Raccolta della giurisprudenza

CONCLUSIONI DELL'AVVOCATO GENERALE
HENRIK SAUGMANDSGAARD ØE
presentate il 19 dicembre 2019[1]

Causa C-311/18

Data Protection Commissioner
contro
Facebook Ireland Limited,
Maximillian Schrems,
con l'intervento di:
The United States of America,
Electronic Privacy Information Centre,
BSA Business Software Alliance, Inc.,
Digitaleurope

[domanda di pronuncia pregiudiziale proposta dalla High Court (Alta Corte, Irlanda)]

«Rinvio pregiudiziale – Protezione delle persone fisiche con riguardo al trattamento dei dati personali – Regolamento (UE) 2016/679 – Articolo 2, paragrafo 2 – Ambito di applicazione – Trasferimento a fini commerciali di dati personali verso gli Stati Uniti – Trattamento da parte delle autorità pubbliche degli Stati Uniti, a fini di sicurezza nazionale, dei dati trasferiti – Articolo 45 – Valutazione dell'adeguatezza del livello di protezione garantito in un paese terzo – Articolo 46 – Garanzie appropriate offerte dal responsabile del trattamento – Clausole tipo di protezione – Articolo 58, paragrafo 2 – Poteri delle autorità nazionali di controllo – Decisione 2010/87/UE – Validità – Decisione di esecuzione (UE) 2016/1250 – "Scudo UE-USA per la privacy" – Validità – Articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea»

Indice

1 Lingua originale: il francese.

I. Introduzione

1. In mancanza di garanzie comuni in materia di protezione dei dati personali a livello mondiale, i flussi transfrontalieri di tali dati sono accompagnati dal rischio di interruzione nella continuità del livello di protezione garantito all'interno dell'Unione europea. Nell'intento di agevolare tali flussi limitando al contempo tale rischio, il legislatore dell'Unione ha istituito tre meccanismi in base ai quali i dati personali possono essere trasferiti dall'Unione a uno Stato terzo.

2. In primo luogo, siffatto trasferimento può essere effettuato in base a una decisione con la quale la Commissione europea constata che lo Stato terzo in questione garantisce un «livello di protezione adeguato» dei dati che vi sono trasferiti [2]. In secondo luogo, in mancanza di siffatta decisione, il trasferimento è autorizzato quando è accompagnato da «garanzie adeguate» [3]. Tali garanzie possono assumere la forma di un contratto tra l'esportatore e l'importatore dei dati contenente clausole tipo di protezione adottate dalla Commissione. Il RGPD prevede, in terzo luogo, talune deroghe, basate in particolare sul consenso della persona interessata, che consentono il trasferimento in un paese terzo anche in mancanza di una decisione di adeguatezza o di garanzie adeguate [4].

2 V. articolo 45 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 (regolamento generale sulla protezione dei dati) (GU 2016, L 119, pag. 1; in prosieguo: il «RGPD»).

3 V. articolo 46 del RGPD.

4 V. articolo 49 del RGPD.

3. La domanda di pronuncia pregiudiziale, proposta dalla High Court (Alta Corte, Irlanda), riguarda il secondo meccanismo. Più in particolare, essa riguarda la validità della decisione 2010/87/UE [5], con la quale la Commissione ha stabilito clausole contrattuali tipo per talune categorie di trasferimenti, alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»).

4. Tale domanda è stata presentata nell'ambito di una controversia tra il Data Protection Commissioner (garante per la protezione dei dati personali, Irlanda; in prosieguo: il «DPC») e Facebook Ireland Ltd. e il sig. Maximillian Schrems. Quest'ultimo ha presentato al DPC una denuncia relativa al trasferimento di dati personali che lo riguardavano da Facebook Ireland a Facebook Inc., la sua società controllante con sede negli Stati Uniti d'America (in prosieguo: gli «Stati Uniti»). Il DPC ritiene che il trattamento di tale denuncia dipenda dalla questione della validità della decisione 2010/87. In tale contesto, esso ha adito il giudice del rinvio chiedendogli di interpellare la Corte al riguardo.

5. Vorrei sottolineare, anzitutto, che l'esame delle questioni pregiudiziali non ha fatto emergere, a mio avviso, alcun elemento atto a inficiare la validità della decisione 2010/87.

6. Inoltre, il giudice del rinvio ha evidenziato taluni dubbi riguardanti, in sostanza, l'adeguatezza del livello di protezione garantito dagli Stati Uniti, considerate le ingerenze che le attività delle autorità di intelligence statunitensi hanno sull'esercizio dei diritti fondamentali delle persone i cui dati sono trasferiti in tale paese terzo. Tali dubbi rimettono indirettamente in discussione le valutazioni effettuate al riguardo dalla Commissione nella decisione di esecuzione (UE) 2016/1250 [6]. Pur se la risoluzione della controversia nel procedimento principale non richiede che la Corte si pronunci su tale questione – e, pertanto, io le propongo di astenersi dal farlo – esporrò in subordine le ragioni che mi inducono a mettere in dubbio la validità di tale decisione.

7. Tutta la mia analisi sarà guidata dalla ricerca di un equilibrio tra, da un lato, la necessità di dimostrare «un ragionevole grado di pragmatismo per consentire l'interazione con il resto del mondo» [7], e, dall'altro, la necessità di affermare i valori fondamentali riconosciuti negli ordinamenti giuridici dell'Unione e dei suoi Stati membri, in particolare dalla Carta.

II. Contesto normativo

A. Direttiva 95/46/CE

8. L'articolo 3, paragrafo 2, della direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [8] disponeva quanto segue:

«Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali;

5 Decisione 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 (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: la «decisione 2010/87»).

6 Decisione 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»).

7 V. discorso dell'ex garante europeo della protezione dei dati (GEPD) P. Hustinx, «Le droit de l'Union européenne sur la protection des données: la révision de la directive 95/46/CE et la proposition de règlement général sur la protection des données [il diritto dell'Unione europea in materia di protezione dei dati: la revisione della direttiva 95/46/CE e la proposta di regolamento generale sulla protezione dei dati]», pag. 49, disponibile all'indirizzo Internet https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_fr.pdf.

8 Direttiva del Parlamento europeo e del Consiglio, del 24 ottobre 1995 (GU 1995, L 281, pag. 31), come modificata dal regolamento (CE) no1882/2003 del Parlamento europeo e del Consiglio, del 29 settembre 2003 (GU 2003, L 284, pag. 1; in prosieguo: la «direttiva 95/46»).

– 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;

– (...)».

9. L'articolo 13, paragrafo 1, di tale direttiva così recitava:

Gli Stati membri possono adottare disposizioni legislative intese a limitare la portata degli obblighi e dei diritti previsti dalle disposizioni dell'articolo 6, paragrafo 1, dell'articolo 10, dell'articolo 11, paragrafo 1 e degli articoli 12 e 21, qualora tale restrizione costituisca una misura necessaria alla salvaguardia:

a) della sicurezza dello Stato;

b) della difesa;

c) della pubblica sicurezza;

d) della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate;

e) di un rilevante interesse economico o finanziario di uno Stato membro o dell'Unione europea, anche in materia monetaria, di bilancio e tributaria;

f) di un compito di controllo, ispezione o disciplina connesso, anche occasionalmente, con l'esercizio dei pubblici poteri nei casi di cui alle lettere c), d) ed e);

g) della protezione della persona interessata o dei diritti e delle libertà altrui».

10. L'articolo 25 di detta direttiva stabiliva quanto segue:

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

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

(...)

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».

11. L'articolo 26, paragrafi 2 e 4, della medesima 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 (...) 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».

12. L'articolo 28, paragrafo 3, della direttiva 95/46 era così formulato:

«Ogni autorità di controllo dispone in particolare:

(...)

– 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;

– (...)».

B. Il RGPD

13. In forza dell'articolo 94, paragrafo 1, il RGPD ha abrogato la direttiva 95/46 con effetto a decorrere dal 25 maggio 2018, data in cui tale regolamento ha iniziato ad essere applicato in conformità dell'articolo 99, paragrafo 1, dello stesso.

14. L'articolo 2, paragrafo 2, di detto regolamento così dispone:

«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;

(...)

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».

15. L'articolo 4, punto 2, del medesimo regolamento definisce il «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, 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».

16. L'articolo 23 del RGPD prevede quanto segue:

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

a) la sicurezza nazionale;

b) la difesa;

c) la sicurezza pubblica;

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

e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro (...);

(...)

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».

17. L'articolo 44 di tale regolamento, intitolato «Principio generale per il trasferimento», stabilisce quanto segue:

«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».

18. Conformemente all'articolo 45 di detto regolamento, intitolato «Trasferimento sulla base di una decisione di adeguatezza»:

«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 stato 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. (...)

4. La Commissione controlla su base continuativa gli sviluppi nei paesi terzi e nelle organizzazioni internazionali che potrebbero incidere sul funzionamento delle decisioni adottate a norma del paragrafo 3 del presente articolo e delle decisioni adottate sulla base dell'articolo 25, paragrafo 6, della [direttiva 95/46].

5. Se risulta dalle informazioni disponibili, in particolare in seguito al riesame di cui al paragrafo 3 del presente articolo, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale non garantiscono più un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, la Commissione revoca, modifica o sospende nella misura necessaria la decisione di cui al paragrafo 3 del presente articolo mediante atti di esecuzione senza effetto retroattivo. (...)

6. La Commissione avvia consultazioni con il paese terzo o l'organizzazione internazionale per porre rimedio alla situazione che ha motivato la decisione di cui al paragrafo 5.

(...)

9. Le decisioni adottate dalla Commissione in base all'articolo 25, paragrafo 6, della [direttiva 95/46] restano in vigore fino a quando non sono modificate, sostituite o abrogate da una decisione della Commissione adottata conformemente al paragrafo 3 o 5 del presente articolo».

19. L'articolo 46 del medesimo regolamento, intitolato «Trasferimento soggetto a garanzie adeguate, è formulato come segue:

«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:

(...)

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

(...)

5. Le autorizzazioni rilasciate da uno Stato membro o dall'autorità di controllo in base all'articolo 26, paragrafo 2, della [direttiva 95/46] restano valide fino a quando non vengono modificate, sostituite o abrogate, se necessario, dalla medesima autorità di controllo. Le decisioni adottate dalla Commissione in base all'articolo 26, paragrafo 4, della [direttiva 95/46] restano in vigore fino a quando non vengono modificate, sostituite o abrogate, se necessario, da una decisione della Commissione adottata conformemente al paragrafo 2 del presente articolo».

20. Ai sensi dell'articolo 58, paragrafi 2, 4 e 5, del RGPD:

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

a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento;

b) rivolgere ammonimenti al titolare (...) del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento;

c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento;

d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine;

e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;

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

(...)

i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso; e

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.

5. Ogni Stato membro dispone per legge che la sua autorità di controllo abbia il potere di intentare un'azione o di agire in sede giudiziale o, ove del caso, stragiudiziale in caso di violazione del presente regolamento per far rispettare le disposizioni dello stesso».

C. Decisione 2010/87

21. L'articolo 26, paragrafo 4 della direttiva 95/46 ha dato luogo all'adozione, da parte della Commissione, di tre decisioni con le quali essa ha constatato che le clausole contrattuali tipo ivi contenute costituiscono garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi (in prosieguo: le «decisioni CCT») [9].

22. Tra esse rientra la decisione 2010/87, il cui articolo 1 dispone che «[l]e 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]».

9 Decisione 2001/497/CE della Commissione, del 15 giugno 2001, relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva [95/46] (GU 2001, L 181, pag. 19); decisione 2004/915/CE della Commissione, del 27 dicembre 2004, che modifica la decisione [2001/497] per quanto riguarda l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi (GU 2004, L 385, pag. 74), nonché la decisione 2010/87.

23. Ai sensi dell'articolo 3 di tale decisione:

«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;

(...)».

24. Nella sua versione iniziale, l'articolo 4 di tale decisione prevedeva, al paragrafo 1, quanto segue:

«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».

25. Nella versione attuale, quale risulta dalla modifica della decisione 2010/87 introdotta dalla decisione di esecuzione (UE) 2016/2297[10], l'articolo 4 della decisione 2010/87 stabilisce che «[q]uando 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».

26. L'allegato della decisione 2010/87 contiene una serie di clausole contrattuali tipo. In particolare, la clausola 3 contenuta in tale allegato, 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. (...)

(...)».

27. La clausola 4 di detto allegato, intitolata «Obblighi dell'esportatore», così dispone:

«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;

c) che l'importatore fornirà sufficienti garanzie per quanto riguarda le misure tecniche e organizzative di sicurezza indicate nell'appendice 2;

d) che, alla luce della normativa sulla protezione dei dati, le misure di sicurezza sono atte a garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali, e che tali misure garantiscono un livello di sicurezza commisurato ai rischi inerenti al trattamento e alla natura dei dati da tutelare, tenuto conto della più recente tecnologia e dei costi di attuazione;

e) che provvederà all'osservanza delle misure di sicurezza;

10 Decisione della Commissione, del 16 dicembre 2016, che modifica la decisione [2001/497] relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva [95/46], e la decisione [2010/87] della Commissione 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 2016, L 344, pag. 100).

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;

h) che fornirà, su richiesta degli interessati, copia delle presenti clausole, esclusa l'appendice 2, e una descrizione generale delle misure di sicurezza, nonché copia dei subcontratti aventi ad oggetto il trattamento da effettuarsi in conformità delle presenti clausole, omettendo le informazioni commerciali eventualmente contenute nelle clausole o nel contratto;

i) che, in caso di subcontratto, il subincaricato svolge l'attività di trattamento in conformità della clausola 11 garantendo un livello di protezione dei dati personali e dei diritti dell'interessato quanto meno uguale a quello cui è tenuto l'importatore ai sensi delle presenti clausole;

j) che provvederà all'osservanza della clausola 4, lettere da a) ad i)».

28. La clausola 5, prevista nel medesimo allegato, intitolata «Obblighi dell'importatore» ([1]), così stabilisce:

«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;

c) di aver applicato le misure tecniche e organizzative di sicurezza indicate nell'appendice 2 prima di procedere al trattamento dei dati personali trasferiti;

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;

e) che risponderà prontamente e adeguatamente a tutte le richieste dell'esportatore relative al trattamento dei dati personali soggetti a trasferimento e che si conformerà al parere dell'autorità di controllo per quanto riguarda il trattamento dei dati trasferiti;

f) che sottoporrà i propri impianti di trattamento, su richiesta dell'esportatore, al controllo dell'esportatore o di un organismo ispettivo composto da soggetti indipendenti, in possesso delle necessarie qualificazioni professionali, vincolati da obbligo di riservatezza e selezionati dall'esportatore, eventualmente di concerto con l'autorità di controllo;

(...)».

29. Secondo la nota 1, cui rinvia il titolo della clausola 5 contenuta nell'allegato alla decisione 2010/87:

«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. Costituiscono esempi di disposizioni vincolanti che non vanno oltre quanto è necessario in una società democratica le sanzioni internazionalmente riconosciute, gli obblighi di informazione in materia fiscale o contro il riciclaggio di capitali».

30. La clausola 6 contenuta in tale allegato, 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, a meno che tutti gli obblighi dell'esportatore siano stati trasferiti, per contratto o per legge, all'eventuale successore, nel qual caso l'interessato può far valere i suoi diritti nei confronti del successore.

(...)»

31. La clausola 7 prevista in detto allegato, intitolata «Mediazione e giurisdizione», dispone quanto segue:

«1. L'importatore dichiara che qualora l'interessato faccia valere il diritto del terzo beneficiario e/o chieda il risarcimento dei danni in base alle presenti clausole, egli accetterà la decisione dello stesso interessato:

a) di sottoporre la controversia alla mediazione di un terzo indipendente o eventualmente dell'autorità di controllo;

b) di deferire la controversia agli organi giurisdizionali dello Stato membro in cui è stabilito l'esportatore.

2. Le parti dichiarano che la scelta compiuta dall'interessato non pregiudica i diritti sostanziali o procedurali spettanti allo stesso relativamente ai rimedi giuridici previsti dalla normativa nazionale o internazionale».

32. La clausola 9 contenuta nel medesimo allegato, intitolata «Legge applicabile», prevede che le clausole contrattuali tipo siano disciplinate dalla legge dello Stato membro in cui è stabilito l'esportatore.

D. Decisione «scudo per la privacy»

33. L'articolo 25, paragrafo 6, della direttiva 95/46 ha costituito la base per l'adozione, da parte della Commissione, di due decisioni successive con le quali essa ha constatato che gli Stati Uniti assicurano un livello adeguato di protezione dei dati personali trasferiti a imprese stabilite negli Stati Uniti che hanno dichiarato di aderire, mediante una procedura di autocertificazione, ai principi enunciati in tali decisioni.

34. In un primo tempo, la Commissione ha adottato la decisione 2000/520/CE 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 [11]. Nella sentenza del 6 ottobre 2015, Schrems [12], la Corte ha dichiarato invalida tale decisione.

35. In seguito a tale sentenza, la Commissione ha adottato, in un secondo tempo, la decisione «scudo per la privacy».

36. L'articolo 1 di tale decisione dispone quanto segue:

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

2. Lo scudo UE-USA 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».

37. L'allegato III A di tale decisione, intitolato «Meccanismo di mediazione dello scudo UE-USA per la privacy in materia di intelligence dei segnali», allegato a una lettera dell'allora Secretary of State (Segretario di Stato, Stati Uniti) John Kerry, datata 7 luglio 2016, contiene un memorandum che descrive una nuova procedura di mediazione con un «Primo coordinatore della diplomazia internazionale per le tecnologie dell'informazione» (in prosieguo: il «mediatore») nominato dal Segretario di Stato.

38. Secondo tale memorandum, detta procedura è stata istituita «secondo modalità consolidate conformi alla legge e alla politica degli [Stati Uniti], per facilitare il trattamento delle domande di accesso motivate dalla sicurezza nazionale ai dati trasmessi dall'[Unione] agli Stati Uniti nell'ambito dello scudo, delle clausole contrattuali tipo, delle norme vincolanti d'impresa, delle "deroghe" o delle "eventuali deroghe future" così come la risposta a tali domande».

11 Decisione del 26 luglio 2000, a norma della direttiva [95/46] (GU 2000, L 215, pag. 7, in prosieguo: la «decisione "approdo sicuro"»).

12 C-362/14 (EU:C:2015:650; in prosieguo: la «sentenza Schrems»).

III. Procedimento principale, questioni pregiudiziali e procedimento dinanzi alla Corte

39. Il signor Schrems, cittadino austriaco residente in Austria, è un utente della rete sociale Facebook. Tutti gli utenti di tale social network, residenti nel territorio dell'Unione, sono tenuti a concludere, al momento dell'iscrizione, un contratto con Facebook Ireland, una controllata di Facebook Inc., la quale ha, a sua volta, sede negli Stati Uniti. I dati personali di tali utenti sono trasferiti, in tutto o in parte, su server di proprietà di Facebook Inc., situati nel territorio degli Stati Uniti, ove vengono trattati.

40. Il 25 giugno 2013, il sig. Schrems ha presentato una denuncia al DPC in cui chiedeva, in sostanza, a quest'ultimo di vietare a Facebook Ireland di trasferire i suoi dati personali negli Stati Uniti. In tale denuncia egli faceva valere che il diritto e le prassi vigenti in tale paese terzo non garantivano una protezione sufficiente dei dati personali conservati nel suo territorio contro le ingerenze derivanti rispetto alle attività di sorveglianza ivi svolte dalle autorità pubbliche. Il sig. Schrems si riferiva, a tal riguardo, alle rivelazioni fatte dal sig. Edward Snowden in merito alle attività dei servizi di intelligence degli Stati Uniti, e in particolare a quelle della National Security Agency (NSA) (Agenzia per la sicurezza nazionale, Stati Uniti).

41. Tale denuncia è stata respinta con la motivazione, in particolare, che qualsiasi questione relativa all'adeguatezza della protezione garantita negli Stati Uniti doveva essere decisa conformemente alla decisione «approdo sicuro». In tale decisione la Commissione aveva constatato che il suddetto paese terzo offriva un livello adeguato di protezione dei dati personali trasferiti a imprese situate nel suo territorio, aderendo ai principi stabiliti nella decisione stessa.

42. Il sig. Schrems ha proposto ricorso contro la decisione di rigetto della denuncia dinanzi alla High Court (Alta Corte). Tale giudice ha considerato che, sebbene il sig. Schrems non avesse formalmente rimesso in discussione la validità della decisione «approdo sicuro», il suo reclamo denunciava effettivamente la legittimità del regime istituito da tale decisione. In tali circostanze, detto giudice ha sottoposto alla Corte questioni volte, in sostanza, ad accertare se le autorità degli Stati membri responsabili della protezione dei dati (in prosieguo: le «autorità di controllo») – quando ricevono una denuncia relativa alla protezione dei diritti e delle libertà di una persona in relazione al trattamento dei dati personali che la riguardano e che sono stati trasferiti in uno Stato terzo – siano vincolate dalle constatazioni sull'adeguatezza del livello di protezione offerto da tale Stato terzo, effettuate dalla Commissione ai sensi dell'articolo 25, paragrafo 6, della direttiva 95/46, anche se il denunciante contesta tali constatazioni.

43. Dopo aver stabilito, ai punti 51 e 52 della sentenza Schrems, che una decisione di adeguatezza vincola le autorità di controllo fino a che essa non sia stata dichiarata invalida, la Corte ha dichiarato quanto segue ai punti 63 e 65 di tale sentenza:

«63. (...) [Q]ualora una persona i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo che è stato oggetto di una decisione della Commissione in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, investa un'autorità nazionale di controllo di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di tali dati e contesti, in occasione di tale domanda (...) la compatibilità di tale decisione con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona, incombe a tale autorità esaminare detta domanda con tutta la diligenza richiesta.

(...)

65. Nell'ipotesi (...) in cui detta autorità reputi fondate le censure sollevate [da tale persona], questa stessa autorità, ai sensi dell'articolo 28, paragrafo 3, primo comma, terzo trattino, della direttiva 95/46, in combinato, segnatamente, con l'articolo 8, paragrafo 3, della Carta, deve poter promuovere azioni giudiziarie. A tal riguardo, incombe al legislatore nazionale prevedere mezzi di ricorso che consentano

all'autorità nazionale di controllo di cui trattasi di far valere le censure che essa reputa fondate dinanzi ai giudici nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di tale autorità in ordine alla validità della decisione della Commissione, ad un rinvio pregiudiziale inteso all'esame della validità di tale decisione».

44. La Corte ha inoltre esaminato, in tale sentenza, la validità della decisione «approdo sicuro» alla luce dei requisiti derivanti dalla direttiva 95/46, in combinato disposto con la Carta. Al termine di tale esame, essa ha dichiarato invalida tale decisione [13].

45. In seguito alla sentenza Schrems il giudice del rinvio ha annullato la decisione con la quale il DPC aveva respinto la denuncia del sig. Schrems e l'ha rinviata al DPC per riesame. Quest'ultimo ha avviato un'indagine e ha invitato il sig. Schrems a riformulare la denuncia, tenuto conto dell'annullamento della decisione «approdo sicuro».

46. A tal fine, il sig. Schrems ha chiesto a Facebook Ireland di individuare le basi giuridiche su cui riposa il trasferimento dei dati personali degli utenti della rete sociale Facebook dall'Unione agli Stati Uniti. Facebook Ireland, senza individuare tutte le basi giuridiche su cui si basa, ha fatto riferimento a un accordo di trasferimento e di trattamento dei dati (*data transfer processing agreement*) concluso tra la stessa e Facebook Inc., applicabile dal 20 novembre 2015, e ha invocato la decisione 2010/87.

47. Nella denuncia riformulata il sig. Schrems fa valere, da un lato, che le clausole contenute in tale accordo non sono conformi alle clausole contrattuali tipo contenute nell'allegato alla decisione 2010/87. D'altro lato, il sig. Schrems sostiene che tali clausole contrattuali tipo non potrebbero, in ogni caso, costituire la base del trasferimento negli Stati Uniti dei dati personali che lo riguardano. Ciò avverrebbe in quanto il diritto statunitense impone a Facebook Inc. di mettere i dati personali degli utenti a disposizione delle autorità statunitensi, come la NSA e il Federal Bureau of Investigation (FBI) (Ufficio investigativo federale, Stati Uniti), nell'ambito di programmi di sorveglianza che ostacolerebbero l'esercizio dei diritti garantiti dagli articoli 7, 8 e 47 della Carta. Il sig. Schrems sostiene che gli interessati non dispongono di alcun mezzo di ricorso per far valere i loro diritti al rispetto della vita privata e alla protezione dei dati personali. In tali circostanze, il sig. Schrems chiede al DPC di sospendere tale trasferimento ai sensi dell'articolo 4 della decisione 2010/87.

48. Facebook Ireland ha riconosciuto, nell'ambito dell'indagine del DPC, di continuare a trasferire negli Stati Uniti i dati personali degli utenti della rete sociale Facebook residenti nell'Unione e di basarsi, a tal fine, in gran parte sulle clausole contrattuali tipo contenute nell'allegato alla decisione 2010/87.

49. L'indagine del DPC mirava a stabilire, da un lato, se gli Stati Uniti garantiscano un'adeguata protezione dei dati personali dei cittadini dell'Unione e, dall'altro, in caso di risposta negativa, se le decisioni CCT forniscano garanzie sufficienti per quanto riguarda la protezione dei loro diritti e libertà fondamentali.

50. A tale riguardo, in un progetto di decisione (*draft decision*), il DPC ha ritenuto, in via provvisoria, che il diritto statunitense non offra mezzi di ricorso efficaci, ai sensi dell'articolo 47 della Carta, per i cittadini dell'Unione i cui dati sono trasferiti negli Stati Uniti, ove rischiano di essere trattati dalle agenzie statunitensi per finalità di sicurezza nazionale in modo incompatibile con gli articoli 7 e 8 della Carta. Le garanzie previste dalle clausole contenute in allegato alle decisioni CCT non porrebbero rimedio a tale lacuna, in quanto non sono vincolanti per le autorità o agenzie statunitensi e conferiscono agli interessati soltanto diritti contrattuali nei confronti dell'esportatore e/o dell'importatore dei dati.

13 V. sentenza Schrems (punto 106).

51. In tali circostanze, il DPC ha ritenuto di non potersi pronunciare sulla denuncia del sig. Schrems senza che la Corte esamini la validità delle decisioni CCT. Conformemente al punto 65 della sentenza Schrems, il DPC ha quindi avviato un procedimento dinanzi al giudice del rinvio affinché quest'ultimo, qualora condivida i dubbi del DPC, investa la Corte di un rinvio pregiudiziale sulla validità di tali decisioni.

52. Il governo degli Stati Uniti, l'Electronic Privacy Information Centre (EPIC), la Business Software Alliance (BSA) e Digitaleurope sono stati autorizzati a intervenire dinanzi al giudice del rinvio.

53. Al fine di stabilire se condivide i dubbi espressi dal DPC sulla validità delle decisioni CCT, la High Court (Alta Corte) ha ricevuto le prove prodotte dalle parti della controversia e ha ascoltato le argomentazioni presentate da queste ultime e dagli intervenienti. In particolare, le disposizioni del diritto statunitense sono state oggetto di prova mediante periti. In diritto irlandese, il diritto estero è considerato una questione di fatto da dimostrare mediante prove allo stesso modo di qualsiasi altro fatto. In base a tali prove, il giudice del rinvio ha valutato le disposizioni di diritto statunitense che autorizzano la sorveglianza da parte delle autorità e agenzie governative, il funzionamento di due programmi di sorveglianza pubblicamente riconosciuti («PRISM» e «Upstream»), i vari mezzi di ricorso a disposizione dei singoli i cui diritti sono stati violati da misure di sorveglianza, nonché le garanzie sistemiche e i meccanismi di controllo. Tale giudice ha documentato i risultati di tale valutazione in una sentenza del 3 ottobre 2017, allegata alla sua ordinanza di rinvio [in prosieguo: la «sentenza della High Court (Alta Corte) del 3 ottobre 2017»].

54. In tale sentenza il giudice del rinvio ha fatto riferimento, tra le basi giuridiche che autorizzano l'intercettazione di comunicazioni estere da parte dei servizi di intelligence statunitensi, all'articolo 702 del Foreign Intelligence and Surveillance Act (FISA) (legge sulla sorveglianza in materia di intelligence esterna) e all'Executive Order 12333 (decreto presidenziale n. 12333, in prosieguo: l'«EO 12333»).

55. Secondo le constatazioni effettuate in tale sentenza, l'articolo 702 del FISA consente all'Attorney General (procuratore generale, Stati Uniti) e al Director of National Intelligence (DNI) (direttore dell'intelligence nazionale, Stati Uniti) di autorizzare congiuntamente, per un periodo di un anno, al fine di ottenere informazioni in materia di intelligence esterna, la sorveglianza di persone che non sono cittadini statunitensi e che non risiedono in modo permanente negli Stati Uniti (le cosiddette «persone non statunitensi»), quando è ragionevole ritenere che si trovino al di fuori del territorio degli Stati Uniti [14]. Secondo il FISA, la nozione di «intelligence esterna» si riferisce alle informazioni relative alla capacità del governo di cautelarsi contro gli attacchi stranieri, il terrorismo, la proliferazione delle armi di distruzione di massa e la gestione degli affari esteri statunitensi [15].

56. Tali autorizzazioni annuali, al pari delle procedure che regolano l'individuazione mirata delle persone da sottoporre a sorveglianza e il trattamento («minimizzazione») delle informazioni raccolte [16], devono essere approvate dal Foreign Intelligence Surveillance Court (FISC; in prosieguo: la «Corte FISA») (tribunale per la sorveglianza dell'intelligence esterna, Stati Uniti). Mentre la sorveglianza «tradizionale» effettuata in base ad altre disposizioni del FISA richiede l'accertamento di una «probabile causa» per sospettare che le persone sottoposte a sorveglianza appartengano a una potenza straniera o ne siano gli agenti, le attività di sorveglianza esercitate ai sensi dell'articolo 702 del FISA

14 50 U.S.C. 1881 (a).

15 50 U.S.C. 1881 (e).

16 Il giudice del rinvio ha constatato che le procedure di individuazione mirata riguardano il modo in cui il potere esecutivo stabilisce che è ragionevole ritenere che un particolare individuo sia una persona non statunitense che si trova al di fuori degli Stati Uniti e che l'individuazione mirata di tale soggetto può portare all'acquisizione di informazioni in materia di intelligence esterna. Le procedure di minimizzazione comprendono l'acquisizione, la conservazione, l'uso e la diffusione di qualsiasi informazione non pubblica riguardante una persona statunitense acquisita ai sensi dell'articolo 702 del FISA.

non sono soggette né all'accertamento di tale «probabile causa» né all'approvazione, da parte della Corte FISA, dell'individuazione mirata di persone determinate. Inoltre, sempre secondo le constatazioni del giudice del rinvio, le procedure di minimizzazione non si applicano alle persone non statunitensi che si trovino al di fuori degli Stati Uniti.

57. In pratica, una volta che l'autorizzazione è stata concessa dalla Corte FISA, la NSA invia ai fornitori di servizi di comunicazione elettronica stabiliti negli Stati Uniti istruzioni contenenti criteri di ricerca, chiamati «selettori», associati a persone individuate specificamente (come numeri di telefono o indirizzi di posta elettronica). Tali fornitori sono allora obbligati a trasmettere alla NSA i dati corrispondenti ai selettori e devono tenere segrete le istruzioni loro rivolte. Essi possono presentare alla Corte FISA una domanda diretta alla modifica o al rigetto di un'istruzione della NSA. La decisione della Corte FISA può essere impugnata presso il Foreign Intelligence Surveillance Court of Review (FISCR) (Tribunale per la revisione in materia di sorveglianza dell'intelligence esterna, Stati Uniti).

58. La High Court (Alta Corte) ha constatato che l'articolo 702 del FISA funge da base giuridica per i programmi PRISM e Upstream.

59. Nell'ambito del programma PRISM, i fornitori di servizi di comunicazione elettronica sono tenuti a sottoporre alla NSA tutte le comunicazioni «dal» o «verso il» selettore comunicato da quest'ultima. Una parte di tali comunicazioni sarebbe trasmessa all'FBI e alla Central Intelligence Agency (CIA) (Agenzia centrale di intelligence, Stati Uniti). Nel 2015, 94 386 persone sarebbero state sottoposte a sorveglianza e, nel 2011, il governo degli Stati Uniti avrebbe acquisito oltre 250 milioni di comunicazioni nell'ambito di tale programma.

