale regolamento, un livello di protezione adeguato, deve essere, infatti, inteso nel senso che esso verte, in sostanza, sulla compatibilità di tale decisione con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona (v., per analogia, per quanto riguarda l'articolo 25, paragrafo 6, e l'articolo 28, paragrafo 4, della direttiva 95/46, sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 59).

159 Nel caso di specie, il sig. Schrems ha chiesto in sostanza al Commissario di vietare o sospendere il trasferimento, da parte di Facebook Ireland, dei suoi dati personali a Facebook Inc., stabilita negli Stati Uniti, in quanto tale paese terzo non garantirebbe un livello di protezione adeguato. Avendo il Commissario, in esito a un'indagine sulle affermazioni del sig. Schrems, adito il giudice del rinvio, quest'ultimo, alla luce delle prove prodotte e del contraddittorio svoltosi dinanzi ad esso, sembra interrogarsi sulla fondatezza dei dubbi del sig. Schrems circa l'adeguatezza del livello di protezione garantito in tale paese terzo, malgrado quanto constatato nel frattempo dalla Commissione nella decisione «scudo per la privacy», e ciò ha indotto tale giudice a sottoporre alla Corte le questioni pregiudiziali quarta, quinta e decima.

160 Come rilevato dall'avvocato generale al paragrafo 175 delle sue conclusioni, tali questioni pregiudiziali devono quindi essere intese nel senso che esse mettono in discussione, in sostanza, la constatazione della Commissione, contenuta nella decisione «scudo per la privacy», secondo la quale gli Stati Uniti garantiscono un livello adeguato di protezione dei dati personali trasferiti dall'Unione verso tale paese terzo e, pertanto, la validità di tale decisione.

161 Alla luce delle considerazioni esposte ai punti 121 e da 157 a 160 della presente sentenza e al fine di fornire una risposta completa al giudice del rinvio, occorre quindi esaminare se la decisione «scudo per la privacy» sia conforme ai requisiti derivanti dal RGPD, letto alla luce della Carta (v., per analogia, sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 67).

162 L'adozione, da parte della Commissione, di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, del RGDP 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 (v., per analogia, per quanto riguarda l'articolo 25, paragrafo 6, della direttiva 95/46, sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 63).

Sul contenuto della decisione «scudo per la privacy»

163 La Commissione ha constatato, all'articolo 1, paragrafo 1, della decisione «scudo per la privacy», che gli Stati Uniti assicurano un livello adeguato di protezione dei dati personali trasferiti dall'Unione verso organizzazioni stabilite negli Stati Uniti nell'ambito dello scudo per la privacy Unione europea-Stati Uniti, il quale, in forza dell'articolo 1, paragrafo 2, di tale decisione, è segnatamente costituito dai principi emanati dal Dipartimento del Commercio degli Stati Uniti il 7 luglio 2016, riportati nell'allegato II della stessa decisione, e dalle dichiarazioni e dagli impegni ufficiali riportati nei documenti di cui agli allegati I e da III a VII.

164 Nondimeno, la decisione «scudo per la privacy», al punto I.5. del suo allegato II rubricato «Principi del regime dello scudo [Unione europea-Stati Uniti] per la privacy», precisa altresì che l'adesione a tali principi può essere limitata «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia». Pertanto, detta decisione, al pari della decisione 2000/520, sancisce il primato delle suddette esigenze rispetto a tali principi, primato in forza del quale

le organizzazioni statunitensi 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 (v., per analogia, per quanto riguarda la decisione 2000/520, sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 86).

165 Alla luce del suo carattere generale, la deroga contenuta al punto I.5. dell'allegato II, della decisione «scudo per la privacy» 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 (v., per analogia, per quanto riguarda la decisione 2000/520, sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 87). Più in particolare, e come constatato nella decisione «scudo per la privacy», siffatte ingerenze possono derivare dall'accesso, da parte delle autorità pubbliche statunitensi, ai dati personali, trasferiti dall'Unione verso gli Stati Uniti, e dall'utilizzo di tali dati nell'ambito dei programmi di sorveglianza PRISM e UPSTREAM fondati sull'articolo 702 del FISA, nonché sulla base dell'E.O. 12333.

