Raccolta della giurisprudenza

CONCLUSIONI DELL'AVVOCATO GENERALE
YVES BOT
presentate il 23 settembre 2015 [1]

Causa C-362/14

Maximillian Schrems
contro
Data Protection Commissioner

[domanda di pronuncia pregiudiziale proposta dalla Corte d'appello (High Court, Irlanda)]

«Rinvio pregiudiziale — Dati personali — Protezione delle persone fisiche con riguardo al trattamento di tali dati — Carta dei diritti fondamentali dell'Unione europea — Articoli 7, 8 e 47 — Direttiva 95/46/CE — Articolo 25 — Decisione 2000/520/CE — Trasferimento di dati personali verso gli Stati Uniti — Valutazione dell'adeguatezza o meno del livello di protezione — Denuncia di una persona fisica i cui dati sono stati trasferiti verso un paese terzo — Autorità nazionale di controllo — Poteri»

I – **Introduzione**

1. Come constatato dalla Commissione europea nella sua comunicazione del 27 novembre 2013 [2], «[i] trasferimenti di dati personali sono un importante e necessario elemento delle relazioni transatlantiche. Fanno parte integrante degli scambi commerciali fra le due sponde dell'Oceano, anche per i nuovi settori emergenti del digitale come i media sociali o il cloud computing, che vedono grosse quantità di dati viaggiare dall'Unione europea agli Stati Uniti» [3].

2. Gli scambi commerciali sono oggetto della decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio 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 [4]. Tale decisione fornisce una base giuridica per il trasferimento di dati personali dall'Unione a società stabilite negli Stati Uniti che hanno aderito ai principi di approdo sicuro.

3. Detta decisione deve oggi fare fronte alla sfida di consentire i flussi di dati fra l'Unione e gli Stati Uniti, garantendo al contempo un elevato livello di protezione a tali dati, come richiesto dal diritto dell'Unione.

4. Infatti, recentemente, da alcune rivelazioni è emersa l'esistenza di programmi statunitensi di raccolta di informazioni su larga scala. Tali rivelazioni hanno gettato un'ombra sul rispetto delle norme del diritto dell'Unione in occasione dei trasferimenti di dati personali verso imprese stabilite negli Stati Uniti e hanno evidenziato i limiti del regime dell'approdo sicuro.

1 — Lingua originale: il francese.

2 — Comunicazione della Commissione al Parlamento europeo e al Consiglio intitolata «Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA» [COM(2013) 846 def.].

3 — Pagina 2.

4 — GU L 215, pag. 7, e rettifica in GU 2001, L 115, pag. 14.

5. Il presente rinvio pregiudiziale invita la Corte a precisare l'atteggiamento che le autorità nazionali di controllo e la Commissione devono tenere allorché si trovano di fronte a disfunzioni nell'applicazione della decisione 2000/520.

6. La direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [5], prevede, al suo capo IV, norme relative al trasferimento di dati personali verso paesi terzi.

7. All'interno di tale capo, il principio sancito dall'articolo 25, paragrafo 1, di tale direttiva, stabilisce che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati ad 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 a tali dati.

8. Per converso, come indicato dal legislatore dell'Unione al considerando 57 di detta direttiva, deve essere vietato il trasferimento di dati personali verso un paese terzo che non offre un livello di protezione adeguato.

9. Ai sensi dell'articolo 25, paragrafo 2, della direttiva 95/46, «[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».

10. Ai sensi dell'articolo 25, paragrafo 6, di tale direttiva, la Commissione può constatare che un paese terzo garantisce, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione adeguato ai dati personali. Non appena la Commissione adotta una decisione in tal senso, il trasferimento di dati personali verso il paese terzo di cui trattasi può avere luogo.

11. In applicazione di detta disposizione, la Commissione ha adottato la decisione 2000/520. Risulta dall'articolo 1, paragrafo 1, di tale decisione, che si considera che i «[p]rincipi di approdo sicuro in materia di riservatezza», applicati in conformità agli orientamenti forniti dalle «Domande più frequenti» [6], garantiscono un livello adeguato di protezione dei dati personali trasferiti dall'Unione a organizzazioni aventi sede negli Stati Uniti.

12. Di conseguenza, la decisione 2000/520 autorizza il trasferimento di dati personali dagli Stati membri verso imprese stabilite negli Stati Uniti che si sono impegnate a rispettare i principi dell'approdo sicuro.

13. La decisione 2000/520 enuncia, al suo allegato I, un certo numero di principi ai quali le imprese possono aderire volontariamente, corredati da limiti e da un sistema di controllo specifico. Il numero di imprese che hanno aderito a quello che potrebbe essere qualificato come un «codice di condotta» era superiore a 3 200 nel 2013.

14. Il regime dell'approdo sicuro poggia su una soluzione che mescola l'autocertificazione, nonché l'autovalutazione da parte delle imprese private, e l'intervento dei poteri pubblici.

5 — GU L 281, pag. 31. Direttiva come modificata dal regolamento (CE) n. 1882/2003 del Parlamento europeo e del Consiglio del 29 settembre 2003 (GU L 284, pag. 1; in prosieguo: la «direttiva 95/46»).

6 — Frequently asked questions; in prosieguo: le «FAQ».

15. I principi dell'approdo sicuro sono stati messi a punto «in consultazione con l'industria e con il grande pubblico per facilitare gli scambi commerciali fra Stati Uniti ed Unione (…). Essi sono destinati unicamente ad organizzazioni americane che ricevono dati personali dall'Unione (…), al fine di permettere a tali organizzazioni di ottemperare al principio di "approdo sicuro" ed alla presunzione di "adeguatezza" che esso comporta» [7].

16. I principi dell'approdo sicuro, figuranti all'allegato I della decisione 2000/520, prevedono, segnatamente:

— un obbligo di informazione in forza del quale «[l]e organizzazioni devono informare i singoli individui in merito alle finalità per cui vengono raccolte e utilizzate le informazioni su di essi, alle modalità per contattare le organizzazioni in relazione ad eventuali quesiti o reclami, alla tipologia dei terzi a cui vengono fornite le informazioni, e infine ad opzioni e mezzi che le organizzazioni mettono a disposizione dei singoli individui per limitare l'utilizzazione e la rivelazione delle informazioni. Queste indicazioni vanno formulate (…) quando si tratti del primo invito a fornire informazioni personali alle organizzazioni rivolto ad una persona oppure non appena ciò risulti successivamente possibile, ma comunque prima che le organizzazioni utilizzino o rivelino per la prima volta a terzi tali informazioni per finalità diverse da quelle per le quali le informazioni stesse erano state originariamente raccolte» [8];

— un obbligo per le organizzazioni di offrire agli individui la possibilità di scegliere se le informazioni personali che li riguardano vadano rivelate a terzi ovvero utilizzate per fini incompatibili con quelli per cui le informazioni stesse erano state originariamente raccolte o con quelli successivamente autorizzati dall'interessato. Nel caso di dati di carattere delicato, «va data la possibilità di scelta affermativa o esplicita (facoltà di consenso) per quanto riguarda la possibilità che le informazioni in questione vengano rivelate a terzi od utilizzate per scopi diversi da quelli per cui esse erano state originariamente raccolte o da quelli successivamente autorizzati dagli interessati con l'esercizio della facoltà di consenso» [9];

— norme relative al trasferimento successivo dei dati. In tal senso, «[l]e organizzazioni che comunicano informazioni a terzi devono applicare i principi di notifica e di scelta» [10];

— quanto alla sicurezza dei dati, un obbligo per «[l]e organizzazioni che detengono, aggiornano, utilizzano o diffondono informazioni personali (…) [di] prendere ragionevoli precauzioni per proteggerle da perdita ed abusi nonché da accesso, rivelazione, alterazione e distruzione non autorizzati» [11];

— quanto all'integrità dei dati, un obbligo per le organizzazioni «[di] prendere provvedimenti ragionevoli per garantire che i dati siano attendibili in funzione dell'uso che si prevede di farne, accurati, completi e aggiornati» [12];

— che gli individui i cui dati sono in possesso di un'organizzazione devono, in linea di principio, «poter accedere alle informazioni personali che li riguardano (…) ed altresì poterle correggere, emendare o cancellare se ed in quanto esse risultino inesatte» [13];

7 — Secondo comma dell'allegato I della decisione 2000/520.