60. Il programma Upstream si basa sull'assistenza obbligatoria delle imprese che gestiscono la «dorsale» – ossia la rete di cavi, commutatori e router – su cui transitano le comunicazioni telefoniche e le comunicazioni Internet. Tali imprese sono tenute a consentire alla NSA di copiare e di filtrare i flussi di traffico Internet al fine di acquisire comunicazioni «da», «verso» o «riguardanti» un selettore menzionato in una istruzione di tale agenzia. Le comunicazioni «riguardanti» un selettore sono quelle che fanno riferimento a tale selettore, senza che la persona non statunitense associata a detto selettore prenda necessariamente parte ad esse. Sebbene da un parere della Corte FISA, del 26 aprile 2017, risulti che, a partire da tale data, il governo statunitense non raccoglie né acquisisce più comunicazioni «riguardanti» un selettore, tale parere non specifica che la NSA abbia cessato di copiare e di filtrare i flussi di comunicazioni che transitano per il suo sistema di sorveglianza. Il programma Upstream implicherebbe infatti l'accesso, da parte della NSA, tanto ai metadati quanto al contenuto delle comunicazioni. Dal 2011 la NSA avrebbe raccolto circa 26,5 milioni di comunicazioni all'anno nell'ambito del programma Upstream, il che, tuttavia, rappresenterebbe solo una piccola parte delle comunicazioni assoggettate al processo di screening di tale programma.

61. Inoltre, secondo le constatazioni della High Court (Alta Corte), l'EO 12333 autorizza la sorveglianza di comunicazioni elettroniche al di fuori del territorio degli Stati Uniti consentendo l'accesso, a fini di intelligence esterna, a dati «in transito» verso tale territorio, oppure «che transitano» attraverso tale territorio senza essere destinati a subirvi un trattamento, nonché la raccolta e la conservazione di tali dati. L'EO 12333 definisce la nozione di «intelligence esterna» nel senso che essa include le informazioni relative alle capacità, intenzioni o attività di governi, organizzazioni o individui stranieri [17].

17 EO 12333, punto 3.5, lettera e).

62. L'EO 12333 autorizzerebbe la NSA ad accedere ai cavi sottomarini, che si trovano sul fondale dell'oceano Atlantico, attraverso i quali i dati sono trasferiti dall'Unione agli Stati Uniti, prima che i dati stessi raggiungano gli Stati Uniti e siano quindi soggetti alle disposizioni del FISA. Tuttavia, non vi sono prove di un qualsivoglia programma attuato ai sensi di tale decreto presidenziale.

63. Sebbene l'EO 12333 preveda limiti riguardanti la raccolta, la conservazione e la diffusione di informazioni, tali limiti non si applicano alle persone non statunitensi. Queste ultime beneficiano unicamente delle garanzie stabilite dalla Presidential Policy Directive 28 (direttiva strategica presidenziale n. 28; in prosieguo: la «PPD 28»), che si applica a tutte le attività di raccolta e uso di informazioni in materia di intelligence esterna di origine elettromagnetica. La PPD 28 dispone che il rispetto della vita privata costituisce parte integrante delle considerazioni di cui tener conto nella pianificazione di tali attività, che l'unico scopo della raccolta deve essere l'acquisizione di informazioni in materia di intelligence esterna e di controspionaggio, e che dette attività devono essere «il più possibile mirate».

64. Secondo il giudice del rinvio, le attività della NSA basate sull'EO 12333, che può essere modificato o revocato in qualsiasi momento dal Presidente degli Stati Uniti, non sono disciplinate dalla legge, non sono soggette a controllo giurisdizionale e non possono essere oggetto di ricorsi giurisdizionali.

65. Sulla base di tali constatazioni, detto giudice considera che gli Stati Uniti procedono a trattamenti massicci e indiscriminati di dati personali che potrebbero esporre gli interessati al rischio di violazione dei loro diritti ai sensi degli articoli 7 e 8 della Carta.

66. Inoltre, detto giudice precisa che i cittadini dell'Unione non hanno accesso agli stessi mezzi di ricorso, contro i trattamenti illeciti dei loro dati personali da parte delle autorità statunitensi, cui hanno accesso i cittadini statunitensi. Il quarto emendamento alla Costituzione degli Stati Uniti, che costituirebbe la protezione più importante contro la sorveglianza illecita, non sarebbe applicabile ai cittadini dell'Unione europea che non presentano un legame volontario e significativo con gli Stati Uniti. Sebbene essi dispongano comunque di altri mezzi di ricorso, si troverebbero ad affrontare ostacoli significativi.

67. In particolare, l'articolo III della Costituzione degli Stati Uniti subordina qualsiasi ricorso dinanzi ai giudici federali alla dimostrazione, da parte dell'interessato, della sua legittimazione ad agire (*standing*). La legittimazione ad agire presuppone, in particolare, che tale persona dimostri di aver subito un danno effettivo che sia, da un lato, concreto e specifico, e, dall'altro, attuale o imminente. Riferendosi, tra l'altro, alla sentenza della Supreme Court of the United States (Corte suprema degli Stati Uniti), Clapper v. Amnesty International US [18], il giudice del rinvio ritiene che tale condizione sia, in pratica, eccessivamente difficile da soddisfare, tenuto conto, in particolare, della mancanza di qualsiasi obbligo di informare gli interessati riguardo alle misure di sorveglianza adottate nei loro confronti [19]. Una parte dei mezzi di ricorso a disposizione dei cittadini dell'Unione sarebbe, inoltre, soggetta al rispetto di altre condizioni restrittive, come la necessità di dimostrare un danno pecuniario. L'immunità sovrana riconosciuta alle agenzie di intelligence e la classificazione delle informazioni in questione osterebbero anch'esse all'utilizzo di taluni mezzi di ricorso [20].

68. La High Court (Alta Corte) menziona inoltre vari meccanismi di controllo e di supervisione delle attività delle agenzie di intelligence.

18 133 S.Ct. 1138 (2013).

19 Il giudice del rinvio ha tuttavia constatato che il principio secondo cui non è richiesta la notifica alla persona soggetta ad una misura di sorveglianza incontra un'eccezione qualora il governo statunitense intenda utilizzare i dati raccolti ai sensi dell'articolo 702 del FISA nei confronti di tale persona nell'ambito di un procedimento penale o amministrativo.

20 In particolare, il giudice del rinvio ha rilevato che, sebbene il Judicial Redress Act (JRA) (legge sulla tutela giurisdizionale) abbia esteso ai cittadini dell'Unione le disposizioni del Privacy Act (legge sulla tutela della vita privata), che consente alle persone fisiche di accedere alle informazioni che le riguardano in possesso di determinate agenzie in relazione a determinati paesi terzi, la NSA non rientra fra le agenzie designate ai sensi del JRA.

69. Tra questi rientrano, da un lato, il meccanismo di certificazione annuale, da parte della Corte FISA, dei programmi basati sull'articolo 702 del FISA, nell'ambito del quale la Corte FISA non approva, tuttavia, i singoli selettori. Inoltre, nessun controllo giurisdizionale preventivo disciplina la raccolta di informazioni in materia di intelligence esterna ai sensi dell'EO 12333.

70. D'altro lato, il giudice del rinvio fa riferimento a diversi meccanismi di controllo extragiudiziale delle attività di intelligence. In particolare, esso menziona il ruolo degli Inspectors General (ispettori generali, Stati Uniti) che, all'interno di ciascuna agenzia di intelligence, sono responsabili della supervisione delle attività di sorveglianza. Inoltre, il Privacy and Civil Liberties Oversight Board (PCLOB) (consiglio di sorveglianza della vita privata e delle libertà civili, Stati Uniti), un'agenzia indipendente all'interno del potere esecutivo, riceve le relazioni di persone designate all'interno di ogni agenzia quali responsabili per le libertà civili o per la privacy (*civil liberties or privacy officers*). Il PCLOB redige regolarmente relazioni destinate alle commissioni parlamentari e al Presidente. Le agenzie interessate devono portare all'attenzione, in particolare del DNI, i casi di inosservanza delle norme e delle procedure relative alla raccolta di informazioni di intelligence esterna. Anche questi casi sono segnalati alla Corte FISA. Il Congresso degli Stati Uniti, attraverso le commissioni di intelligence della Camera e del Senato, è anch'esso responsabile del controllo delle attività di intelligence esterna.

71. Tuttavia, la High Court (Alta Corte) sottolinea la differenza fondamentale tra, da un lato, le norme volte a garantire che i dati siano ottenuti legittimamente e che, una volta ottenuti, non ne sia fatto abuso e, dall'altro, i mezzi di ricorso disponibili in caso di violazione di tali norme. La tutela dei diritti fondamentali degli interessati sarebbe garantita solo mezzi di ricorso effettivi consentano loro di far valere i propri diritti in caso di inosservanza di tali norme.

72. In tali circostanze, il giudice del rinvio considera fondati gli argomenti, fatti valere dal DPC, secondo i quali le limitazioni imposte dal diritto statunitense al diritto di ricorso dei soggetti, i cui dati sono trasferiti dall'Unione, non rispettano il contenuto essenziale del diritto garantito dall'articolo 47 della Carta e, in ogni caso, costituiscono un'ingerenza sproporzionata nell'esercizio di tale diritto.

73. Secondo la High Court (Alta Corte), l'introduzione, da parte del governo degli Stati Uniti, del meccanismo di mediazione descritto nella decisione «scudo per la privacy» non rimette in discussione tale valutazione. Dopo aver sottolineato che tale meccanismo è accessibile ai cittadini dell'Unione che ritengono, su base ragionevole, che i loro dati siano stati trasferiti conformemente alle decisioni CCT[21], tale giudice ha osservato che il Mediatore non è un organo giurisdizionale che soddisfa i requisiti di cui all'articolo 47 della Carta e, in particolare, non è indipendente dal potere esecutivo[22]. Detto giudice dubita inoltre che l'intervento del mediatore, le cui decisioni non possono essere oggetto di un ricorso giurisdizionale, rappresenti un mezzo di ricorso effettivo. Infatti, tale intervento non consente alle persone i cui dati personali sono stati raccolti, trattati o condivisi illegalmente di ottenere un risarcimento o un'ingiunzione a porre fine agli atti illeciti, in quanto il Mediatore non conferma né nega che un richiedente sia stato oggetto di una misura di sorveglianza elettronica.

74. Dopo aver così esposto le proprie preoccupazioni riguardo all'equivalenza sostanziale tra le garanzie previste dal diritto statunitense e i requisiti derivanti dagli articoli 7, 8 e 47 della Carta, il giudice del rinvio ha espresso dubbi quanto al fatto che le clausole contrattuali tipo previste dalle decisioni CCT – che, per loro natura, non sono vincolanti per le autorità statunitensi – possano comunque garantire la tutela dei diritti fondamentali degli interessati. Detto giudice ne ha concluso che condivide i dubbi del DPC circa la validità di tali decisioni.

21 Il giudice del rinvio fa riferimento, a tal proposito, all'allegato III A della decisione «scudo per la privacy» (v. paragrafi 37 e 38 delle presenti conclusioni).

22 Il giudice del rinvio menziona la sentenza 27 gennaio 2005, Denuit e Cordenier (C-125/04, EU:C:2005:69, punto 12).

75. A tale riguardo, il giudice del rinvio considera, in particolare, che l'articolo 28, paragrafo 3, della direttiva 95/46, cui fa riferimento l'articolo 4 della decisione 2010/87, poiché riconosce alle autorità di controllo il potere di sospendere o di vietare i trasferimenti basati sulle clausole contrattuali tipo previste da tale decisione, non è sufficiente a dissipare tali dubbi. Oltre al fatto che, a suo avviso, tale potere ha carattere esclusivamente discrezionale, il giudice del rinvio si chiede, alla luce del considerando 11 della decisione 2010/87, se esso possa essere esercitato quando le carenze riscontrate non riguardano un caso particolare ed eccezionale, ma hanno carattere generale e sistemico [23]. Tale giudice considera altresì che il rischio che siano pronunciate decisioni divergenti nei diversi Stati membri potrebbe ostare a che la constatazione di tali carenze sia affidata alle autorità di controllo.

76. In tali circostanze, la High Court (Alta Corte) ha deciso, con provvedimento del 4 maggio 2018 [24], pervenuto alla cancelleria della Corte il 9 maggio 2018, di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se, in circostanze 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 2010/87] 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 in relazione alla sicurezza nazionale e le disposizioni di cui al primo trattino dell'articolo 3, paragrafo 2, della [direttiva 95/46] in relazione 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 [2010/87], 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 (in prosieguo: la "CEDU" (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 nell'ambito della 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:

   a) le 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;

23 Nel considerando 11 della decisione 2010/87 si dichiara quanto segue: «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».

24 Facebook Ireland ha interposto appello contro la decisione di rinvio dinanzi alla Supreme Court (Corte Suprema, Irlanda). Tale appello è stato respinto con sentenza del 31 maggio 2019, The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems, Appeal n. 2018/68 [in prosieguo: la «sentenza della Supreme Court (Corte suprema) del 31 maggio 2019»].

oppure

b) le 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, considerando i 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 [2010/87] violi i diritti degli individui ai sensi degli articoli 7 e/o 8 della Carta.

5) Se, considerando i 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 [2010/87]:

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 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 di sicurezza nazionale.

6) a) 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] alla luce delle disposizioni [di tale direttiva], e in particolare [dei suoi] articoli 25 e 26, letti alla luce della Carta.

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 [2010/87] 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 l'ulteriore trattamento i dati personali trasferiti ai sensi delle clausole di cui alla decisione [2010/87], escluda che le clausole offrano garanzie sufficienti, come previsto 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 di controllo], sono in contrasto con le clausole tipo o con gli articoli 25 e 26 della direttiva [95/46] e/o con la Carta, un'[autorità di controllo] 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 oppure se l'esercizio di tali poteri sia limitato solo ai casi eccezionali, alla luce del considerando 11 della decisione [2010/87], oppure se un'[autorità di controllo] 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 di controllo] e i giudici degli Stati membri, nel senso che 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 svolta sull'adeguatezza delle garanzie fornite ai dati trasferiti verso gli Stati Uniti ai sensi della decisione [2010/87].

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 III A] della decisione ["scudo per la privacy"], congiuntamente al regime in vigore negli Stati Uniti, garantisca che gli Stati Uniti prevedano un mezzo di ricorso in favore degli interessati i cui dati personali sono trasferiti negli Stati Uniti ai sensi della decisione [2010/87] che sia compatibile con l'articolo 47 della Carta.

11) Se la decisione [2010/87] violi gli articoli 7, 8 e/o 47 della Carta».

77. Il DPC, Facebook Ireland, il sig. Schrems, il governo degli Stati Uniti, l'EPIC, la BSA, Digitaleurope, l'Irlanda, i governi belga, ceco, tedesco, dei Paesi Bassi, austriaco, polacco, portoghese e del Regno Unito, il Parlamento europeo e la Commissione hanno presentato osservazioni scritte alla Corte. Il DPC, Facebook Ireland, il sig. Schrems, il governo degli Stati Uniti, l'EPIC, la BSA, Digitaleurope, l'Irlanda, i governi tedesco, francese, dei Paesi Bassi, austriaco e del Regno Unito, il Parlamento, la Commissione e il comitato europeo per la protezione dei dati (EDPB) sono stati rappresentati all'udienza del 9 luglio 2019.

IV. Analisi

A. Considerazioni preliminari

78. A seguito dell'annullamento della decisione «approdo sicuro», da parte della Corte nella sentenza Schrems, i trasferimenti di dati personali verso gli Stati Uniti sono proseguiti in base ad altri fondamenti giuridici. In particolare, le società esportatrici hanno potuto ricorrere a contratti con importatori contenenti clausole tipo elaborate dalla Commissione. Tali clausole fungono altresì da base giuridica per i trasferimenti verso molti altri paesi terzi riguardo ai quali la Commissione non ha adottato una decisione di adeguatezza [25]. La decisione «scudo per la privacy» consente ormai alle imprese che abbiano autocertificato la loro adesione ai principi ivi enunciati di trasferire dati personali verso gli Stati Uniti senza ulteriori formalità.

79. Come espressamente dichiarato nella decisione di rinvio e come sottolineato dalla BSA, da Digitaleurope, dall'Irlanda, dai governi austriaco e francese, dal Parlamento e dalla Commissione, il procedimento principale, pendente dinanzi alla High Court (Alta Corte), ha come unico scopo quello di determinare se sia valida la decisione con cui la Commissione ha introdotto le clausole contrattuali tipo fatte valere a sostegno dei trasferimenti menzionati nella denuncia del sig. Schrems, vale a dire la decisione 2010/87 [26].

80. La presente controversia ha origine da una domanda con la quale il DPC ha chiesto al giudice del rinvio di sottoporre alla Corte una questione pregiudiziale relativa alla validità della decisione 2010/87. A detta di tale giudice, il procedimento principale riguarda, pertanto, l'esercizio del mezzo di ricorso che la Corte ha imposto agli Stati membri di prevedere al punto 65 della sentenza Schrems.

25 La BSA afferma che il 70% delle imprese ad essa aderenti, che hanno risposto a un'indagine in materia, hanno dichiarato di aver fatto ricorso a clausole contrattuali tipo come base principale per i trasferimenti di dati personali verso paesi terzi. Digitaleurope ritiene inoltre che le clausole contrattuali tipo rappresentino il principale strumento giuridico invocato a sostegno di tali trasferimenti.

26 Sebbene il giudice del rinvio precisi che la sua domanda di pronuncia pregiudiziale riguarda la validità delle tre decisioni CCT, essendo esse esaminate nel progetto di decisione DPC e nella sentenza del 3 ottobre 2017, le questioni pregiudiziali si riferiscono esclusivamente alla decisione 2010/87. Ciò avviene anche per il fatto che, dinanzi a tale giudice, Facebook Ireland ha individuato tale decisione quale base giuridica dei trasferimenti di dati degli utenti europei della rete sociale Facebook verso gli Stati Uniti. La mia analisi verterà quindi esclusivamente su tale decisione.

81. Si ricorda che la Corte ha statuito, al punto 63 di tale sentenza, che l'autorità di controllo è tenuta a trattare con la dovuta diligenza una denuncia con la quale una persona, i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo che è stato oggetto di una decisione di adeguatezza, contesta la compatibilità di tale decisione con i diritti fondamentali sanciti dalla Carta. Secondo il punto 65 di tale sentenza, nell'ipotesi in cui detta autorità reputi fondate le censure sollevate in tale denuncia, essa deve, ai sensi dell'articolo 28, paragrafo 3, primo comma, terzo trattino, della direttiva 95/46 (al quale corrisponde l'articolo 58, paragrafo 5, del RGPD, in combinato con l'articolo 8, paragrafo 3, della Carta, poter promuovere azioni giudiziarie.

A tal riguardo, il legislatore nazionale deve prevedere mezzi di ricorso che gli consentano di far valere tali censure dinanzi ai giudici nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di tale autorità, ad un rinvio pregiudiziale riguardante la validità della decisione di cui trattasi.

82. Al pari del giudice del rinvio, ritengo che tali conclusioni si applichino per analogia nel caso in cui, in sede di trattamento di una denuncia di cui è investita, un'autorità di controllo nutra dubbi sulla validità non di una decisione di adeguatezza, ma di una decisione, come la decisione 2010/87, che stabilisce clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi. Contrariamente a quanto sostiene il governo tedesco, non ha rilevanza il fatto che tali dubbi corrispondano a censure portate alla sua attenzione dall'autore della denuncia o che tale autorità, di sua iniziativa, rimetta in discussione la validità della decisione di cui trattasi. Infatti, i requisiti derivanti dall'articolo 58, paragrafo 5, del RGPD e dall'articolo 8, paragrafo 3, della Carta, su cui si basa la motivazione della Corte, si applicano indipendentemente dal fondamento giuridico del trasferimento oggetto della denuncia presentata all'autorità di controllo e dalle ragioni che hanno portato tale autorità a dubitare della validità della decisione in questione nel trattare tale denuncia.

83. Ciò premesso, se il DPC ha chiesto al giudice del rinvio di interpellare la Corte sulla validità della decisione 2010/87, ciò è avvenuto perché ritiene che un chiarimento della Corte al riguardo sia necessario per trattare la denuncia con cui il sig. Schrems gli chiede di esercitare il potere, di cui era investito in forza dell'articolo 28, paragrafo 3, secondo trattino, della direttiva 95/46 – ora conferitogli dall'articolo 58, paragrafo 2, lettera f), del RGPD – di sospendere il trasferimento di dati personali che lo riguardano da parte di Facebook Ireland a Facebook Inc.

84. Pertanto, mentre il procedimento principale riguarda unicamente la validità in astratto della decisione 2010/87, la procedura sottostante, pendente dinanzi al DPC, attiene all'esercizio, da parte di quest'ultimo, del potere di adottare misure correttive *in un caso specifico*. Proporrò alla Corte di limitarsi a esaminare le questioni sollevate nella misura necessaria per statuire sulla validità della decisione 2010/87, poiché tale esame sarà sufficiente a consentire al giudice del rinvio di risolvere la controversia pendente dinanzi ad esso [27].

85. Prima di valutare la validità di tale decisione, occorre respingere talune obiezioni sollevate contro la ricevibilità della domanda di pronuncia pregiudiziale.

B. Sulla ricevibilità del rinvio pregiudiziale

86. La ricevibilità della domanda di pronuncia pregiudiziale è stata contestata per vari motivi attinenti, essenzialmente, all'inapplicabilità ratione temporis della direttiva 95/46 cui fanno riferimento le questioni pregiudiziali (sezione 1), al fatto che il procedimento dinanzi al DPC non avrebbe raggiunto uno stadio sufficientemente avanzato da giustificarne l'utilità (sezione 2) e al fatto che perdura l'incertezza circa il quadro fattuale descritto dal giudice del rinvio (sezione 3).

27 V. paragrafi da 167 a 186 delle presenti conclusioni.

87. Risponderò a tali eccezioni di irricevibilità tenendo presente la presunzione di pertinenza di cui beneficiano le questioni sottoposte alla Corte ai sensi dell'articolo 267 TFUE. Secondo una giurisprudenza costante, la Corte può rifiutarsi di statuire su una domanda di pronuncia pregiudiziale soltanto qualora risulti in modo manifesto che l'interpretazione richiesta del diritto dell'Unione non ha alcun rapporto con la realtà effettiva o con l'oggetto della controversia nel procedimento principale, oppure qualora il problema sia di natura ipotetica, o anche quando la Corte non disponga degli elementi di fatto o di diritto necessari per rispondere utilmente alle questioni che le vengono sottoposte [28].

1. Sull'applicabilità ratione temporis della direttiva 95/46

88. Facebook Ireland eccepisce l'irricevibilità delle questioni pregiudiziali sulla base del rilievo che esse fanno riferimento alla direttiva 95/46, sebbene tale direttiva sia stata abrogata e sostituita dal RGPD con effetto a decorrere dal 25 maggio 2018 [29].

89. Condivido la tesi secondo cui la validità della decisione 2010/87 deve essere esaminata alla luce delle disposizioni del GPD.

90. Conformemente all'articolo 94, paragrafo 2, di tale regolamento, «[i] riferimenti alla direttiva abrogata si intendono fatti [a detto regolamento]». Ne deriva, a mio avviso, che la decisione 2010/87, nella parte in cui menziona quale base giuridica l'articolo 26, paragrafo 4, della direttiva 95/46, deve essere intesa nel senso che fa riferimento all'articolo 46, paragrafo 2, lettera c), del RGPD, che ne riproduce essenzialmente il contenuto [30]. Pertanto, le decisioni di esecuzione adottate dalla Commissione in forza dell'articolo 26, paragrafo 4, della direttiva 95/46, prima dell'entrata in vigore del RGPD, devono essere interpretate alla luce di tale regolamento. Ed è sempre alla luce di tale regolamento che occorre valutare, se del caso, la loro validità.

91. Tale conclusione non è rimessa in discussione dalla giurisprudenza secondo la quale la legittimità di un atto dell'Unione deve essere valutata in base alla situazione di fatto e di diritto esistente al momento in cui l'atto è stato adottato. Tale giurisprudenza riguarda, infatti, l'esame della validità di un atto dell'Unione alla luce delle circostanze di fatto pertinenti al momento dell'adozione [31] o delle norme procedurali che ne disciplinano l'adozione [32]. Per contro, la Corte ha esaminato ripetutamente la validità di atti di diritto derivato alla luce di norme sostanziali di rango superiore entrate in vigore dopo l'adozione di tali atti [33].

92. Tuttavia, l'indicazione nel testo delle questioni pregiudiziali di un atto non più applicabile ratione temporis, anche se giustifica la riformulazione di tali questioni, non può comportarne l'irricevibilità [34]. Come sostenuto dal DPC e dal sig. Schrems, i riferimenti alla direttiva 95/46 nel testo delle questioni pregiudiziali possono essere spiegati, peraltro, alla luce del calendario procedurale della presente causa, in quanto tali questioni sono state sottoposte alla Corte prima dell'entrata in vigore del RGPD.

28 V., in particolare, sentenze del 10 dicembre 2018, Wightman e a. (C-621/18, EU:C:2018:999, punto 27) e del 19 novembre 2019, A.K. e a. (Indipendenza della Sezione disciplinare della Corte suprema) (C-585/18, C-624/18 e C-625/18, EU:C:2019:982, punto 98).

29 V. articolo 94, paragrafo 1, e articolo 99, paragrafo 1, del RGPD.

30 Ricordo che, conformemente all'articolo articolo 46, paragrafo 5, del RGPD, le decisioni adottate dalla Commissione in base all'articolo 26, paragrafo 4, della direttiva 95/46 restano in vigore fino a quando non vengono modificate, sostituite o abrogate.

31 V., in particolare, sentenze del 7 febbraio 1979, Francia/Commissione (15/76 et 16/76, EU:C:1979:29, punto 7), del 17 maggio 2001, IECC/Commissione (C-449/98 P, EU:C:2001:275, punto 87), e del 17 ottobre 2013, Schaible (C-101/12, EU:C:2013:661, punto 50).

32 V., in particolare, sentenze del 16 aprile 2015, Parlamento/Consiglio (C-540/13, EU:C:2015:224, punto 35), del 16 aprile 2015, Parlamento/Consiglio (C-317/13 e C-679/13, EU:C:2015:223, punto 45), e del 22 settembre 2016, Parlamento/Consiglio (C-14/15 e C-116/15, EU:C:2016:715, punto 48).

33 In particolare, nella sentenza Schrems, la Corte ha valutato la validità della decisione «approdo sicuro» alla luce delle disposizioni della Carta, la cui adozione è successiva a quella di tale decisione. V. anche sentenze del 17 marzo 2011, AJD Tuna (C-221/09, EU:C:2011:153, punto 48) e dell'11 giugno 2015, Pfeifer & Langen (C-51/14, EU:C:2015:380, punto 42).

34 V., in particolare, sentenze del 15 luglio 2010, Pannon Gép Centrum (C-368/09, EU:C:2010:441, punti da 30 a 35), del 10 febbraio 2011, Andersson (C-30/10, EU:C:2011:66, punti 20 e 21), nonché del 25 ottobre 2018, Roche Lietuva (C-413/17, EU:C:2018:865, punti da 17 a 20).

93. In ogni caso, le disposizioni del RGPD che saranno esaminate al termine dell'analisi delle questioni pregiudiziali – ossia, in particolare, gli articoli 45, 46 e 58 di esso – riprendono essenzialmente, pur sviluppandolo e con qualche leggera differenza, il contenuto degli articoli 25, 26 e 28 della direttiva 95/46. Per quanto riguarda gli aspetti rilevanti ai fini della pronuncia sulla validità della decisione 2010/87, non ravviso alcuna ragione per attribuire a tali disposizioni del RGPD una portata diversa da quella delle corrispondenti disposizioni della direttiva 95/46 [35].

2. Sulla natura provvisoria dei dubbi espressi dal DPC

94. Secondo il governo tedesco, la domanda di pronuncia pregiudiziale è irricevibile per il fatto che il procedimento di ricorso menzionato al punto 65 della sentenza Schrems presuppone che l'autorità di controllo si sia formata un'opinione definitiva sulla fondatezza delle censure dedotte dal ricorrente riguardo alla validità della decisione di cui trattasi. Ciò non sarebbe avvenuto nel caso di specie, in quanto il DPC ha espresso i suoi dubbi sulla validità della decisione 2010/87, che il sig. Schrems peraltro non contesta, in un progetto di decisione emesso in via provvisoria, fatta salva l'eventuale presentazione di osservazioni complementari da parte di Facebook Ireland e del sig. Schrems.

95. A mio avviso, la natura provvisoria dei dubbi espressi dal DPC non incide sulla ricevibilità del rinvio pregiudiziale. Infatti, i criteri di ricevibilità di una questione pregiudiziale devono essere valutati rispetto all'oggetto della controversia come definito dal giudice del rinvio [36], Orbene, è pacifico che quest'ultimo riguarda la validità della decisione 2010/87. Secondo la decisione di rinvio e la sentenza ad essa allegata, tale giudice ha considerato che i dubbi espressi dal DPC – indipendentemente dal fatto che siano stati espressi in via provvisoria o definitiva – sono fondati e ha pertanto interpellato la Corte sulla validità di tale decisione. In tali circostanze, il chiarimento della Corte al riguardo è indubbiamente pertinente per consentirgli di risolvere la controversia di cui è investito.

3. Sulle incertezze relative alla definizione del quadro fattuale

96. Il governo del Regno Unito afferma che il quadro fattuale descritto dal giudice del rinvio contiene diverse lacune che compromettono la ricevibilità delle questioni pregiudiziali. Tale giudice non avrebbe chiarito se i dati personali relativi al sig. Schrems siano stati effettivamente trasferiti negli Stati Uniti né, in caso affermativo, se siano stati raccolti dalle autorità statunitensi. Neppure la base giuridica di tali eventuali trasferimenti sarebbe stata individuata con certezza, in quanto la decisione di rinvio si limita ad affermare che i dati degli utenti europei della rete sociale Facebook sono trasferiti «in gran parte» in base a clausole contrattuali tipo previste dalla decisione 2010/87. In ogni caso, non sarebbe stato dimostrato che il contratto tra Facebook Ireland e Facebook Inc., invocato a sostegno del trasferimento controverso, incorpori fedelmente tali clausole. Il governo tedesco contesta del pari la ricevibilità del rinvio pregiudiziale per il fatto che il giudice del rinvio non ha esaminato se il sig. Schrems abbia indubitabilmente prestato il suo consenso ai trasferimenti in questione, nel qual caso essi sarebbero stati validamente fondati sull'articolo 26, paragrafo 1, della direttiva 95/46 [di cui l'articolo 49, paragrafo 1, lettera a), del RGPD riprende sostanzialmente il contenuto].

97. Tali argomenti non rimettono affatto in discussione la pertinenza del rinvio pregiudiziale rispetto all'oggetto del procedimento principale. Poiché tale controversia ha origine nell'esercizio, da parte del DPC, del mezzo di ricorso previsto al punto 65 della sentenza Schrems, il suo stesso oggetto consiste nell'ottenere dal giudice nazionale un rinvio pregiudiziale sulla validità della decisione 2010/87. I governi tedesco e del Regno Unito contestano, in realtà, la necessità delle questioni pregiudiziali al fine non già di stabilire se tale decisione sia valida, bensì di consentire al DPC di pronunciarsi in concreto sulla denuncia del sig. Schrems.

35 V., a tale riguardo, conclusioni dell'avvocato generale Bobek nella causa Fashion ID (C-40/17, EU:C:2018:1039, paragrafo 87).

36 V. paragrafo 87 delle presenti conclusioni.

98. In ogni caso, anche sotto il profilo di tale procedura sottostante al procedimento principale, le questioni pregiudiziali riguardanti la validità della decisione 2010/87 non mi sembrano irrilevanti. Infatti, il giudice del rinvio ha accertato che Facebook Ireland ha continuato a trasferire i dati dei suoi utenti negli Stati Uniti dopo l'annullamento della decisione «approdo sicuro» e che tali trasferimenti sono basati, almeno in parte, sulla decisione 2010/87. Inoltre, pur se può essere vantaggioso che tutti i fatti pertinenti siano accertati prima di esercitare la propria competenza ai sensi dell'articolo 267 TFUE, spetta unicamente al giudice del rinvio valutare in quale fase del procedimento necessita di una pronuncia pregiudiziale della Corte [37].