166 In tale contesto, la Commissione ha valutato, ai punti da 67 a 135 della decisione «scudo per la privacy», le limitazioni e le garanzie previste nella normativa statunitense, in particolare all'articolo 702 del FISA, nell'E.O. 12333 e nella PPD-28, per quanto riguarda l'accesso ai dati personali trasferiti nell'ambito dello scudo per la privacy Unione europea-Stati Uniti e l'utilizzo di tali dati da parte delle autorità pubbliche statunitensi a fini di sicurezza nazionale, amministrazione della giustizia o di interesse pubblico.

167 In esito a detta valutazione la Commissione ha constatato, al punto 136 di tale decisione, che «gli Stati Uniti d'America assicur[a]no un livello di protezione adeguato dei dati personali trasferiti nell'ambito dello scudo dall'Unione alle organizzazioni statunitensi che si sono autocertificate» e, al punto 140 della stessa decisione, ha considerato che «[i]n base alle informazioni sull'ordinamento giuridico statunitense disponibili, (...) l'ingerenza nei diritti fondamentali della persona i cui dati sono trasferiti dall'Unione verso gli Stati Uniti nell'ambito dello [«scudo per la privacy»], compiuta dall'autorità pubblica statunitense per esigenze di sicurezza nazionale, amministrazione della giustizia o altro scopo d'interesse pubblico, e le conseguenti limitazioni relative al rispetto dei principi imposte alle organizzazioni che si sono autocertificate come aderenti al regime, si limitino a quanto strettamente necessario per conseguire l'obiettivo legittimo ricercato e che contro le ingerenze di tale natura esiste una tutela giuridica efficace».

Sulla constatazione relativa al livello di protezione adeguato

168 Alla luce degli elementi menzionati dalla Commissione nella decisione «scudo per la privacy» nonché di quelli accertati dal giudice del rinvio nell'ambito del procedimento principale, tale giudice nutre dubbi in merito alla questione se il diritto degli Stati Uniti garantisca effettivamente il livello di protezione adeguato richiesto dall'articolo 45 del RGPD, letto alla luce dei diritti fondamentali garantiti agli articoli 7, 8 e 47 della Carta. In particolare, detto giudice ritiene che il diritto di tale paese terzo non preveda le limitazioni e le garanzie necessarie rispetto alle ingerenze autorizzate dalla sua normativa nazionale e non assicuri neppure una tutela giurisdizionale effettiva contro tali ingerenze. A quest'ultimo riguardo, il suddetto giudice aggiunge che l'instaurazione del Mediatore dello scudo per la privacy non può, a suo avviso, porre rimedio a tali lacune in quanto detto Mediatore non sarebbe assimilabile ad un giudice, ai sensi dell'articolo 47 della Carta.

169 Per quanto riguarda, in primo luogo, gli articoli 7 e 8 della Carta, che fanno parte del livello di protezione richiesto all'interno dell'Unione e il cui rispetto deve essere constatato dalla Commissione prima di adottare una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 1, del RGPD, occorre ricordare che l'articolo 7 della Carta garantisce ad ogni persona il diritto al rispetto della

propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni. Quanto all'articolo 8, paragrafo 1, della Carta, esso riconosce esplicitamente a ogni persona il diritto alla protezione dei dati personali che la riguardano.

170 Pertanto, l'accesso a dati personali di una persona fisica ai fini della loro conservazione o del loro utilizzo incide sul diritto fondamentale di tale persona al rispetto della vita privata, garantito dall'articolo 7 della Carta, e tale diritto si riferisce a qualsiasi informazione riguardante una persona fisica identificata o identificabile. Tali trattamenti di dati rientrano anche nell'ambito dell'articolo 8 della Carta a motivo del fatto che essi costituiscono trattamenti di dati a carattere personale ai sensi di tale articolo e devono, di conseguenza, necessariamente soddisfare gli obblighi di protezione dei dati previsti a detto articolo [v., in tal senso, sentenze del 9 novembre 2010, Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, EU:C:2010:662, punti 49 e 52, nonché dell'8 aprile 2014, Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 29, e parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punti 122 e 123].