8 — V. allegato I, sub «Notifica».

9 — V. allegato I, sub «Scelta».

10 — V. allegato I, sub «Trasferimento successivo».

11 — V. allegato I, sub «Sicurezza».

12 — V. allegato I, sub «Integrità dei dati».

13 — V. allegato I, sub «Accesso».

— un obbligo di prevedere «meccanismi volti a garantire il rispetto dei principi [dell'approdo sicuro], la possibilità di ricorso per gli individui cui si riferiscono i dati che vedano lesi i propri interessi dal mancato rispetto dei principi stessi, e la non impunità di un'organizzazione che non rispetti i principi» [14].

17. Un'organizzazione americana che desideri aderire ai principi dell'approdo sicuro è tenuta a dichiarare, nella sua politica di tutela della sfera privata, di rendere pubblico il fatto di aderire a tali principi e di conformarvisi effettivamente e ad autocertificare, con dichiarazione al Dipartimento del commercio degli Stati Uniti, di essere rispettosa dei medesimi principi [15].

18. Le organizzazioni dispongono di più strumenti per conformarsi ai principi dell'approdo sicuro. Così esse possono, ad esempio, «aderi[re] ad un programma di tutela della riservatezza, messo a punto dal settore privato e tale da ottemperare ai principi in questione [oppure] qualificarsi per l'approdo sicuro sviluppa[ndo] proprie politiche in fatto di riservatezza dei dati personali, purché queste siano conformi ai principi indicati (…). Inoltre, anche le organizzazioni soggette a disposizioni (o a norme) legislative, regolamentari, amministrative o d'altro tipo che tutelino efficacemente la riservatezza dei dati personali possono compiere quanto necessario per godere dei vantaggi dell'approdo sicuro» [16].

19. Esistono diversi meccanismi, i quali mescolano l'arbitrato privato e il controllo ad opera dei poteri pubblici, per verificare il rispetto dei principi dell'approdo sicuro. Il controllo può in tal senso essere assicurato tramite un sistema di risoluzione extragiudiziale delle controversie da parte di un terzo indipendente. Inoltre, le imprese possono impegnarsi a cooperare con il panel dell'Unione sulla protezione dei dati. Infine, la Commissione federale del commercio (Federal Trade Commission; in prosieguo: la «FTC»), sulla base dei poteri conferitile in forza della sezione 5 della legge sulla Commissione federale del commercio (Federal Trade Commission Act), nonché il ministero dei Trasporti (Department of Transportation), sulla base dei poteri che gli sono stati conferiti in virtù dell'articolo 41712 del Codice degli Stati Uniti (United States Code) figurante al suo titolo 49, sono competenti ad esaminare le denunce.

20. Ai sensi del quarto comma dell'allegato I della decisione 2000/520, l'adesione ai principi dell'approdo sicuro può essere limitata, segnatamente, «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia» e «da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione» [17].

21. Inoltre, la possibilità, per le autorità competenti degli Stati membri, di sospendere flussi di dati è subordinata a diverse condizioni, le quali sono previste all'articolo 3, paragrafo 1, della decisione 2000/520.

22. La presente domanda di pronuncia pregiudiziale induce a porsi interrogativi sulla portata della decisione 2000/520, alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»), nonché degli articoli 25, paragrafo 6, e 28 della direttiva 95/46. Tale domanda è stata presentata nell'ambito di una controversia fra il sig. Schrems e il Data

14 — V. allegato I, sub «Garanzie d'applicazione».

15 — Articolo 1, paragrafi 2 e 3, della decisione 2000/520. V., parimenti, allegato II, FAQ 6.

16 — Terzo comma dell'allegato I.

17 — V., parimenti, allegato IV, B.

Protection Commissioner (Commissario per la protezione dei dati; in prosieguo: il «commissario») concernente il rifiuto, da parte di quest'ultimo, di istruire una denuncia presentata dal sig. Schrems per il fatto che la Facebook Ireland Ltd (in prosieguo: «Facebook Ireland») conserva i dati personali dei propri iscritti su server ubicati negli Stati Uniti.

23. Il sig. Schrems è un cittadino austriaco residente in Austria. Egli è iscritto al media sociale Facebook dal 2008.

24. A tutti gli utenti di Facebook residenti nel territorio dell'Unione viene chiesto di sottoscrivere un contratto con Facebook Ireland, la quale è una controllata della società madre Facebook Inc., stabilita negli Stati Uniti (in prosieguo: «Facebook USA»). I dati degli iscritti a Facebook Ireland residenti nel territorio dell'Unione vengono, in tutto o in parte, trasferiti e archiviati in server di Facebook USA ubicati nel territorio degli Stati Uniti.

25. Il 25 giugno 2013 il sig. Schrems ha depositato una denuncia dinanzi al commissario, facendo valere, in sostanza, che il diritto e la prassi statunitensi non offrono alcuna protezione effettiva dei dati conservati negli Stati Uniti contro la sorveglianza dello Stato. Ciò emergerebbe dalle rivelazioni fatte dal sig. Snowden a partire dal maggio 2013 in merito alle attività dei servizi di intelligence americani, e in particolare alle attività della National Security Agency (in prosieguo: la «NSA»).

26. Emerge, segnatamente, da tali rivelazioni, che la NSA avrebbe creato un programma chiamato «PRISM», nell'ambito del quale tale agenzia avrebbe ottenuto libero accesso ai dati conservati in massa su server ubicati negli Stati Uniti, posseduti o controllati da una serie di società operanti nel settore di Internet e della tecnologia come Facebook USA.

27. Il commissario ha ritenuto di non essere obbligato ad istruire la denuncia, in quanto essa era priva di fondamento giuridico. Tale autorità ha considerato che non esistevano prove del fatto che la NSA avesse avuto accesso ai dati del sig. Schrems. Inoltre, a suo avviso, la denuncia doveva essere respinta a causa della decisione 2000/520, con la quale la Commissione ha constatato che gli Stati Uniti assicurano, nell'ambito del regime dell'approdo sicuro, un livello adeguato di protezione ai dati personali trasferiti. Ogni questione concernente il carattere adeguato della protezione di tali dati negli Stati Uniti dovrebbe essere risolta in conformità a detta decisione, la quale gli impedirebbe di esaminare il problema sollevato dalla denuncia.

28. La normativa nazionale che ha indotto il commissario a respingere la denuncia è la seguente.

29. L'articolo 10, paragrafo 1, della legge del 1988 sulla protezione dei dati (Data Protection Act 1988), come modificata dalla legge del 2003 sulla protezione dei dati [Data Protection (Amendment) Act 2003; in prosieguo: la «legge sulla protezione dei dati»] gli conferisce il potere di esaminare le denunce e così recita:

«a) Il commissario può verificare o far verificare se disposizioni della presente legge siano state, siano o rischino di essere violate nei confronti di una determinata persona, o quando tale persona presenta al medesimo una denuncia per una violazione di una qualsiasi di tali disposizioni, o quando il commissario ritenga che una siffatta violazione possa esistere.

b) Qualora una persona presenti una denuncia dinanzi al commissario in forza della lettera a) del presente paragrafo, il commissario:

i) istruisce o fa istruire la denuncia, a meno che non concluda che essa sia defatigatoria o vessatoria, e

ii) qualora egli o ella non sia in grado, entro un termine ragionevole, di ottenere dalle parti interessate una risoluzione extragiudiziale dell'oggetto della denuncia, lo stesso notifica per iscritto al denunciante la decisione adottata in ordine alla medesima, indicando che, qualora tale decisione gli arrechi pregiudizio, il denunciante può impugnarla in forza dell'articolo 26 della presente legge, entro 21 giorni a partire dal ricevimento della notifica».

30. Nella specie, il commissario ha concluso che la denuncia del sig. Schrems era «defatigatoria o vessatoria», nel senso che essa era destinata al fallimento, in quanto priva di fondamento giuridico. È su tale base che esso si è rifiutato di istruire tale denuncia.