99. Tenuto conto di tutte le suesposte considerazioni, ritengo che la domanda di pronuncia pregiudiziale sia ricevibile.

C. Sull'applicabilità del diritto dell'Unione ai trasferimenti di dati personali a fini commerciali verso un paese terzo che può trattarli a fini di sicurezza nazionale (prima questione)

100. Con la prima questione, il giudice del rinvio chiede se il diritto dell'Unione si applichi a un trasferimento di dati personali da parte di una società con sede in uno Stato membro verso una società stabilita in un paese terzo effettuato per motivi commerciali quando, dopo l'inizio del trasferimento, i dati possono essere trattati dalle autorità pubbliche di tale paese terzo per finalità che comprendono la protezione della sicurezza nazionale.

101. L'importanza della presente questione per la risoluzione della controversia nel procedimento principale consiste nel fatto che, qualora tale trasferimento non rientrasse nell'ambito di applicazione del diritto dell'Unione, tutte le obiezioni sollevate contro la validità della decisione 2010/87 nel caso di specie sarebbero prive di fondamento.

102. Come osservato dal giudice del rinvio, i trattamenti di dati personali aventi ad oggetto la sicurezza nazionale erano esclusi dall'ambito di applicazione della direttiva 95/46 in forza dell'articolo 3, paragrafo 2, di tale direttiva. L'articolo 2, paragrafo 2, del RGPD precisa ora che tale regolamento non si applica, in particolare, al trattamento di dati nell'ambito di un'attività che non rientra nell'ambito di applicazione del diritto dell'Unione o da parte delle autorità competenti a fini di protezione della pubblica sicurezza. Tali disposizioni riflettono la riserva di competenza che l'articolo 4, paragrafo 2, TUE riconosce agli Stati membri in materia di protezione della sicurezza nazionale.

103. Il DPC, il sig. Schrems, l'Irlanda, i governi tedesco, austriaco, belga, ceco, dei Paesi Bassi, polacco, portoghese, nonché il Parlamento e la Commissione sostengono che a trasferimenti come quelli menzionati nella denuncia del sig. Schrems non si applicano tali disposizioni e rientrano quindi nell'ambito di applicazione del diritto dell'Unione. Facebook Irlanda difende la tesi contraria. Concordo con il punto di vista dei primi.

37 V., in tal senso, sentenze del 1º aprile 1982, Holdijk e a. (da 141/81 a 143/81, EU:C:1982:122, punto 5) e del 9 dicembre 2003, Gasser (C-116/02, EU:C:2003:657, punto 27).

104. A tale riguardo, occorre sottolineare che il trasferimento di dati personali da uno Stato membro a un paese terzo costituisce, in quanto tale, un «trattamento», ai sensi dell'articolo 4, punto 2, del RGPD, effettuato nel territorio di uno Stato membro [38]. La prima questione pregiudiziale ha come scopo proprio quello di stabilire se il diritto dell'Unione si applichi al *trattamento costituito dal trasferimento in quanto tale*. Tale questione non riguarda l'applicabilità del diritto dell'Unione a eventuali trattamenti successivi, da parte delle autorità statunitensi per finalità di sicurezza nazionale, dei dati trasferiti verso gli Stati Uniti, i quali non rientrano nell'ambito di applicazione territoriale del RGPD [39].

105. In tale prospettiva, nel determinare se al trasferimento dei dati in questione si applichi il diritto dell'Unione, deve essere presa in considerazione solo l'attività nell'ambito della quale avviene il trasferimento stesso, a prescindere dalla finalità degli eventuali trattamenti successivi che i dati trasferiti subiranno da parte delle autorità pubbliche del paese terzo di destinazione [40].

106. Orbene, dalla decisione di rinvio risulta che il trasferimento oggetto della denuncia del sig. Schrems fa parte di un'attività commerciale. Tale trasferimento non avviene, peraltro, allo scopo di consentire il trattamento successivo dei dati in questione da parte delle autorità statunitensi a fini di sicurezza nazionale.

107. Per di più, l'approccio proposto da Facebook Ireland priverebbe di effetto utile le disposizioni del RGPD relative ai trasferimenti verso paesi terzi, in quanto non si può mai escludere che dati trasferiti nell'ambito di un'attività commerciale siano trattati per finalità di sicurezza nazionale dopo il trasferimento.

108. L'interpretazione che raccomando è confermata dalla formulazione dell'articolo 45, paragrafo 2, lettera a), del RGPD. Tale disposizione precisa che, nell'adottare una decisione di adeguatezza, la Commissione tiene conto, in particolare, della legislazione del paese terzo considerato *in materia di sicurezza nazionale*. Se ne può dedurre che la possibilità che i dati subiscano, da parte delle autorità del paese terzo di destinazione, un trattamento a fini della protezione della sicurezza nazionale non rende inapplicabile il diritto dell'Unione al trattamento costituito dal trasferimento di dati verso tale paese terzo.

109. Anche il ragionamento e le conclusioni adottati dalla Corte nella sentenza Schrems si basano su tale premessa. In particolare, la Corte ha esaminato, in tale sentenza, la validità della decisione «approdo sicuro» per la parte riguardante il trasferimento di dati personali verso gli Stati Uniti, ove potevano essere raccolti e trattati a fini di protezione della sicurezza nazionale, alla luce dell'articolo 25, paragrafo 6, della direttiva 95/46, in combinato disposto con la Carta [41].

110. Tenuto conto di tali considerazioni, ritengo che il diritto dell'Unione si applichi al trasferimento di dati personali da uno Stato membro verso un paese terzo, quando tale trasferimento si inserisce in un'attività commerciale, senza che rilevi il fatto che i dati trasferiti rischino di subire, da parte delle autorità pubbliche di tale paese terzo, trattamenti miranti a tutelare la sicurezza nazionale.

38 V., in tal senso, sentenza del 30 maggio 2006, Parlamento/Consiglio e Commissione (C-317/04 e C-318/04, EU:C:2006:346; in prosieguo: la «sentenza PNR», punto 56), nonché sentenza Schrems (punto 45). L'articolo 4, punto 2, del RGPD riprende essenzialmente la definizione della nozione di «trattamento» di cui all'articolo 2, lettera b), della direttiva 95/46.

39 Conformemente all'articolo 3, paragrafo 1, del RGPD, tale regolamento si applica a qualsiasi trattamento effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione. La questione dell'applicabilità del diritto dell'Unione ai trattamenti da parte dei servizi di intelligence di un paese terzo al di fuori dell'Unione deve essere distinta dalla questione della pertinenza delle norme e delle prassi relative a tali trattamenti nel paese terzo in questione, al fine di determinare se sia ivi garantito un livello adeguato di protezione. Quest'ultima tematica è oggetto della seconda questione pregiudiziale e sarà esaminata ai paragrafi da 201 a 229 delle presenti conclusioni.

40 Nelle mie conclusioni nella causa Ministerio Fiscal (C-207/16, EU:C:2018:300, paragrafo 47), ho sottolineato la distinzione fra, da un lato, il trattamento diretto di dati personali nel contesto delle attività sovrane dello Stato, e, dall'altro, il trattamento commerciale seguito dall'uso da parte delle autorità pubbliche.

41 Analogamente, nel parere 1/15 (Accordo PNR UE-Canada), del 26 luglio 2017 (UE:C:2017:592; in prosieguo: il «parere 1/15»), la Corte ha esaminato la conformità agli articoli 7, 8 e 47 della Carta di un progetto di accordo internazionale tra il Canada e l'Unione riguardante dati che, una volta trasferiti in Canada, erano destinati ad essere trattati dalle autorità pubbliche a fini di protezione della sicurezza nazionale.

D. Sul livello di protezione richiesto nell'ambito di un trasferimento basato su clausole contrattuali tipo (prima parte della sesta questione)

111. Con la prima parte della sesta questione, il giudice nazionale chiede di accertare quale sia il livello di tutela dei diritti fondamentali degli interessati, che deve essere garantito affinché i dati personali possano essere trasferiti in un paese terzo in forza delle clausole contrattuali tipo previste dalla decisione 2010/87.

112. Tale giudice sottolinea che, nella sentenza Schrems, la Corte ha interpretato l'articolo 25, paragrafo 6, della direttiva 95/46 (il cui contenuto è ripreso essenzialmente nell'articolo 45, paragrafo 3, del RGPD), nella parte in cui prevedeva che la Commissione può adottare una decisione di adeguatezza solo dopo aver accertato che il paese terzo interessato garantisce un livello di protezione *adeguato*, nel senso che presuppone che essa constati che tale paese garantisce un livello di tutela dei diritti e delle libertà fondamentali *sostanzialmente equivalente* a quello garantito all'interno dell'Unione ai sensi di tale direttiva, letta alla luce della Carta [42].

113. In tale contesto, la prima parte della sesta questione pregiudiziale invita la Corte a stabilire se l'applicazione delle «clausole contrattuali tipo» adottate dalla Commissione ai sensi dell'articolo 26, paragrafo 4, della direttiva 95/46 – corrispondenti alle «clausole tipo di protezione» ora menzionate all'articolo 46, paragrafo 2, lettera c), del RGPD – debba consentire di raggiungere un livello di protezione corrispondente allo stesso standard di «equivalenza sostanziale».

114. A tal proposito, l'articolo 46, paragrafo 1, del RGPD prevede che il titolare del trattamento può, in mancanza di una decisione di adeguatezza, 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» (il corsivo è mio) [43]. Ai sensi dell'articolo 46, paragrafo 2, lettera c), del RGPD, tali garanzie possono risultare, in particolare, da clausole tipo di protezione elaborate dalla Commissione.

115. Al pari del DPC, del sig. Schrems e dell'Irlanda, ritengo che le «garanzie adeguate» fornite dal titolare del trattamento cui fa riferimento l'articolo 46, paragrafo 1, del RGPD debbano garantire che i diritti delle persone i cui dati sono trasferiti godano, come nell'ambito di un trasferimento basato su una decisione di adeguatezza, di un livello di protezione sostanzialmente equivalente a quello risultante dal RGPD, letto alla luce della Carta.

116. Tale conclusione deriva dall'obiettivo della suddetta disposizione e dello strumento di cui fa parte.

117. L'obiettivo degli articoli 45 e 46 del RGPD è quello di garantire la continuità dell'elevato livello di protezione dei dati personali garantito da tale regolamento quando tali dati sono trasferiti al di fuori dell'Unione. Infatti, l'articolo 44 del RGPD, intitolato «Principio generale per il trasferimento», apre il capo V relativo ai trasferimenti verso paesi terzi prevedendo che tutte le disposizioni di tale capo siano applicate al fine di assicurare che il livello di protezione garantito dal RGPD non sia pregiudicato in caso di trasferimento verso uno Stato terzo [44]. Tale norma mira a evitare che gli standard di protezione derivanti dal diritto dell'Unione siano elusi trasferendo dati personali verso un paese terzo al fine di sottoporli a trattamento in tale paese [45]. Con riferimento a tale obiettivo, è

42 Sentenza Schrems (punto 73). La Corte ha confermato tale conclusione nel parere 1/15 (punto 134).

43 L'articolo 26, paragrafo 2, della direttiva 95/46 prevedeva che uno Stato membro può autorizzare tale trasferimento «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» (il corsivo è mio). Le nozioni di «garanzie sufficienti» e di «garanzie adeguate», menzionate rispettivamente in questa disposizione e nell'articolo 46, paragrafo 1, del RGPD, presentano, a mio avviso, lo stesso contenuto.

44 A tale riguardo, nel considerando 6 del RGPD si precisa che deve essere garantito un «elevato livello» di protezione dei dati sia all'interno dell'Unione che in caso di trasferimento al di fuori di essa.

45 V. sentenza Schrems (punto 73) e parere 1/15 (punto 214).

irrilevante che il trasferimento sia fondato su una decisione di adeguatezza o su garanzie offerte dal titolare del trattamento, in particolare mediante clausole contrattuali. I requisiti per la tutela dei diritti fondamentali garantiti dalla Carta non fanno alcuna distinzione a seconda della base giuridica su cui si fonda un determinato trasferimento [46].

118. Per contro, il modo in cui viene preservata la continuità dell'elevato livello di protezione varia a seconda della base giuridica del trasferimento.

119. Da un lato, l'obiettivo di una decisione di adeguatezza è constatare che il paese terzo interessato garantisca esso stesso un livello di protezione sostanzialmente equivalente a quello che deve essere raggiunto all'interno dell'Unione. L'adozione di una decisione di adeguatezza presuppone che la Commissione valuti preventivamente, per un determinato paese terzo, il livello di protezione garantito dal diritto e dalle prassi di tale paese terzo alla luce dei fattori di cui all'articolo 45, paragrafo 3, del RGPD. I dati personali possono essere in tal caso trasferiti verso tale paese terzo senza che il titolare del trattamento debba ottenere un'autorizzazione specifica.

120. D'altro lato, come spiegato in modo più dettagliato nella sezione seguente, le garanzie adeguate offerte dal titolare del trattamento sono intese a garantire un elevato livello di protezione in caso di insufficienza delle garanzie disponibili nel paese terzo di destinazione. Pertanto, sebbene l'articolo 46, paragrafo 1, del RGPD consenta il trasferimento di dati personali verso Stati terzi che non garantiscono un livello di protezione adeguato, tale disposizione autorizza siffatti trasferimenti solo quando sono fornite garanzie adeguate con altri mezzi. Le clausole contrattuali tipo adottate dalla Commissione rappresentano, a tale riguardo, un meccanismo generale applicabile ai trasferimenti indipendentemente dal paese terzo di destinazione e dal livello di protezione ivi garantito.

E. Sulla validità della decisione 2010/87 alla luce degli articoli 7, 8 e 47 della Carta (questioni settima, ottava e undicesima)

121. Con la settima questione, il giudice nazionale chiede, in sostanza, se la decisione 2010/87 sia invalida in quanto non vincola le autorità di Stati terzi verso i quali sono trasferiti i dati in forza delle clausole contrattuali tipo previste nell'allegato a tale decisione e, in particolare, non impedisce loro di esigere che l'importatore metta tali dati a loro disposizione. Pertanto, tale questione rimette in discussione la possibilità stessa di garantire un livello adeguato di protezione di tali dati mediante meccanismi di natura esclusivamente contrattuale. L'undicesima questione verte più in generale sulla validità della decisione 2010/87 alla luce degli articoli 7, 8 e 47 della Carta.

122. L'ottava questione invita la Corte a stabilire se un'autorità di controllo sia tenuta a esercitare i poteri ad essa conferiti dall'articolo 58, paragrafo 2, lettere f) e j), del RGPD per sospendere un trasferimento verso un paese terzo basato sulle clausole contrattuali tipo previste dalla decisione 2010/87, qualora ritenga che l'importatore di dati sia ivi soggetto ad obblighi che gli impediscono di rispettare tali clausole e hanno come conseguenza che non è garantita un'adeguata protezione dei dati trasferiti. Dato che la risposta a tale questione incide, a mio avviso, sulla validità della decisione 2010/87 [47], la esaminerò congiuntamente alla settima e all'undicesima questione.

123. Il dettato dell'articolo 46, paragrafo 1, del RGPD, per la parte in cui prevede che, «*[i]n 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 (...) solo *se ha fornito* garanzie adeguate (...)» (il corsivo è mio), mette in evidenza la logica da cui prendono le mosse i meccanismi contrattuali come quello previsto nella decisione 2010/87. Come sottolineato dai considerando 108 e 114 del

46 Ciò non pregiudica la possibilità di trasferire dati personali, anche in mancanza di garanzie adeguate, sulla base dei motivi di deroga di cui all'articolo 49, paragrafo 1, del RGPD.

47 V. paragrafo 128 delle presenti conclusioni.

RGPD, lo scopo di tali meccanismi è quella di consentire i trasferimenti verso paesi terzi per i quali la Commissione non ha adottato una decisione di adeguatezza, in quanto le eventuali insufficienze della protezione garantita nell'ordinamento giuridico di tale paese terzo sono *compensate* da garanzie che l'esportatore e l'importatore dei dati s impegnano a rispettare contrattualmente.

124. Poiché la ragion d'essere delle garanzie contrattuali consiste proprio nel colmare le possibili lacune nella protezione offerta dai paesi terzi di destinazione quali essi siano, la validità di una decisione con la quale la Commissione constata che talune clausole tipo colmano adeguatamente tali lacune non può dipendere dal livello di protezione garantito in ciascuno dei singoli paesi terzi verso i quali i dati potrebbero essere trasferiti. La validità di tale decisione dipende unicamente dalla solidità delle garanzie previste da tali clausole per compensare un'eventuale insufficiente protezione nel paese terzo di destinazione. L'efficacia di tali garanzie deve essere valutata anche alla luce delle salvaguardie costituite dai poteri delle autorità di controllo di cui all'articolo 58, paragrafo 2, del RGPD.

125. A tale riguardo, come rilevato in sostanza dal DPC, dal sig. Schrems, dalla BSA, dall'Irlanda, dai governi austriaco, francese, polacco e portoghese, nonché dalla Commissione, le garanzie contenute nelle clausole contrattuali tipo possono essere sminuite o addirittura vanificate allorché il diritto del paese terzo di destinazione impone all'importatore obblighi contrari a quanto richiesto da tali clausole. Pertanto, il contesto giuridico esistente nel paese terzo di destinazione può, a seconda delle circostanze specifiche del trasferimento [48], rendere impossibile l'adempimento degli obblighi previsti da tali clausole.

126. In tali circostanze, come hanno sottolineato il sig. Schrems e la Commissione, il meccanismo contrattuale previsto dall'articolo 46, paragrafo 2, lettera c), del RGPD si basa sulla responsabilità dell'esportatore e, in subordine, delle autorità di controllo. È *caso per caso*, per ogni specifico trasferimento, che il titolare del trattamento o, in mancanza, l'autorità di controllo, esaminerà se il diritto del paese terzo di destinazione osti all'esecuzione delle clausole tipo e, pertanto, a un'adeguata protezione dei dati trasferiti, cosicché i trasferimenti devono essere vietati o sospesi.

127. Alla luce di tali osservazioni, ritengo che il fatto che la decisione 2010/87 e le clausole contrattuali tipo dalla stessa previste non siano vincolanti per le autorità del paese terzo di destinazione non rende di per sé invalida tale decisione. La conformità della decisione 2010/87 agli articoli 7, 8 e 47 della Carta dipende, a mio avviso, dalla questione se esistano meccanismi sufficientemente solidi che consentano di garantire che i trasferimenti basati sulle clausole contrattuali tipo siano sospesi o vietati in caso di violazione di tali clausole o di impossibilità a rispettarle.

128. A tal proposito, l'articolo 46, paragrafo 1, del RGPD prevede che un trasferimento basato su garanzie adeguate può aver luogo solo «a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi». Occorrerà verificare se le garanzie previste dalle clausole contenute nell'allegato alla decisione 2010/87, integrate dai poteri delle autorità di controllo, consentano di garantire il rispetto di tale condizione. Ciò avviene, a mio avviso, solo nei limiti in cui esiste un *obbligo* – gravante sui responsabili del trattamento (sezione 1) e, in caso di inerzia di questi ultimi, sulle autorità di controllo (sezione 2) – di sospendere o di vietare un trasferimento quando, a causa di un conflitto tra gli obblighi derivanti dalle clausole tipo e quelli imposti dal diritto del paese terzo di destinazione, tali clausole non possono essere rispettate.

48 Immaginiamo, ad esempio, che un paese terzo preveda l'obbligo per i fornitori di servizi di telecomunicazione di concedere alle autorità pubbliche l'accesso ai dati trasferiti senza limitazioni né garanzie. Pur se tali fornitori si troverebbero nell'impossibilità di rispettare le clausole contrattuali tipo, le imprese che non sono soggette a tale obbligo non sarebbero comunque impedite dal farlo.

1. Sugli obblighi dei responsabili del trattamento

129. In primo luogo, le clausole contrattuali tipo contenute nell'allegato alla decisione 2010/87 richiedono che, in caso di conflitto tra gli obblighi che esse prevedono e i requisiti derivanti dal diritto del paese terzo di destinazione, tali clausole non siano invocate a sostegno di un trasferimento verso tale paese terzo o, se il trasferimento è già stato avviato in base a dette clausole, l'esportatore sia informato di tale conflitto e possa sospendere tale trasferimento.

130. Pertanto, in forza della clausola 5, lettera a), l'importatore si impegna a trattare i dati personali trasferiti esclusivamente per conto e secondo le istruzioni dell'esportatore, nonché a norma delle clausole contrattuali tipo. L'importatore, se si trova nell'impossibilità di ottemperare a tali clausole, si impegna a informare prontamente l'esportatore, nel qual caso quest'ultimo ha facoltà di sospendere il trasferimento e/o di risolvere il contratto [49].

131. La nota 5 relativa alla clausola 5 precisa che le clausole tipo non sono violate quando l'importatore rispetta le esigenze imperative della legislazione nazionale ad esso applicabile nel paese terzo, a condizione che tali requisiti non vadano oltre quanto è necessario in una società democratica per tutelare uno degli interessi di cui all'articolo 13, paragrafo 1, della direttiva 95/46 (il cui contenuto è essenzialmente ripreso all'articolo 23, paragrafo 1, del RGPD), fra i quali rientra la pubblica sicurezza e la sicurezza dello Stato. Per contro, l'inosservanza di tali clausole al fine di rispettare un obbligo contrario ai sensi del diritto del paese terzo di destinazione che va oltre quanto è proporzionato per la salvaguardia di un interesse legittimo riconosciuto dall'Unione è trattata come una violazione di dette clausole.

132. A mio avviso, come sostenuto dal sig. Schrems e dalla Commissione, la clausola 5, lettera a), non può essere interpretata nel senso che esso implica che la sospensione del trasferimento o la risoluzione del contratto è solo facoltativa allorché l'importatore non è in grado di rispettare le clausole tipo. Sebbene tale clausola si limiti a menzionare un diritto in tal senso a favore dell'esportatore, detta formulazione deve essere intesa con riferimento al quadro contrattuale in cui si inserisce. Il fatto che l'esportatore sia investito del diritto, *nei suoi rapporti bilaterali con l'importatore*, di sospendere il trasferimento o di risolvere il contratto quando quest'ultimo si trova nell'impossibilità di rispettare le clausole tipo lascia impregiudicato l'obbligo gravante sull'esportatore di procedere in tal senso *alla luce degli obblighi di protezione dei diritti degli interessati derivanti dal RGPD*. Qualsiasi altra interpretazione comporterebbe l'invalidità della decisione 2010/87 in quanto le clausole contrattuali tipo da essa previste non consentirebbero di contornare il trasferimento con «garanzie adeguate», come richiesto dall'articolo 46, paragrafo 1, del RGPD, letto alla luce delle disposizioni della Carta [50].

49 Osservo, inoltre, che la clausola 5, lettera d), punto i), esonera l'importatore dall'obbligo di informare l'esportatore di una richiesta giuridicamente vincolante di divulgazione presentata da autorità giudiziarie o di polizia del paese terzo, qualora il diritto di tale paese terzo osti a tale informazione. In tale caso di specie l'esportatore non ha la possibilità di sospendere il trasferimento se tale divulgazione, di cui non è a conoscenza, violi le clausole tipo. Tuttavia, in forza della clausola 5, lettera a), l'importatore resta tenuto ad informare l'esportatore, se del caso, del fatto che, a suo avviso, la legislazione di tale paese terzo gli impedisce di adempiere gli obblighi derivanti dalle clausole contrattuali concordate.

50 Dalla giurisprudenza risulta che le disposizioni di un atto di esecuzione devono essere interpretate conformemente alle disposizioni dell'atto di base con cui il legislatore ne ha autorizzato l'adozione [v., in tal senso, segnatamente, sentenze del 26 luglio 2017, Repubblica ceca/Commissione (C-696/15 P, EU:C:2017:595, punto 51), del 17 maggio 2018, Evonik Degussa (C-229/17, EU:C:2018:323, punto 29), e del 20 giugno 2019, ExxonMobil Production Deutschland (C-682/17, EU:C:2019:518, punto 112)]. Inoltre, un atto dell'Unione dev'essere interpretato, nei limiti del possibile, in modo da non inficiare la sua validità e in conformità con il diritto primario nel suo complesso e, in particolare, con le disposizioni della Carta [v., in particolare, sentenza del 14 maggio 2019, M e a. (Revoca dello status di rifugiato) (C-391/16, C-77/17 e C-78/17, EU:C:2019:403, punto 77 e giurisprudenza ivi citata)].

133. Inoltre, ai sensi della clausola 5, lettera b), l'importatore certifica 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. Egli comunicherà all'esportatore, senza indugio, qualsiasi modificazione di tale normativa che possa pregiudicare le garanzie e gli obblighi previsti dalle clausole tipo, nel qual caso l'esportatore ha facoltà di sospendere il trasferimento e/o di risolvere il contratto. Conformemente alla clausola 4, lettera g), l'esportatore deve trasmettere, all'autorità di controllo competente la comunicazione presentata dall'importatore ove decida di proseguire il trasferimento.

134. Ritengo necessario fornire in questa sede alcune precisazioni relative al contenuto dell'esame che le parti del contratto devono effettuare per determinare, alla luce della nota alla clausola 5, se gli obblighi imposti all'importatore dal diritto dello Stato terzo costituiscano una violazione delle clausole tipo e quindi impediscano che il trasferimento sia contornato di garanzie adeguate. Tale problematica è stata sollevata, in sostanza, nella seconda parte della sesta questione pregiudiziale.

135. Tale esame implica, a mio avviso, che siano prese in considerazione tutte le circostanze che caratterizzano ogni trasferimento, tra le quali si possono annoverare la natura dei dati e la loro eventuale natura sensibile, i meccanismi messi in atto dall'esportatore e/o dall'importatore per garantirne la sicurezza [51], la natura e le finalità dei trattamenti da parte delle autorità pubbliche del paese terzo a cui i dati saranno esposti, le modalità di tali trattamenti nonché le limitazioni e le garanzie fornite da tale paese terzo. Gli elementi che caratterizzano le attività di trattamento da parte delle autorità pubbliche e le garanzie applicabili nell'ordinamento giuridico di detto paese terzo possono, a mio avviso, sovrapporsi a quelli di cui all'articolo 45, paragrafo 2, del RGPD.

136. In secondo luogo, le clausole contrattuali tipo di cui all'allegato della decisione 2010/87 istituiscono a favore degli interessati diritti azionabili e mezzi di ricorso nei confronti dell'esportatore e, in subordine, nei confronti dell'importatore.

137. Così, la clausola 3, intitolata «Terzo beneficiario», prevede, al paragrafo 1, un diritto di ricorso dell'interessato nei confronti dell'esportatore in caso di violazione, in particolare, della clausola 5, lettera a) o b). Conformemente alla clausola 3, paragrafo 2, qualora l'esportatore sia scomparso di fatto o abbia giuridicamente cessato di esistere, l'interessato può far valere tale clausola nei confronti dell'importatore.

138. La clausola 6, paragrafo 1, conferisce all'interessato che abbia subito un pregiudizio per violazione degli obblighi di cui alla clausola 3, il diritto di ottenere dall'esportatore il risarcimento del danno sofferto. In forza della clausola 7, paragrafo 1, l'importatore dichiara che, qualora l'interessato faccia valere il diritto del terzo beneficiario e/o chieda il risarcimento dei danni, egli accetterà la decisione dello stesso interessato di sottoporre la controversia alla mediazione di un terzo indipendente o eventualmente dell'autorità di controllo, oppure di adire gli organi giurisdizionali dello Stato membro in cui è stabilito l'esportatore.

139. Oltre ai mezzi di ricorso di cui dispongono in virtù delle clausole contrattuali tipo di cui all'allegato della decisione 2010/87, gli interessati possono, qualora ritengano che tali clausole siano state violate, chiedere alle autorità di controllo di adottare misure correttive ai sensi dell'articolo 58, paragrafo 2, del RGPD, al quale rinvia l'articolo 4 della decisione 2010/87 [52].

51 A tale riguardo, il considerando 109 del RGPD incoraggia l'esportatore e l'importatore ad aggiungere alle clausole tipo di protezione garanzie supplementari, in particolare in via contrattuale.

52 Anche se l'articolo 4, paragrafo 1, della decisione 2010/87 fa riferimento all'articolo 28, paragrafo 3, della direttiva 95/46, ricordo che, ai sensi dell'articolo 94, paragrafo 2, del RGPD, i riferimenti a tale direttiva devono essere intesi nel senso che rinviano alle disposizioni corrispondenti del RGPD.

2. Sugli obblighi delle autorità di vigilanza

140. Le seguenti ragioni mi inducono a ritenere, al pari del sig. Schrems, dell'Irlanda, dei governi tedesco, austriaco, belga, dei Paesi Bassi e portoghese nonché dell'EDPB, che l'articolo 58, paragrafo 2, del RGPD obblighi le autorità di controllo, qualora esse ritengano, al termine di un esame diligente, che i dati trasferiti verso un paese terzo non godano di adeguata protezione a causa del mancato rispetto delle clausole contrattuali concordate, ad adottare misure appropriate per porre rimedio a tale illegittimità, se necessario ordinando la sospensione del trasferimento.

141. In primo luogo, osservo che, contrariamente a quanto sostenuto dal DPC, nessuna disposizione della decisione 2010/87 limita a casi eccezionali l'esercizio dei poteri di «imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento» e di «ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo», di cui dispongono le autorità di controllo in forza dell'articolo 58, paragrafo 2, lettere f) e j), del RGPD.

142. È vero che la versione iniziale dell'articolo 4 de la decisione 2010/87 limitava, al suo paragrafo 1, l'esercizio, da parte delle autorità di controllo, dei poteri di vietare o sospendere i flussi transfrontalieri di dati a talune ipotesi in cui era dimostrato che un trasferimento basato su termini contrattuali rischiava di avere conseguenze negative, rilevanti per le garanzie destinate a tutelare l'interessato. Tuttavia, l'articolo 4 di tale decisione, come modificato dalla Commissione nel 2016 per conformarsi alla sentenza Schrems [53], si limita ora a fare riferimento a tali poteri, senza restringerli in alcun modo. In ogni caso, una decisione di esecuzione della Commissione, come la decisione 2010/87, non può limitare validamente i poteri conferiti alle autorità di controllo in forza dello stesso RGPD [54].

143. Tale conclusione non è rimessa in discussione dal considerando 11 della decisione 2010/87, in cui si afferma che i poteri di sospensione e di divieto di trasferimento possono essere esercitati dalle autorità di controllo solo in «casi eccezionali». Detto considerando, già presente nella versione iniziale di tale decisione, faceva riferimento al precedente articolo 4, paragrafo 1, della stessa decisione, che limitava i poteri delle autorità di controllo. Al momento della revisione della decisione 2010/87, ad opera della decisione 2016/2297, la Commissione ha omesso di revocare o di modificare tale considerando per adeguarne il contenuto al disposto del nuovo articolo 4. Il considerando 5 della decisione 2016/2297 ha tuttavia riaffermato il potere delle autorità di controllo di sospendere o di vietare qualsiasi trasferimento che esse ritengano contrario al diritto dell'Unione, in particolare a causa dell'inosservanza, da parte dell'importatore, delle clausole contrattuali tipo. Il considerando 11 della decisione 2010/87, in quanto contraddice ormai sia la formulazione che l'obiettivo di una disposizione giuridicamente vincolante di tale decisione, deve essere qualificato come obsoleto [55].

144. In secondo luogo, contrariamente a quanto sostenuto altresì dal DPC, l'esercizio dei poteri di sospensione e di divieto previsti all'articolo 58, paragrafo 2, lettere f) e j), del RGPD, non costituisce neppure una mera facoltà rimessa al potere discrezionale delle autorità di controllo. Tale conclusione deriva, a mio avviso, da un'interpretazione dell'articolo 58, paragrafo 2, del RGPD alla luce di altre disposizioni di tale regolamento e della Carta, nonché del sistema generale e degli obiettivi della decisione 2010/87.

53 V. considerando 6 e 7 della decisione 2016/2297. Ai punti da 101 a 104 della sentenza Schrems, la Corte aveva dichiarato l'invalidità di una disposizione della decisione «approdo sicuro» che limitava a «casi eccezionali» i poteri conferiti alle autorità di controllo dall'articolo 28 della direttiva 95/46, con la motivazione che la Commissione non era competente a limitare tali poteri.

54 V. sentenza Schrems (punto 103).

55 In ogni caso, il preambolo di un atto dell'Unione non ha valore giuridico vincolante e non può essere fatto valere per derogare alle disposizioni stesse di tale atto. V. sentenze del 19 novembre 1998, Nilsson e a. (C-162/97, EU:C:1998:554, punto 54), del 12 maggio 2005, Meta Fackler (C-444/03, EU:C:2005:288, punto 25), e del 10 gennaio 2006, IATA e ELFAA (C-344/04, EU:C:2006:10, punto 76).