171 Come già dichiarato dalla Corte, la comunicazione di dati personali a un terzo, quale un'autorità pubblica, costituisce un'ingerenza nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta, indipendentemente dall'uso ulteriore delle informazioni comunicate. Ciò vale altresì per la conservazione dei dati personali e l'accesso a tali dati al fine del loro utilizzo da parte delle pubbliche autorità, indipendentemente dal fatto che le informazioni relative alla vita privata di cui trattasi abbiano o meno natura sensibile, o che gli interessati abbiano o meno subito eventuali inconvenienti per effetto di tale ingerenza [v., in tal senso, sentenze del 20 maggio 2003, Österreichischer Rundfunk e a., C-465/00, C-138/01 e C-139/01, EU:C:2003:294, punti 74 e 75, nonché dell'8 aprile 2014, Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punti da 33 a 36, e parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punti 124 e 126].

172 Tuttavia, i diritti sanciti agli articoli 7 e 8 della Carta non appaiono come prerogative assolute, ma vanno considerati alla luce della loro funzione sociale [v., in tal senso, sentenze del 9 novembre 2010, Volker und Markus Schecke e Eifert, C-92/09 e C-93/09, EU:C:2010:662, punto 48 e giurisprudenza ivi citata, nonché del 17 ottobre 2013, Schwarz, C-291/12, EU:C:2013:670, punto 33 e giurisprudenza ivi citata, e altresì parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punto 136].

173 A tale riguardo, occorre rilevare altresì che ai sensi dell'articolo 8, paragrafo 2, della Carta, i dati personali devono, in particolare, essere trattati «per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge».

174 Inoltre, ai sensi dell'articolo 52, paragrafo 1, prima frase, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla stessa Carta devono essere previste dalla legge e devono rispettare il contenuto essenziale di detti diritti e libertà. Secondo l'articolo 52, paragrafo 1, seconda frase, della Carta, nel rispetto del principio di proporzionalità, possono essere apportate limitazioni a tali diritti e libertà solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

175 Occorre aggiungere, a quest'ultimo riguardo, che il requisito secondo cui qualsiasi limitazione nell'esercizio dei diritti fondamentali deve essere prevista dalla legge implica che la base giuridica che consente l'ingerenza in tali diritti deve definire essa stessa la portata della limitazione dell'esercizio del diritto considerato [v. parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punto 139 e giurisprudenza ivi citata].

176 Infine, per soddisfare il requisito di proporzionalità secondo cui le deroghe alla protezione dei dati personali devono operare nei limiti dello stretto necessario, la normativa controversa che comporta l'ingerenza deve prevedere 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 sono trasferiti dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali

contro il rischio di abusi. In particolare, essa deve indicare in quali circostanze e a quali condizioni possa essere adottata una misura che prevede il trattamento di siffatti dati, garantendo così che l'ingerenza sia limitata allo stretto necessario. La necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatizzato [v., in tal senso, parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017, EU:C:2017:592, punti 140 e 141 e giurisprudenza ivi citata].

177 A tal fine, l'articolo 45, paragrafo 2, lettera a), del RGPD precisa che, nel valutare l'adeguatezza del livello di protezione garantito da un paese terzo, la Commissione prende in considerazione in particolare «i diritti effettivi e azionabili degli interessati» i cui dati personali sono trasferiti.

178 Nel caso di specie, la constatazione effettuata dalla Commissione nella decisione «scudo per la privacy», secondo la quale gli Stati Uniti garantiscono un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione dal RGPD, letto alla luce degli articoli 7 e 8 della Carta, è stata rimessa in discussione, in particolare, sulla base del rilievo che le ingerenze risultanti dai programmi di sorveglianza fondati sull'articolo 702 del FISA e sull'E.O. 12333 non sarebbero soggette a requisiti che garantiscano, nel rispetto del principio di proporzionalità, un livello di protezione sostanzialmente equivalente a quello garantito dall'articolo 52, paragrafo 1, seconda frase, della Carta. Occorre quindi esaminare se detti programmi di sorveglianza siano attuati nel rispetto di tali requisiti, senza che sia necessario verificare preliminarmente il rispetto, da parte di tale paese terzo, di condizioni sostanzialmente equivalenti a quelle previste dall'articolo 52, paragrafo 1, prima frase, della Carta.

179 A tal proposito, per quanto riguarda i programmi di sorveglianza basati sull'articolo 702 del FISA, la Commissione ha constatato, al punto 109 della decisione «scudo per la privacy» che ai sensi di tale articolo «la Corte FISA non autorizza singole misure di sorveglianza, ma piuttosto programmi di sorveglianza (quali PRISM e UPSTREAM) basandosi sulle certificazioni annuali preparate dal Procuratore generale e dal Direttore dell'intelligence nazionale [DNI]». Come risulta da quello stesso punto, il controllo esercitato dalla Corte FISA mira quindi a verificare se tali programmi di sorveglianza corrispondano all'obiettivo di ottenere informazioni in materia di intelligence esterna, ma non verte sulla questione «se la persona costituisca un obiettivo adatto per acquisire informazioni di intelligence esterna».