31. L'articolo 11 della legge sulla protezione dei dati disciplina il trasferimento dei dati personali al di fuori del territorio nazionale. L'articolo 11, paragrafo 2, lettera a), della medesima prevede quanto segue:

«Qualora, in un procedimento disciplinato dalla presente legge, venga sollevata una questione:

i) per determinare se il livello di protezione adeguato specificato al paragrafo 1 del presente articolo sia assicurato da un paese o da un territorio al di fuori dello Spazio economico europeo [(SEE)] verso il quale vengono trasferiti dati personali, e

ii) sia stata effettuata una constatazione da parte dell'Unione per quanto attiene al tipo di trasferimenti in questione,

la questione verrà esaminata in conformità a tale constatazione».

32. L'articolo 11, paragrafo 2, lettera b), della legge sulla protezione dei dati, definisce la nozione di constatazione dell'Unione nei seguenti termini:

«Alla lettera a) del presente paragrafo, per "constatazione dell'Unione" si intende una constatazione che la Commissione (...) ha fatto ai sensi del paragrafo 4 o del paragrafo 6 dell'articolo 25 della direttiva [95/46], nell'ambito del procedimento previsto all'articolo 31, paragrafo 2, della [medesima] al fine di determinare se il livello di protezione adeguato specificato al paragrafo 1 del presente articolo sia assicurato da un paese o un territorio al di fuori del [SEE]».

33. Il commissario ha osservato che la decisione 2000/520 era una «constatazione dell'Unione» ai sensi dell'articolo 11, paragrafo 2, lettera a), della legge sulla protezione dei dati, cosicché, in forza di tale legge, ogni questione relativa all'adeguatezza della protezione dei dati personali nel paese terzo in cui essi vengono trasferiti doveva essere esaminata in conformità a tale constatazione. Dal momento che in ciò consisteva essenzialmente la denuncia del sig. Schrems, vale a dire il trasferimento di dati personali in un paese terzo che, in pratica, non assicurava un livello di protezione adeguato, il commissario ha ritenuto che la natura e l'esistenza stessa della decisione 2000/520 gli impedissero di esaminare tale questione.

34. Il sig. Schrems ha presentato un ricorso dinanzi alla Corte d'appello avverso la decisione del commissario di respingere la sua denuncia. Dopo aver esaminato le prove prodotte nel procedimento principale, tale giudice ha constatato che la sorveglianza elettronica e l'intercettazione dei dati personali rispondono a finalità necessarie e indispensabili per l'interesse pubblico, ossia il mantenimento della sicurezza nazionale e la prevenzione dei crimini gravi. La Corte d'appello indica, a tal riguardo, che la sorveglianza e l'intercettazione dei dati personali trasferiti dall'Unione verso gli Stati Uniti servono obiettivi legittimi connessi alla lotta contro il terrorismo.

35. Secondo questo stesso giudice, le rivelazioni fatte dal sig. Snowden hanno tuttavia dimostrato che la NSA e altri enti simili avevano commesso eccessi considerevoli. Sebbene la Foreign Intelligence Surveillance Court (in prosieguo: la «FISC»), la quale interviene nell'ambito della legge del 1978 sulla sorveglianza dei servizi di intelligence stranieri (Foreign Intelligence Surveillance Act of 1978)[18], eserciti una supervisione, il procedimento dinanzi alla medesima si svolgerebbe tuttavia segretamente e inaudita altera parte. Inoltre, a parte il fatto che le decisioni relative all'accesso ai dati personali verrebbero adottate sulla base del diritto americano, i cittadini dell'Unione non avrebbero alcun diritto effettivo ad essere sentiti sulla questione della sorveglianza e dell'intercettazione dei loro dati.

36. Emergerebbe chiaramente dai voluminosi documenti che corredano le dichiarazioni giurate rese nel procedimento principale che l'esattezza di una considerevole quantità delle rivelazioni del sig. Snowden non viene rimessa in discussione. La Corte d'appello ha pertanto concluso che, una volta che i dati personali vengono trasferiti negli Stati Uniti, la NSA nonché altre agenzie di sicurezza americane, come il Federal Bureau of Investigation (FBI) possono accedervi nel corso di operazioni di sorveglianza e intercettazioni di massa indiscriminate.

37. La Corte d'appello rileva che, nel diritto irlandese, l'importanza dei diritti costituzionali alla vita privata e all'inviolabilità del domicilio esige che qualsiasi ingerenza in tali diritti sia conforme ai requisiti previsti dalla legge e sia proporzionata. L'accesso massiccio e indiscriminato a dati personali non soddisferebbe affatto il requisito di proporzionalità e dovrebbe pertanto essere considerato contrario alla Costituzione irlandese[19].

38. La Corte d'appello rileva che, affinché intercettazioni di comunicazioni elettroniche possano essere considerate costituzionalmente legittime, occorrerebbe dimostrare che determinate intercettazioni di comunicazioni e la sorveglianza su talune persone o su taluni gruppi sono oggettivamente giustificate nell'interesse della sicurezza nazionale e della repressione della criminalità, e che esistono garanzie adeguate e verificabili.

39. Pertanto, la Corte d'appello indica che, se la presente causa dovesse essere trattata unicamente sulla base del diritto irlandese, si porrebbe un problema considerevole quanto alla questione se gli Stati Uniti «garantisc[a]no un livello adeguato di protezione della riservatezza e dei diritti e delle libertà fondamentali», ai sensi dell'articolo 11, paragrafo 1, della legge sulla protezione dei dati. Ne consegue che, sulla base del diritto irlandese, e in particolare dei suoi requisiti di carattere costituzionale, il commissario non avrebbe potuto respingere la denuncia del sig. Schrems, ma avrebbe dovuto esaminare tale questione.

40. Tuttavia, la Corte d'appello constata che la causa della quale è investita verte sull'attuazione del diritto dell'Unione ai sensi dell'articolo 51, paragrafo 1, della Carta, cosicché la legittimità della decisione del commissario dovrebbe essere valutata alla luce del diritto dell'Unione.

41. Il problema che il commissario ha dovuto affrontare viene spiegato dalla Corte d'appello nei seguenti termini. Ai sensi dell'articolo 11, paragrafo 2, lettera a) della legge sulla protezione dei dati, il commissario deve risolvere la questione dell'adeguatezza della protezione dei dati nello Stato terzo «in conformità» ad una constatazione dell'Unione effettuata dalla Commissione ai sensi dell'articolo 25, paragrafo 6, della direttiva 95/46. Ne consegue che il commissario non potrebbe discostarsi da una

18 — V. articolo 702 di tale legge, come modificata dalla legge del 2008 (Foreign Intelligence Surveillance Act of 2008). È in applicazione di tale articolo che la NSA detiene una banca dati conosciuta con il nome di «PRISM» (v. report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection del 27 novembre 2013).

19 — La Corte d'appello fa riferimento, in particolare, al rispetto della dignità umana e alla libertà della persona (preambolo), all'autonomia personale (articolo 40, paragrafo 3, punti 1 e 2), all'inviolabilità del domicilio (articolo 40, paragrafo 5) e alla protezione della vita familiare (articolo 41).

siffatta constatazione. Poiché la Commissione, nella sua decisione 2000/520, ha constatato che gli Stati Uniti garantiscono un livello di protezione adeguato quanto al trattamento dei dati da parte delle società che aderiscono ai principi dell'approdo sicuro, una denuncia che fa valere l'inadeguatezza di una siffatta protezione dovrebbe inevitabilmente essere respinta dal commissario.

42. Constatando al contempo che il commissario ha in tal modo dato prova di essersi scrupolosamente attenuto alla lettera della direttiva 95/46 e della decisione 2000/520, la Corte d'appello rileva che il sig. Schrems muove in realtà obiezioni nei confronti dei termini del regime dell'approdo sicuro stesso piuttosto che nei confronti del modo in cui il commissario l'ha applicato, sottolineando al contempo che egli non ha contestato direttamente la validità della direttiva 95/46 né quella della decisione 2000/520.