145. In particolare, l'articolo 58, paragrafo 2, del RGPD deve essere interpretato alla luce dell'articolo 8, paragrafo 3, della Carta e dell'articolo 16, paragrafo 2, TFUE. Conformemente a tali disposizioni, il rispetto dei requisiti del diritto fondamentale alla protezione dei dati personali è soggetto al controllo di autorità indipendenti. Tale compito di sorveglianza attinenti al rispetto dei requisiti relativi alla protezione dei dati personali, menzionato anche all'articolo 57, paragrafo 1, lettera a), del RGPD, implica un obbligo per le autorità di controllo di agire in modo da garantire la corretta applicazione di tale regolamento.

146. Pertanto, un'autorità di controllo deve esaminare con tutta la dovuta diligenza la denuncia presentata da una persona i cui dati sono asseritamente trasferiti verso uno Stato terzo in violazione delle clausole contrattuali tipo applicabili al trasferimento [56]. L'articolo 58, paragrafo 1, del RGPD conferisce, a tal fine, rilevanti poteri d'indagine alle autorità di controllo [57].

147. L'autorità di controllo competente è inoltre tenuta a reagire in modo adeguato alle eventuali violazioni dei diritti dell'interessato da essa constatate al termine della sua indagine. A tale riguardo, ogni autorità di controllo dispone, in forza dell'articolo 58, paragrafo 2, del RGPD, di un'ampia gamma di mezzi – i vari poteri di adottare le misure correttive elencate in tale disposizione – per svolgere il compito assegnatole [58].

148. Sebbene la scelta del mezzo più efficace rientri nel potere discrezionale dell'autorità di controllo competente, alla luce di tutte le circostanze del trasferimento in questione, essa è tenuta a svolgere pienamente il compito di sorveglianza affidatole. Se del caso, tale autorità è tenuta a sospendere il trasferimento se conclude che le clausole contrattuali tipo non sono rispettate e non è possibile garantire con altri mezzi un'adeguata protezione dei dati trasferiti, se l'esportatore non ha cessato esso stesso il trasferimento.

149. Tale interpretazione è suffragata dall'articolo 58, paragrafo 4, del RGPD, il quale prevede che l'esercizio, da parte delle autorità di controllo, dei poteri ad esse attribuiti da tale articolo è soggetto a garanzie adeguate, incluso il ricorso giurisdizionale effettivo conformemente all'articolo 47 della Carta. L'articolo 78, paragrafi 1 e 2, del RGPD riconosce, peraltro, il diritto di ogni persona di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante di un'autorità di controllo che la riguarda o se tale autorità omette di trattare la sua denuncia [59].

150. Tali disposizioni implicano, come sostengono in sostanza il sig. Schrems, la BSA, l'Irlanda, i governi polacco e del Regno Unito nonché la Commissione, che una decisione con la quale un'autorità di controllo si astiene dal vietare o dal sospendere un trasferimento verso un paese terzo, su richiesta di una persona che invoca il rischio che i dati che la riguardano siano trattati in tale paese in violazione dei suoi diritti fondamentali, può essere oggetto di un controllo giurisdizionale. Orbene, il riconoscimento di un diritto a un ricorso giurisdizionale presuppone l'esistenza di una competenza vincolata, e non puramente discrezionale, delle autorità di controllo. Inoltre, il sig. Schrems e la Commissione hanno sottolineato, correttamente, che l'esercizio del diritto a un controllo

56 V., per analogia, sentenza Schrems (punto 63).

57 Aggiungo che, in forza della clausola 8, paragrafo 2, contenuta nell'allegato alla decisione 2010/87, le parti del contratto dichiarano di conferire all'autorità di controllo il potere di sottoporre a controlli l'importatore secondo le stesse modalità previste per l'esportatore dalla normativa applicabile.

58 V., in tal senso, sentenza Schrems (punto 43).

59 Secondo il considerando 141 del RGPD, ogni persona deve avere diritto a un ricorso giurisdizionale effettivo ai sensi dell'articolo 47 della Carta se l'autorità di controllo «non agisce quando è necessario intervenire per proteggere i diritti [di tale persona]». V. anche i considerando 129 e 143 del RGPD.

giurisdizionale effettivo implica che l'autorità da cui promana l'atto contestato lo motivi adeguatamente [60]. Tale obbligo di motivazione si estende, a mio avviso, alla scelta da parte delle autorità di controllo di avvalersi di uno dei poteri ad esse conferiti dall'articolo 58, paragrafo 2, del RGPD.

151. È ancora necessario, tuttavia, rispondere agli argomenti con cui il DPC sostiene che, quand'anche le autorità di controllo fossero tenute a sospendere o a vietare un trasferimento quando ciò è richiesto dalla tutela dei diritti dell'interessato, non sarebbe comunque garantita la validità della decisione 2010/87.

152. In primo luogo, il DPC ritiene che siffatto obbligo non risolverebbe i problemi sistemici relativi alla mancanza di garanzie adeguate in un paese terzo come gli Stati Uniti. Infatti, i poteri delle autorità di controllo possono essere esercitati solo caso per caso, mentre le lacune che caratterizzano il diritto statunitense sarebbero di natura generale e strutturale. Ne deriverebbe il rischio che autorità di vigilanza diverse adottino decisioni divergenti relativamente a trasferimenti analoghi.

153. A tal proposito, non posso ignorare le difficoltà pratiche associate alla scelta legislativa di affidare alle autorità di controllo la responsabilità di garantire il rispetto dei diritti fondamentali delle persone interessate nel contesto di trasferimenti specifici o di flussi verso un determinato destinatario. Tuttavia, non mi sembra che tali difficoltà comportino l'invalidità della decisione 2010/87.

154. Infatti, il diritto dell'Unione non richiede, a mio avviso, che sia prevista una soluzione generale e preventiva per tutti i trasferimenti verso un determinato paese terzo che possono comportare gli stessi rischi di violazione dei diritti fondamentali.

155. Inoltre, il rischio di frammentazione degli approcci seguiti dalle diverse autorità di controllo è intrinseco al sistema di sorveglianza decentralizzata auspicato dal legislatore [61]. Per di più, come sottolineato dal governo tedesco, il capo VII del RGPD, intitolato «Cooperazione e coerenza», istituisce meccanismi destinati a evitare tale rischio. L'articolo 60 di tale regolamento prevede, in caso di trattamento transfrontaliero di dati, una procedura di cooperazione tra le autorità di controllo interessate e l'autorità di controllo dello stabilimento del titolare del trattamento, la cosiddetta «autorità di controllo capofila» [62]. In caso di opinioni divergenti, la controversia deve essere risolta dall'EDPB [63]. Quest'ultimo è anche competente a formulare, su richiesta di un'autorità di controllo, pareri su qualsiasi questione oggetto di interesse da parte di più Stati membri [64].

156. In secondo luogo, il DPC eccepisce l'invalidità della decisione 2010/87 alla luce dell'articolo 47 della Carta, sulla base del rilievo che le autorità di controllo possono tutelare i diritti degli interessati solo per il futuro, senza offrire una soluzione a coloro i cui dati sono già stati trasferiti. In particolare, il DPC rileva che l'articolo 58, paragrafo 2, del RGPD non prevede un diritto di accesso, di rettifica e di cancellazione dei dati raccolti dalle autorità pubbliche del paese terzo né la possibilità di risarcimento dei danni subiti dagli interessati.

60 V., in particolare, le sentenze del 28 luglio 2011, Samba Diouf (C-69/10, EU:C:2011:524, punto 57) e del 17 novembre 2011, Gaydarov (C-430/10, EU:C:2011:749, punto 41).

61 V., a tal proposito, sentenza del 5 giugno 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388, punti da 69 a 73).

62 V. articolo 56, paragrafo 1, del RGPD. Conformemente all'articolo 61 di tale regolamento, le autorità di controllo sono tenute a prestarsi reciproca assistenza. L'articolo 62 di detto regolamento le autorizza a condurre operazioni congiunte.

63 V. articolo 65 del RGPD.

64 V. articolo 64, paragrafo 2, del RGPD.

157. Per quanto riguarda la presunta mancanza di un diritto di accesso, di rettifica e di cancellazione dei dati raccolti, si deve necessariamente constatare che, qualora nel paese terzo di destinazione non esista un ricorso effettivo, i mezzi di ricorso previsti all'interno dell'Unione nei confronti del titolare del trattamento non consentono di ottenere, dalle autorità pubbliche di tale paese terzo, l'accesso a tali dati oppure la loro rettifica o cancellazione.

158. A mio avviso, tale obiezione non giustifica tuttavia l'incompatibilità della decisione 2010/87 con l'articolo 47 della Carta. Infatti, la validità di tale decisione non dipende dal livello di protezione esistente in ciascun paese terzo verso il quale i dati potrebbero essere trasferiti in base alle clausole contrattuali tipo da essa stabilite. Se il diritto dello Stato terzo di destinazione impedisce all'importatore di rispettare tali clausole imponendogli di concedere alle autorità pubbliche l'accesso ai dati non contornato da adeguate possibilità di ricorso, spetta alle autorità di controllo adottare misure correttive, ove l'esportatore non abbia sospeso il trasferimento in forza della clausola 5, lettera a) o b), contenuta nell'allegato alla decisione 2010/87.

159. Inoltre, come ha sottolineato il sig. Schrems, le persone i cui diritti siano stati violati godono oramai, ai sensi dell'articolo 82 del RGPD, di un diritto al risarcimento del danno materiale o morale subito, per effetto di una violazione di tale regolamento, nei confronti del titolare del trattamento o del responsabile del trattamento [65].

160. Come risulta da tutte le suesposte considerazioni, la mia analisi non ha messo in luce alcun elemento atto ad incidere sulla validità della decisione 2010/87 alla luce degli articoli 7, 8 e 47 della Carta.

F. Sulla mancanza della necessità di rispondere alle altre questioni pregiudiziali e di esaminare la validità della decisione «scudo per la privacy»

161. Nella presente sezione, espongo le ragioni, relative principalmente alla limitazione dell'oggetto della controversia nel procedimento principale alla validità della decisione 2010/87, per cui ritengo che non sia necessario rispondere alle questioni pregiudiziali dalla seconda alla quinta nonché nona e decima né pronunciarsi sulla validità della decisione «scudo per la privacy».

162. La seconda questione pregiudiziale attiene all'individuazione delle norme di protezione che un paese terzo deve rispettare affinché i dati possano esservi legittimamente trasferiti in base a clausole contrattuali tipo qualora tali dati, dopo il loro trasferimento, possano essere trattati dalle autorità di tale paese terzo per finalità di sicurezza nazionale. La terza questione sottoposta alla Corte riguarda la determinazione degli elementi che caratterizzano il regime di protezione applicabile nello Stato terzo di destinazione, di cui occorre tener conto per verificare se esso soddisfi tali norme.

163. Con la quarta, la quinta e la decima questione, il giudice del rinvio mira essenzialmente ad accertare se, tenuto conto dei fatti accertati in relazione al diritto statunitense, siano previste in tale paese adeguate garanzie contro le ingerenze da parte delle autorità di intelligence statunitensi nell'esercizio dei diritti fondamentali al rispetto della vita privata, alla protezione dei dati personali e ad una tutela giurisdizionale effettiva.

164. La nona questione pregiudiziale riguarda l'incidenza che riveste, nell'esame con il quale un'autorità di controllo verifica se un trasferimento negli Stati Uniti basato sulle clausole contrattuali tipo previste dalla decisione 2010/87 sia accompagnato da garanzie adeguate, il fatto che la Commissione, nella decisione «scudo per la privacy», ha constatato che gli Stati Uniti offrono un livello adeguato di protezione dei diritti fondamentali delle persone interessate contro tali ingerenze.

65 L'articolo 83, paragrafo 5, lettera c), del RGPD prevede anche l'imposizione di ammende al titolare del trattamento in caso di violazione degli articoli da 44 a 49 di detto regolamento.

165. La questione della validità della decisione «scudo per la privacy» non è stata, a sua volta, esplicitamente sollevata dal giudice del rinvio, anche se, come spiegato più avanti [66], le questioni pregiudiziali quarta, quinta e decima rimettono indirettamente in dubbio la fondatezza dell'accertamento di adeguatezza svolto dalla Commissione in tale decisione.

166. A mio avviso, alla luce degli elementi risultanti dall'analisi precedente, il chiarimento di tali questioni da parte della Corte non potrebbe influire sulla sua conclusione circa la validità in astratto della decisione 2010/87 né, pertanto, influire sulla risoluzione della controversia nel procedimento principale (sezione 1). Inoltre, anche se le risposte della Corte a tali questioni potrebbero, in una fase successiva, rivelarsi utili al DPC al fine di stabilire, nell'ambito della procedura sottesa a tale controversia, se i trasferimenti in questione debbano, in concreto, essere sospesi a causa della presunta mancanza di garanzie adeguate, sarebbe, a mio avviso, prematuro definirle nell'ambito della causa in esame (sezione 2).

1. Sulla mancanza di necessità delle risposte della Corte con riferimento all'oggetto del procedimento principale.

167. Il procedimento principale è risultante, lo ricordo, dall'esercizio, da parte del DPC, del mezzo di ricorso descritto al punto 65 della sentenza Schrems, secondo cui ogni Stato membro deve consentire all'autorità di controllo, qualora lo ritenga necessario ai fini del trattamento di una denuncia di cui è investita, di chiedere a un giudice nazionale di sottoporre alla Corte una questione pregiudiziale relativa alla validità di una decisione di adeguatezza – o, per analogia, di una decisione che introduce clausole contrattuali tipo.

168. A tale riguardo, la High Court (Alta Corte) ha sottolineato che le uniche opzioni di cui dispone, dopo essere stata adita dal DPC, erano o quella di presentare la domanda di pronuncia pregiudiziale sulla validità della decisione 2010/87 richiesta dal DPC nel caso in cui avesse condiviso i suoi dubbi sulla validità di tale decisione, o quella di rifiutare di accogliere tale domanda in caso contrario. Tale giudice considera che, se avesse seguito questa seconda via, avrebbe dovuto respingere l'istanza, poiché la denuncia del DPC non aveva altro scopo [67].

169. Sulla stessa linea, la Supreme Court (Corte suprema), investita di un appello interposto da Facebook Ireland contro la decisione di rinvio, ha descritto il procedimento principale come un procedimento dichiarativo con il quale il DPC chiedeva al giudice del rinvio di sottoporre alla Corte una questione pregiudiziale sulla validità della decisione 2010/87. Secondo il giudice supremo irlandese, l'unica questione sostanziale sollevata dinanzi al giudice del rinvio e dinanzi alla Corte riguarda, quindi, la validità di tale decisione [68].

170. Tenuto conto dell'oggetto del procedimento principale così circoscritto, il giudice del rinvio ha sottoposto alla Corte le sue prime dieci questioni pregiudiziali in quanto considerava che il loro esame rientrasse nella valutazione globale necessaria alla Corte per pronunciarsi, in risposta all'undicesima questione, sulla validità della decisione 2010/87 alla luce degli articoli 7, 8 e 47 della Carta. Tale questione rappresenta, secondo la decisione di rinvio, l'esito logico delle questioni che la precedono.

66 V. paragrafo 175 delle presenti conclusioni.

67 Sentenza della High Court (Alta Corte) del 3 ottobre 2017 (punto 337).

68 Secondo la sentenza della Supreme Court (Corte suprema) del 31 maggio 2019 (punto 2.7), «[t]he sole relief claimed by the DPC is, in substance, a reference to the CJEU under Article 267 [TFUE]». Il punto 2.9 di tale sentenza prosegue nel modo seguente: «Here, the only issue of substance which arises before either the Irish courts or the CJEU is the question of the validity or otherwise of Union measures. Whatever the view taken by the CJEU on that issue, *the Irish courts will have no further role, for the measures under question will either be found to be valid or invalid and in either event, that will be the end of the matter*» (il corsivo è mio).

171. In tale ottica, le questioni dalla seconda alla quinta nonché la nona e la decima mi sembrano fondate sulla premessa secondo la quale la validità della decisione 2010/87 dipenderebbe dal livello di protezione dei diritti fondamentali previsto in ciascun paese terzo verso il quale possono essere trasferiti i dati in base alle clausole contrattuali tipo da essa previste. Orbene, come si evince dalla mia analisi della settima questione [69], tale premessa è, a mio avviso, errata. L'esame del diritto del paese terzo di destinazione interviene solo quando la Commissione adotta una decisione di adeguatezza o quando il titolare del trattamento – o, in mancanza, l'autorità di controllo competente – verifica che, nell'ambito di un trasferimento basato su garanzie adeguate ai sensi dell'articolo 46, paragrafo 1, del RGPD, gli obblighi imposti all'importatore dal diritto di tale paese terzo non compromettano l'effettività della protezione fornita da tali garanzie.

172. Pertanto, le risposte della Corte alle questioni summenzionate non possono influire sulla sua conclusione relativa all'undicesima questione [70]. Non è pertanto necessario rispondere a tali questioni dal punto di vista dell'oggetto del procedimento principale.

173. Propongo alla Corte di limitarsi a trattare la causa in esame sotto il profilo dell'oggetto di tale controversia. A mio avviso, la Corte non dovrebbe andare oltre quanto necessario per la soluzione di detta controversia esaminando le questioni pregiudiziali dal punto di vista della procedura sottostante, pendente dinanzi al DPC. Come di seguito esposto, tale invito a limitarsi dipende, da un lato, dalla preoccupazione di non eludere il normale svolgimento del procedimento che dovrà proseguire dinanzi al DPC dopo che la Corte avrà statuito sulla validità decisione 2010/87. D'altro lato, alla luce dei fatti del caso di specie, mi sembrerebbe un po' precipitoso, anche dal punto di vista dell'oggetto di tale procedimento, che la Corte esamini le problematiche poste dalle questioni dalla seconda alla quinta nonché dalle questioni nona e decima.

2. Sulle ragioni che militano contro un esame, da parte della Corte, alla luce dell'oggetto del procedimento pendente dinanzi al DPC

174. Nella denuncia presentata al DPC, il sig. Schrems chiede a tale autorità di controllo di esercitare i poteri di cui dispone in forza dell'articolo 58, paragrafo 2, lettera f), del RGPD, ordinando a Facebook Ireland di sospendere il trasferimento, effettuato in base a clausole contrattuali, dei suoi dati personali verso gli Stati Uniti. A sostegno di tale domanda, il sig. Schrems invoca essenzialmente l'inadeguatezza di tali garanzie contrattuali in relazione alle ingerenze nell'esercizio dei suoi diritti fondamentali derivanti dalle attività dei servizi di intelligence statunitensi.

69 V. paragrafo 124 delle presenti conclusioni.

70 Per lo stesso motivo, la Supreme Court (Corte suprema), nella sentenza del 31 maggio 2019 (punti da 8.1 a 8.5), pur riconoscendo di non essere competente a rimettere in discussione la decisione del giudice del rinvio di sottoporre alla Corte le questioni pregiudiziali e a modificarne i termini, ha espresso dubbi sulla necessità di alcune di tali questioni. In particolare, il punto 8.5 di tale sentenza stabilisce quanto segue: «The sole purpose of the proceedings before the courts in Ireland was to enable the High Court to refer that question of validity to the CJEU and obtain a definitive answer from the only court which has competence to make the decision in question. It is difficult, therefore, to see how the High Court needs answers to many of the questions which have been referred, for the answers to those questions are only relevant to the question of the validity of the challenged measures (...)».

175. L'argomento del sig. Schrems rimette in discussione la constatazione, effettuata dalla Commissione nella decisione «scudo per la privacy», secondo cui gli Stati Uniti garantiscono un livello di protezione adeguato dei dati trasferiti in base a tale decisione, tenuto conto delle restrizioni apportate all'accesso a tali dati e al loro uso da parte delle autorità di intelligence statunitensi nonché della tutela giuridica offerta agli interessati [71]. Le preoccupazioni espresse dal DPC in via provvisoria [72], nonché dal giudice del rinvio nell'ambito delle questioni quarta, quinta e decima, suscitano anche, indirettamente, dubbi sulla fondatezza di tale constatazione.

176. È vero che la decisione «scudo per la privacy» si limita a constatare l'adeguatezza del livello di protezione dei dati personali trasferiti, conformemente ai principi da essa sanciti, verso un'impresa con sede negli Stati Uniti che abbia autocertificato la sua adesione a tali principi [73]. Tuttavia, le considerazioni in essa contenute vanno oltre il contesto dei trasferimenti cui si riferisce tale decisione, in quanto riguardano il diritto e le prassi in vigore in tale paese terzo riguardo al trattamento, a fini di protezione della sicurezza nazionale, dei dati trasferiti. Come hanno osservato, in sostanza, Facebook Ireland, il sig. Schrems, il governo degli Stati Uniti e la Commissione, la sorveglianza esercitata dalle autorità di intelligence statunitensi, nonché le garanzie contro il rischio di abusi che essa comporta e i meccanismi diretti a controllarne il rispetto, si applicano, dal punto di vista del diritto dell'Unione, indipendentemente dalla base giuridica invocata a sostegno del trasferimento.

177. In tale prospettiva, la questione se le constatazioni effettuate al riguardo nella decisione «scudo per la privacy» siano vincolanti per le autorità di controllo quando esaminano la legittimità di un trasferimento effettuato in base a clausole contrattuali tipo potrebbe rivelarsi pertinente ai fini del trattamento della denuncia del sig. Schrems da parte del DPC. In caso di risposta affermativa a tale questione, si porrebbe la questione della piena validità di tale decisione.

178. Tuttavia, sconsiglio alla Corte di pronunciarsi su tali questioni al solo scopo di aiutare il DPC a trattare tale denuncia, mentre non è necessario rispondere alle stesse per consentire al giudice del rinvio di risolvere la controversia nel procedimento principale. Poiché il procedimento di cui all'articolo 267 del TFUE instaura un dialogo tra giudici, la Corte non è chiamata a fornire chiarimenti unicamente al fine di assistere un'autorità amministrativa nell'ambito di una procedura sottostante a tale controversia.

179. A mio avviso, la riserva è tanto più necessaria in quanto non le è stata espressamente sottoposta la questione della validità della decisione «scudo per la privacy», e tale decisione è già, peraltro, oggetto di un ricorso di annullamento pendente dinanzi al Tribunale dell'Unione europea [74].

180. Inoltre, pronunciandosi sulle problematiche sopra descritte, la Corte perturberebbe, a mio avviso, il normale corso del procedimento che si dovrà svolgere dopo la pronuncia della sua sentenza nella presente causa. Nell'ambito di tale procedimento, spetterà al DPC trattare la denuncia del sig. Schrems tenendo conto della risposta che la Corte fornirà relativamente all'undicesima questione pregiudiziale. Qualora la Corte dichiari, come da me proposto e contrariamente a quanto sostenuto dal DPC dinanzi ad essa, che la decisione 2010/87 non è invalida alla luce degli articoli 7, 8 e 47 della

71 V. considerando da 64 a 141 della decisione «scudo per la privacy». Ricordo che, come risulta dall'articolo 1, paragrafo 2, di tale decisione, lo scudo per la privacy è costituito non solo da principi ai quali devono attenersi le imprese che intendono trasferire dati in base a tale decisione, ma anche dalle dichiarazioni e impegni ufficiali da parte del governo degli Stati Uniti e contenuti nei documenti ad essa allegati.

72 Il progetto di decisione del DPC precede l'adozione della decisione «scudo per la privacy». Come precisato dal DPC in tale progetto, sebbene abbia concluso in tale progetto, provvisoriamente, che le garanzie previste dal diritto degli Stati Uniti non consentivano, quantomeno, di garantire la conformità dei trasferimenti verso tale paese terzo con l'articolo 47 della Carta, *esso non ha esaminato o preso in considerazione, in tale fase, le nuove disposizioni previste nel progetto di accordo relativo allo «scudo per la privacy», in quanto quest'ultimo non era stato ancora adottato*. Ciò premesso, al punto 307 della sentenza del 3 ottobre 2017, la High Court (Alta Corte) considera quanto segue: «It is fair to conclude (...) that the decision of the Commission in regard to the adequacy of the protections afforded to EU citizens against interference by the intelligence authorities in the [U.S.] with the fundamental rights of EU citizens whose data are transferred from the [EU] to the [U.S.], conflicts with the case made by the DPC to this court».

73 V. articolo 1, paragrafi 1 e 3, nonché considerando da 14 a 16 della decisione «scudo per la privacy».

74 Causa pendente T-738/16, La Quadrature du Net e a./Commissione (GU 2017, C 6, pag. 39).

Carta, il DPC dovrebbe avere, a mio avviso, la possibilità di riesaminare il fascicolo del procedimento dinanzi ad esso pendente. Nel caso in cui il DPC ritenesse di non essere in grado di pronunciarsi sulla denuncia del sig. Schrems senza che la Corte abbia preliminarmente accertato se la decisione «scudo per la privacy» osti all'esercizio dei suoi poteri di sospensione del trasferimento in questione e confermasse di nutrire dubbi sulla validità di tale decisione, il CPD potrebbe adire nuovamente i giudici nazionali affinché questi ultimi interpellino la Corte al riguardo [75].

181. A quel punto verrebbe avviato un procedimento che consentirebbe a qualsiasi parte e a qualsiasi interessato di cui all'articolo 23, secondo comma, dello Statuto della Corte di presentare alla Corte osservazioni riguardanti specificamente la validità della decisione «scudo per la privacy», indicando, se del caso, le valutazioni specifiche che contesta e le ragioni per cui ritiene che la Commissione abbia superato, in tale decisione, il ridotto margine di discrezionalità di cui disponeva [76]. Nell'ambito di tale procedimento la Commissione avrebbe l'opportunità di rispondere in modo preciso e dettagliato a ciascuna delle eventuali critiche mosse contro tale decisione. Sebbene la causa in esame abbia offerto la possibilità alle parti e agli interessati che hanno presentato osservazioni alla Corte di discutere su taluni aspetti pertinenti al fine di valutare la conformità della decisione «scudo per la privacy» agli articoli 7, 8 e 47 della Carta, tale questione merita, data la sua importanza, che le sia dedicato uno scambio esauriente e approfondito.

182. A mio avviso, la prudenza impone di attendere che si siano svolte tali fasi procedurali prima che la Corte esamini l'incidenza della decisione «scudo per la privacy» sul trattamento, da parte di un'autorità di controllo, di una domanda di sospensione di un trasferimento effettuato verso gli Stati Uniti ai sensi dell'articolo 46, paragrafo 1, del RGPD e si pronunci sulla validità di tale decisione.

183. Ciò vale, a maggior ragione, in quanto il fascicolo presentato alla Corte non consente di concludere che il trattamento della denuncia del sig. Schrems, da parte del DPC, dipenderà necessariamente dalla questione se la decisione «scudo per la privacy» osti all'esercizio, da parte delle autorità di controllo, dei loro poteri di sospensione di un trasferimento basato su clausole contrattuali tipo.

184. A tale riguardo, in primo luogo, non è escluso che il DPC sia indotto a sospendere il trasferimento in questione per ragioni diverse da quelle attinenti alla presunta inadeguatezza del livello di protezione garantito negli Stati Uniti contro lesioni dei diritti fondamentali degli interessati derivanti dalle attività dei servizi di intelligence statunitensi. In particolare, il giudice del rinvio ha precisato che il sig. Schrems sostiene, nella sua denuncia al DPC, che le clausole contrattuali invocate da Facebook Ireland a sostegno di tale trasferimento non rispecchiano fedelmente quelle contenute nell'allegato alla decisione 2010/87. Il sig. Schrems sostiene inoltre che detto trasferimento rientra nell'ambito di applicazione non già di tale decisione, bensì delle altre decisioni CCT [77].

185. In secondo luogo, il DPC e il giudice del rinvio hanno sottolineato che Facebook Ireland non ha invocato, a sostegno del trasferimento oggetto della denuncia del sig. Schrems, la decisione «scudo per la privacy» [78], circostanza che tale società ha confermato in udienza. Sebbene Facebook Inc. abbia autocertificato la sua adesione ai principi dello scudo per la privacy dal 30 settembre 2016 [79], Facebook Ireland afferma che tale adesione riguarda soltanto il trasferimento di talune categorie di dati, ossia quelle concernenti i partner commerciali di Facebook Inc. Riterrei inopportuno che la Corte

75 Osservo peraltro che, nelle sue osservazioni scritte, il DPC non ha preso posizione sull'incidenza della decisione «scudo per la privacy» sul trattamento della denuncia di cui è investito.

76 V., a tale riguardo, sentenza Schrems (punto 78).

77 A sostegno di tale argomentazione, il sig. Schrems fa valere che Facebook Inc. deve essere considerata non solo come responsabile del trattamento, ma anche come «titolare del trattamento» ai sensi dell'articolo 4, punto 7, del RGPD, per quanto riguarda il trattamento dei dati personali degli utenti della rete sociale Facebook. V., a tale riguardo, sentenza del 5 giugno 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388, punto 30).

78 V. sentenza della High Court (Alta Corte) del 3 ottobre 2017 (punto 66).

79 V. sito Internet dello «scudo per la privacy» (https://www.privacyshield.gov/participant_search).

anticipasse gli interrogativi che potrebbero sorgere al riguardo, esaminando se, nel caso in cui Facebook Ireland non possa fondarsi sulla decisione 2010/87 a sostegno del trasferimento in questione, tale trasferimento rientrerebbe comunque nella decisione «scudo per la privacy», anche se quest'ultima non ha dedotto tale argomento né dinanzi al giudice del rinvio né dinanzi al DPC.

186. Concludo che non è necessario rispondere alle questioni pregiudiziali dalla seconda alla quinta nonché alle questioni pregiudiziali nona e decima né esaminare la validità della decisione «scudo per la privacy».

G. Osservazioni in subordine relative agli effetti e alla validità della decisione «scudo per la privacy»

187. Sebbene l'analisi precedente mi induca a proporre alla Corte, in via principale, di astenersi dal pronunciarsi sull'incidenza della decisione «scudo per la privacy» sul trattamento di una denuncia come quello presentata dal sig. Schrems dinanzi al DPC e sulla validità di tale decisione, mi è sembrato utile formulare, in subordine e con riserva, alcune osservazioni non esaustive al riguardo.

1. Sull'incidenza della decisione «scudo per la privacy» nel trattamento, da parte di un'autorità di controllo, di una denuncia relativa alla legittimità di un trasferimento basato su garanzie contrattuali

188. La nona questione pregiudiziale pone il problema se la constatazione effettuata nella decisione «scudo per la privacy» circa l'adeguatezza – alla luce delle limitazioni apportate all'accesso ai dati trasferiti e al loro uso da parte delle autorità statunitensi a fini della sicurezza nazionale e della protezione giuridica delle persone interessate – del livello di protezione garantito negli Stati Uniti osti a che un'autorità di controllo sospenda un trasferimento verso tale paese terzo effettuato in forza di clausole contrattuali tipo.

189. Tale problematica deve essere considerata, a mio avviso, alla luce dei punti 51 e 52 della sentenza Schrems, da cui risulta che una decisione di adeguatezza è vincolante per le autorità di controllo fino a quando non viene dichiarata nulla. L'autorità di controllo investita della denuncia di una persona i cui dati sono trasferiti verso il paese terzo oggetto di una decisione di adeguatezza non può, pertanto, sospendere il trasferimento per il motivo che il livello di protezione è, in tale paese, inadeguato, senza che la Corte abbia preventivamente dichiarato l'invalidità di tale decisione [80].

190. Il giudice del rinvio chiede essenzialmente se, nel caso di una decisione di adeguatezza – come la decisione «scudo per la privacy» o, prima di essa, la decisione «approdo sicuro» – basata sull'adesione volontaria delle imprese ai principi che essa stabilisce, tale conclusione valga solo nei limiti in cui il trasferimento verso il paese terzo in questione è contemplato da tale decisione, o anche quando è fondato su una base giuridica distinta.