180 Appare quindi che l'articolo 702 del FISA non fa emergere in alcun modo l'esistenza di limitazioni all'autorizzazione che esso comporta per l'attuazione dei programmi di sorveglianza ai fini dell'intelligence esterna, né l'esistenza di garanzie per i cittadini stranieri potenzialmente oggetto di tali programmi. In tali circostanze, e come sostanzialmente rilevato dall'avvocato generale ai paragrafi 291, 292 e 297 delle sue conclusioni, tale articolo non è idoneo a garantire un livello di tutela sostanzialmente equivalente a quello garantito dalla Carta, come interpretata dalla giurisprudenza ricordata ai punti 175 e 176 della presente sentenza, secondo cui, per soddisfare il principio di proporzionalità, una base giuridica che consente ingerenze nei diritti fondamentali deve definire essa stessa la portata della limitazione dell'esercizio del diritto di cui trattasi e prevedere norme chiare e precise che regolino la portata e l'applicazione della misura e impongano requisiti minimi.

181 In base alle constatazioni contenute nella decisione «scudo per la privacy, è vero che i programmi di sorveglianza fondati sull'articolo 702 del FISA devono essere attuati nel rispetto dei requisiti risultanti dalla PPD-28. Tuttavia, sebbene la Commissione abbia sottolineato, ai punti 69 e 77 della decisione «scudo per la privacy, che siffatti requisiti sono vincolanti per i servizi di intelligence statunitensi, il governo degli Stati Uniti ha ammesso, in risposta ad un quesito della Corte, che la PPD-28 non conferisce agli interessati diritti nei confronti delle autorità statunitensi azionabili dinanzi ai giudici. Pertanto, essa non è idonea a garantire un livello di protezione sostanzialmente equivalente a quello risultante dalla Carta, contrariamente a quanto richiesto dall'articolo 45, paragrafo 2, lettera a), del

RGPD, secondo il quale la constatazione di tale livello dipende, in particolare, dall'esistenza dei diritti effettivi e azionabili di cui godono le persone i cui dati sono stati trasferiti verso il paese terzo di cui trattasi.

182 Per quanto riguarda i programmi di sorveglianza basati sull'E.O. 12333, dal fascicolo di cui dispone la Corte risulta che neppure tale decreto conferisce diritti nei confronti delle autorità statunitensi azionabili dinanzi ai giudici.

183 Occorre aggiungere che la PPD-28, che deve essere rispettata nell'ambito dell'applicazione dei programmi di cui ai due punti precedenti, consente di procedere ad una «raccolta in blocco (...) di un volume relativamente consistente di informazioni o dati nell'ambito dell'intelligence dei segnali in circostanze in cui la comunità dell'intelligence non può rendere mirata la raccolta ricorrendo a un identificatore associato a un obiettivo specifico», come precisato in una lettera del 21 giugno 2016 dell'Ufficio del direttore dell'intelligence nazionale (Office of the Director of National Intelligence) al Dipartimento del Commercio degli Stati Uniti e all'Amministrazione del commercio internazionale, contenuta nell'allegato VI della decisione «scudo per la privacy». Orbene, tale possibilità, che consente, nell'ambito dei programmi di sorveglianza basati sull'E.O. 12333, di accedere a dati in transito verso gli Stati Uniti senza che tale accesso sia oggetto di un qualsivoglia controllo giudiziario, non circoscrive, in ogni caso, in modo sufficientemente chiaro e preciso la portata di siffatta raccolta in blocco di dati personali.

184 Risulta, pertanto, che né l'articolo 702 del FISA, né l'E.O. 12333, in combinato disposto con la PPD-28, corrispondono ai requisiti minimi connessi, nel diritto dell'Unione, al principio di proporzionalità, cosicché non si può considerare che i programmi di sorveglianza basati su tali disposizioni siano limitati allo stretto necessario.