43. Secondo la Corte d'appello, la questione fondamentale sarebbe dunque se, alla luce del diritto dell'Unione e tenuto conto, in particolare, della successiva entrata in vigore degli articoli 7 e 8 della Carta, il commissario sia vincolato in maniera assoluta dalla constatazione della Commissione enunciata nella decisione 2000/520 in relazione all'adeguatezza del diritto e della prassi in materia di protezione dei dati personali negli Stati Uniti.

44. La Corte d'appello precisa inoltre che, nel ricorso del quale è investita, non è stata dedotta alcuna censura in ordine ai comportamenti di Facebook Ireland e di Facebook USA in quanto tali. Orbene, l'articolo 3, paragrafo 1, lettera b), della decisione 2000/520, il quale consente alle autorità nazionali competenti di ordinare ad un'impresa di sospendere i flussi di dati verso un paese terzo, si applicherebbe, secondo tale giudice, solo nei casi in cui la denuncia è diretta avverso la condotta dell'impresa di cui trattasi, il che non avverrebbe nel caso di specie.

45. La Corte d'appello sottolinea pertanto che la reale obiezione non riguarda la condotta di Facebook USA di per sé, bensì il fatto che la Commissione abbia ritenuto che il diritto e la prassi in materia di protezione dei dati negli Stati Uniti forniscano una protezione adeguata, mentre risulta chiaro, dalle rivelazioni del sig. Snowden, che i dati personali dei cittadini che vivono nel territorio dell'Unione sono accessibili alle autorità americane massicciamente e in maniera indifferenziata [20].

46. Su tale punto, la Corte d'appello ritiene che sia difficile immaginare come la decisione 2000/520 possa, nella prassi, soddisfare i requisiti degli articoli 7 e 8 della Carta, a maggior ragione alla luce dei principi elaborati dalla Corte nella sua sentenza Digital Rights Ireland e a. [21]. In particolare, la garanzia prevista all'articolo 7 della Carta e dai valori fondamentali comuni alle tradizioni degli Stati membri sarebbe compromessa qualora si ammettesse che le comunicazioni elettroniche possano essere oggetto di accesso da parte delle autorità statali su base casuale e generalizzata, senza che sia richiesta una motivazione oggettiva in base a considerazioni di sicurezza nazionale o prevenzione di crimini specificamente riguardanti i singoli interessati, e senza la previsione di garanzie adeguate e verificabili. Poiché il ricorso del sig. Schrems suggerisce che la decisione 2000/520 potrebbe essere astrattamente incompatibile con gli articoli 7 e 8 della Carta, la Corte potrebbe ritenere che sia possibile interpretare la direttiva 95/46, e segnatamente il suo articolo 25, paragrafo 6, nonché la decisione 2000/520 in un senso che consenta alle autorità nazionali di condurre autonomamente indagini al fine di stabilire se il trasferimento di dati personali verso un paese terzo soddisfi i requisiti risultanti dagli articoli 7 e 8 della Carta.

20 — La Corte d'appello indica, a tal riguardo, che il motivo principale dedotto dal sig. Schrems dinanzi alla medesima consisteva nell'affermare che, alla luce delle recenti rivelazioni del sig. Snowden e del fatto che taluni dati personali sono stati messi a disposizione dei servizi di intelligence degli Stati Uniti su larga scala, il commissario non poteva trarre legittimamente la conclusione che, in tale paese terzo, esistesse un adeguato livello di protezione di detti dati.

21 — C-293/12 e C-594/12, EU:C:2014:238, punti da 65 a 69.

47. In tale contesto, la Corte d'appello ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

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

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

II – **Analisi**

48. Le due questioni formulate dalla Corte d'appello invitano la Corte a precisare i poteri di cui dispongono le autorità nazionali di controllo allorché esse vengono investite di una denuncia concernente un trasferimento di dati personali verso un'impresa stabilita in un paese terzo e allorché viene dedotto, a sostegno di tale denuncia, che tale paese terzo non garantisce un livello di protezione adeguato ai dati trasferiti, sebbene la Commissione abbia adottato, sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, una decisione che riconosce l'adeguatezza del livello di protezione assicurato da detto paese terzo.

49. Osservo che la denuncia depositata dal sig. Schrems presso il commissario è caratterizzata da una duplice dimensione. Essa è intesa a contestare il trasferimento di dati personali da Facebook Ireland a Facebook USA. Il sig. Schrems chiede la cessazione di tale trasferimento poiché, a suo avviso, gli Stati Uniti non assicurerebbero un livello di protezione adeguato ai dati personali che vengono trasferiti nell'ambito del regime dell'approdo sicuro. Più precisamente, a tale paese terzo è addebitata la creazione del programma PRISM, il quale consente alla NSA di accedere liberamente ai dati conservati in massa in server ubicati negli Stati Uniti. In tal senso, la denuncia ha specificamente ad oggetto i trasferimenti di dati personali da Facebook Ireland a Facebook USA, mettendo al contempo in discussione in maniera più generale il livello di protezione assicurato a tali dati nell'ambito del regime approdo sicuro.

50. Il commissario ha ritenuto che l'esistenza stessa di una decisione della Commissione che riconosce che gli Stati Uniti assicurano, nell'ambito del regime dell'approdo sicuro, un livello di protezione adeguato, gli impedisse di istruire la denuncia.

51. Occorre pertanto esaminare congiuntamente le due questioni, con le quali si chiede, in sostanza, se l'articolo 28 della direttiva 95/46, in combinato disposto con gli articoli 7 e 8 della Carta, debba essere interpretato nel senso che l'esistenza di una decisione adottata dalla Commissione sulla base dell'articolo 25, paragrafo 6, di questa direttiva produca l'effetto di impedire ad un'autorità nazionale di controllo di istruire una denuncia con la quale lamenta che un paese terzo non assicura un livello di protezione adeguato ai dati personali trasferiti e, se del caso, di sospendere il trasferimento di tali dati.

52. L'articolo 7 della Carta garantisce il diritto al rispetto della vita privata, mentre il suo articolo 8 proclama espressamente il diritto alla protezione dei dati di carattere personale. I paragrafi 2 e 3 di quest'ultimo articolo precisano che tali dati devono essere trattati secondo il principio di lealtà, per finalità' determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge, che ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica e che il rispetto di tali regole è soggetto al controllo di un'autorità' indipendente.

A – *Sui poteri delle autorità nazionali di controllo in caso di decisione della Commissione che dichiara l'adeguatezza*

53. Come indicato dal sig. Schrems nelle sue osservazioni, ai fini della denuncia di cui al procedimento principale, la questione centrale concerne il trasferimento di dati personali da Facebook Ireland a Facebook USA alla luce dell'accesso generalizzato, da parte della NSA e di altre agenzie di sicurezza americane, ai dati conservati presso Facebook USA in forza dei poteri loro conferiti dalla legislazione americana.

54. Quando è investita di una denuncia intesa a rimettere in discussione la constatazione secondo la quale un paese terzo garantisce un livello di protezione adeguato ai dati trasferiti, secondo il sig. Schrems l'autorità nazionale di controllo ha il potere, qualora disponga di elementi che depongono nel senso della fondatezza delle allegazioni contenute in tale denuncia, di ordinare la sospensione del trasferimento di dati effettuato dall'impresa designata in detta denuncia.

55. Alla luce degli obblighi del commissario di proteggere i diritti fondamentali del sig. Schrems, quest'ultimo sostiene che il commissario è tenuto non solo ad indagare, bensì anche, in caso di accoglimento della denuncia, ad utilizzare i propri poteri per sospendere il flusso di dati fra Facebook Ireland e Facebook USA.

56. Orbene, il commissario ha respinto la denuncia sulla base delle disposizioni della legge sulla protezione dei dati che elencano i suoi poteri. Tale conclusione era fondata sulla convinzione del commissario di essere vincolato dalla decisione 2000/520.

57. Ne consegue che la questione centrale nella presente causa è di chiarire se la valutazione della Commissione sull'adeguatezza del livello di protezione, contenuta nella decisione 2000/520, vincoli in maniera assoluta l'autorità nazionale di protezione dei dati e le impedisca di indagare su affermazioni intese a rimettere in discussione tale constatazione. Le questioni pregiudiziali vertono dunque sulla portata dei poteri di indagine delle autorità nazionali di protezione dei dati quando la Commissione ha emanato una decisione che dichiara l'adeguatezza.