191. Secondo il sig. Schrems, i governi tedesco, dei Paesi Bassi, polacco e portoghese nonché la Commissione, la constatazione di adeguatezza effettuata nella decisione «scudo per la privacy» non priva le autorità di controllo del loro potere di sospendere o di vietare un trasferimento verso gli Stati Uniti eseguito in forza di clausole contrattuali tipo. Qualora il trasferimento negli Stati Uniti non sia basato sulla decisione «scudo per la privacy», le autorità di controllo non sarebbero formalmente vincolate da tale decisione nell'esercizio dei poteri loro conferiti dall'articolo 58, paragrafo 2, del RGPD. In altri termini, tali autorità potrebbero prendere le distanze dalle constatazioni effettuate dalla Commissione sull'adeguatezza del livello di protezione contro le ingerenze delle autorità pubbliche statunitensi nell'esercizio dei diritti fondamentali delle persone interessate. Il governo dei Paesi Bassi e

80 V., in tal senso, sentenza Schrems (punto 59).

la Commissione precisano che le autorità di controllo devono, tuttavia, tenerne conto allorché si avvalgono di tali poteri. Secondo il governo tedesco, tali autorità potrebbero effettuare valutazioni contrarie solo al termine di un esame nel merito, comprese le indagini pertinenti, delle constatazioni della Commissione.

192. Per contro, Facebook Ireland e il governo degli Stati Uniti affermano, in sostanza, che l'effetto vincolante di una decisione di adeguatezza implica, alla luce dei principi di certezza del diritto e di applicazione uniforme del diritto dell'Unione, che le autorità di controllo non siano autorizzate a rimettere in discussione le constatazioni contenute in tale decisione, neppure nell'ambito del trattamento di una denuncia diretta a ottenere la sospensione di trasferimenti effettuati verso il paese terzo in questione su una base diversa dalla suddetta decisione.

193. Concordo con il primo di questi due approcci. Poiché l'ambito di applicazione della decisione «scudo per la privacy» è limitato ai trasferimenti eseguiti verso un'impresa autocertificata ai sensi di tale decisione, detta decisione non può essere formalmente vincolante per le autorità di controllo in caso di trasferimenti che non rientrano in tale ambito di applicazione. Correlativamente, la decisione «scudo per la privacy» è volta a garantire la certezza del diritto solo a vantaggio degli esportatori che trasferiscono dati nell'ambito da essa stabilito. A mio avviso, l'indipendenza che l'articolo 52 del RGPD riconosce alle autorità di controllo tende anche a ostare a che esse siano vincolate dalle constatazioni effettuate dalla Commissione in una decisione di adeguatezza, persino al là del suo ambito di applicazione.

194. Naturalmente, le constatazioni contenute nella decisione «scudo per la privacy», relative all'adeguatezza del livello di protezione garantito negli Stati Uniti contro le ingerenze connesse alle attività dei loro servizi di intelligence, costituiscono il punto di partenza dell'analisi con cui un'autorità di controllo valuta, caso per caso, se un trasferimento basato su clausole contrattuali tipo debba essere sospeso a causa di tali ingerenze. Tuttavia, a mio avviso, l'autorità di controllo compente, se, al termine di un'indagine approfondita, ritenga di non poter concordare con tali constatazioni riguardo al trasferimento portato alla sua attenzione, mantiene la facoltà di esercitare i poteri ad essa conferiti dall'articolo 58, paragrafo 2, lettere f) e j), del RGPD.

195. Ciò premesso, per l'ipotesi in cui la Corte riservasse alla questione in esame una risposta contraria a quella che sto propugnando, sarebbe necessario esaminare se tali poteri non debbano nondimeno essere ripristinati a causa dell'invalidità della decisione «scudo per la privacy».

2. Sulla validità della decisione «scudo per la privacy»

196. Le osservazioni che seguono solleveranno taluni interrogativi sulla fondatezza delle valutazioni contenute nella decisione «scudo per la privacy» per quanto riguarda l'adeguatezza, ai sensi dell'articolo 45, paragrafo 1, del RGPD, del livello di protezione garantito dagli Stati Uniti in relazione alle attività di sorveglianza delle comunicazioni elettroniche svolte dalle autorità di intelligence statunitensi. Tali osservazioni non intendono esporre una posizione definitiva o esaustiva sulla validità di tale decisione. Esse si limiteranno a fornire talune riflessioni che potrebbero rivelarsi utili alla Corte qualora, contrariamente a quanto raccomando, volesse pronunciarsi su questo punto.

197. A tal proposito, dal considerando 64 e dal punto I.5 dell'allegato II della decisione «scudo per la privacy» risulta che l'adesione delle imprese ai principi enunciati in tale decisione può essere limitata, in particolare, da esigenze relative alla sicurezza nazionale, all'interesse pubblico e all'osservanza della legge o da obblighi contrastanti ai sensi del diritto statunitense.

198. La Commissione ha pertanto valutato le garanzie previste nel diritto degli Stati Uniti per quanto riguarda l'accesso ai dati trasferiti e il loro uso da parte delle autorità pubbliche statunitensi a fini, in particolare, di sicurezza nazionale [81]. Essa ha ottenuto che il governo statunitense assumesse taluni impegni riguardanti, da un lato, le limitazioni all'accesso e all'uso, da parte delle autorità statunitensi, dei dati trasferiti nonché, dall'altro, la tutela giuridica offerta agli interessati [82].

199. Dinanzi alla Corte, il sig. Schrems eccepisce l'invalidità della decisione «scudo per la privacy» con la motivazione che le garanzie così descritte non sono sufficienti ad assicurare un livello adeguato di protezione dei diritti fondamentali delle persone i cui dati sono trasferiti negli Stati Uniti. Il DPC, l'EPIC nonché i governi austriaco, polacco e portoghese, senza rimettere direttamente in discussione la validità di tale decisione, contestano le valutazioni in essa effettuate dalla Commissione quanto all'adeguatezza del livello di protezione contro le ingerenze derivanti dalle attività dei servizi di intelligence statunitensi. Tali dubbi riflettono le preoccupazioni espresse dal Parlamento [83], dall'EDPB [84] e dal GEPD [85].

200. Prima di esaminare la fondatezza della constatazione di adeguatezza effettuata nella decisione «scudo per la privacy», è necessario precisare la metodologia cui deve attenersi tale esame.

a) Precisazioni riguardanti il contenuto dell'esame di validità di una decisione di adeguatezza

1) Sui termini di paragone che consentono di valutare l'«equivalenza sostanziale» del livello di protezione

201. Conformemente all'articolo 45, paragrafo 3, del RGPD e alla giurisprudenza della Corte [86], la Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato solo a condizione di aver concluso, in modo debitamente motivato, che il livello di protezione dei diritti fondamentali degli persone interessati, in tale paese, è «sostanzialmente equivalente»» a quello richiesto nell'Unione ai sensi di tale regolamento letto alla luce della Carta.

202. Pertanto, la verifica dell'adeguatezza del livello di protezione garantito in un paese terzo implica necessariamente un confronto tra le norme e le prassi esistenti in tale paese terzo, da un lato, e gli standard di protezione in vigore nell'Unione, dall'altro. Con la seconda questione, il giudice del rinvio chiede alla Corte di precisare i termini di tale confronto [87].

81 V. considerando 65 della decisione «scudo per la privacy».

82 V. allegati da III a VII della decisione «scudo per la privacy».

83 Risoluzioni del Parlamento europeo del 6 aprile 2017 sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy, P8_TA(2017)0131 e del 5 luglio 2018 sull'adeguatezza della protezione garantita dallo scudo UE-USA per la privacy, P8_TA(2018)0315.

84 V. gruppo di lavoro «articolo 29» sulla protezione dei dati (in prosieguo: il «Gruppo 29»), Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, 13 aprile 2016, WP 238; Gruppo 29, EU-US Privacy Shield – First Annual Joint Review, 28 novembre 2017, WP 255, e EDPB, EU-US Privacy Shield – Second Annual Joint Review, 22 gennaio 2019. Il gruppo 29 era stato istituito ai sensi dell'articolo 29, paragrafo 1, della direttiva 95/46, che ne prevedeva la natura consultiva e indipendente. Ai sensi del paragrafo 2 di tale articolo, il gruppo era composto da un rappresentante di ciascuna autorità di controllo nazionale, da un rappresentante di ciascuna autorità creata per le istituzioni e gli organismi comunitari e da un rappresentante della Commissione. Dall'entrata in vigore del RGPD, il Gruppo 29 è stato sostituito dall'EDPB (v. articolo 94, paragrafo 2, di tale regolamento).

85 V. GEPD, parere 4/2016 riguardante lo «scudo UE-USA per la privacy» (Privacy Shield) – Progetto di decisione di adeguatezza del 30 maggio 2016. Il GEPD è stato istituito dall'articolo 1, paragrafo 2, del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU 2001, L 8, pag. 1). Esso controlla l'applicazione delle disposizioni di tale regolamento.

86 V. paragrafo 112 delle presenti conclusioni.

87 Ricordo che l'equivalenza sostanziale del livello di protezione garantito da uno Stato terzo rispetto a quello che è richiesto nell'Unione deve essere valutata anche quando, nell'ambito di uno specifico trasferimento basato sulle clausole contrattuali tipo previste dalla decisione 2010/87, il titolare del trattamento o, in mancanza, l'autorità di controllo competente verifica se le autorità pubbliche del paese terzo di destinazione sottopongano l'importatore a obblighi che superano i limiti di quanto necessario in una società democratica (v. clausola 5 contenuta nell'allegato alla decisione 2010/87 e relativa nota a piè di pagina). V. paragrafi 115, 134 e 135 delle presenti conclusioni.

203. Più specificamente, tale giudice chiede se la riserva di competenza riconosciuta, dall'articolo 4, paragrafo 2, TUE e dall'articolo 2, paragrafo 2, del RGPD, agli Stati membri in materia di protezione della sicurezza nazionale implichi che l'ordinamento giuridico dell'Unione non include standard di protezione ai quali dovrebbero essere raffrontate, per valutarne l'adeguatezza, le garanzie che disciplinano, in un paese terzo, il trattamento a fini di protezione della sicurezza nazionale, da parte delle autorità pubbliche, dei dati ivi trasferiti. In caso di risposta affermativa, detto giudice chiede come debba essere determinato il quadro di riferimento pertinente.

204. A tale riguardo, occorre tenere presente che la ragion d'essere delle restrizioni apportate dal diritto dell'Unione ai trasferimenti internazionali di dati personali, nell'esigere che sia garantita la continuità del livello di protezione dei diritti delle persone interessate, mira a evitare il rischio di elusione degli standard applicabili all'interno dell'Unione [88]. Come affermato, in sostanza, da Facebook Ireland, non sarebbe in alcun modo giustificato, alla luce di tale obiettivo, attendersi che un paese terzo rispetti requisiti che non corrispondono ad obblighi incombenti agli Stati membri.

205. Orbene, conformemente all'articolo 51, paragrafo 1, la Carta è applicabile agli Stati membri esclusivamente nell'attuazione del diritto dell'Unione. Di conseguenza, la validità di una decisione di adeguatezza alla luce delle restrizioni all'esercizio dei diritti fondamentali degli interessati derivanti dalla normativa del paese terzo di destinazione dipende da un confronto tra tali restrizioni e quelle che sarebbero autorizzate per gli Stati membri in base alle disposizioni della Carta *solo nei limiti in cui norme analoghe di uno Stato membro rientrino nell'ambito di applicazione del diritto dell'Unione*.

206. Tuttavia, l'adeguatezza del livello di protezione garantito nel paese terzo di destinazione non può essere valutata ignorando le eventuali ingerenze nell'esercizio dei diritti fondamentali degli interessati derivanti da misure statali, in particolare nel settore della sicurezza nazionale, che, se fossero adottate da uno Stato membro, esulerebbero dall'ambito di applicazione del diritto dell'Unione. Ai fini di tale valutazione, l'articolo 45, paragrafo 2, lettera a), del RGPD richiede che si tenga conto, senza alcuna limitazione, delle norme in materia di sicurezza nazionale in vigore in tale Stato terzo.

207. Valutare l'adeguatezza del livello di protezione alla luce di tali misure statali implica, a mio avviso, il confronto tra le garanzie da cui sono contornate e il livello di protezione richiesto all'interno dell'Unione in forza del diritto degli Stati membri, compresi gli impegni da essi assunti a norma della CEDU. Poiché l'adesione degli Stati membri alla CEDU li obbliga a rendere i loro diritti interni conformi alle disposizioni di tale convenzione e costituisce quindi, come hanno sottolineato, in sostanza, Facebook Ireland, i governi tedesco e ceco nonché la Commissione, un denominatore comune agli Stati membri, considererò tali disposizioni come il termine di paragone pertinente ai fini della presente valutazione.

208. Nella fattispecie, come già menzionato in precedenza [89], i requisiti relativi alla sicurezza nazionale degli Stati Uniti prevalgono sugli obblighi delle imprese autocertificati ai sensi della decisione «scudo per la privacy». Pertanto, la validità di tale decisione dipende dalla questione se tali requisiti siano contornati da garanzie che offrano un livello di protezione sostanzialmente equivalente a quello che deve essere garantito nell'Unione.

209. La risposta a tale questione richiede, in via preliminare, di individuare gli standard – vale a dire quelli derivanti dalla Carta o dalla CEDU – ai quali dovrebbero corrispondere, all'interno dell'Unione, normative in materia di controllo delle comunicazioni elettroniche simili a quelle esaminate dalla Commissione nella decisione «scudo per la privacy». La determinazione degli standard applicabili

88 V. paragrafo 117 delle presenti conclusioni.

89 V. paragrafo 197 delle presenti conclusioni.

dipende dalla questione se normative come l'articolo 702 del FISA e l'EO 12333, ove promanate da uno Stato membro, rientrerebbero o meno nella limitazione apportata all'ambito di applicazione del RGPD ai sensi dell'articolo 2, paragrafo 2, di tale regolamento, letto alla luce dell'articolo 4, paragrafo 2, TUE.

210. A tal proposito, dalla formulazione dell'articolo 4, paragrafo 2, TUE e dalla giurisprudenza consolidata risulta che il diritto dell'Unione e, in particolare, gli atti di diritto derivato relativi alla protezione dei dati personali non si applicano alle attività in materia di protezione della sicurezza nazionale, in quanto costituiscono attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei singoli [90].

211. Tale principio implica, *da un lato*, che una normativa nel settore della protezione della sicurezza nazionale non rientra nell'ambito di applicazione del diritto dell'Unione allorché disciplina unicamente attività statali, senza disciplinare alcuna attività esercitata da privati. Di conseguenza tale diritto non si applica, a mio avviso, a misure nazionali relative alla raccolta e all'uso di dati personali direttamente attuate dallo Stato a fini di protezione della sicurezza nazionale, senza imporre obblighi specifici a operatori privati. In particolare, come ha sostenuto la Commissione in udienza, una misura adottata da uno Stato membro che, al pari dell'EO 12333, autorizzi l'accesso diretto, da parte dei suoi servizi di sicurezza, ai dati in transito, sarebbe esclusa dall'ambito di applicazione del diritto dell'Unione [91].

212. Ben più complessa è la questione se, *d'altro lato*, disposizioni nazionali che, al pari dell'articolo 702 del FISA, obbligano i fornitori di servizi di comunicazione elettronica ad offrire la loro assistenza alle autorità competenti in materia di sicurezza nazionale per consentire loro di accedere a determinati dati personali esulino anch'esse dall'ambito di applicazione del diritto dell'Unione.

213. Mentre la sentenza PNR depone a favore di una risposta affermativa a tale questione, il ragionamento adottato nelle sentenze Tele2 Sverige e Ministerio Fiscal potrebbe giustificare che a tale questione sia data una risposta negativa.

214. Nella sentenza PNR la Corte ha annullato la decisione nella quale la Commissione aveva constatato l'adeguatezza del livello di protezione dei dati personali contenuti nelle schede nominative dei passeggeri aerei (Passenger Name Records, PNR), trasferiti all'autorità statunitense competente in materia di dogane e di protezione delle frontiere [92]. La Corte ha dichiarato che il trattamento sul quale verteva tale decisione – ossia il trasferimento dei dati PNR da parte delle compagnie aeree all'autorità in questione – rientrava, tenuto conto del suo scopo, nell'esclusione dall'ambito di applicazione della direttiva 95/46, prevista dall'articolo 3, paragrafo 2, della stessa. Secondo la Corte tale trattamento era necessario non già per la realizzazione di una prestazione di servizi, bensì per la salvaguardia della sicurezza pubblica e a fini repressivi. Poiché il trasferimento in questione si inseriva in un quadro

90 V., in particolare, sentenza del 6 novembre 2003, Lindqvist (C-101/01, EU:C:2003:596, punti 43 et 44), sentenza PNR (punto 58), sentenza del 16 dicembre 2008, Satakunnan Markkinapörssi e Satamedia (C-73/07, EU:C:2008:727, punto 41), sentenza del 21 dicembre 2016, Tele2 Sverige e Watson e a. (C-203/15 e C-698/15, EU:C:2016:970; in prosieguo: la «sentenza Tele2 Sverige», punto 69), nonché sentenza del 2 ottobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788; in prosieguo: la «sentenza Ministerio Fiscal», punto 32).

91 Al fine di evitare qualsiasi confusione su questo punto, sottolineo che, nella decisione «scudo per la privacy», la Commissione non è stata in grado di stabilire se gli Stati Uniti intercettino effettivamente le comunicazioni che transitano sui cavi transatlantici, in quanto le autorità statunitensi non hanno né confermato né smentito tale affermazione [v. considerando 75 di tale decisione e lettera del sig. Robert Litt, del 22 febbraio 2016, contenuta nel suo allegato VI, punto I, lettera a)]. Tuttavia, poiché il governo degli Stati Uniti non ha negato la raccolta di dati in transito in base all'EO 12333, mi sembra che, prima di procedere alla constatazione dell'adeguatezza, la Commissione avrebbe dovuto ottenere, da parte di quest'ultimo, l'assicurazione che siffatta raccolta, se fosse avvenuta, sarebbe stata accompagnata da sufficienti garanzie contro i rischi di abuso. È in quest'ottica che la Commissione ha esaminato, ai considerando da 68 a 77 di tale decisione, le limitazioni e le garanzie che dovrebbero essere applicate in un'ipotesi del genere ai sensi della PPD 28.

92 Si trattava della decisione 2004/535/CE della Commissione, del 14 maggio 2004, relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti (United States' Bureau of Customs and Border Protection) (GU 2004, L235, pag. 11).

istituito dalle autorità pubbliche e finalizzato alla sicurezza pubblica, esso era escluso dall'ambito di applicazione di tale direttiva nonostante il fatto che i dati PNR fossero inizialmente raccolti da operatori privati nell'ambito di un'attività commerciale rientrante in tale campo di applicazione e che detto trasferimento fosse organizzato da questi ultimi [93].

215. Nella successiva sentenza Tele2 Sverige [94], la Corte ha dichiarato che le disposizioni nazionali, basate sull'articolo 15, paragrafo 1, della direttiva 2002/58/CE [95], che disciplinano tanto la conservazione, da parte dei fornitori di servizi di telecomunicazione, di dati relativi al traffico e all'ubicazione, quanto l'accesso delle autorità pubbliche ai dati memorizzati per le finalità menzionate in tale disposizione – che comprendono la repressione degli illeciti penali e la protezione della sicurezza nazionale – rientrano nell'ambito di applicazione di tale direttiva e, pertanto, della Carta. Secondo la Corte, né le disposizioni sulla conservazione dei dati né quelle sull'accesso ai dati memorizzati rientrano nell'esclusione dall'ambito di applicazione di tale direttiva di cui all'articolo 1, paragrafo 3, che fa riferimento, in particolare, alle attività dello Stato nel settore della repressione e della protezione della sicurezza nazionale [96]. La Corte ha confermato tale giurisprudenza nella sentenza Ministerio Fiscal [97].

216. L'articolo 702 del FISA differisce, tuttavia, da siffatta normativa in quanto tale disposizione non impone ai fornitori di servizi di comunicazione elettronica alcun obbligo di conservare i dati n" di effettuare qualsivoglia altro trattamento in mancanza di una domanda di accesso ai dati da parte delle autorità di intelligence.

217. Sorge quindi la questione se rientrino nell'ambito di applicazione del RGPD e, pertanto, della Carta, misure nazionali che impongono a tali fornitori l'obbligo di mettere i dati a disposizione delle autorità pubbliche a fini di sicurezza nazionale, *indipendentemente da qualsiasi obbligo di conservazione* [98].

218. Un *primo approccio* potrebbe consistere nel conciliare, per quanto possibile, le due linee giurisprudenziali summenzionate interpretando la conclusione raggiunta dalla Corte nelle sentenze Tele2 Sverige e Ministerio Fiscal, riguardante l'applicabilità del diritto dell'Unione alle misure che disciplinano l'accesso ai dati da parte delle autorità nazionali per finalità, in particolare, di protezione

93 Sentenza PNR (punti da 56 a 58). Inoltre, nella sentenza del 10 febbraio 2009, Irlanda/Parlamento e Consiglio (C-301/06, EU:C:2009:68, punti 90 e 91), la Corte ha dichiarato che le considerazioni formulate nella sentenza PNR non potevano essere estese ai trattamenti di cui alla direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (GU 2006, L 105, pag. 54). La Corte ha giustificato tale conclusione con il fatto che la direttiva 2006/24, a differenza della decisione controversa nella sentenza PNR, disciplinava soltanto le attività dei fornitori di servizi nel mercato interno, senza disciplinare le attività delle autorità pubbliche a fini repressivi. Con tale ragionamento, la Corte sembra aver affermato che, a contrario, la conclusione raggiunta nella sentenza PNR avrebbe potuto essere estesa a disposizioni relative all'accesso ai dati memorizzati o al loro uso da parte di tali autorità.

94 Sentenza Tele2 Sverige (punti da 67 a 81).

95 Direttiva del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU 2002, L 201, pag. 37).

96 Poiché la direttiva 2002/58 dà concreta attuazione ai requisiti della direttiva 95/46, ora abrogata dal RGPD, che ne riprende ampiamente il contenuto, la giurisprudenza relativa all'interpretazione dell'articolo 1, paragrafo 3, della direttiva 2002/58 è, a mio avviso, applicabile per analogia all'interpretazione dell'articolo 2, paragrafo 2, del RGPD.V., in tal senso, sentenze Tele2 Sverige (punto 69) e Ministerio Fiscal (punto 32).

97 Sentenza Ministerio Fiscal (punti 34, 35 e 37).

98 La stessa questione è stata sollevata in altri tre rinvii pregiudiziali pendenti dinanzi alla Corte. V. causa C-623/17, Privacy International (GU 2018, C 22, pag. 29) e cause riunite C-511/18 e C-512/18, La Quadrature du Net e a. e French Data Network e a. (GU 2018, C 392, pag. 7).

della sicurezza nazionale [99], come limitata ai casi di specie in cui i dati sono stati memorizzati *in virtù di un obbligo giuridico* imposto ai sensi dell'articolo 15, paragrafo 1, della direttiva 2002/58. Tale conclusione non si applicherebbe, per contro, al contesto fattuale distinto della sentenza PNR, che riguardava il trasferimento, di propria iniziativa, ad un'autorità statunitense competente in materia di sicurezza interna di dati memorizzati dalle compagnie aeree a fini commerciali.

219. In base a un *secondo approccio*, che la Commissione auspica e che ritengo più convincente, il ragionamento adottato nelle sentenze Tele2 Sverige e Ministerio Fiscal giustificherebbe l'applicabilità del diritto dell'Unione a norme nazionali che impongono ai fornitori di servizi di comunicazione elettronica di prestare assistenza alle autorità responsabili della sicurezza nazionale affinché queste ultime possano accedere a determinati dati, *indipendentemente dal fatto che tali norme siano o meno accompagnate da un obbligo preventivo di conservazione dei dati*.

220. Il fulcro di tale ragionamento riposa, infatti, non già sull'obiettivo delle disposizioni in questione, come nella sentenza PNR, bensì sul fatto che tali disposizioni disciplinavano le attività dei fornitori imponendo loro di effettuare un trattamento di dati. Tali attività non costituivano attività statali nei settori menzionati all'articolo 1, paragrafo 3, della direttiva 2002/58 e all'articolo 3, paragrafo 2, della direttiva 95/46, il cui contenuto si riflette essenzialmente nell'articolo 2, paragrafo 2, del RGPD.

221. Così, nella sentenza Tele2 Sverige, la Corte ha osservato che «l'accesso ai dati conservati [dai] fornitori, ha ad oggetto attività di trattamento di dati personali realizzate *da questi ultimi*, attività che rientrano nell'ambito di applicazione della direttiva in parola» [100]. Analogamente, essa ha dichiarato, nella sentenza Ministerio Fiscal, che misure legislative che impongano ai fornitori di accordare alle autorità competenti l'accesso ai dati conservati «implicano necessariamente un trattamento, *da parte dei fornitori suddetti*, di questi dati» [101].

222. Orbene, la messa a disposizione di dati da parte del titolare del trattamento a favore di un'autorità pubblica risponde alla definizione di «trattamento» di cui all'articolo 4, punto 2, del RGPD [102]. Lo stesso dicasi per il filtraggio preliminare dei dati mediante criteri di ricerca al fine di isolare quelli relativamente ai quali le autorità pubbliche hanno richiesto l'accesso [103].

223. Concludo che, secondo il ragionamento adottato dalla Corte nelle sentenze Tele2 Sverige e Ministerio Fiscal, il RGPD e, di conseguenza, la Carta si applicano a una normativa nazionale che impone a un fornitore di servizi di comunicazioni elettroniche di offrire il proprio contributo alle autorità responsabili della sicurezza nazionale, mettendo loro a disposizione i dati, eventualmente dopo averli filtrati, anche indipendentemente da qualsiasi obbligo giuridico di conservazione di tali dati.

99 Nella sentenza Tele2 Sverige, sebbene la Corte si sia concentrata sull'esame della giustificazione delle ingerenze derivanti dalle misure di conservazione e di accesso in questione alla luce dell'obiettivo di lotta contro i reati, la conclusione alla quale è giunta si applica, mutatis mutandis, anche quando tali misure perseguono un obiettivo di protezione della sicurezza nazionale. Infatti, l'articolo 15, paragrafo 1, della direttiva 2002/58 menziona, tra gli obiettivi che possono giustificare tali misure, sia la lotta contro i reati che la protezione della sicurezza nazionale. Inoltre, l'articolo 1, paragrafo 3, della direttiva 2002/58 e l'articolo 2, paragrafo 2, del RGPD escludono dall'ambito di applicazione di tali strumenti le attività dello Stato tanto in materia di sicurezza nazionale quanto nel settore penale. Le misure in questione nella causa che ha dato luogo alla sentenza Tele2 Sverige perseguivano, peraltro, anche una finalità connessa alla sicurezza nazionale. Al punto 119 di tale sentenza, la Corte ha espressamente trattato la questione della giustificazione di misure relative alla conservazione e all'accesso ai dati relativi al traffico e all'ubicazione alla luce dell'obiettivo di protezione della sicurezza nazionale, in quanto include la lotta contro il terrorismo.

100 Sentenza Tele2 Sverige (punto 78, il corsivo è mio). Come dimostrato dall'uso del termine «[i]noltre», è solo per confermare la sua conclusione relativa all'applicabilità della direttiva 2002/58 che la Corte ha sottolineato, al punto 79 di tale sentenza, il nesso intrinseco tra l'obbligo di conservazione dei dati di cui trattasi nella causa che ha dato luogo a tale sentenza e le disposizioni relative all'accesso delle autorità nazionali ai dati conservati.

101 Sentenza Ministerio Fiscal (punto 37, il corsivo è mio).

102 V., in tal senso, sentenza Ministerio Fiscal (punto 38).

103 V., in tal senso, sentenza del 13 maggio 2014, Google Spain e Google (C-131/12, EU:C:2014:317, punto 28).

224. Per di più, tale interpretazione sembra derivare, almeno implicitamente, dalla sentenza Schrems. Come sottolineato dal DPC, dai governi austriaco e polacco nonché dalla Commissione, la Corte, nell'esaminare la validità della decisione «approdo sicuro», ha dichiarato che il diritto del paese terzo oggetto di una decisione di adeguatezza deve prevedere, contro le ingerenze a fini di sicurezza nazionale, da parte delle sue autorità pubbliche, nei diritti fondamentali degli interessati, garanzie sostanzialmente equivalenti a quelle derivanti, in particolare, dagli articoli 7, 8 e 47 della Carta [104].

225. Più specificamente, ne consegue che una misura nazionale che impone ai fornitori di servizi di comunicazione elettronica di rispondere ad una domanda, da parte delle autorità competenti in materia di sicurezza nazionale, di accedere a determinati dati conservati da tali fornitori nell'ambito delle loro attività commerciali – indipendentemente da qualsiasi obbligo giuridico – individuando preventivamente i dati richiesti mediante l'applicazione di selettori (come nel programma PRISM), non rientrerebbe nell'ambito di applicazione dell'articolo 2, paragrafo 2, del RGPD. Lo stesso avverrebbe per una misura nazionale che esiga dalle imprese che gestiscono la «dorsale» delle telecomunicazioni di fornire, alle autorità responsabili della sicurezza nazionale, l'accesso a dati che transitano attraverso le infrastrutture da esse gestite (come nel programma Upstream).

226. Per contro, una volta che i dati in questione sono giunti nelle mani delle autorità statali, la loro conservazione e il loro successivo utilizzo da parte di tali autorità a fini di sicurezza nazionale sono, a mio avviso, per le stesse ragioni menzionate al paragrafo 211 delle presenti conclusioni, compresi nella deroga prevista all'articolo 2, paragrafo 2, del RGPD, cosicché non rientrano nell'ambito di applicazione di tale regolamento né, di conseguenza, della Carta.

227. Tenuto conto di tutte le suesposte considerazioni, ritengo che il controllo della validità della decisione «scudo per la privacy» alla luce delle limitazioni ai principi in essa enunciati, che possono derivare dalle attività delle autorità di intelligence statunitensi, implichi una doppia verifica.

228. *In primo luogo*, occorrerà esaminare se gli Stati Uniti garantiscano un livello di protezione sostanzialmente equivalente a quello derivante dalle disposizioni del RGPD e della Carta contro le limitazioni risultanti dall'applicazione dell'articolo 702 del FISA, nella parte in cui tale disposizione consente alla NSA di imporre ai fornitori di mettere i dati personali a sua disposizione.

229. *In secondo luogo*, le disposizioni della CEDU costituiranno il quadro di riferimento pertinente per valutare se le limitazioni che potrebbero derivare dall'attuazione dell'EO 12333, nella parte in cui autorizza le autorità di intelligence a raccogliere esse stesse – senza l'assistenza di operatori privati – i dati personali, rimettano in discussione l'adeguatezza del livello di protezione garantito negli Stati Uniti. Tali disposizioni forniranno anche i metri di paragone per valutare l'adeguatezza di tale livello di protezione per quanto riguarda la conservazione e l'uso dei dati acquisiti da tali autorità a fini di sicurezza nazionale.

230. Tuttavia, occorre ancora stabilire se una constatazione di adeguatezza presupponga che la raccolta di dati a norma dell'EO 12333 si accompagnato da un livello di protezione sostanzialmente equivalente a quello che deve essere garantito all'interno dell'Unione, *anche nei casi in cui tale raccolta avvenga al di fuori del territorio degli Stati Uniti*, durante la fase di transito dei dati dall'Unione verso tale paese terzo.

104 Sentenza Schrems (punti da 91 a 96). Nei considerando 90, 124 e 141 della decisione «scudo per la privacy», la Commissione fa, del resto, riferimento alle disposizioni della Carta, accettando così il principio secondo cui le limitazioni dei diritti fondamentali che rispondono ad un obiettivo di protezione della sicurezza nazionale devono essere conformi alla Carta.

2) Sulla necessità di garantire un adeguato livello di protezione durante la fase di transito dei dati

231. Sono state propugnate dinanzi alla Corte tre posizioni distinte per quanto riguarda la necessità o meno che, al fine di valutare l'adeguatezza del livello di protezione garantito in un paese terzo, la Commissione tenga conto delle misure nazionali relative all'accesso ai dati da parte delle autorità di tale paese terzo, al di fuori del suo territorio, durante la fase di transito dei dati dall'Unione verso tale territorio.

232. In primo luogo, Facebook Ireland nonché i governi degli Stati Uniti e del Regno Unito affermano, in sostanza, che l'esistenza di tali misure è ininfluente nel quadro di una constatazione dell'adeguatezza. Questi ultimi si fondano, a sostegno di tale approccio, sull'impossibilità per uno Stato terzo di controllare tutti i canali di comunicazione, situati al di fuori del suo territorio, attraverso i quali transitano i dati provenienti dall'Unione, cosicché non si potrebbe mai garantire, per ipotesi, che un altro Stato terzo non raccolga segretamente dati durante il loro transito.