185 In tali circostanze, le limitazioni alla protezione dei dati personali, che derivano dalla normativa interna degli Stati Unit in materia di accesso e utilizzo, da parte delle autorità pubbliche statunitensi, di tali dati trasferiti dall'Unione verso gli Stati Uniti e che la Commissione ha valutato nella decisione «scudo per la privacy», non sono inquadrate in modo da corrispondere a requisiti sostanzialmente equivalenti a quelli richiesti, nel diritto dell'Unione, dall'articolo 52, paragrafo 1, seconda frase, della Carta.

186 Per quanto attiene, in secondo luogo, all'articolo 47 della Carta, che è anch'esso parte del livello di protezione richiesto all'interno dell'Unione e il cui rispetto deve essere constatato dalla Commissione prima di adottare una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 1, del RGPD, occorre ricordare che il primo comma di tale articolo 47 esige che ogni persona i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati abbia diritto a un ricorso effettivo dinanzi a un giudice nel rispetto delle condizioni previste da tale articolo. Ai sensi del secondo comma di tale articolo, ogni persona ha diritto a che la sua causa sia esaminata da un giudice indipendente e imparziale.

187 Secondo costante giurisprudenza, l'esistenza stessa di un controllo giurisdizionale effettivo, destinato a garantire il rispetto delle disposizioni del diritto dell'Unione, è intrinseca all'esistenza di uno Stato di diritto. Pertanto, 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 (sentenza del 6 ottobre 2015, Schrems, C-362/14, EU:C:2015:650, punto 95 e giurisprudenza ivi citata).

188 A tal fine, l'articolo 45, paragrafo 2, lettera a), del RGPD esige che, nel valutare l'adeguatezza del livello di protezione garantito da un paese terzo, la Commissione prenda in considerazione in particolare i mezzi di «ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento». Il considerando 104 del RGDP sottolinea, a tal proposito, che il paese terzo «dovrebbe assicurare un effettivo controllo indipendente della protezione dei dati e dovrebbe

prevedere meccanismi di cooperazione con autorità di protezione dei dati degli Stati membri» e precisa che «agli interessati dovrebbero essere riconosciuti diritti effettivi e azionabili e un mezzo di ricorso effettivo in sede amministrativa e giudiziale».

189 L'esistenza di tali effettive possibilità di ricorso nel paese terzo considerato riveste un'importanza particolare nel contesto di un trasferimento di dati personali verso tale paese terzo, in quanto, come risulta dal considerando 116 del RGPD, gli interessati possono trovarsi di fronte all'insufficienza dei poteri e dei mezzi delle autorità amministrative e giudiziarie degli Stati membri per poter dare utilmente seguito ai loro reclami fondati su un asserito trattamento illecito, in tale paese terzo, dei loro dati in tal modo trasferiti, il che può costringerli a rivolgersi alle autorità e ai giudici nazionali di siffatto paese terzo.

190 Nel caso di specie, la constatazione da parte della Commissione, nella decisione «scudo per l'Europa», che gli Stati Uniti assicurano un livello di protezione sostanzialmente equivalente a quello garantito dall'articolo 47 della Carta, è stata rimessa in discussione sulla base, in particolare, del rilievo che l'istituzione del Mediatore dello scudo per la privacy non può colmare le lacune constatate dalla Commissione stessa per quanto riguarda la tutela giurisdizionale delle persone i cui dati personali sono trasferiti verso tale paese terzo.

191 A tal proposito, la Commissione rileva, al punto 115 della decisione «scudo per la privacy», che «sebbene la persona, compreso l'interessato dell'[Unione], sottoposta a sorveglianza (elettronica) illecita per finalità di sicurezza nazionale disponga di una serie di possibilità di ricorso, altrettanto pacifico è che queste non contemplano almeno alcune delle basi giuridiche di cui possono avvalersi le autorità di intelligence statunitensi (ad esempio l'EO 12333)». Pertanto, riguardo all'E.O. 12333, in tale punto 115 essa ha sottolineato la mancanza di qualsiasi mezzo di ricorso, Orbene, secondo la giurisprudenza ricordata al punto 187 della presente sentenza, una lacuna siffatta nella tutela giurisdizionale rispetto alle ingerenze collegate ai programmi di intelligence basati su tale decreto presidenziale osta a che si concluda – come ha fatto la Commissione nella decisione «scudo per la privacy» – che il diritto degli Stati Uniti garantisce un livello di protezione sostanzialmente equivalente a quello garantito dall'articolo 47 della Carta.