58. Secondo la Commissione, occorre tenere conto del rapporto fra i poteri della medesima e quelli delle autorità nazionali di protezione dei dati. Le competenze di queste ultime sarebbero focalizzate sull'applicazione della normativa in tale materia in singoli casi, mentre il riesame generale dell'applicazione della decisione 2000/520, inclusa ogni decisione che ne comporta la sospensione o l'abrogazione, rientrerebbe nella competenza della Commissione.

59. La Commissione fa valere che il sig. Schrems non avrebbe dedotto argomenti specifici che inducano a pensare che lo stesso correva un rischio imminente di subire danni gravi a causa del trasferimento di dati fra Facebook Ireland e Facebook USA. Al contrario, a causa della loro natura astratta e generale, le preoccupazioni espresse dal sig. Schrems a proposito dei programmi di sorveglianza attuati dalle agenzie di sicurezza americane sarebbero identiche a quelle che hanno condotto la Commissione ad avviare il riesame della decisione 2000/520.

60. Secondo la Commissione, le autorità nazionali di controllo interferirebbero nelle competenze di cui essa dispone per rinegoziare le condizioni di tale decisione con gli Stati Uniti o, se necessario, per sospenderla, qualora adottassero misure sulla base di denunce che si limitano ad enunciare preoccupazioni strutturali ed astratte.

61. Non condivido l'opinione della Commissione. A mio avviso, l'esistenza di una decisione adottata dalla Commissione sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46 non può elidere e neppure ridurre i poteri di cui dispongono le autorità nazionali di controllo in forza dell'articolo 28 di tale direttiva. Contrariamente a quanto afferma la Commissione, se le autorità nazionali di controllo

vengono adite nell'ambito di denunce individuali, ciò non impedisce loro, a mio avviso, in forza dei loro poteri di indagine e della loro indipendenza, di formarsi un'opinione autonoma sul livello generale di protezione assicurato da un paese terzo e di trarne le conseguenze allorché esse statuiscono su singoli casi concreti.

62. Discende da costante giurisprudenza della Corte che, ai fini dell'interpretazione delle disposizioni di diritto dell'Unione, si deve tener conto non soltanto della lettera delle stesse, ma anche del loro contesto e degli scopi perseguiti dalla normativa di cui esse fanno parte [22].

63. Risulta dal considerando 62 della direttiva 95/46 che «la designazione di autorità di controllo che agiscano in modo indipendente in ciascuno Stato membro è un elemento essenziale per la tutela delle persone con riguardo al trattamento di dati personali».

64. Ai sensi dell'articolo 28, paragrafo 1, primo comma, di tale direttiva, «[o]gni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri». L'articolo 28, paragrafo 1, secondo comma, di detta direttiva dispone che «[t]ali autorità sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite».

65. L'articolo 28, paragrafo 3, della direttiva 95/46 elenca i poteri di cui ogni autorità di controllo dispone, vale a dire poteri investigativi, poteri effettivi d'intervento che le consentono, segnatamente, di vietare a titolo provvisorio o definitivo un trattamento, nonché il potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione di tale direttiva ovvero di adire per dette violazioni le autorità giudiziarie.

66. Inoltre, ai sensi dell'articolo 28, paragrafo 4, primo comma, della direttiva 95/46, «[q]ualsiasi persona (…) può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali». L'articolo 28, paragrafo 4, secondo comma, di tale direttiva, precisa che «[q]ualsiasi persona può, in particolare, chiedere a un'autorità di controllo di verificare la liceità di un trattamento quando si applicano le disposizioni nazionali adottate a norma dell'articolo 13 [di detta] direttiva». Preciso che quest'ultima disposizione consente agli Stati membri di adottare misure di legge intese a limitare la portata di diversi obblighi e diritti previsti nella direttiva 95/46, qualora tale restrizione costituisca una misura necessaria alla salvaguardia, segnatamente, della sicurezza dello Stato, della difesa, della pubblica sicurezza, nonché della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali.

67. Come già rilevato dalla Corte, l'esigenza di un controllo, da parte di un'autorità indipendente, dell'osservanza delle norme del diritto dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali risulta altresì dal diritto primario dell'Unione, segnatamente dall'articolo 8, paragrafo 3, della Carta e dall'articolo 16, paragrafo 2, TFUE [23]. Essa ha parimenti rammentato che «[l]'istituzione, negli Stati membri, di autorità di controllo indipendenti costituisce quindi un elemento essenziale del rispetto della tutela delle persone con riguardo al trattamento dei dati personali» [24].

68. La Corte ha anche statuito che «l'articolo 28, paragrafo 1, secondo comma, della direttiva 95/46 deve essere interpretato nel senso che le autorità di controllo competenti per la vigilanza del trattamento dei dati personali devono godere di un'indipendenza che consenta loro di svolgere le proprie funzioni senza subire influenze esterne. Tale indipendenza esclude in particolare qualsiasi

22 — V., segnatamente, sentenza Koushkaki (C-84/12, EU:C:2013:862, punto 34 e la giurisprudenza ivi citata).

23 — V. sentenze Commissione/Austria (C-614/10, EU:C:2012:631, punto 36) e Commissione/Ungheria (C-288/12, EU:C:2014:237, punto 47).

24 — V., segnatamente, sentenze Commissione/Ungheria (C-288/12, EU:C:2014:237, punto 48 e la giurisprudenza ivi citata). V. parimenti, in tal senso, la sentenza Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238, punto 68, nonché la giurisprudenza ivi citata).

imposizione e ogni altra influenza esterna di qualunque forma, sia diretta che indiretta, che possano orientare le loro decisioni e che potrebbero quindi rimettere in discussione lo svolgimento, da parte di dette autorità, del loro compito, consistente nello stabilire un giusto equilibrio tra la protezione del diritto alla vita privata e la libera circolazione dei dati personali» [25].

69. La Corte ha parimenti precisato che «[l]a garanzia dell'indipendenza delle autorità nazionali di controllo è diretta ad assicurare l'efficacia e l'affidabilità del controllo del rispetto delle disposizioni in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali» [26]. Tale garanzia d'indipendenza è stata disposta «per rafforzare la protezione delle persone e degli organismi interessati dalle (…) decisioni [di tali autorità nazionali di controllo]» [27].

70. Come emerge in particolare dal considerando 10 e dall'articolo 1 della direttiva 95/46, essa si propone di garantire, all'interno dell'Unione, «un elevato grado di tutela delle libertà e dei diritti fondamentali con riguardo al trattamento dei dati personali» [28]. Secondo la Corte, «[l]e autorità di controllo previste all'art[icolo] 28 della direttiva 95/46 sono quindi le custodi dei menzionati diritti e libertà fondamentali» [29].

71. Tenuto conto dell'importanza del ruolo svolto dalle autorità nazionali di controllo in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, i loro poteri di intervento devono permanere anche quando la Commissione ha adottato una decisione sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46.

72. Osservo, a tal riguardo, che nulla indica che i regimi di trasferimento di dati personali verso paesi terzi siano esclusi dall'ambito di applicazione ratione materiae dell'articolo 8, paragrafo 3, della Carta, il quale consacra al livello più alto della gerarchia delle norme nel diritto dell'Unione l'importanza del controllo esercitato da un'autorità indipendente per quanto attiene al rispetto delle norme relative alla protezione dei dati personali.

73. Se le autorità nazionali di controllo fossero vincolate in maniera assoluta dalle decisioni adottate dalla Commissione, ciò limiterebbe inevitabilmente la loro totale indipendenza. In conformità al loro ruolo di custodi dei diritti fondamentali, le autorità nazionali di controllo devono poter indagare, in piena indipendenza, sui reclami loro sottoposti, nell'interesse superiore della protezione dei singoli con riguardo al trattamento dei dati personali.