233. In secondo luogo, il DPC, il sig. Schrems, l'EPIC, i governi austriaco e dei Paesi Bassi, il Parlamento e l'EDPB sostengono che il requisito di continuità del livello di protezione, stabilito all'articolo 44 del RGPD, implica che tale livello deve essere adeguato durante tutto il trasferimento, anche quando i dati transitano attraverso cavi sottomarini prima di raggiungere il territorio del paese terzo di destinazione.

234. Pur riconoscendo tale principio, la Commissione sostiene, in terzo luogo, che lo scopo di una constatazione di adeguatezza è limitato alla protezione garantita dal paese terzo interessato *all'interno delle sue frontiere*, cosicché il fatto che non sia garantito un livello di protezione adeguato *durante il transito* verso tale paese terzo non rimette in discussione la validità di una decisione di adeguatezza. Tuttavia, conformemente all'articolo 32 del RGPD, spetterebbe al titolare del trattamento garantire la sicurezza del trasferimento proteggendo, per quanto possibile, i dati personali durante la fase di transito verso tale paese terzo.

235. A tale riguardo, osservo che l'articolo 44 del RGPD subordina il trasferimento verso un paese terzo al rispetto delle condizioni stabilite nelle disposizioni del capo V di detto regolamento, in quanto i dati possono essere oggetto di un trattamento «dopo tale trasferimento». Detti termini potrebbero essere intesi nel senso, come sostenuto dal governo degli Stati Uniti nella sua risposta scritta ai quesiti della Corte, che tali condizioni devono essere soddisfatte *una volta che i dati siano giunti a destinazione*, oppure che si impongono *dopo che il trasferimento è stato avviato* (anche durante la fase di transito).

236. Poiché la formulazione dell'articolo 44 del RGPD non è concludente, un'interpretazione teleologica mi porta a sottoscrivere la seconda di tali interpretazioni e, pertanto, ad aderire al secondo approccio summenzionato. Infatti, qualora si ritenesse che il requisito della continuità del livello di protezione previsto da tale disposizione riguardi soltanto le misure di sorveglianza attuate all'interno del territorio del paese terzo di destinazione, tale requisito potrebbe essere eluso allorché detto paese terzo applichi tali misure al di fuori del suo territorio, durante la fase di transito dei dati. Per evitare tale rischio, la valutazione dell'adeguatezza del livello di protezione garantito da un paese terzo deve riguardare tutte le disposizioni, in particolare in materia di sicurezza nazionale, dell'ordinamento giuridico di tale paese terzo [105], tra le quali rientrano sia quelle relative alla sorveglianza attuata nel suo territorio sia quelle che consentono il controllo dei dati in transito verso tale territorio [106].

105 V., in tal senso, sentenza Schrems (punti 74 e 75).

106 V., in tal senso, EDPB, EU-US Privacy Shield – Second Annual Joint Review, del 22 gennaio 2019 (pag. 17, punto 86).

237. Non è, tuttavia, contestato il fatto che, come ha sottolineato l'EDPB, la valutazione dell'adeguatezza del livello di protezione riguarda unicamente, come risulta dall'articolo 45, paragrafo 1, del RGPD, le disposizioni dell'ordinamento giuridico *del paese terzo di destinazione dei dati*. L'impossibilità, eccepita da Facebook Ireland e dai governi degli Stati Uniti e del Regno Unito, di garantire che un altro Stato terzo non raccolga segretamente tali dati durante il transito non incide su tale valutazione. Per di più, tale rischio non può essere escluso anche dopo che i dati sono giunti nel territorio dello Stato terzo di destinazione.

238. È anche vero, peraltro, che la Commissione, quando valuta l'adeguatezza del livello di protezione garantito da un paese terzo, potrebbe trovarsi, eventualmente, di fronte alla mancata comunicazione, da parte di tale paese terzo, dell'esistenza di taluni programmi segreti di sorveglianza. Da ciò non consegue, tuttavia, che, *quando tali programmi sono portati alla sua attenzione*, la Commissione può astenersi dal tenerne conto nell'esaminare l'adeguatezza. Analogamente, se, dopo l'adozione di una decisione di adeguatezza, le è rivelata l'esistenza di taluni programmi segreti di sorveglianza, attuati dal paese terzo interessato nel suo territorio o durante il transito verso di esso, la Commissione è tenuta a riesaminare la sua constatazione circa l'adeguatezza del livello di protezione garantito da tale paese terzo, qualora tale rivelazione susciti dubbi al riguardo [107].

3) Sulla presa in considerazione delle constatazioni di fatto effettuate dalla Commissione e dal giudice del rinvio riguardo al diritto degli Stati Uniti

239. Pur se è pacifico che la Corte non è competente a fornire un'interpretazione del diritto di un paese terzo che potrebbe essere vincolante nell'ordinamento giuridico di quest'ultimo, la validità della decisione «scudo per la privacy» dipende dalla fondatezza delle valutazioni effettuate dalla Commissione riguardo al livello di protezione, garantito dal diritto e dalle prassi degli Stati Uniti, dei diritti fondamentali delle persone i cui dati sono trasferiti verso tale paese terzo. Infatti, la Commissione era tenuta a motivare la sua constatazione di adeguatezza alla luce degli elementi, riguardanti in particolare il contenuto del diritto di tale paese terzo, menzionati all'articolo 45, paragrafo 2, del RGPD [108].

240. La High Court (Alta Corte) ha presentato, nella sentenza del 3 ottobre 2017, constatazioni dettagliate che descrivevano gli aspetti pertinenti del diritto statunitense dopo aver valutato le prove fornite dalle parti della controversia [109]. Tale esposizione ricalca ampiamente le constatazioni effettuate dalla Commissione, nella decisione «scudo per la privacy», riguardanti il contenuto delle norme riguardanti la raccolta e l'accesso, da parte delle autorità di intelligence statunitensi, ai dati trasferiti nonché i mezzi di ricorso e i meccanismi di vigilanza inerenti a tali attività.

241. Il giudice del rinvio, nonché numerose parti e persone interessate che hanno presentato osservazioni alla Corte, rimettono in discussione piuttosto le conseguenze giuridiche che la Commissione ha tratto da tali constatazioni – vale a dire la conclusione che gli Stati Uniti garantiscono un livello adeguato di protezione dei diritti fondamentali delle persone i cui dati sono trasferiti in forza di tale decisione – che la descrizione fatta dalla Commissione del contenuto del diritto statunitense.

107 V. articolo 45, paragrafo 5, del RGPD.V. anche sentenza Schrems (punto 76).

108 Così, la decisione «approdo sicuro» è stata dichiarata invalida con la motivazione che la Commissione non aveva affermato, in tale decisione, che gli Stati Uniti garantivano effettivamente un livello di protezione adeguato in considerazione della loro legislazione nazionale o dei loro impegni internazionali (sentenza Schrems, punto 97). In particolare, la Commissione non aveva constatato l'esistenza di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone interessate (sentenza Schrems, punto 88), né di una tutela giuridica efficace nei confronti di tali ingerenze (sentenza Schrems, punto 89).

109 Tali constatazioni sono sintetizzate nei paragrafi da 54 a 73 delle presenti conclusioni.

242. In tali circostanze, valuterò essenzialmente la validità della decisione «scudo per la privacy» alla luce delle constatazioni effettuate dalla Commissione stessa riguardo al contenuto del diritto statunitense, esaminando se esse giustificassero l'adozione di tale decisione di adeguatezza.

243. A tal proposito, non concordo con l'opinione, sostenuta dal DPC e dal sig. Schrems, secondo cui le constatazioni effettuate dalla High Court (Alta Corte) riguardo al diritto degli Stati Uniti sarebbero vincolanti per la Corte nell'esame della validità della decisione «scudo per la privacy». Questi ultimi sostengono che, poiché il diritto straniero costituisce una questione di fatto ai sensi del diritto processuale irlandese, il giudice del rinvio ha competenza esclusiva per determinarne il contenuto.

244. È vero che la giurisprudenza costante riconosce al giudice nazionale la competenza esclusiva ad accertare gli elementi di fatto pertinenti nonché a interpretare il diritto di uno Stato membro e ad applicarlo alla controversia pendente dinanzi ad esso [110]. Tale giurisprudenza è espressione della ripartizione delle funzioni tra la Corte e il giudice del rinvio nell'ambito del procedimento istituito dall'articolo 267 TFUE. Mentre la Corte ha competenza esclusiva ad interpretare il diritto dell'Unione e a pronunciarsi sulla validità del diritto derivato, spetta al giudice nazionale, chiamato a decidere su una specifica controversia pendente dinanzi ad esso, accertarne il contesto fattuale e normativo affinché la Corte possa fornirgli una risposta utile.

245. La ragion d'essere di tale competenza esclusiva del giudice del rinvio non mi sembra possa essere trasposta all'accertamento del diritto di un paese terzo come elemento tale da influire sulla conclusione della Corte relativa alla validità di un atto di diritto derivato [111]. Poiché la dichiarazione di invalidità di tale atto è vincolante erga omnes nell'ordinamento giuridico dell'Unione [112], la conclusione della Corte non può dipendere dall'origine del rinvio pregiudiziale. Orbene, come hanno sottolineato Facebook Ireland e il governo degli Stati Uniti, la Corte ne sarebbe dipendente se fosse vincolata dalle constatazioni effettuate dal giudice del rinvio relative al diritto di uno Stato terzo, constatazioni che peraltro possono variare a seconda del giudice nazionale che ne è autore.

246. Alla luce di tali considerazioni, ritengo che, quando la risposta a una questione pregiudiziale vertente sulla validità di un atto dell'Unione implica la valutazione del contenuto del diritto di uno Stato terzo, la Corte non è vincolata dalle constatazioni effettuate dal giudice del rinvio relative al diritto di tale Stato terzo, pur potendo essa tenerne conto. La Corte può, se del caso, discostarsi da esse o integrarle prendendo in considerazione, nel rispetto del principio del contraddittorio, altre fonti, al fine di accertare gli elementi necessari per valutare la validità dell'atto in questione [113].

4) Sulla portata del criterio dell'«equivalenza sostanziale»

247. La validità della decisione «scudo per la privacy» dipende, lo ricordo, dalla questione se l'ordinamento giuridico degli Stati Uniti garantisca, a favore delle persone i cui dati sono trasferiti dall'Unione verso tale paese terzo, un livello di protezione «sostanzialmente equivalente» a quello garantito negli Stati membri ai sensi del RGPD e della Carta e, nei settori esclusi dall'ambito di applicazione del diritto dell'Unione, degli impegni da essi assunti ai sensi della CEDU.

110 V., in particolare, sentenze del 4 maggio 1999, Sürül (C-262/96, EU:C:1999:228, punto 95), dell'11 settembre 2008, Eckelkamp e a. (C-11/07, EU:C:2008:489, punto 32), e del 26 ottobre 2016, Senior Home (C-195/15, EU:C:2016:804, punto 20).

111 V., a tale riguardo, sentenza della Supreme Court (Corte Suprema) del 31 maggio 2019 (punto 6.18).

112 V. sentenza del 13 maggio 1981, International Chemical Corporation (66/80, EU:C:1981:102, punti 12 e 13).

113 V., a tale riguardo, sentenza del 22 marzo 2012, GLS (C-338/10, EU:C:2012:158, punti 15, 33 e 34), in cui la Corte ha tenuto conto, per valutare la validità di un regolamento che istituiva un dazio antidumping, delle statistiche Eurostat prodotte dalla Commissione su richiesta della Corte. V. anche sentenza del 22 ottobre 1991, Nölle (C-16/90, EU:C:1991:402, punti 17, 23 e 24). Analogamente, nella sentenza Schrems (punto 90), la Corte ha preso in considerazione, nell'esaminare la validità della decisione «approdo sicuro», alcune comunicazioni della Commissione.

248. Come sottolineato dalla Corte nella sentenza Schrems [114], tale criterio non significa che il livello di protezione deve essere «identico» a quello richiesto nell'Unione. Pur se i mezzi ai quali ricorre un paese terzo per proteggere i diritti delle persone interessate possono differire da quelli prescritti dal RGPD, letto alla luce della Carta, «tali strumenti devono (...) rivelarsi efficaci, nella prassi, al fine di assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione».

249. Ne consegue inoltre, a mio avviso, che il diritto dello Stato terzo di destinazione può riflettere la propria scala di valori, nella quale il peso rispettivo dei vari interessi in gioco può differire da quello ad essi attribuito nell'ordinamento giuridico dell'Unione. Per di più, la protezione dei dati personali esistente nell'Unione risponde a uno standard particolarmente elevato rispetto al livello di protezione in vigore nel resto del mondo. Il criterio dell'«equivalenza sostanziale» dovrebbe pertanto essere applicato, a mio avviso, in modo da preservare una certa flessibilità per tener conto delle diverse tradizioni giuridiche e culturali. Tale criterio implica, tuttavia – a meno privarlo di sostanza – che talune garanzie minime e taluni requisiti generali di protezione dei diritti fondamentali derivanti dalla Carta e dalla CEDU trovino il loro equivalente nell'ordinamento giuridico del paese terzo di destinazione [115].

250. A tale riguardo, conformemente all'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà da essa sanciti devono essere previste dalla legge, rispettare il loro contenuto essenziale e, nel rispetto del principio di proporzionalità, essere necessarie e rispondere effettivamente a una finalità di interesse generale riconosciuta dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. Tali requisiti corrispondono essenzialmente a quelli stabiliti all'articolo 8, paragrafo 2, della CEDU [116].

251. Conformemente all'articolo 52, paragrafo 3, della Carta, laddove i diritti garantiti dagli articoli 7, 8 e 47 corrispondano a quelli sanciti dagli articoli 8 e 13 della CEDU, essi ne condividono il significato e la portata, fermo restando che il diritto dell'Unione può comunque attribuire loro una protezione più estesa. In tale ottica, come risulterà dalla mia presentazione, gli standard derivanti dagli articoli 7, 8 e 47 della Carta, come interpretati da questa Corte, sono per certi versi più rigorosi di quelli derivanti dall'articolo 8 della CEDU, secondo l'interpretazione datane dalla Corte europea dei diritti dell'uomo (in prosieguo: la «Corte EDU»).

252. Osservo inoltre che talune cause pendenti dinanzi a ciascuno di tali organi giurisdizionali invitano questi ultimi a riconsiderare taluni aspetti della rispettiva giurisprudenza. Così, da un lato, due recenti sentenze della Corte EDU in materia di sorveglianza delle comunicazioni elettroniche – ossia le sentenze Centrüm för Rättvisa c. Svezia [117] e Big Brother Watch c. Regno Unito [118] – sono state rinviate alla Grande Sezione per essere riesaminate. D'altro lato, tre giudici nazionali hanno investito questa Corte di rinvii pregiudiziali, che aprono il dibattito sulla necessità o meno di modificare la giurisprudenza derivante dalla sentenza Tele2 Sverige [119].

253. Dopo aver apportato tali chiarimenti, esamino ora la validità della decisione «scudo per la privacy» con riferimento all'articolo 45, paragrafo 1, del RGPD, letto alla luce della Carta e della CEDU, per la parte in cui garantiscono i diritti, da un lato, al rispetto della vita privata e alla protezione dei dati personali [sezione b)], e, dall'altro, alla tutela giurisdizionale effettiva [sezione c)].

114 Sentenza Schrems (punti 73 e 74).

115 V, in tal senso, Gruppo 29, «Adequacy Referential (updated)», 28 novembre 2017, WP 254 (pagg. 3, 4 e 9).

116 L'articolo 8, paragrafo 2, della CEDU non fa tuttavia riferimento alla nozione di «contenuto essenziale» del diritto al rispetto della vita privata. V., a tale riguardo, nota 161 delle presenti conclusioni.

117 Corte EDU, 19 giugno 2018 (CE:ECHR:2018:0619JUD003525208; in prosieguo: la «sentenza Centrüm för Rättvisa»).

118 Corte EDU, 13 settembre 2018 (CE:ECHR:2018:0913JUD005817013; in prosieguo: la «sentenza Big Brother Watch»).

119 V. cause citate alla nota 98 delle presenti conclusioni nonché causa C-520/18, Ordre des barreaux francophones et germanophones e a. (GU 2018, C 408, pag. 39).

b) Sulla validità della decisione «scudo per la privacy» alla luce dei diritti al rispetto della vita privata e alla protezione dei dati personali

254. Nella quarta questione il giudice del rinvio rimette essenzialmente in discussione l'equivalenza sostanziale tra il livello di protezione garantito dagli Stati Uniti e quello di cui gli interessati godono, all'interno dell'Unione, in base ai loro diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali.

1) Sull'esistenza di ingerenze

255. Nei considerando da 67 a 124 della decisione «scudo per la privacy», la Commissione fa riferimento alla possibilità che le autorità pubbliche statunitensi accedano ai dati trasferiti dall'Unione e li utilizzino a fini di sicurezza nazionale nell'ambito di programmi basati, in particolare, sull'articolo 702 del FISA o sull'EO 12333.

256. L'attuazione di tali programmi comporta intrusioni da parte dei servizi di intelligence statunitensi che, se provenissero dalle autorità di uno Stato membro, sarebbero considerate come ingerenze nell'esercizio del diritto al rispetto della vita privata garantito dall'articolo 7 della Carta e dall'articolo 8 della CEDU. Essa espone inoltre gli interessati al rischio che i loro dati personali siano trattati in modo non conforme ai requisiti di cui all'articolo 8 della Carta [120].

257. Preciso anzitutto che i diritti al rispetto della vita privata e alla protezione dei dati personali comprendono la protezione non solo del contenuto delle comunicazioni, ma anche i dati relativi al traffico [121] e all'ubicazione (insieme denominati con il termine «metadati»). Sia questa Corte che la Corte EDU hanno, infatti, riconosciuto che i metadati, come i dati di contenuto, possono rivelare informazioni assai precise riguardo alla vita privata di un individuo [122].

258. Secondo la giurisprudenza della Corte, è irrilevante, ai fini dell'accertamento dell'esistenza di un'ingerenza nell'esercizio del diritto garantito dall'articolo 7 della Carta, che i dati in questione siano o meno delicati e che gli interessati abbiano o meno subito eventuali inconvenienti in conseguenza della misura di sorveglianza in questione [123].

259. Ciò detto, i programmi di sorveglianza basati sull'articolo 702 del FISA comportano, in primo luogo, ingerenze nell'esercizio dei diritti fondamentali delle persone le cui comunicazioni rispondono ai selettori scelti dalla NSA e sono, pertanto, trasmesse a quest'ultima dai fornitori di servizi di comunicazione elettronica [124]. Più in particolare, l'obbligo gravante sui fornitori di *mettere* i dati *a disposizione* della NSA, nei limiti in cui deroga al principio di riservatezza delle comunicazioni [125],

120 Sebbene un trattamento possa violare al contempo gli articoli 7 e 8 della Carta, il quadro di analisi pertinente ai fini dell'applicazione dell'articolo 8 è strutturalmente diverso da quello relativo all'articolo 7. Il diritto alla protezione dei dati personali implica, ai sensi dell'articolo 8, paragrafo 2, della Carta che: «[t]ali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge» e che «[o]gni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica». La violazione di tale diritto presuppone che i dati personali subiscano un trattamento in violazione di tali requisiti. Così avviene, in particolare, nel caso in cui il trattamento non sia basato né sul consenso dell'interessato *né su un altro fondamento legittimo previsto dalla legge*. In tale situazione, mentre la questione dell'esistenza di un'ingerenza e quella della sua giustificazione sono concettualmente distinte nell'ambito dell'articolo 7, esse si confondono per quanto riguarda l'articolo 8 della Carta.

121 L'articolo 2, secondo comma, lettera b) della direttiva 2002/58 definisce la nozione di «dati relativi al traffico» come «qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione».

122 V. sentenza dell'8 aprile 2014, Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238; in prosieguo: la «sentenza Digital Rights Ireland», punto 27), e sentenza Tele2 Sverige (punto 99). V. anche Corte EDU, 2 agosto 1984, Malone c. Regno Unito (CE:ECHR:1984:0802JUD000869179, § 84), e 8 febbraio 2018, Ben Faiza c. Francia (CE:ECHR:2018:0208JUD003144612, § 66).

123 V. sentenza Digital Rights Ireland (punto 33), parere 1/15 (punto 124), nonché sentenza Ministerio Fiscal (punto 51).

124 V. considerando da 78 a 81 nonché allegato VI, punto II, della decisione «scudo per la privacy».

125 V., a tale riguardo, sentenza Digital Rights Ireland (punto 32).

comporta di per sé un'ingerenza quand'anche tali dati non siano successivamente consultati e utilizzati dalle autorità di intelligence [126]. La *conservazione* e l'*accesso* effettivo, da parte di tali autorità, ai metadati e al contenuto delle comunicazioni messe a loro disposizione, al pari dell'*utilizzo* di tali dati, costituiscono altrettante ingerenze aggiuntive [127].

260. Inoltre, secondo le constatazioni del giudice del rinvio [128] e altre fonti quali la relazione del PCLOB sui programmi attuati in forza dell'articolo 702 del FISA, portata all'attenzione della Corte dal governo statunitense [129], la NSA, nell'ambito del programma Upstream, avrebbe già *accesso ai fini del loro filtraggio* a grandi corpus («pacchetti») di dati che fanno parte di flussi di comunicazioni che attraversano la «dorsale» delle telecomunicazioni e includono comunicazioni che non contengono i selettori individuati dalla NSA. La NSA potrebbe esaminare tali corpus di dati solo per determinare rapidamente, in modo automatizzato, se contengono tali selettori. Solo le comunicazioni così filtrate sarebbero a quel punto salvate nelle banche dati della NSA. Tale accesso ai dati a fini di filtraggio costituirebbe anch'esso, a mio avviso, un'ingerenza nell'esercizio del diritto al rispetto della vita privata degli interessati, indipendentemente dal successivo utilizzo dei dati conservati [130].

261. Peraltro, la messa a disposizione e il filtraggio dei dati in questione [131], l'accesso a tali dati da parte delle autorità di intelligence, nonché, eventualmente, la conservazione, l'analisi e l'uso di tali dati rientrano nella nozione di «trattamento» ai sensi dell'articolo 4, punto 2, del RGPD e dell'articolo 8, paragrafo 2, della Carta. Tali trattamenti devono quindi soddisfare i requisiti previsti da quest'ultima disposizione [132].

262. La sorveglianza ai sensi dell'EO 12333 potrebbe implicare, a sua volta, l'accesso diretto, da parte delle autorità di intelligence, ai dati in transito, che comporta un'ingerenza nell'esercizio del diritto garantito dall'articolo 8 della CEDU. A tale ingerenza si aggiungerebbe quella costituita dall'eventuale uso successivo di tali dati.

2) Sul requisito che le ingerenze siano «previste dalla legge»

263. Secondo la giurisprudenza di questa Corte [133] e della Corte EDU [134], il requisito secondo cui qualsiasi ingerenza nell'esercizio dei diritti fondamentali deve essere «prevista dalla legge», ai sensi dell'articolo 52, paragrafo 1, della Carta e dell'articolo 8, paragrafo 2, della CEDU, implica non solo che la misura che prevede l'ingerenza deve avere una base giuridica nel diritto nazionale, ma anche che tale base giuridica deve avere determinate qualità di accessibilità e di prevedibilità in modo da evitare il rischio di arbitrarietà.

264. A tale riguardo, le parti e gli interessati che hanno presentato osservazioni alla Corte non concordano, in sostanza, sulla questione se l'articolo 702 del FISA e l'EO 12333 soddisfino la condizione relativa alla prevedibilità della legge.

126 V., in tal senso, parere 1/15 (punti 124 e 125), da cui risulta che la comunicazione di dati a terzi costituisce un'ingerenza nell'esercizio dei diritti fondamentali degli interessati, a prescindere dal loro successivo utilizzo.

127 V., in tal senso, sentenza Digital Rights Ireland (punto 35), sentenza Schrems (punto 87), e parere 1/15 (punti da 123 a 126).

128 V. paragrafo 60 delle presenti conclusioni.

129 PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the [FISA], 2 luglio 2014 (in prosieguo: la «relazione del PCLOB», pagg. 84 e 111). V. anche Gruppo 29, EU-U.S. Privacy Shield – First Annual Joint Review, 28 novembre 2017, WP 255 (lettera B.1.1, pag. 15).

130 V. nota 126 delle presenti conclusioni.

131 V., a tal proposito, paragrafo 222 delle presenti conclusioni.

132 V. parere 1/15 (punto 123 e giurisprudenza ivi citata).

133 V., in particolare, parere 1/15 (punto 146).

134 V., in particolare, Corte EDU, 2 agosto 1984, Malone c. Regno Unito (CE:ECHR:1984:0802JUD000869179, § 66), decisione 29 giugno 2006, Weber e Saravia c. Germania (CE:ECHR:2006:0629DEC005493400,; in prosieguo: la «decisione Weber e Saravia», § 84 e giurisprudenza ivi citata), e sentenza 4 dicembre 2015, Zakharov c. Russia (CE:ECHR:2015:1204JUD004714306; in prosieguo: la «sentenza Zakharov», § 228).

265. Tale condizione, come interpretata dalla Corte [135] e dalla Corte EDU [136], richiede che una normativa che comporta un'ingerenza nell'esercizio del diritto al rispetto della vita privata stabilisca norme chiare e precise che disciplinano la portata e l'applicazione della misura in questione e impongono requisiti minimi, in modo da fornire agli interessati garanzie sufficienti a proteggere i loro dati contro il rischio di abusi e contro qualsiasi accesso o uso illecito degli stessi. Tali norme devono indicare, in particolare, in quali circostanze e a quali condizioni le autorità pubbliche possono conservare dati personali, accedervi e utilizzarli [137]. Inoltre, la base giuridica che consente l'ingerenza deve definire essa stessa la portata della limitazione all'esercizio del diritto al rispetto della vita privata [138].

266. Dubito, al pari del sig. Schrems e dell'EPIC, che l'EO 12333, come la PPD 28, che stabilisce garanzie che contornano tutte le attività di intelligence riguardanti le trasmissioni elettromagnetiche [139], siano sufficientemente prevedibili da poter assumere la «qualità di legge».

267. Tali strumenti menzionano espressamente il fatto che essi non conferiscono diritti giuridicamente azionabili agli interessati [140]. Questi ultimi non possono quindi far valere garanzie previste dalla PPD 28 dinanzi agli organi giurisdizionali [141]. La Commissione ha peraltro ritenuto, nella decisione «scudo per la privacy», che le garanzie menzionate in tale direttiva presidenziale, sebbene abbiano natura vincolante per i servizi di intelligence [142], «non sono formulate in un linguaggio giuridico» [143]. L'EO 12333 e la PPD 28 sono simili piuttosto a istruzioni amministrative interne, che possono essere revocate o modificate dal presidente degli Stati Uniti. Orbene, la Corte EDU ha già dichiarato che le direttive amministrative interne non rivestono la qualità di «legge» [144].

135 V., in particolare, sentenza Digital Rights Ireland (punti 54 e 65), sentenza Schrems (punto 91), sentenza Tele2 Sverige (punto 109), e parere 1/15 (punto 141).

136 V., in particolare, decisione Weber e Saravia (§§ 94 e 95), sentenza Zakharov (§ 236), e Corte EDU, 12 gennaio 2016, Szabó e Vissy c. Ungheria (CE:ECHR:2016:0112JUD003713814; in prosieguo: la «sentenza Szabó e Vissy», § 59).

137 V. sentenza Tele2 Sverige (punto 117) e parere 1/15 (punto 190). V. anche, in particolare, Corte EDU, 2 agosto 1984, Malone c. Regno Unito (CE:ECHR:1984:0802JUD000869179, § 67), sentenza Zakharov (§ 229), e sentenza Szabó e Vissy (§ 62). La Corte EDU precisa, in tali sentenze, che il requisito di prevedibilità non ha, in materia di intercettazione delle comunicazioni, la stessa portata che in altri settori. Nel contesto delle misure di sorveglianza occulta, «il requisito di prevedibilità non può significare che si debba consentire a qualcuno di prevedere se e quando le sue comunicazioni rischiano di essere intercettate dalle autorità, in modo da poter regolare di conseguenza il proprio comportamento».

138 Parere 1/15 (punto 139). V. anche, in tal senso, Corte EDU, 25 marzo 1983, Silver e a. c. Regno Unito (CE:ECHR:1983:0325JUD000594772, §§ 88 e 89).

139 I considerando da 69 a 77 nonché l'allegato VI, punto I, della decisione sullo «scudo per la privacy» contengono una presentazione della PPD 28. In essi si precisa che tale direttiva presidenziale si applica tanto alle attività di intelligence basate sull'articolo 702 del FISA quanto a quelle svolte al di fuori del territorio degli Stati Uniti.

140 Il punto 3.7, lettera c), dell'EO 12333 stabilisce quanto segue: «[t]his order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person». L'articolo 6, lettera d), della PPD 28 prevede altresì che: «This directive is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person».

141 V., in tal senso, EDPB, EU-US Privacy Shield – Second Annual Joint Review, del 22 gennaio 2019 (punto 99).

142 V. considerando 69 e 77 della decisione «scudo per la privacy».

143 Considerando 76 della decisione «scudo per la privacy».

144 V. Corte EDU, 25 marzo 1983, Silver e a. c. Regno Unito (EC:ECHR:1983:0325JUD000594772, §§ 26 e 86).

268. Per quanto riguarda l'articolo 702 del FISA, la prevedibilità di tale disposizione è rimessa in discussione dal sig. Schrems per il motivo che non disciplinerebbe la scelta dei criteri di selezione utilizzati per filtrare i dati con garanzie sufficienti contro il rischio di abusi. Poiché tale aspetto attiene anche alla natura strettamente necessaria delle ingerenze previste dall'articolo 702 del FISA, lo esaminerò nella parte restante della mia trattazione [145].

269. La terza questione pregiudiziale si sovrappone alla tematica del rispetto del requisito relativo alla «qualità di legge». Con tale questione, il giudice del rinvio chiede, in sostanza, se l'adeguatezza del livello di protezione garantito in un paese terzo debba essere esaminata unicamente alla luce delle norme giuridicamente vincolanti in vigore in tale paese terzo e delle prassi volte a garantirne il rispetto, o anche dei vari strumenti non vincolanti e dei meccanismi di controllo extragiudiziari ivi applicati.

270. A tale riguardo, l'articolo 45, paragrafo 2, lettera a), del RGPD contiene un elenco non esaustivo di circostanze di cui la Commissione deve tener conto nel valutare l'adeguatezza del livello di protezione offerto da un paese terzo. Tra dette circostanze rientrano la normativa applicabile nonché le sue modalità di attuazione. Tale disposizione menziona anche l'incidenza di altri tipi di norme, come le regole professionali e le misure di sicurezza. Essa richiede inoltre che siano presi in considerazione i «diritti effettivi e azionabili» e un «ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento» [146].

271. Letta nel suo complesso e alla luce della natura non tassativa dell'elenco che essa contiene, tale disposizione implica, a mio avviso, che prassi o strumenti non fondati su una base giuridica accessibile e prevedibile possono essere presi in considerazione nella valutazione complessiva del livello di protezione garantito dal paese terzo in questione in modo da corroborare garanzie che hanno a loro volta una base giuridica che presenta tali caratteristiche. Per contro, come sostenuto in sostanza dal DPC, dal sig. Schrems, dal governo austriaco e dall'EDPB, prassi o strumenti di tal genere non possono sostituirsi a siffatte garanzie né, pertanto, garantire di per sé il livello di protezione richiesto.

3) Sulla mancanza di violazione del contenuto essenziale dei diritti fondamentali

272. Il requisito di cui all'articolo 52, paragrafo 1, della Carta, secondo cui qualsiasi limitazione dei diritti o delle libertà garantiti dalla Carta deve rispettarne il contenuto essenziale, implica che, quando un'ingerenza leda tali diritti e libertà, nessun obiettivo legittimo può giustificarla. L'ingerenza è in tal caso considerata contraria alla Carta senza che sia necessario esaminare se sia idonea o necessaria alla realizzazione dell'obiettivo perseguito.

145 V. paragrafi da 295 a 301 delle presenti conclusioni. Nella sentenza Tele2 Sverige (punti 116 e 117) e nel parere 1/15 (punti 140 e 141), la condizione della prevedibilità della legge è stata presentata come intrinsecamente legata all'esigenza della necessità e della proporzionalità dell'ingerenza. Analogamente, secondo la giurisprudenza della Corte EDU, l'esistenza di garanzie effettive contro il rischio di abusi rientra tanto nel requisito della «prevedibilità» dell'ingerenza quanto in quello della sua natura «necessaria in una società democratica», e il rispetto di queste due condizioni viene esaminato congiuntamente. V., in particolare, Corte EDU, 18 maggio 2010, Kennedy c. Regno Unito (CEDU:ECHR:2010:0518JUD002683905, § 155), sentenza Zakharov (§ 236), sentenza Centrüm för Rättvisa (§ 107) e sentenza Big Brother Watch (§ 322).