192 Inoltre, per quanto riguarda tanto i programmi di sorveglianza fondati sull'articolo 702 del FISA, quanto quelli fondati sull'E.O. 12333, è stato rilevato ai punti 181 e 182 della presente sentenza, che né la PPD-28 né l'E.O. 12333 conferiscono agli interessati diritti nei confronti delle autorità statunitensi azionabili dinanzi ai giudici, cosicché tali interessati non dispongono di un diritto di ricorso effettivo.

193 Ai punti 115 e 116 della decisione «scudo per la privacy», tuttavia, la Commissione ha constatato che per effetto dell'esistenza del meccanismo di mediazione istituito dalle autorità statunitensi – quale descritto nella lettera inviata il 7 luglio 2016 dal Segretario di Stato statunitense alla Commissaria europea per la Giustizia, i Consumatori e la parità di genere, contenuta all'allegato III di tale decisione – e della natura della missione affidata al Mediatore, ossia quella di «Primo coordinatore della diplomazia internazionale per le tecnologie dell'informazione», si poteva considerare che gli Stati Uniti assicurano un livello di protezione sostanzialmente equivalente a quello garantito all'articolo 47 della Carta.

194 L'esame della questione se il meccanismo di mediazione di cui alla decisione «scudo per la privacy» sia effettivamente idoneo ad ovviare alle limitazioni del diritto a una tutela giurisdizionale accertate dalla Commissione deve, conformemente ai requisiti che derivano dall'articolo 47 della Carta e dalla giurisprudenza ricordata al punto 187 della presente sentenza, partire dal principio che i singoli devono disporre della possibilità di esperire mezzi di ricorso dinanzi a un giudice indipendente e imparziale al fine di avere accesso a dati personali che li riguardano, o di ottenere la rettifica o la soppressione di tali dati.

195 Orbene, nella lettera menzionata al punto 193 della presente sentenza, è indicato che il Mediatore dello scudo per la privacy, pur se descritto come «indipendente dalla comunità dell'intelligence statunitense», «riferisce direttamente al segretario di Stato, il quale assicura che svolga la sua funzione con obiettività e senza indebite ingerenze che possano influire sulla risposta apportata». Per di più, oltre al fatto che, come constatato dalla Commissione al punto 116 di tale decisione, il Mediatore è designato dal Segretario di Stato e costituisce parte integrante del Dipartimento di Stato degli Stati Uniti, la suddetta decisione, come rilevato dall'avvocato generale al paragrafo 337 delle sue conclusioni, non contiene alcuna indicazione che la revoca del Mediatore o l'annullamento della sua nomina siano accompagnate da garanzie particolari, circostanza che è idonea a mettere in dubbio l'indipendenza del Mediatore rispetto al potere esecutivo (v., in tal senso, sentenza del 21 gennaio 2020, Banco de Santander, C-274/14, EU:C:2020:17, punti 60 e 63 e giurisprudenza ivi citata).

196 Del pari, come sottolineato dall'avvocato generale al paragrafo 338 delle sue conclusioni, sebbene il punto 120 della decisione «scudo per la privacy» menzioni un impegno del governo statunitense a far sì che la componente interessata dei servizi di intelligence sia tenuta a rettificare qualsiasi violazione delle norme applicabili individuata dal Mediatore dello scudo per la privacy, detta decisione non contiene alcuna indicazione che tale Mediatore sia autorizzato ad adottare decisioni vincolanti nei confronti dei suddetti servizi e non menziona neppure garanzie giuridiche da cui sarebbe contornato il suddetto impegno e delle quali potrebbero avvalersi gli interessati.

197 Pertanto, il meccanismo di mediazione di cui alla decisione «scudo per la privacy» non fornisce mezzi di ricorso dinanzi a un organo che offra alle persone i cui dati sono trasferiti verso gli Stati Uniti garanzie sostanzialmente equivalenti a quelle richieste dall'articolo 47 della Carta.

198 Di conseguenza, nel constatare, all'articolo 1, paragrafo 1, della decisione «scudo per la privacy», che gli Stati Uniti assicurano un livello adeguato di protezione dei dati personali trasferiti dall'Unione verso organizzazioni stabilite in tale paese terzo nell'ambito dello scudo Unione europea-Stati Uniti per la privacy, la Commissione ha disatteso i requisiti di cui all'articolo 45, paragrafo 1, del RGPD, letto alla luce degli articoli 7, 8 e 47 della Carta.