74. Inoltre, come rilevato giustamente dal governo belga e dal Parlamento europeo in udienza, non esiste alcun vincolo gerarchico fra il capo IV della direttiva 95/46, relativo al trasferimento di dati personali verso paesi terzi, e il capo VI della medesima, il quale è dedicato, segnatamente, al ruolo delle autorità nazionali di controllo. Nulla, nel capo VI, suggerisce che le disposizioni relative alle autorità nazionali di controllo siano subordinate in una qualsivoglia maniera alle disposizioni distinte sui trasferimenti enunciate nel capo IV della direttiva 95/46.

75. Al contrario, risulta in maniera esplicita dall'articolo 25, paragrafo 1, di tale direttiva, figurante al capo IV della medesima, che l'autorizzazione del trasferimento di dati personali verso un paese terzo che garantisce un livello di protezione adeguato vale solo fatte salve le misure nazionali di attuazione delle altre disposizioni di detta direttiva.

25 — V., segnatamente, sentenza Commissione/Ungheria (C-288/12, EU:C:2014:237, punto 51 e la giurisprudenza ivi citata).

26 — Sentenza Commissione/Germania (C-518/07, EU:C:2010:125, punto 25).

27 — Idem.

28 — Ibidem (punto 22 e la giurisprudenza ivi citata).

29 — Ibidem (punto 23). V., parimenti, in tal senso, sentenze Commissione/Austria (C-614/10, EU:C:2012:631, punto 52) e Commissione/Ungheria (C-288/12, EU:C:2014:237, punto 53).

76. Ricordo, a tal riguardo, che, in forza di tale disposizione, gli Stati membri devono prevedere, nella loro legislazione nazionale, 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 direttiva 95/46.

77. Ai sensi dell'articolo 28, paragrafo 1, di tale direttiva, le autorità nazionali di controllo sono incaricate di sorvegliare, nel territorio di ciascuno Stato membro, l'applicazione delle disposizioni di attuazione di detta direttiva, adottate dagli Stati membri.

78. L'accostamento fra queste due disposizioni consente di ritenere che la regola enunciata all'articolo 25, paragrafo 1, della direttiva 95/46, secondo la quale il trasferimento di dati personali può aver luogo soltanto se il paese terzo destinatario garantisce loro un livello di protezione adeguato, faccia parte delle regole di cui le autorità nazionali di controllo devono sorvegliare l'applicazione.

79. Occorre interpretare estensivamente, in conformità all'articolo 8, paragrafo 3, della Carta, i poteri delle autorità nazionali di controllo di indagare in completa indipendenza sui reclami di cui esse vengono investite ai sensi dell'articolo 28 della direttiva 95/46. Tali poteri non possono pertanto essere limitati dai poteri conferiti dal legislatore dell'Unione alla Commissione, ai sensi dell'articolo 25, paragrafo 6, di tale direttiva, al fine di accertare l'adeguatezza del livello di protezione offerto da un paese terzo.

80. Alla luce del loro ruolo fondamentale in materia di protezione dei dati personali, le autorità nazionali di controllo devono poter indagare allorché esse vengono investite di una denuncia che indica elementi che potrebbero essere in grado di rimettere in discussione il livello di protezione assicurato da un paese terzo, incluso il caso in cui la Commissione ha constatato, in una decisione adottata sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, che il paese terzo interessato assicura un livello di protezione adeguato.

81. Se, al termine delle indagini condotte da un'autorità nazionale di controllo, essa ritiene che il trasferimento di dati contestato arrechi pregiudizio alla protezione di cui devono beneficiare i cittadini dell'Unione quanto al trattamento dei loro dati, essa ha il potere di sospendere il trasferimento di dati in parola, e ciò a prescindere dalla valutazione generale effettuata dalla Commissione nella sua decisione.

82. È infatti pacifico, ai sensi dell'articolo 25, paragrafo 2, della direttiva 95/46, che l'adeguatezza del livello di protezione offerto da un paese terzo viene valutata in funzione di un insieme di circostanze sia di fatto che di diritto. Se una di tali circostanze muta e risulta idonea a rimettere in discussione l'adeguatezza del livello di protezione offerto da un paese terzo, l'autorità nazionale di controllo investita di una denuncia deve poterne trarre le conseguenze rispetto al trasferimento contestato.

83. Effettivamente, come rilevato dall'Irlanda, il commissario, al pari delle altre autorità statali, è vincolato dalla decisione 2000/520. Risulta infatti dall'articolo 288, quarto comma, TFUE, che una decisione adottata da un'istituzione dell'Unione è obbligatoria in tutti i suoi elementi. Di conseguenza, la decisione 2000/520 vincola gli Stati membri ai quali è destinata.

84. Rilevo, a tal riguardo, che la stessa decisione 2000/520 dispone, al suo articolo 5, che «[g]li Stati membri adottano le misure necessarie per conformarsi alla [medesima] entro 90 giorni dalla data di notifica delle stesse». Inoltre, l'articolo 6 di tale decisione conferma che «[g]li Stati membri sono destinatari della [stessa]».

85. Tuttavia ritengo che, alla luce delle summenzionate disposizioni della direttiva 95/46 e della Carta, l'effetto vincolante della decisione 2000/520 non sia idoneo ad escludere qualsiasi indagine del commissario su denunce con le quali si fa valere che trasferimenti di dati personali effettuati verso gli Stati Uniti nell'ambito di tale decisione non presentano le garanzie necessarie di protezione richieste dal diritto dell'Unione. In altre parole, un siffatto effetto vincolante non implica che ogni denuncia di questo tipo debba essere respinta sommariamente, ossia immediatamente e senza alcun esame della sua fondatezza.

86. Aggiungo che si evince inoltre dall'impianto dell'articolo 25 della direttiva 95/46 che l'accertamento se un paese terzo assicuri o meno un livello di protezione adeguato può essere effettuato vuoi dagli Stati membri vuoi dalla Commissione. Si tratta pertanto di una competenza ripartita.

87. Risulta dall'articolo 25, paragrafo 6, di tale direttiva che, qualora la Commissione constati che un paese terzo garantisce un livello di protezione adeguato, ai sensi dell'articolo 25, paragrafo 2, di detta direttiva, gli Stati membri devono adottare le misure necessarie per conformarsi alla decisione della Commissione.

88. Dato che una siffatta decisione produce l'effetto di consentire i trasferimenti di dati personali verso un paese terzo il cui livello di protezione è considerato adeguato dalla Commissione, gli Stati membri devono quindi consentire, in linea di principio, che siffatti trasferimenti siano effettuati dalle imprese stabilite nel loro territorio.

89. L'articolo 25 della direttiva 95/46 non attribuisce tuttavia alla Commissione una competenza esclusiva in materia di accertamento dell'adeguatezza o meno del livello di protezione dei dati personali trasferiti. L'impianto di tale articolo dimostra che gli Stati membri ricoprono parimenti un ruolo in materia. È vero che una decisione della Commissione svolge un ruolo importante per l'uniformazione delle condizioni di trasferimento valide all'interno degli Stati membri. Tuttavia, tale uniformazione può perdurare solo fintantoché tale accertamento non venga messo in discussione.

90. L'argomento della necessaria uniformazione delle condizioni di trasferimento dei dati personali verso un paese terzo trova il proprio limite, a mio avviso, in una situazione come quella di cui al procedimento principale, nella quale non solo la Commissione è al corrente del fatto che la sua constatazione è soggetta a critiche, ma è anche essa stessa che formula siffatte critiche e conduce negoziati per porvi rimedio.

91. La valutazione dell'adeguatezza o meno del livello della protezione offerto da un paese terzo può parimenti sfociare in una cooperazione fra gli Stati membri e la Commissione. L'articolo 25, paragrafo 3, della direttiva 95/46 prevede, a tal riguardo, che «[g]li Stati membri e la Commissione si comunicano a vicenda i casi in cui, a loro parere, un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2». Come osservato dal Parlamento, ciò dimostra chiaramente che gli Stati membri e la Commissione devono svolgere un ruolo equivalente per individuare i casi in cui un paese terzo non assicura un livello di protezione adeguato.