146 V. anche il considerando 104 del RGPD.

273. A tal proposito, la Corte ha dichiarato che una normativa nazionale che autorizza un accesso generalizzato al *contenuto* delle comunicazioni elettroniche da parte delle autorità pubbliche pregiudica l'essenza stessa del diritto al rispetto della vita privata garantito dall'articolo 7 della Carta [147]. Per contro, pur sottolineando i rischi connessi all'accesso e all'analisi dei *dati relativi al traffico e all'ubicazione* [148], la Corte ha considerato che il contenuto essenziale di tale diritto non è pregiudicato quando una normativa nazionale autorizza un accesso generalizzato a tali dati da parte delle autorità statali [149].

274. L'articolo 702 del FISA non può essere considerato, a mio avviso, nel senso che autorizza le autorità di intelligence statunitensi ad accedere in modo generalizzato al contenuto delle comunicazioni elettroniche.

275. Infatti, da un lato, l'accesso ai dati da parte delle autorità di intelligence, ai sensi dell'articolo 702 del FISA, *ai fini della loro analisi e del loro utilizzo* eventuali è limitato ai dati che soddisfano i criteri di selezione associati a singoli obiettivi.

276. D'altro lato, il programma Upstream potrebbe, certamente, implicare un accesso generalizzato al contenuto delle comunicazioni elettroniche *ai fini del loro filtraggio automatizzato* nel caso in cui siano applicati selettori non solo ai campi «da» e «verso», ma anche all'intero contenuto dei flussi di comunicazioni (ricerca «relativa» al selettore) [150]. Tuttavia, come sostiene la Commissione e contrariamente a quanto affermato dal sig. Schrems e dall'EPIC, l'accesso temporaneo delle autorità di intelligence a tutto il contenuto delle comunicazioni elettroniche al solo fine del loro filtraggio mediante l'applicazione di criteri di selezione non può essere assimilato a un accesso generalizzato a tale contenuto [151]. A mio avviso, la gravità dell'ingerenza derivante da tale accesso limitato nel tempo a fini di filtraggio automatizzato non è pari alla gravità dell'ingerenza risultante da un accesso generalizzato a tale contenuto, da parte delle autorità pubbliche, a fini della sua analisi e del suo eventuale utilizzo [152]. L'accesso temporaneo ai fini del filtraggio non consente a tali autorità di conservare i metadati o il contenuto delle comunicazioni che non soddisfano i criteri di selezione né, segnatamente – come ha osservato il governo degli Stati Uniti – di stabilire profili riguardanti gli individui non sono specificamente l'obiettivo di tali criteri.

147 V. sentenza Schrems (punto 94). V. anche sentenze Digital Rights Ireland (punto 39) e Tele2 Sverige (punto 101). Tenuto conto dello stretto legame tra i diritti al rispetto della vita privata e alla protezione dei dati personali, una misura nazionale che conferisca alle autorità pubbliche un accesso generalizzato al contenuto delle comunicazioni violerebbe anche, a mio avviso, il contenuto essenziale del diritto sancito dall'articolo 8 della Carta.

148 V. paragrafo 257 delle presenti conclusioni. Nella sentenza Tele2 (punto 99), la Corte ha sottolineato che i metadati forniscono, in particolare, gli strumenti per stabilire il profilo degli interessati. Nel parere 04/2014 sulla sorveglianza delle comunicazioni elettroniche a fini di intelligence e di sicurezza nazionale, del 10 aprile 2014, WP 215 (pag. 5), il Gruppo 29 ha osservato che, grazie alla loro natura strutturata, i metadati sono più facili da incrociare e da analizzare rispetto ai dati di contenuto.

149 V. sentenza Tele2 Sverige (punto 99). Taluni commentatori hanno messo in dubbio la fondatezza della distinzione tra l'accesso generalizzato al contenuto delle comunicazioni e l'accesso generalizzato ai metadati alla luce degli sviluppi delle tecnologie e delle modalità di comunicazione. V. Falot, N. e Hijmans, H., «Tele2: de afweging tussen privacy en veiligheid nader omlijnd», *Nederlands Tijdschrift voor Europees Recht*, n. 3, 2017 (pag. 48) nonché Ojanen, T., «Making essence of the rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter» (commento alla sentenza Schrems), *European Constitutional Law Review*, 2016 (pag. 5).

150 V. nota 87 della decisione «scudo per la privacy». Tuttavia, secondo le osservazioni dell'EPIC e la risposta scritta del governo degli Stati Uniti ai quesiti posti dalla Corte, la Corte FISA avrebbe richiesto, nel 2017, la sospensione delle ricerche «relative» a un selezionatore a causa di irregolarità che avevano viziato le ricerche di questo tipo. Tuttavia, il Congresso avrebbe previsto, nell'atto di riautorizzazione del FISA, adottato nel 2018, la possibilità di reintrodurre questo tipo di ricerca con l'accordo della Corte FISA e del Congresso. V. anche EDPB, EU-US Privacy Shield – Second Annual Joint Review, 22 gennaio 2019 (pag. 27, punto 55).

151 In quest'ottica, il giudice del rinvio, ai punti 188 e 189 della sentenza del 3 ottobre 2017, distingue la ricerca «in blocco» dall'acquisizione, dalla raccolta o dalla conservazione «in blocco». Tale giudice considera, in sostanza, che, pur se il programma Upstream comporta una ricerca «in blocco» all'interno di tutti i flussi di dati che transitano per la «dorsale» delle telecomunicazioni, l'acquisizione, la raccolta e la conservazione sono mirate nel senso che hanno ad oggetto solo i dati contenenti i selettori in questione.

152 V., in tal senso, sentenza della Supreme Court (Corte suprema) del 31 maggio 2019 (punti 11.2 e 11.3). Tale giudice rileva quanto segue: «[I]t is inevitable that any screening process designed to identify data of interest will necessarily involve all of the data available, for the whole point of the screening process is to identify within that entire universe of available data the relevant material which may be of interest and thus require closer scrutiny. Perhaps part of the problem lies in the fact that the term "processing" covers a wide range of activity, apparently, in the view of the DPC, including screening. On the assumption that that is a correct view of the law, then it is technically correct to describe bulk screening as involving indiscriminate processing. But the use of that terminology might be taken to imply that other forms of processing, which are significantly more invasive, are carried out on an indiscriminate basis».

277. Tuttavia, la questione se l'individuazione mirata, mediante selettori nell'ambito dei programmi basati sull'articolo 702 del FISA, limiti effettivamente i poteri delle autorità di intelligence dipende da come è inquadrata la scelta dei selettori [153]. Il sig. Schrems sostiene, al riguardo, che, in mancanza di un controllo sufficiente a tal fine, il diritto degli Stati Uniti non prevede garanzie contro un accesso generalizzato al contenuto delle comunicazioni già in fase di filtraggio, cosicché viola l'essenza stessa del diritto al rispetto della vita privata delle persone interessate.

278. Come spiegherò più dettagliatamente in seguito [154], tendo a condividere tali dubbi sull'adeguatezza del quadro giuridico per la scelta dei selezionatori al fine di soddisfare i criteri di prevedibilità e proporzionalità delle ingerenze. Tuttavia, l'esistenza di tale quadro, sia pure imperfetto, osta alla conclusione che l'articolo 702 del FISA autorizzi un accesso generalizzato, da parte delle autorità pubbliche, al contenuto delle comunicazioni elettroniche e, pertanto, equivale a una violazione dell'essenza stessa del diritto sancito dall'articolo 7 della Carta.

279. Sottolineo inoltre che, nel parere 1/15, la Corte ha considerato che il contenuto essenziale del diritto alla protezione dei dati personali, garantito dall'articolo 8 della Carta, è preservato quando le finalità del trattamento sono circoscritte e il trattamento è accompagnato da norme destinate a garantire, in particolare, la sicurezza, la riservatezza e l'integrità dei dati, nonché a proteggerli da accessi e trattamenti illeciti [155].

280. Nella decisione «scudo per la privacy» la Commissione ha constatato che tanto l'articolo 702 del FISA quanto la PPD 28 delimitano le finalità per le quali possono essere raccolti i dati nell'ambito dei programmi attuati ai sensi dell'articolo 702 del FISA [156]. In tale decisione la Commissione ha altresì rilevato che la PPD 28 prevede norme che disciplinano l'accesso ai dati nonché la loro archiviazione e la loro diffusione al fine di garantirne la sicurezza e di preservarli dagli accessi non autorizzati [157]. Come sarà dimostrato dalla parte restante della mia trattazione [158], nutro dubbi in particolare, sulla questione se le finalità dei trattamenti in questione siano definite con sufficiente chiarezza e precisione per garantire un livello di protezione sostanzialmente equivalente a quello esistente nell'ordinamento giuridico dell'Unione. Tuttavia, queste eventuali carenze non sarebbero, a mio avviso, sufficienti a consentire di constatare che programmi siffatti, se fossero attuati all'interno dell'Unione, violerebbero il contenuto essenziale del diritto alla protezione dei dati personali.

281. Peraltro, l'adeguatezza del livello di protezione garantito nel contesto di attività di sorveglianza ai sensi dell'EO 12333 deve essere valutata, lo ricordo, alla luce delle disposizioni della CEDU. A tal proposito, dalla decisione «scudo per la privacy» risulta che le uniche restrizioni all'attuazione delle misure basate sull'EO 12333 per la raccolta dei dati relativi a persone non statunitensi sono quelle previste dalla PPD 28 [159]. Tale direttiva presidenziale stabilisce che il ricorso all'intelligence esterna

153 V. parere 1/15 (punto 122). V. anche la relazione della Commissione europea per la democrazia attraverso il diritto (Commissione di Venezia) sul controllo democratico delle agenzie di raccolta di informazioni di origine elettromagnetica [rapport de la Commission européenne pour la démocratie par le droit (Commission de Venise) sur le contrôle démocratique des agences de collecte de renseignements d'origine électromagnétique], del 15 dicembre 2015, studio n. 719/2013 [CDL-AD(2015)011]: «[In pratica, la questione se tale processo limiti adeguatamente le intrusioni superflue nelle comunicazioni personali innocenti equivale a stabilire se il selettore sia sufficientemente pertinente e specifico, e se la qualità dell'algoritmo del software utilizzato per individuare i dati pertinenti entro i parametri scelti sia soddisfacente (...)]».

154 V. paragrafi da 297 a 301 delle presenti conclusioni.

155 Parere 1/15 (punto 150).

156 V. considerando 70, 103 e 109 della decisione «scudo per la privacy».

157 V. considerando da 83 a 87 nonché allegato VI, punto I, lettera c), della decisione «scudo per la privacy». Osservo che, secondo la relazione del PCLOB (pagg. da 51 a 66), le procedure di «minimizzazione» della NSA ai sensi dell'articolo 702 del FISA riguardano, per la maggior parte dei loro aspetti, esclusivamente persone statunitensi. La PPD 28 mirava ad estendere le garanzie applicabili a persone non statunitensi. V. PCLOB, Report to the President on the Implementation of [PPD 28]: Signals Intelligence Activities, disponibile all'indirizzo https://www.pclob.gov/reports/report-PPD28/ (pag. 2). Tuttavia, l'archiviazione e l'uso dei dati a fini di sicurezza nazionale, dopo che sono stati acquisiti dalle autorità pubbliche, non rientrano, a mio avviso, nell'ambito di applicazione del diritto dell'Unione (v. paragrafo 226 delle presenti conclusioni). L'adeguatezza del livello di protezione garantito nel contesto di tali attività deve pertanto essere valutata esclusivamente alla luce dell'articolo 8 della CEDU.

158 V. paragrafi da 283 a 289 delle presenti conclusioni.

159 In particolare, al considerando 127 della decisione «scudo per la privacy», la Commissione ha constatato che il quarto emendamento della Costituzione degli Stati Uniti non si applica alle persone non statunitensi.

deve essere «il più mirato possibile». Tuttavia, essa menziona espressamente la possibilità di raccogliere dati «in blocco» al di fuori del territorio degli Stati Uniti, al fine di perseguire taluni obiettivi specifici di sicurezza nazionale [160]. Secondo il sig. Schrems, le disposizioni della PPD 28, la quale del resto non crea diritti per i singoli, non proteggono gli interessati dal rischio di un accesso generalizzato al contenuto delle loro comunicazioni elettroniche.

282. Mi limiterò a osservare, a tal proposito, che la Corte EDU, nella giurisprudenza relativa all'articolo 8 della CEDU, non ha fatto ricorso al concetto di violazione del contenuto essenziale, o della sostanza stessa, del diritto al rispetto della vita privata [161]. Fino ad ora quest'ultima non ha considerato che regimi che consentivano l'intercettazione, anche massiccia, delle comunicazioni elettroniche, *eccedevano, in quanto tali, i limiti del potere discrezionale degli Stati membri*. La Corte EDU considera che tali regimi sono compatibili con l'articolo 8, paragrafo 2, della CEDU purché siano accompagnati da una serie di garanzie minime [162]. In tali circostanze, non mi sembra confacente concludere che un regime di sorveglianza come quello previsto dall'EO 12333 superi i limiti del potere discrezionale degli Stati membri senza procedere a un qualsivoglia esame delle eventuali garanzie che lo accompagnano.

4) Sul perseguimento di un obiettivo legittimo

283. Ai sensi dell'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti da essa riconosciuti devono rispondere effettivamente a una finalità di interesse generale riconosciuta dall'Unione. L'articolo 8, paragrafo 2, della Carta dispone inoltre che qualsiasi trattamento di dati personali che non sia basato sul consenso dell'interessato deve essere basato su un «fondamento legittimo previsto dalla legge». L'articolo 8, paragrafo 2, della CEDU elenca, a sua volta, le finalità che possono giustificare un'ingerenza nell'esercizio del diritto al rispetto della vita privata.

284. In forza della decisione «scudo per la privacy», l'adesione ai principi da essa sanciti può essere limitata per soddisfare obblighi relativi alla sicurezza nazionale, all'interesse pubblico e al rispetto della legge [163]. I considerando da 67 a 124 di tale decisione esaminano più in particolare le limitazioni derivanti dall'accesso ai dati e dal loro uso, da parte delle autorità pubbliche statunitensi, a fini di sicurezza nazionale.

160 V. considerando 73 e 74 nonché allegato VI, punto I, lettera b), della decisione «scudo per la privacy». Tali obiettivi comprendono la lotta contro lo spionaggio e contro altre minacce e attività dirette da potenze straniere contro gli Stati Uniti e i suoi interessi; contro le minacce terroristiche; contro le minacce derivanti dallo sviluppo, dal possesso, dalla proliferazione o dall'uso di armi di distruzione di massa; contro le minacce alla sicurezza informatica; contro le minacce alle forze armate degli Stati Uniti o dei suoi alleati; e contro le minacce derivanti dalla criminalità transnazionale. Ai sensi della nota a piè di pagina 5 della PPD 28, la limitazione degli obiettivi che giustificano l'uso di dati raccolti «in blocco» non si applica quando tale raccolta è solo temporanea e destinata a facilitare una raccolta mirata.

161 Sebbene le disposizioni della CEDU non facciano riferimento al «contenuto essenziale» dei diritti fondamentali, nella giurisprudenza della Corte EDU relativa ad alcune di queste disposizioni è rinvenibile la nozione equivalente di «sostanza stessa» di un diritto fondamentale. V., per quanto riguarda la sostanza stessa del diritto a un processo equo garantito dall'articolo 6 della CEDU, in particolare, Corte EDU, 25 maggio 1985, Ashingdane c. Regno Unito (CE:ECHR:1985:0528JUD000822578, §§ 57 e 59), 21 dicembre 2000, Heaney e McGuinness c. Irlanda (CE:ECHR:2000:1221JUD003472097, §§ 55 e 58), e 23 giugno 2016, Baka c. Ungheria (CE:ECHR:2016:0623JUD002026112, § 121). Per quanto riguarda la sostanza stessa del diritto al matrimonio sancito all'articolo 12 della CEDU, v. Corte EDU, 11 luglio 2002, Christine Goodwin c. Regno Unito (CE:ECHR:2002:0711JUD002895795, §§ 99 e 101). Per quanto riguarda la sostanza stessa del diritto all'istruzione garantito dall'articolo 2 del Protocollo n. 1 della CEDU, v. Corte EDU, 23 luglio 1968, causa «relativa a taluni aspetti del regime linguistico dell'istruzione in Belgio» (CE:ECHR:1968:0723JUD000147462, § 5).

162 V., in particolare, sentenze Centrüm för Rättvisa (§§ da 112 a 114 e giurisprudenza ivi citata) e Big Brother Watch (§ 337).

163 V. paragrafo 197 delle presenti conclusioni.

285. È pacifico che la protezione della sicurezza nazionale costituisce un obiettivo legittimo che può giustificare deroghe agli obblighi derivanti dal RGPD [164], nonché ai diritti fondamentali sanciti dagli articoli 7 e 8 della Carta [165], così come dall'articolo 8, paragrafo 2, della CEDU. Tuttavia, il sig. Schrems, il governo austriaco e l'EPIC hanno osservato che gli obiettivi perseguiti nell'ambito dei programmi di sorveglianza basati sull'articolo 702 del FISA e sull'EO 12333 vanno al di là della sola sicurezza nazionale. Infatti, tali strumenti hanno come obiettivo la realizzazione dell'«intelligence esterna», nozione comprendente diversi tipi di informazioni tra cui rientrano quelle relative alla sicurezza nazionale senza esservi necessariamente limitate [166]. Rientrano quindi nella nozione di «intelligence esterna», ai sensi dell'articolo 702 del FISA, i dati riguardanti la gestione degli affari esteri [167]. L'EO 12333 definisce, a sua volta, tale nozione nel senso che include le informazioni relative alle capacità, intenzioni o attività di governi, organizzazioni o individui stranieri [168]. Il sig. Schrems rimette in discussione la legittimità dell'obiettivo così inteso in quanto eccederebbe l'ambito della sicurezza nazionale.

286. A mio avviso, l'ambito della sicurezza nazionale può includere, entro certi limiti, la protezione di interessi relativi alla gestione degli affari esteri [169]. Peraltro, non è inconcepibile che talune finalità diverse dalla protezione della sicurezza nazionale rientranti nella nozione di «intelligence esterna», come definita dall'articolo 702 del FISA e dall'EO 12333, corrispondano a obiettivi rilevanti di interesse generale che possono giustificare un'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali. Tali obiettivi avrebbero, in ogni caso, un peso minore rispetto alla salvaguardia della sicurezza nazionale nell'ambito di un bilanciamento tra i diritti fondamentali delle persone interessate e lo scopo perseguito con l'ingerenza [170].

287. Tuttavia, ai sensi dell'articolo 52, paragrafo 1, della Carta, occorre altresì che la sicurezza nazionale o un altro obiettivo legittimo sia effettivamente perseguito dalle misure che prevedono le ingerenze in questione [171]. Inoltre, le finalità delle ingerenze devono essere definite in modo da soddisfare i requisiti di chiarezza e precisione [172].

164 V. articolo 23, paragrafo 1, lettera a), del RGPD.

165 V. sentenza Schrems (punto 88). La Corte ha considerato la nozione simile di «pubblica sicurezza», ai sensi delle disposizioni del TFUE che autorizzano deroghe alle libertà fondamentali dallo stesso garantite, come una nozione autonoma di diritto dell'Unione comprendente la sicurezza sia interna che esterna degli Stati membri [v., in particolare, sentenze del 26 ottobre 1999, Sirdar (C-273/97, EU:C:1999:523, punto 17) nonché del 13 settembre 2016, CS (C-304/14, EU:C:2016:674, punto 39 e giurisprudenza ivi citata)]. Mentre la sicurezza interna può essere pregiudicata, in particolare, da una minaccia diretta alla tranquillità e alla sicurezza fisica della popolazione dello Stato membro interessato, la sicurezza esterna può essere messa a repentaglio, in particolare, dal rischio di un grave turbamento delle relazioni esterne o della coesistenza pacifica dei popoli. Senza poter determinare unilateralmente il contenuto di tali nozioni, ogni Stato membro dispone di un certo margine di discrezionalità per definire i propri interessi essenziali in termini di sicurezza. V., in particolare, sentenza del 2 maggio 2018, K. e H.F. (Diritto di soggiorno e allegazioni di crimini di guerra) (C-331/16 e C-366/16, EU:C:2018:296, punti da 40 a 42 e giurisprudenza ivi citata). Tali considerazioni sono, a mio avviso, trasponibili all'interpretazione della nozione di «sicurezza nazionale» come interesse la cui tutela può giustificare restrizioni alle disposizioni del RGPD e ai diritti garantiti dagli articoli 7 e 8 della Carta.

166 V., a tale riguardo, considerando 89 e nota 97 della decisione «scudo per la privacy».

167 V. paragrafo 55 delle presenti conclusioni.

168 V. paragrafo 61 delle presenti conclusioni.

169 Nella sentenza Centrüm för Rättvisa (§ 111), la Corte EDU ha dichiarato che le attività di sorveglianza volte a sostenere la politica estera, la politica di difesa e la politica di sicurezza della Svezia nonché a individuare le minacce esterne organizzate in Svezia perseguivano obiettivi legittimi relativi alla sicurezza nazionale.

170 V., a tale riguardo, sentenze Tele2 Sverige (punto 115) e Ministerio Fiscal (punto 55). La Corte ha sottolineato, in tali sentenze, il nesso tra il grado di gravità di un'ingerenza e quello dell'interesse invocato per giustificarla.

171 Il Gruppo 29, nel documento di lavoro sulla sorveglianza delle comunicazioni elettroniche a fini di intelligence e di sicurezza nazionale, del 5 dicembre 2014, WP 228 (pag. 27), ha insistito sull'importanza di valutare criticamente se la sorveglianza sia effettivamente realizzata a fini di sicurezza nazionale.

172 V. parere 1/15 (punto 181), in cui la Corte ha dichiarato che la formulazione delle disposizioni legislative che prevedevano le ingerenze non soddisfaceva i requisiti di chiarezza e precisione, cosicché tali ingerenze non erano limitate allo stretto necessario. Nella stessa ottica, l'avvocato generale Bot ha ritenuto, nelle sue conclusioni nella causa Schrems (C-362/14, EU:C:2015:627, paragrafi da 181 a 184), che le finalità delle misure di sorveglianza erano formulate in modo troppo ampio per essere considerate obiettivi di interesse generale, fatta eccezione per la sicurezza nazionale.

288. Orbene, secondo il sig. Schrems, la finalità delle misure di sorveglianza previste dall'articolo 702 del FISA e dall'EO 12333 non è indicata con precisione sufficiente da rispettare le garanzie di prevedibilità e proporzionalità. Ciò sarebbe particolarmente vero in quanto tali strumenti definiscono la nozione di «intelligence esterna» in modo particolarmente ampio. Inoltre, la Commissione ha constatato, al considerando 109 della decisione «scudo per la privacy» che l'articolo 702 del FISA stabilisce che la raccolta di informazioni di intelligence esterna costituisce «uno degli scopi rilevanti» della raccolta, e tale formulazione non esclude, a prima vista e come rilevato dall'EPIC, il perseguimento di altri obiettivi non determinati.

289. Per tali ragioni, senza escludere la possibilità che le misure di sorveglianza di cui all'articolo 702 del FISA o dell'EO 12333 soddisfino obiettivi legittimi, ci si può chiedere se questi ultimi siano definiti in modo sufficientemente chiaro e preciso da prevenire il rischio di abusi e da consentire un controllo della proporzionalità delle ingerenze che ne derivano [173].

5) Sulla necessarietà e proporzionalità delle ingerenze

290. La Corte ha ripetutamente sottolineato che i diritti sanciti dagli articoli 7 e 8 della Carta non costituiscono prerogative assolute, ma devono essere considerati alla luce della loro funzione nella società e contemperati con altri diritti fondamentali, in ossequio del principio di proporzionalità [174]. Come ha sottolineato Facebook Ireland, tra questi altri diritti rientra il diritto alla sicurezza garantito dall'articolo 6 della Carta.

291. A tale riguardo, secondo una giurisprudenza altrettanto costante, qualsiasi ingerenza nell'esercizio dei diritti garantiti dagli articoli 7 e 8 della Carta deve essere soggetta a un rigoroso controllo di proporzionalità [175].

292. In particolare, dalla sentenza Schrems risulta che «non è limitata allo stretto necessario una normativa che autorizza in maniera generale la conservazione di tutti i dati (...) senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta» [176].

293. La Corte ha del pari dichiarato che, salvi i casi di urgenza debitamente giustificati, l'accesso deve essere subordinato a un controllo preliminare effettuato da un giudice o da un ente amministrativo indipendente la cui decisione sia diretta a limitare l'accesso ai dati e il loro uso a quanto strettamente necessario per la realizzazione dell'obiettivo perseguito [177].

294. L'articolo 23, paragrafo 2, del RGPD stabilisce ora una serie di garanzie che uno Stato membro deve prevedere quando deroga alle disposizioni di tale regolamento. La normativa che consente tale deroga deve contenere disposizioni relative, in particolare, alle finalità del trattamento, alla portata della deroga, alle garanzie destinate a prevenire gli abusi, ai periodi di conservazione e al diritto degli interessati di essere informati della deroga, a meno che ciò non rischi di pregiudicarne la finalità.

173 Dubbi analoghi sono stati espressi dal GEPD nel parere 4/2016 riguardante lo «scudo UE-USA per la privacy» (Privacy Shield) – Progetto di decisione di adeguatezza del 30 maggio 2016 (pag. 8).

174 V. sentenza del 9 novembre 2010, Volker und Markus Schecke e Eifert (C-92/09 e C-93/09, EU:C:2010:662, punto 48), parere 1/15 (punto 136), e sentenza del 24 settembre 2019, Google (Portata territoriale della deindicizzazione) (C-507/17, EU:C:2019:772, punto 60).

175 V., in particolare, sentenza del 16 dicembre 2008, Satakunnan Markkinapörssi et Satamedia (C-73/07, EU:C:2008:727, punto 56), sentenza Digital Rights Ireland (punti 48 e 52), sentenza Schrems (punti 78 e 92), nonché parere 1/15 (punti 139 e 140). V. anche il considerando 140 della decisione «scudo per la privacy».

176 Sentenza Schrems (punto 93). V. anche, in tal senso, sentenza Digital Rights Ireland (punto 60).

177 V. sentenza Tele2 Sverige (punto 120) e parere 1/15 (punto 202).

295. Nel caso di specie, il sig. Schrems sostiene che l'articolo 702 del FISA non fornisce garanzie sufficienti contro i rischi di abuso e di accesso illecito ai dati. In particolare, la scelta dei criteri di selezione non sarebbe sufficientemente disciplinata, cosicché tale disposizione non offrirebbe garanzie contro un accesso generalizzato al contenuto delle comunicazioni.

296. Il governo degli Stati Uniti e la Commissione sostengono, al contrario, che l'articolo 702 del FISA limita la scelta dei selettori in base a criteri oggettivi, poiché tale disposizione consente unicamente la raccolta dei dati di comunicazioni elettroniche di persone non statunitensi che si trovano al di fuori degli Stati Uniti al fine di ottenere informazioni di intelligence esterna.

297. A mio avviso, è lecito dubitare del fatto che tali criteri di selezione siano sufficientemente chiari e precisi e che esistano garanzie sufficienti per prevenire i rischi di abuso.

298. Anzitutto, il considerando 109 della decisione «scudo per la privacy» precisa che i selettori non sono singolarmente approvati dalla Corte FISA o da un altro organo giudiziario o amministrativo indipendente prima della loro applicazione. La Commissione ha constatato, in tale considerando, che «la Corte FISA non autorizza singole misure di sorveglianza, ma piuttosto programmi di sorveglianza (...) basandosi sulle certificazioni annuali», circostanza che è stata confermata dal governo degli Stati Uniti dinanzi alla Corte. Tale considerando precisa che «le certificazioni che la Corte FISA deve approvare non contengono informazioni sul singolo potenziale obiettivo, ma indicano piuttosto categorie di informazioni di intelligence esterna», che possono essere raccolte. La Commissione constata inoltre, in tale considerando, che «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», sebbene controlli che ricorra il requisito che «uno degli scopi rilevanti dell'acquisizione dev'essere quello di ottenere informazioni di intelligence esterna».

299. Inoltre, secondo detto considerando, l'articolo 702 del FISA autorizza la NSA a raccogliere comunicazioni «solo se si può ragionevolmente ritenere che un determinato mezzo di comunicazione sia usato per comunicare informazioni di intelligence esterna». Il considerando 70 della decisione «scudo per la privacy» aggiunge che la scelta dei selettori è effettuata in base al quadro delle priorità dell'intelligence nazionale (National Intelligence Priorities Framework, NIPF). Tale decisione non fa riferimento a requisiti più precisi per motivare o giustificare la scelta dei selettori alla luce di tali priorità amministrative che sarebbero richieste alla NSA [178].

300. Infine, il considerando 71 della decisione «scudo per la privacy» fa riferimento alla condizione prevista nella PPD 28, secondo cui la rilevazione dei dati di intelligence esterna dovrebbe essere «quanto più possibile mirata». Oltre al fatto che tale direttiva presidenziale non crea diritti per i singoli, mi sembra tutt'altro che evidente l'equivalenza sostanziale tra il criterio di un'attività «quanto più possibile mirata» e quello di «stretta necessità», che l'articolo 52, paragrafo 1, della Carta impone per giustificare un'ingerenza nell'esercizio dei diritti garantiti dagli articoli 7 e 8 [179].

178 La relazione del PCLOB (pag. 45) precisa quanto segue: «With respect to the foreign intelligence purpose, the NSA targeting procedures require the analyst only to "identify" the foreign power or foreign territory regarding which the foreign intelligence information is to be acquired. By policy, but not as a requirement of the targeting procedures, the NSA also requires that all taskings be accompanied by a very brief statement (typically no more than one sentence long) that further explains the analyst's rationale for assessing that tasking the selector in question will result in the acquisition of the types of foreign intelligence information authorized by the Section 702 certification».

179 V., in tal senso, Gruppo 29, Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, 13 aprile 2016, WP 238 (punto 3.3.1, pag. 38); risoluzione del Parlamento del 6 aprile 2017 sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy, P8_TA(2017)0131 (punto 17), nonché relazione del Parlamento sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto, del 20 febbraio 2017, A8-0044/2017 (punto 17).

301. Alla luce di tali considerazioni, non è sicuro che, sulla base degli elementi esposti nella decisione «scudo per la privacy», le misure di sorveglianza basate sull'articolo 702 del FISA siano accompagnate da garanzie, relative alla limitazione delle persone che possono essere oggetto di una misura di sorveglianza e delle finalità per le quali i dati possono essere raccolti, sostanzialmente equivalenti a quelle richieste dal RGPD, letto alla luce degli articoli 7 e 8 della Carta [180].

302. Inoltre, per quanto riguarda la valutazione dell'adeguatezza del livello di protezione relativo alla sorveglianza ai sensi dell'EO 12333, la Corte EDU riconosce agli Stati membri un ampio potere discrezionale per scegliere i mezzi per proteggere la propria sicurezza nazionale, tale potere è tuttavia limitato dall'obbligo di prevedere garanzie adeguate e sufficienti contro gli abusi [181]. Nella giurisprudenza relativa alle misure di sorveglianza occulta, la Corte EDU verifica se il diritto nazionale su cui si basano tali misure contenga garanzie e misure di salvaguardia sufficienti ed efficaci, idonee a soddisfare i requisiti di «prevedibilità» e di «necessità in una società democratica» [182].

303. La Corte EDU enuncia una serie di garanzie minime al riguardo. Tali garanzie riguardano la chiara indicazione della natura dei reati che possono dar luogo a un'autorizzazione alle intercettazioni, la definizione delle categorie di persone le cui comunicazioni possono essere intercettate, la fissazione di un limite alla durata dell'esecuzione del provvedimento, la procedura da seguire per l'esame, l'uso e la conservazione dei dati raccolti, le precauzioni da adottare per la comunicazione dei dati ad altri soggetti e le circostanze in cui può o deve avvenire la cancellazione o la distruzione delle registrazioni [183].

304. L'adeguatezza e l'efficacia delle garanzie che contornano l'ingerenza dipende da tutte le circostanze del caso, compresa la natura, la portata e la durata delle misure, i motivi che ne giustificano l'ordine, le autorità competenti a consentirle, eseguirle e controllarle, nonché il tipo di ricorso previsto dal diritto nazionale [184].