199 Ne consegue che l'articolo 1 della decisione «scudo per la privacy» è incompatibile con l'articolo 45, paragrafo 1, del RGPD, letto alla luce degli articoli 7, 8 e 47 della Carta, e che esso è per tale motivo invalido.

200 Poiché l'articolo 1 della decisione «scudo per la privacy» è inscindibile dagli articoli da 2 a 6, nonché dagli allegati della medesima, la sua invalidità ha l'effetto di inficiare la validità di tale decisione nel suo complesso.

201 Alla luce di tutte le considerazioni che precedono, si deve concludere che la decisione «scudo per la privacy» è invalida.

202 Quanto alla questione se occorra mantenere gli effetti di tale decisione al fine di evitare la creazione di una lacuna giuridica (v., in tal senso, sentenza del 28 aprile 2016, Borealis Polyolefine e a., C-191/14, C-192/14, C-295/14, C-389/14 e da C-391/14 a C-393/14, EU:C:2016:311, punto 106), occorre rilevare che, in ogni caso, tenuto conto dell'articolo 49 del RGPD, l'annullamento di una decisione di adeguatezza come la decisione «scudo per la privacy» non è idoneo a creare una lacuna giuridica siffatta. Tale articolo stabilisce, infatti, in modo preciso, a quali condizioni possono aver luogo trasferimenti di dati personali verso paesi terzi in assenza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, di detto regolamento o di garanzie appropriate ai sensi dell'articolo 46 del medesimo regolamento.

Sulle spese

203 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 2, paragrafi 1 e 2, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), deve essere interpretato nel senso che rientra nell'ambito di applicazione di tale regolamento un trasferimento di dati personali effettuato a fini commerciali da un operatore economico stabilito in uno Stato membro verso un altro operatore economico stabilito in un paese terzo, nonostante il fatto che, durante o in seguito a tale trasferimento, i suddetti dati possano essere sottoposti a trattamento da parte delle autorità del paese terzo considerato a fini di sicurezza pubblica, di difesa e sicurezza dello Stato.**

2) **L'articolo 46, paragrafo 1, e l'articolo 46, paragrafo 2, lettera c), del regolamento 2016/679 devono essere interpretati nel senso che le garanzie adeguate, i diritti azionabili e i mezzi di ricorso effettivi richiesti da tali disposizioni devono garantire che i diritti delle persone i cui dati personali sono trasferiti verso un paese terzo sul fondamento di clausole tipo di protezione dei dati godano di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione da tale regolamento, letto alla luce della Carta dei diritti fondamentali dell'Unione europea. A tal fine, la valutazione del livello di protezione garantito nel contesto di un trasferimento siffatto deve, in particolare, prendere in considerazione tanto le clausole contrattuali convenute tra il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione e il destinatario del trasferimento stabilito nel paese terzo interessato quanto, per quel che riguarda un eventuale accesso delle autorità pubbliche di tale paese terzo ai dati personali così trasferiti, gli elementi rilevanti del sistema giuridico di quest'ultimo, in particolare quelli enunciati all'articolo 45, paragrafo 2, di detto regolamento.**

3) **L'articolo 58, paragrafo 2, lettere f) e j), del regolamento 2016/679 deve essere interpretato nel senso che, a meno che esista una decisione di adeguatezza validamente adottata dalla Commissione europea, l'autorità di controllo competente è tenuta a sospendere o a vietare un trasferimento di dati verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati adottate dalla Commissione, qualora detta autorità di controllo ritenga, alla luce del complesso delle circostanze proprie di tale trasferimento, che le suddette clausole non siano o non possano essere rispettate in tale paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione, segnatamente dagli articoli 45 e 46 di tale regolamento e dalla Carta dei diritti fondamentali, non possa essere garantita con altri mezzi, ove il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione non abbiano essi stessi sospeso il trasferimento o messo fine a quest'ultimo.**

4) **Dall'esame della decisione 2010/87/UE della Commissione, del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, come modificata dalla decisione di esecuzione (UE) 2016/2297 della Commissione, del 16 dicembre 2016, alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali non è emerso alcun elemento idoneo ad inficiarne la validità.**

5) La decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy, è invalida.

Firme