92. La decisione di adeguatezza è intesa ad autorizzare il trasferimento di dati personali verso il paese terzo interessato. Ciò non implica che le autorità di controllo non possano più essere investite dai cittadini dell'Unione di una domanda volta a proteggere i loro dati personali. Osservo, a tal riguardo, che l'articolo 28, paragrafo 4, primo comma, della direttiva 95/46, secondo il quale «[q]ualsiasi persona (…) può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali», non prevede eccezioni a tale principio in caso di esistenza di una decisione adottata dalla Commissione in applicazione dell'articolo 25, paragrafo 6, di tale direttiva.

93. Pertanto, se una decisione adottata dalla Commissione in applicazione dei poteri esecutivi che le sono conferiti da quest'ultima disposizione ha l'effetto di consentire il trasferimento di dati personali verso un paese terzo, una siffatta decisione non può avere come effetto, per contro, di togliere ogni potere agli Stati membri, e in particolare alle loro autorità nazionali di controllo, o anche soltanto di restringere le loro competenze, allorché esse si trovano di fronte ad affermazioni di violazioni di diritti fondamentali.

94. Un'autorità nazionale di controllo deve essere in grado di esercitare i poteri previsti all'articolo 28, paragrafo 3, della direttiva 95/46, fra cui quello di vietare a titolo provvisorio o definitivo un trattamento di dati personali. Pur se l'elencazione dei poteri, prevista a tale disposizione, non prevede esplicitamente poteri relativi ad un trasferimento da uno Stato membro verso un paese terzo, si deve ritenere, a mio avviso, che un siffatto trasferimento costituisca un trattamento di dati [30]. Come si evince dal testo di detta disposizione, l'elencazione non è, inoltre, esaustiva. In ogni caso, alla luce del ruolo fondamentale svolto dalle autorità nazionali di controllo nel sistema predisposto dalla direttiva 95/46, esse devono disporre del potere di sospendere un trasferimento di dati in caso di violazione effettiva o potenziale dei diritti fondamentali.

95. Aggiungo che privare l'autorità nazionale di controllo dei suoi poteri di indagine in circostanze come quelle di cui alla presente causa sarebbe contrario non solo al principio di indipendenza, ma anche all'obiettivo della direttiva 95/46, quale risulta dall'articolo 1, paragrafo 1, della stessa.

96. Come rilevato dalla Corte, «[r]isulta dai considerando 3, 8 e 10 della direttiva 95/46 che il legislatore dell'Unione ha inteso facilitare la libera circolazione dei dati personali ravvicinando le legislazioni degli Stati membri pur salvaguardando i diritti fondamentali della persona, in particolare il diritto alla tutela della vita privata, e garantendo un elevato grado di tutela nell'Unione. L'articolo 1 di tale direttiva prevede infatti che gli Stati membri debbano garantire la tutela dei diritti e delle libertà fondamentali delle persone fisiche, in particolare della loro vita privata, con riguardo al trattamento dei dati personali» [31].

97. Le disposizioni della direttiva 95/46 devono pertanto essere interpretate in conformità all'obiettivo della medesima, consistente nel garantire un livello elevato di protezione delle libertà e dei diritti fondamentali delle persone fisiche, e segnatamente della loro vita privata, con riguardo al trattamento dei dati personali all'interno dell'Unione.

98. L'importanza di tale obiettivo e il ruolo che gli Stati membri devono svolgere per conseguirlo implicano che, qualora circostanze particolari vengano a fondare un dubbio serio quanto al rispetto dei diritti fondamentali garantiti dalla Carta in caso di trasferimento di dati personali verso un paese terzo, gli Stati membri e dunque, al loro interno, le autorità nazionali di controllo, non possono essere vincolati in maniera assoluta da una decisione di adeguatezza della Commissione.

99. La Corte ha già statuito che «le disposizioni della direttiva 95/46, disciplinando il trattamento di dati personali che possono arrecare pregiudizio alle libertà fondamentali e, segnatamente, al diritto alla vita privata, devono necessariamente essere interpretate alla luce dei diritti fondamentali che, secondo una costante giurisprudenza, formano parte integrante dei principi generali del diritto di cui la Corte garantisce l'osservanza e che sono ormai iscritti nella Carta» [32].

30 — V. conclusioni dell'avvocato generale Léger nella causa Parlamento/Consiglio e Commissione (C-317/04, EU:C:2005:710, paragrafi da 92 a 95). V., parimenti, sentenza Parlamento/Consiglio e Commissione (C-317/04 e C-318/04, EU:C:2006:346, punto 56).

31 — V., segnatamente, sentenza IPI (C-473/12, EU:C:2013:715, punto 28 e la giurisprudenza ivi citata).

32 — V., segnatamente, sentenza Google Spain e Google (C-131/12, EU:C:2014:317, punto 68 e la giurisprudenza ivi citata).

100. Mi riferisco, inoltre, alla giurisprudenza secondo la quale «gli Stati membri sono tenuti non solo a interpretare il loro diritto nazionale conformemente al diritto dell'Unione, ma anche a fare in modo di non basarsi su un'interpretazione di norme di diritto derivato che entri in conflitto con i diritti fondamentali tutelati dall'ordinamento giuridico dell'Unione o con gli altri principi generali del diritto dell'Unione» [33].

101. La Corte ha in tal senso statuito, nella sua sentenza N.S. e a.[34], che «un'applicazione del regolamento [(CE)] n. 343/2003 [[35]] sulla base di una presunzione assoluta che i diritti fondamentali del richiedente asilo saranno rispettati nello Stato membro di regola competente a conoscere della sua domanda è incompatibile con l'obbligo degli Stati membri di interpretare e di applicare il regolamento n. 343/2003 in conformità ai diritti fondamentali» [36].

102. A tal riguardo, la Corte ha ammesso, laddove si trattava dello status degli Stati membri quali paesi di origine reciprocamente sicuri a tutti i fini giuridici e pratici connessi a questioni inerenti l'asilo, che si deve presumere che il trattamento riservato ai richiedenti asilo in ciascuno Stato membro sia conforme a quanto prescritto dalla Carta, alla Convenzione relativa allo status dei rifugiati, firmata a Ginevra il 28 luglio 1951[37], nonché alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950[38]. Tuttavia, la Corte ha dichiarato che «non si può escludere che tale sistema incontri, in pratica, gravi difficoltà di funzionamento in un determinato Stato membro, cosicché sussiste un rischio serio che un richiedente asilo sia, in caso di trasferimento verso detto Stato membro, trattato in modo incompatibile con i suoi diritti fondamentali» [39].

103. Di conseguenza, la Corte ha statuito che «gli Stati membri, compresi gli organi giurisdizionali nazionali, sono tenuti a non trasferire un richiedente asilo verso lo "Stato membro competente" ai sensi del regolamento n. 343/2003 quando non possono ignorare che le carenze sistemiche nella procedura di asilo e nelle condizioni di accoglienza dei richiedenti asilo in tale Stato membro costituiscono motivi seri e comprovati di credere che il richiedente corra un rischio reale di subire trattamenti inumani o degradanti ai sensi dell'art[icolo] 4 della Carta» [40].

104. Mi sembra che l'apporto della sentenza N.S. e a.[41] possa essere esteso ad una situazione come quella di cui al procedimento principale. In tal senso, un'interpretazione del diritto derivato dell'Unione che poggi su una presunzione assoluta che i diritti fondamentali saranno rispettati – indifferentemente, da parte di uno Stato membro, dalla Commissione o da un paese terzo – deve essere considerata incompatibile con l'obbligo degli Stati membri di interpretare e applicare il diritto derivato dell'Unione in maniera conforme ai diritti fondamentali. L'articolo 25, paragrafo 6, della direttiva 95/46 non sancisce pertanto una siffatta presunzione assoluta di rispetto dei diritti fondamentali per quanto attiene alla valutazione, da parte della Commissione, dell'adeguatezza del livello di protezione offerto da un paese terzo. Al contrario, la presunzione, sottesa a tale disposizione, secondo la quale il trasferimento di dati verso un paese terzo rispetta i diritti fondamentali, deve essere

33 — V., segnatamente, sentenza N.S. e a. (C-411/10 e C-493/10, EU:C:2011:865, punto 77, nonché la giurisprudenza ivi citata).