305. In particolare, al fine di valutare la giustificazione di una misura di sorveglianza occulta, la Corte EDU tiene conto di tutti i controlli esercitati «al momento in cui viene disposta», «durante l'esecuzione» e «dopo la sua cessazione» [185]. Per quanto riguarda la prima di queste tre fasi, la Corte EDU richiede che tale misura sia autorizzata da un organismo indipendente. Sebbene il potere giudiziario rappresenti, a suo avviso, la migliore garanzia di indipendenza, imparzialità e regolarità del procedimento, l'organismo in questione non deve necessariamente far parte dell'ordinamento giudiziario [186]. Un controllo giurisdizionale approfondito in una fase successiva può controbilanciare eventuali carenze nel procedimento di autorizzazione [187].

306. Nel caso di specie, dalla decisione «scudo per la privacy» risulta che le uniche garanzie che limitano la raccolta e l'uso di dati al di fuori del territorio degli Stati Uniti sono contenute nella PPD 28, in quanto l'articolo 702 del FISA non si applica al di fuori di tale territorio. Non sono convinto che tali garanzie siano sufficienti a soddisfare le condizioni di «prevedibilità» e «necessità in una società democratica».

180 V., in tal senso, Gruppo 29, EU-U.S. Privacy Shield – First Annual Joint Review, 28 novembre 2017, WP 255 (pag. 3); risoluzione del Parlamento europeo del 5 luglio 2018 sull'adeguatezza della protezione garantita dallo scudo UE-USA per la privacy, P8_TA(2018)0315 (punto 22), e EDPB, EU-U.S. Privacy Shield – Second Annual Joint Review, 22 gennaio 2019 (punti da 81 a 83 e 87).

181 V., in particolare, sentenze Zakharov (§ 232) e Szabó e Vissy (§ 57).

182 V., in particolare, sentenze Zakharov (§ 237), Centrüm för Rättvisa (§ 111), e Big Brother Watch (§ 322).

183 V., in particolare, decisione Weber e Saravia (§ 95), Corte EDU, 28 giugno 2007, Association pour l'intégration européenne et les droits de l'homme e Ekimdjiev (CE:ECHR:2007:0628JUD006254000, § 76), nonché sentenza Zakharov (§ 231).

184 V., in particolare, decisione Weber e Saravia (§ 106), sentenza Zakharov (§ 232), e sentenza Centrüm för Rättvisa (§ 104).

185 V., in particolare, Corte EDU, 6 settembre 1978, Klass e. a. c. Germania (CE:ECHR:1978:0906JUD000502971, § 55), sentenza Zakharov (§ 233), nonché sentenza Centrüm för Rättvisa (§ 105).

186 V., in particolare, sentenza Klass (§ 56), Corte EDU, 18 maggio 2010, Kennedy c. Regno Unito (CE:ECHR:2010:0518JUD002683905, § 167), nonché sentenza Zakharov (§§ 233 e 258).

187 V. sentenze Szabó e Vissy (§ 77) e Centrüm för Rättvisa (§ 133).

307. Innanzi tutto, ho già rilevato che tale direttiva presidenziale non crea diritti per i singoli. Inoltre, dubito che l'obbligo di garantire una sorveglianza «quanto più possibile mirata» sia formulato in termini sufficientemente chiari e precisi per preservare adeguatamente gli interessati dal rischio di abusi [188]. Infine, la decisione «scudo per la privacy» non prevede che la sorveglianza basata sull'EO 12333 sia soggetta a un controllo preliminare da parte di un organo indipendente o possa essere oggetto di un controllo giurisdizionale a posteriori [189].

308. In tali circostanze, nutro dubbi sulla fondatezza della constatazione secondo cui gli Stati Uniti garantiscono, nell'ambito delle attività dei loro servizi di intelligence ai sensi dell'articolo 702 del FISA e dell'EO 12333, un adeguato livello di protezione ai sensi dell'articolo 45, paragrafo 1, del RGPD, letto alla luce degli articoli 7 e 8 della Carta e dell'articolo 8 CEDU.

c) Sulla validità della decisione «scudo per la privacy» per quanto riguarda il diritto a un ricorso effettivo

309. La quinta questione pregiudiziale invita la Corte a stabilire se le persone i cui dati sono trasferiti negli Stati Uniti godano in tale paese di una tutela giurisdizionale sostanzialmente equivalente a quella che deve essere garantita nell'Unione in forza dell'articolo 47 della Carta. Con la decima questione, il giudice del rinvio chiede, in sostanza, se la quinta questione richieda una risposta affermativa alla luce dell'introduzione, con la decisione «scudo per la privacy», del meccanismo di mediazione.

310. Constato anzitutto che, nel considerando 115 di tale decisione, la Commissione riconosce che il sistema giuridico statunitense presenta lacune nella tutela giurisdizionale dei singoli.

311. Secondo tale considerando, in primo luogo, le possibilità di ricorso giurisdizionale «non contemplano almeno alcune delle basi giuridiche di cui possono avvalersi le autorità di intelligence statunitensi (ad esempio l'EO 12333)». Infatti, l'EO 12333 e la PPD 28 non conferiscono diritti agli interessati e non possono essere invocati da queste ultime dinanzi agli organi giurisdizionali. Orbene, una tutela giurisdizionale effettiva presuppone, quantomeno, che i singoli abbiano diritti che possono essere invocati in giudizio.

312. In secondo luogo, «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 (...) 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»

313. Dai considerando da 116 a 124 della decisione «scudo per la privacy» risulta che l'istituzione del Mediatore mira a compensare tali limitazioni. La Commissione conclude, al considerando 139 di tale decisione, che «*nel complesso*, i meccanismi di *vigilanza* e di *ricorso* previsti dallo scudo (...) offr[o]no all'interessato mezzi di ricorso che gli consentono di accedere ai dati personali che lo riguardano e, in ultima analisi, di ottenerne la rettifica o cancellazione» (il corsivo è mio).

314. Tenendo presenti i principi generali che emergono dalla giurisprudenza di questa Corte e della Corte EDU sul diritto di ricorso contro misure di sorveglianza delle comunicazioni, esaminerò se i ricorsi giurisdizionali previsti dal diritto statunitense, quali descritti nella decisione «scudo per la privacy», consentano di garantire una tutela giurisdizionale adeguata delle persone interessate [sezione 1)]. Stabilirò poi se l'introduzione del meccanismo di mediazione extragiudiziale consenta, se del caso, di colmare le eventuali lacune che caratterizzano la tutela giurisdizionale di tali persone [sezione 2)].

188 Ciò vale a maggior ragione alla luce delle considerazioni esposte al paragrafo 281 delle presenti conclusioni.

189 V. paragrafi 330 e 331 delle presenti conclusioni.

1) Sull'effettività dei ricorsi giurisdizionali previsti dal diritto degli Stati Uniti

315. In primo luogo, l'articolo 47, primo comma, della Carta riconosce il diritto di ogni persona – i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati – a un ricorso effettivo dinanzi a un giudice [190]. 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 [191]. L'accesso a un giudice indipendente rientra nel contenuto essenziale del diritto garantito dall'articolo 47 della Carta [192].

316. Tale diritto alla tutela giurisdizionale individuale si aggiunge all'obbligo, gravante sugli Stati membri ai sensi degli articoli 7 e 8 della Carta, di sottoporre qualsiasi misura di sorveglianza, salvo casi d'urgenza debitamente giustificati, a un controllo preliminare da parte di un giudice o di un'autorità amministrativa indipendente [193].

317. È vero che, come hanno sostenuto i governi tedesco e francese, il diritto a un ricorso giurisdizionale effettivo non costituisce una garanzia assoluta [194], in quanto tale diritto può essere limitato per ragioni di sicurezza nazionale. Tuttavia, le deroghe sono autorizzate solo a condizione che non ledano il suo contenuto essenziale e siano strettamente necessarie alla realizzazione di un obiettivo legittimo.

318. A tale riguardo, la Corte ha dichiarato, nella sentenza Schrems, che 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 sancito all'articolo 47 della Carta [195].

319. Sottolineo che tale diritto di accesso implica la possibilità per una persona di ottenere dalle autorità pubbliche, salvo deroghe strettamente necessarie al perseguimento di un interesse legittimo, *la conferma del fatto che esse trattano o meno dati personali che la riguardano* [196]. È questa, a mio avviso, la portata pratica del diritto di accesso quando l'interessato ignora se le autorità pubbliche abbiano conservato dati personali che la riguardano al termine, in particolare, di un processo di filtraggio automatizzato dei flussi di comunicazioni elettroniche.

190 Nelle spiegazioni relative alla Carta si afferma, al riguardo, che «nel diritto dell'Unione, la tutela [prevista dall'articolo 47 della Carta] è più estesa [di quella conferita dall'articolo 13 della CEDU] in quanto essa garantisce il diritto a un ricorso effettivo dinanzi a un giudice». V. anche conclusioni dell'avvocato generale Wathelet nella causa Berlioz Investment Fund (C-682/15, EU:C:2017:2, paragrafo 37).

191 Per valutare la qualità di «giudice» di un organo nell'applicazione dell'articolo 47 della Carta, occorre tener conto del suo fondamento legale, del suo carattere permanente, dell'obbligatorietà della sua giurisdizione, della natura contraddittoria del procedimento, del fatto che l'organo applica norme giuridiche ed è indipendente. V. sentenza del 27 febbraio 2018, Associação Sindical dos Juízes Portugueses (C-64/16, EU:C:2018:117, punto 38 e giurisprudenza ivi citata).

192 V., in particolare, sentenze del 25 luglio 2018, Minister for Justice and Equality (Carenze del sistema giudiziario) (C-216/18 PPU, EU:C:2018:586, punti 59 e 63), del 5 novembre 2019, Commissione/Polonia (Indipendenza dei tribunali ordinari) (C-192/18, EU:C:2019:924, punto 106), e del 19 novembre 2019, A.K. e a. (Indipendenza della Sezione disciplinare della Corte suprema) (C-585/18, C-624/18 e C-625/18, EU:C:2019:982, punto 120).

193 V. paragrafo 293 delle presenti conclusioni. L'articolo 45, paragrafo 3, lettera a), del RGPD prevede che, nel valutare l'adeguatezza del livello di protezione fornito da uno Stato terzo, si tenga conto dell'esistenza in esso di un «ricorso effettivo in sede amministrativa e *giudiziaria*» per gli interessati (il corsivo è mio). Analogamente, secondo il considerando 104 del RGPD, l'adozione di una decisione di adeguatezza dovrebbe essere subordinata alla condizione che agli interessati sia riconosciuto, nel paese terzo considerato, «un mezzo di ricorso effettivo in sede amministrativa *e giudiziale*» (il corsivo è mio). V. anche Gruppo 29, EU-U.S. Privacy Shield – First Annual Joint Review, 28 novembre 2017, WP 255 (punto B.3), risoluzione del Parlamento del 5 luglio 2018 sull'adeguatezza della protezione garantita dallo scudo UE-USA per la privacy, P8_TA(2018)0315 (punti 25 e 30), e EDPB, EU-U.S. Privacy Shield – Second Annual Joint Review, 22 gennaio 2019 (punti da 94 a 97).

194 V., in tal senso, sentenza del 28 febbraio 2013, Riesame Arango Jaramillo e a./BEI (C-334/12 RX-II, EU:C:2013:134, punto 43).

195 Sentenza Schrems (punto 95).

196 L'articolo 15 del RGPD, intitolato «Diritto di accesso dell'interessato», prevede al paragrafo 1, che tale persona «ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che [la] riguardano e in tal caso, di ottenere l'accesso ai dati». Il «principio dell'accesso» di cui all'allegato II, punto II.8, lettera a) della decisione «scudo per la privacy» ha lo stesso significato.

320. Inoltre, dalla giurisprudenza risulta che le autorità di uno Stato membro sono tenute, in linea di principio, a notificare l'accesso ai dati *a partire dal momento in cui tale comunicazione non è suscettibile di compromettere le indagini condotte* [197]. Siffatta notifica costituisce, infatti, un presupposto per l'esercizio del diritto di ricorso ai sensi dell'articolo 47 della Carta [198]. Tale obbligo è ora ripreso all'articolo 23, paragrafo 2, lettera h), del RGPD.

321. I considerando da 111 a 135 della decisione «scudo per la privacy» illustrano brevemente tutti i mezzi di ricorso a disposizione delle persone i cui dati sono trasferiti quando temono che tali dati siano stati trattati dai servizi di intelligence statunitensi dopo il trasferimento. Tali mezzi di ricorso sono stati descritti anche nella sentenza della High Court (Alta Corte) del 3 ottobre 2017 nonché nelle osservazioni, tra l'altro, del governo degli Stati Uniti.

322. Non è necessario ricordare in dettaglio il contenuto di tali esposizioni. Il giudice del rinvio rimette, infatti, in discussione l'adeguatezza delle garanzie relative alla tutela giuridica delle persone interessate per il fatto che, in sostanza, i requisiti particolarmente rigorosi in materia di legittimazione ad agire (*standing*) [199], unitamente alla mancanza di qualsiasi obbligo di notifica alle persone che sono state oggetto di una misura di sorveglianza *anche quando la notifica non ne pregiudicherebbe più gli obiettivi*, renderebbero, in pratica, eccessivamente difficile l'esercizio dei mezzi di ricorso previsti dal diritto degli Stati Uniti. Tali dubbi sono condivisi dal DPC, dal sig. Schrems, dai governi austriaco, polacco e portoghese nonché dall'EDPB [200].

323. Mi limiterò, a tale riguardo, a ricordare che le norme in materia di legittimazione ad agire non possono pregiudicare la tutela giurisdizionale effettiva [201], nonché a constatare che la decisione «scudo per la privacy» non menziona alcun obbligo di informare le persone interessate del fatto che sono state oggetto di una misura di sorveglianza [202]. Poiché potrebbe impedire l'esercizio dei mezzi di ricorso giurisdizionali, la mancanza dell'obbligo di notificare siffatta misura, anche quando la comunicazione all'interessato non pregiudicherebbe più la sua efficacia, risulta problematica alla luce della giurisprudenza menzionata al paragrafo 320 delle presenti conclusioni.

324. La nota 169 della decisione «scudo per la privacy» riconosce inoltre che i motivi per adire le vie legali «implicano l'esistenza di un danno (...) oppure la dimostrazione del fatto che il governo intende usare o divulgare le informazioni ottenute (...) dalla sorveglianza elettronica della persona contro questa stessa persona». Come sottolineato dal giudice del rinvio, dal DPC e dal sig. Schrems, tale requisito contrasta con la giurisprudenza della Corte secondo la quale, ai fini dell'accertamento di un'ingerenza nel diritto al rispetto della vita privata dell'interessato, non è necessario che quest'ultimo abbia subito eventuali inconvenienti a causa dell'asserita ingerenza [203].

197 Sentenza Tele2 Sverige (punto 121), nonché parere 1/15 (punto 220). Come ha osservato Facebook Ireland, la notifica dell'accesso ai dati, da parte delle autorità pubbliche, non può quindi essere richiesta sistematicamente. A tal proposito, la Corte EDU considera che «[N]ella pratica non è possibile richiedere una notifica a posteriori», in quanto la minaccia oggetto delle misure di sorveglianza «può persistere per anni o addirittura per decenni» dopo la revoca di tali misure, cosicché la notifica può «compromettere l'obiettivo a lungo termine che giustificava originariamente la sorveglianza», nonché «rivelare i metodi di lavoro dei servizi di intelligence, i loro settori di attività e (...) l'identità dei loro agenti» [sentenza Zakharov (§ 287 e giurisprudenza citata)]. In mancanza di notifica, pur se i mezzi di ricorso individuali non sono quindi esperibili in caso di violazione degli obblighi di legge, altre garanzie possono essere sufficienti a tutelare il diritto al rispetto della vita privata (v. anche sentenza Centrüm för Rättvisa, §§ da 164 a 167 e da 171 a 178). V. paragrafo 330 delle presenti conclusioni.

198 V., a tale riguardo, la nota 210 delle presenti conclusioni.

199 V. paragrafo 67 delle presenti conclusioni.

200 V. EDPB, EU-US Privacy Shield – Second Annual Joint Review, 22 gennaio 2019 (pag. 18, punto 97).

201 V., in particolare, sentenze dell'11 luglio 1991, Verholen e a. (da C-87/90 a C-89/90, EU:C:1991:314, punto 24 e giurisprudenza ivi citata), nonché del 28 febbraio 2013, Riesame Arango Jaramillo e a./BEI (C-334/12 RX-II, EU:C:2013:134, punto 43).

202 Tuttavia, il governo degli Stati Uniti ha precisato, al pari del giudice del rinvio, che una misura di sorveglianza ai sensi dell'articolo 702 del FISA deve essere notificata alla persona che ne è specificamente oggetto se i dati raccolti sono utilizzati a suo carico nell'ambito un procedimento giurisdizionale.

203 Sentenza del 20 maggio 2003, Österreichischer Rundfunk e a. (C-465/00, C-138/01 e C-139/01, EU:C:2003:294, punto 75), sentenza Digital Rights Ireland (punto 33), sentenza Schrems (punto 87), e parere 1/15 (punto 124).

325. Inoltre, non mi convince il punto di vista espresso da Facebook Ireland e dal governo degli Stati Uniti, secondo cui le carenze che caratterizzano la tutela giurisdizionale delle persone i cui dati sono trasferiti negli Stati Uniti sarebbero compensate dai controlli preventivi e a posteriori effettuati dalla Corte FISA, nonché dai molteplici meccanismi di sorveglianza istituiti all'interno dei poteri esecutivo e legislativo [204].

326. Ho già rilevato che, da un lato, conformemente alle constatazioni contenute nella decisione «scudo per la privacy», la Corte FISA non controlla le singole misure di sorveglianza prima della loro attuazione [205]. Come precisato al considerando 109 di tale decisione e confermato dal governo degli Stati Uniti nella sua risposta scritta ai quesiti posti dalla Corte, l'obiettivo del controllo ex post dell'applicazione dei selettori è, d'altro lato, quello di verificare – quando un'agenzia di intelligence porta all'attenzione della Corte FISA un incidente relativo all'eventuale inosservanza delle procedure di individuazione mirata e di minimizzazione [206] – il rispetto delle condizioni che disciplinano la scelta dei selettori previste nella certificazione annuale. La procedura dinanzi alla Corte FISA non sembra pertanto offrire un mezzo di ricorso individuale effettivo alle persone i cui dati sono trasferiti verso gli Stati Uniti.

327. I meccanismi di controllo extragiudiziale menzionati ai considerando da 95 a 110 della decisione «scudo per la privacy», pur se potrebbero rafforzare, se del caso, eventuali mezzi di ricorso giurisdizionali, non sarebbero, a mio avviso, sufficienti a garantire un livello di protezione adeguato alla luce del diritto di ricorso degli interessati. In particolare, gli ispettori generali, che fanno parte della struttura interna di ciascuna agenzia, non costituiscono, a mio avviso, meccanismi di controllo indipendenti. La sorveglianza esercitata dal PCLOB e delle commissioni di intelligence del Congresso non costituisce, a sua volta, un meccanismo di ricorso individuale contro le misure di sorveglianza.

328. Occorrerà pertanto esaminare se l'istituzione del Mediatore colmi tali lacune, fornendo agli interessati un mezzo di ricorso effettivo dinanzi a un organo indipendente e imparziale [207].

329. In secondo luogo, al fine di valutare la fondatezza della constatazione di adeguatezza effettuata nella decisione «scudo per la privacy» con riferimento ai mezzi di ricorso a disposizione delle persone che ritengono di essere state sottoposte a sorveglianza in base all'OE 12333, il quadro di riferimento pertinente è costituito, lo ricordo, dalle disposizioni della CEDU.

330. Come esposto in precedenza [208], la Corte EDU, al fine di valutare se una misura di sorveglianza soddisfi le condizioni di «prevedibilità» e di «necessità in una società democratica» ai sensi dell'articolo 8, paragrafo 2, CEDU [209], procede a un esame d'insieme dei meccanismi di controllo e supervisione attuati «prima, durante e dopo» la sua esecuzione. Qualora l'esercizio di un ricorso individuale sia impedito dal fatto che la notifica della misura di sorveglianza non è possibile senza

204 Tali meccanismi sono descritti nei considerando da 95 a 110 della decisione «scudo per la privacy». La Commissione distingue, in tali considerando, all'interno della categoria delle norme relative alla «tutela giurisdizionale effettiva», i «meccanismi di vigilanza» (v. considerando da 92 a 110) dai «ricorsi individuali» (v. considerando da 111 a 124).

205 V. paragrafo 298 delle presenti conclusioni.

206 Secondo il considerando 109 della decisione «scudo per la privacy», «[i]l Procuratore generale e il Direttore [della NSA] verificano la conformità e gli enti sono tenuti a segnalare tutti i casi di inosservanza alla Corte FISA (...), che su tale base può modificare l'autorizzazione».

207 V. paragrafi da 333 a 340 delle presenti conclusioni.

208 V. paragrafo 305 delle presenti conclusioni.

209 Nella giurisprudenza relativa alle misure di sorveglianza delle telecomunicazioni, la Corte EDU ha trattato la questione dei mezzi di ricorso nell'ambito dell'esame della «qualità di legge» e della necessità di un'ingerenza nell'esercizio del diritto garantito dall'articolo 8 della CEDU [v., in particolare, sentenze Zakharov (§ 236) e Centrüm för Rättvisa (§ 107)]. La Corte EDU, nella sentenza del 1º luglio 2008, Liberty e a. c. Regno Unito (CE:ECHR:2008:0701JUD005824300, § 73) e nella sentenza Zakharov (§ 307), dopo aver constatato una violazione dell'articolo 8 della CEDU, non ha ritenuto necessario esaminare separatamente la censura relativa all'articolo 13 di tale convenzione.

comprometterne l'efficacia [210], tale lacuna può essere compensata dall'attuazione di un controllo indipendente prima dell'applicazione della misura in questione [211]. Pertanto, la Corte EDU, anche se considera tale notifica «auspicabile» non appena può aver luogo senza alterare l'efficacia della misura di sorveglianza, non l'ha resa obbligatoria [212].

331. A tale riguardo, la decisione «scudo per la privacy» non mostra che le misure di sorveglianza basate sull'EO 12333 siano notificate agli interessati o disciplinate da meccanismi di controllo giurisdizionale o amministrativo indipendenti in qualsiasi fase della loro adozione o attuazione.

332. In tali circostanze, si deve esaminare se il ricorso al Mediatore consenta comunque di garantire un controllo indipendente delle misure di sorveglianza, anche quando sono basate sull'EO 12333.

2) Sull'incidenza del meccanismo di mediazione sul livello di protezione del diritto a un ricorso effettivo

333. Ai sensi del considerando 116 della decisione «scudo per la privacy», il meccanismo di mediazione descritto nell'allegato III A di tale decisione mira a offrire un'ulteriore via di ricorso a tutti gli interessati i cui dati sono trasferiti dall'Unione agli Stati Uniti.

334. Come ha sottolineato il governo degli Stati Uniti, la ricevibilità di una denuncia al Mediatore non è subordinata al rispetto di norme in materia di legittimazione ad agire simili a quelle che disciplinano l'accesso ai giudici statunitensi. Il considerando 119 di tale decisione precisa, a tal proposito, che il ricorso al Mediatore non presuppone che l'interessato dimostri che il governo degli Stati Uniti ha consultato dati personali che la riguardano.

335. Al pari del DPC, del sig. Schrems, dei governi polacco e portoghese nonché dell'EPIC, dubito che tale meccanismo possa compensare le carenze della protezione giudiziaria offerta alle persone i cui dati sono trasferiti dall'Unione verso gli Stati Uniti.

336. Anzitutto, sebbene un meccanismo di ricorso extragiudiziale possa costituire un mezzo di ricorso effettivo ai sensi dell'articolo 47 TFUE, ciò avviene solo se, in particolare, l'organismo in questione ha un fondamento legale e soddisfa il requisito di indipendenza [213].

210 Secondo la Corte EDU, anche se la mancanza di notifica in qualsiasi fase non impedisce necessariamente che una misura di sorveglianza soddisfi la condizione di «necessità in una società democratica», essa compromette l'accesso alla giustizia e, di conseguenza, l'effettività dei ricorsi [v., in particolare, sentenza del 6 settembre 1978, Klass e a. c. Germania (CE:ECHR:1978:0906JUD000502971, §§ 57 e 58), décision Weber e Saravia (§ 135), e sentenza Zakharov (§ 302)].

211 V., in tal senso, sentenza Centrum för Rättvisa (§ 105).

212 Nella sentenza Big Brother Watch (§ 317), la Corte EDU ha rifiutato di aggiungere, tra le garanzie minime applicabili ad un regime di sorveglianza caratterizzato da un'intercettazione massiccia delle comunicazioni elettroniche, l'obbligo di notificare la sorveglianza agli interessati. V. anche sentenza Centrüm för Rättvisa (§ 164). Il rinvio di tali sentenze dinanzi alla Grande Camera della Corte EDU è finalizzato, in particolare, al riesame di tale conclusione.

213 La nozione di indipendenza comprende un primo aspetto, esterno, che presuppone che l'organo in questione sia tutelato contro gli interventi o le pressioni esterne che possono mettere a repentaglio l'indipendenza di giudizio dei suoi membri per quanto riguarda le controversie ad essi sottoposte. Il secondo aspetto, interno, di tale nozione si ricollega a quella di «imparzialità» e riguarda l'equidistanza rispetto alle parti della controversia e ai loro rispettivi interessi in relazione all'oggetto di quest'ultima. V., in particolare, sentenze del 19 settembre 2006, Wilson (C-506/04, EU:C:2006:587, punti da 50 a 52), del 25 luglio 2018, Minister for Justice and Equality (Carenze del sistema giudiziario) (C-216/18 PPU, EU:C:2018:586, punti 63 e 65), e del 19 novembre 2019, A.K. e a. (Indipendenza della Sezione disciplinare della Corte suprema) (C-585/18, C-624/18 e C-625/18, EU:C:2019:982, punti 121 e 122). Conformemente al principio di separazione dei poteri, l'indipendenza dei giudici deve essere garantita nei confronti, in particolare, del potere esecutivo. V. sentenza del 19 novembre 2019, A.K. e a. (Indipendenza della Sezione disciplinare della Corte suprema) (C-585/18, C-624/18 e C-625/18, EU:C:2019:982, punto 127 e giurisprudenza ivi citata).

337. Orbene, dalla decisione «scudo per la privacy» risulta che il meccanismo di mediazione, che trae origine dalla PPD 28 [214], non ha fondamento legale. Il Mediatore è designato dal Segretario di Stato e costituisce parte integrante del Dipartimento di Stato degli Stati Uniti [215]. Tale decisione non contiene alcuna indicazione che la revoca del Mediatore o l'annullamento della sua nomina siano accompagnate da garanzie particolari [216]. Sebbene sia presentato come indipendente dalla «comunità dell'intelligence», il Mediatore rende conto al Segretario di Stato e non è quindi indipendente dal potere esecutivo [217].

338. Inoltre, l'effettività di un mezzo di ricorso extragiudiziale dipende anche, a mio avviso, dalla possibilità per l'organo in questione di adottare decisioni vincolanti e motivate. A tale riguardo, la decisione «scudo per la privacy» non contiene alcuna indicazione che il Mediatore adotterebbe tali decisioni. Essa non dimostra che l'istituzione del Mediatore consentirebbe ai richiedenti di accedere ai dati che li riguardano e di farli rettificare o cancellare, né che il Mediatore accorderebbe un risarcimento alle persone danneggiate da una misura di sorveglianza. In particolare, come risulta dall'allegato III A, punto 4, lettera e), di tale decisione, «il Mediatore non conferma né nega che la persona sia stata sottoposta a sorveglianza né indica la specifica misura correttiva applicata» [218]. Sebbene il governo degli Stati Uniti si sia impegnato affinché la componente interessata dei servizi di intelligence sia tenuta a rettificare qualsiasi violazione delle norme applicabili individuata dal Mediatore [219], tale decisione non menziona garanzie giuridiche che accompagnino tale impegno e di cui potrebbero avvalersi gli interessati.

339. Pertanto, l'istituzione del Mediatore non fornisce, a mio avviso, un mezzo di ricorso dinanzi a un organo indipendente che offra alle persone i cui dati sono trasferiti la possibilità di far valere il loro diritto di accesso ai dati o di contestare eventuali violazioni delle norme applicabili da parte dei servizi di intelligence.

340. Infine, conformemente alla giurisprudenza, il rispetto del diritto garantito dall'articolo 47 della Carta implicherebbe quindi che la decisione di tale autorità amministrativa, che non soddisfa di per sé il requisito di indipendenza, sia soggetta a un controllo successivo da parte di un organo giurisdizionale competente a trattare tutte le questioni pertinenti [220]. Tuttavia, secondo le indicazioni fornite nella decisione «scudo per la privacy», le decisioni del Mediatore non sono soggette a un controllo giurisdizionale indipendente.

214 L'allegato III A della decisione «scudo per la privacy» fa riferimento, a tale riguardo, all'articolo 4, lettera d), della PPD 28.

215 V. considerando 116 della decisione «scudo per la privacy».

216 Nella sentenza del 31 maggio 2005, Syfait e a. (C-53/03, EU:C:2005:333, punto 31), la Corte ha sottolineato l'importanza di tali garanzie per soddisfare la condizione dell'indipendenza. V. anche, a tale riguardo, sentenze del 24 giugno 2019, Commissione/Polonia (Indipendenza della Corte suprema) (C-619/18, EU:C:2019:531, punto 76) e del 5 novembre 2019, Commissione/Polonia (Indipendenza dei tribunali ordinari) (C-192/18, EU:C:2019:924, punto 113).

217 V. considerando 65 e 121 nonché allegato III A, punto 1, della decisione «scudo per la privacy».

218 Inoltre il considerando 121 della decisione «scudo per la privacy» precisa che «il Mediatore deve confermare: i) che il reclamo è stato esaminato adeguatamente; e ii) che è stata rispettata la legge statunitense applicabile, comprese in particolare le limitazioni e le garanzie illustrate nell'allegato VI, oppure, se non è stata rispettata, che l'inosservanza è stata nel frattempo sanata».

219 La Commissione ha constatato, nella terza revisione annuale dello scudo per la privacy, che, secondo le dichiarazioni del governo degli Stati Uniti, nel caso in cui l'indagine del Mediatore riveli una violazione delle procedure di individuazione mirata e di minimizzazione approvate dalla Corte FISA, tale violazione dovrebbe essere portata all'attenzione di tale giudice. La Corte FISA condurrà quindi un'indagine indipendente e, se necessario, ordinerà all'agenzia di intelligence interessata di porre rimedio a tale violazione. V. Commission staff working document accompanying the report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU-U.S. Privacy Shield, 23 ottobre 2019, SWD(2019) 390 final, pag. 28. La Commissione fa ivi riferimento al documento intitolato «Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure», disponibile all'indirizzo https://www.state.gov/wp-content/uploads/2018/12/Ombudsperson-Mechanism-Implementation-Procedures-UNCLASSIFIED.pdf (pagg. 4 e 5).

220 V. sentenze del 16 maggio 2017, Berlioz Investment Fund (C-682/15, EU:C:2017:373, punto 55) e del 13 dicembre 2017, El Hassani (C-403/16, EU:C:2017:960, punto 39).

341. In tali circostanze, come sostenuto dal DPC, dal sig. Schrems, dall'EPIC nonché dai governi polacco e portoghese, l'equivalenza sostanziale tra la protezione giurisdizionale offerta nell'ordinamento giuridico statunitense alle persone i cui dati vi sono trasferiti dall'Unione e quella risultante dal RGPD, letto alla luce dell'articolo 47 della Carta e dell'articolo 8 CEDU, mi sembra dare adito a dubbi.

342. Alla luce di tutte le suesposte considerazioni, nutro alcuni dubbi quanto alla conformità della decisione «scudo per la privacy» con l'articolo 45, paragrafo 1, del RGPD, letto alla luce degli articoli 7, 8 e 47 della Carta e dell'articolo 8 CEDU.

V. Conclusione

343. Propongo alla Corte di rispondere come segue alle questioni pregiudiziali sollevate dalla High Court (Alta Corte, Irlanda):

L'analisi delle questioni pregiudiziali non ha rivelato elementi atti a inficiare 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/CE del Parlamento europeo e del Consiglio, come modificata dalla decisione di esecuzione (UE) 2016/2297 della Commissione, del 16 dicembre 2016.