34 — C-411/10 e C-493/10, EU:C:2011:865.

35 — Regolamento del Consiglio del 18 febbraio 2003, che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda d'asilo presentata in uno degli Stati membri da un cittadino di un paese terzo (GU L 50, pag. 1).

36 — Punto 99 di tale sentenza.

37 — *Recueil des traités des Nations unies*, vol. 189, pag. 150, n. 2545 (1954).

38 — V. sentenza N.S. e a. (C-411/10 e C-493/10, EU:C:2011:865, punto 80).

39 — Ibidem (punto 81).

40 — Ibidem (punto 94).

41 — C-411/10 e C-493/10, EU:C:2011:865.

considerata relativa [42]. Di conseguenza, detta disposizione non dovrebbe essere interpretata nel senso che essa rimette in discussione le garanzie figuranti segnatamente all'articolo 28, paragrafo 3, della direttiva 95/46 e all'articolo 8, paragrafo 3, della Carta, intesi alla protezione e al rispetto del diritto alla protezione dei dati personali.

105. Deduco pertanto dalla detta sentenza che, in caso di carenze sistemiche constatate nel paese terzo verso il quale vengono trasferiti dati personali, gli Stati membri devono poter adottare le misure necessarie alla salvaguardia dei diritti fondamentali protetti dagli articoli 7 e 8 della Carta.

106. Inoltre, come rilevato dal governo italiano nelle sue osservazioni, l'adozione, da parte della Commissione, di una decisione di adeguatezza non può produrre l'effetto di ridurre la protezione dei cittadini dell'Unione con riguardo al trattamento dei loro dati allorché questi ultimi vengono trasferiti verso un paese terzo, rispetto al livello di protezione di cui tali persone beneficerebbero se i loro dati fossero oggetto di un trattamento all'interno dell'Unione. Le autorità nazionali di controllo devono pertanto essere in grado di intervenire e di esercitare i loro poteri nei confronti di trasferimenti di dati verso paesi terzi oggetto di una decisione sull'adeguatezza. In caso contrario, i cittadini dell'Unione godrebbero di una protezione inferiore che nel caso di trattamento dei loro dati all'interno dell'Unione.

107. Pertanto, l'adozione, da parte della Commissione, di una decisione in applicazione dell'articolo 25, paragrafo 6, della direttiva 95/46 ha come unico effetto la rimozione del divieto generale di esportazione dei dati personali verso paesi terzi che garantiscono un livello di protezione comparabile a quello offerto da tale direttiva. In altre parole, non si tratta di creare un regime speciale derogatorio e meno protettivo per i cittadini dell'Unione rispetto al regime generale previsto da detta direttiva per i trattamenti di dati che vengono effettuati all'interno dell'Unione.

108. È vero che la Corte ha indicato, al punto 63 della sentenza Lindqvist [43], che «[i]l capo IV della direttiva 95/46, nel quale figura l'art[icolo] 25, predispone un regime speciale». Tuttavia, ciò non significa, a mio avviso, che un siffatto regime debba essere meno protettivo. Al contrario, al fine di conseguire l'obiettivo di protezione dei dati fissato all'articolo 1, paragrafo 1, della direttiva 95/46, l'articolo 25 della medesima impone vari obblighi agli Stati membri e alla Commissione [44], e tale articolo 25 sancisce il principio secondo il quale, quando un paese terzo non offre un livello di protezione adeguato, il trasferimento di dati personali verso tale paese dev'essere vietato [45].

109. Per quanto attiene più specificamente al regime dell'approdo sicuro, la Commissione prevede l'intervento delle autorità nazionali di controllo e la sospensione, da parte delle medesime, dei flussi di dati, solo nell'ambito tracciato dall'articolo 3, paragrafo 1, lettera b), della decisione 2000/520.

110. Secondo il considerando 8 di tale decisione, «[n]ell'interesse della trasparenza, e per salvaguardare la facoltà delle competenti autorità degli Stati membri di assicurare la protezione degli individui riguardo al trattamento dei dati personali, è necessario che la presente decisione specifichi le circostanze eccezionali in cui può essere giustificata la sospensione di specifici flussi di dati anche in caso di constatazione di adeguata protezione».

111. Nell'ambito della presente causa, è più in particolare l'applicazione dell'articolo 3, paragrafo 1, lettera b), di detta decisione che è stata discussa. In tal senso, in forza di tale disposizione, le autorità nazionali di controllo possono decidere di sospendere flussi di dati nei casi in cui «sia molto probabile che i principi vengano violati; vi siano ragionevoli motivi per ritenere che l'organismo di esecuzione

42 — Punto 104 di tale sentenza.

43 — C-101/01, EU:C:2003:596.

44 — Punto 65.

45 — Punto 64.

competente non stia adottando o non adotterà misure adeguate e tempestive per risolvere un caso concreto, la continuazione del trasferimento dei dati potrebbe determinare un rischio imminente di gravi danni per gli interessati e le autorità competenti dello Stato membro abbiano fatto il possibile, date le circostanze, per informare l'organizzazione dandole l'opportunità di replicare».

112. Detta disposizione pone varie condizioni che hanno formato oggetto di diverse interpretazioni ad opera delle parti nel corso del presente procedimento [46]. Senza entrare nel dettaglio di tali interpretazioni, ne emerge che tali condizioni regolano in maniera restrittiva il potere delle autorità nazionali di controllo di sospendere flussi di dati.

113. Orbene, contrariamente a quanto fatto valere dalla Commissione, l'articolo 3, paragrafo 1, lettera b), della decisione 2000/520 deve essere interpretato in conformità all'obiettivo di protezione dei dati personali perseguito dalla direttiva 95/46, nonché alla luce dell'articolo 8 della Carta. La necessità di un'interpretazione conforme ai diritti fondamentali milita a favore di un'interpretazione estensiva di tale disposizione.

114. Ne consegue che le condizioni previste all'articolo 3, paragrafo 1, lettera b), della decisione 2000/520 non possono, a mio avviso, impedire ad un'autorità nazionale di controllo di esercitare in piena indipendenza i poteri di cui è investita in forza dell'articolo 28, paragrafo 3, della direttiva 95/46.

115. Come indicato in sostanza dai governi belga e austriaco in udienza, l'uscita di emergenza costituita dall'articolo 3, paragrafo 1, lettera b), della decisione 2000/520 è talmente stretta che è difficile sfruttarla. Essa impone criteri cumulativi ed è eccessivamente esigente. Orbene, alla luce dell'articolo 8, paragrafo 3, della Carta, è impossibile che il potere discrezionale delle autorità nazionali di controllo concernente le prerogative che risultano dall'articolo 28, paragrafo 3, della direttiva 95/46 sia a tal punto limitato che esse non possano più essere esercitate.

116. A tal riguardo, il Parlamento ha giustamente osservato che è il legislatore dell'Unione ad avere deciso quali fossero i poteri che dovevano spettare alle autorità nazionali di controllo. Orbene, il potere di esecuzione accordato dal legislatore dell'Unione alla Commissione all'articolo 25, paragrafo 6, della direttiva 95/46 non pregiudica i poteri conferiti da questo stesso legislatore alle autorità nazionali di controllo all'articolo 28, paragrafo 3, di tale direttiva. In altre parole, la Commissione non è competente a restringere i poteri delle autorità nazionali di controllo.

117. Di conseguenza, al fine di assicurare una protezione adeguata dei diritti fondamentali delle persone fisiche con riguardo al trattamento dei dati personali, le autorità nazionali di controllo devono essere autorizzate, qualora vengano dedotte violazioni di tali diritti, a condurre indagini. Se, al termine di tali indagini, dette autorità ritengono che esistano, in un paese terzo coperto da una decisione di adeguatezza, indizi seri di una violazione del diritto dei cittadini dell'Unione alla protezione dei loro dati personali, esse devono poter sospendere il trasferimento di dati verso il destinatario stabilito in tale paese terzo.

118. In altre parole, le autorità nazionali di controllo devono poter condurre le loro indagini e, se del caso, sospendere un trasferimento di dati, a prescindere dalle condizioni restrittive fissate all'articolo 3, paragrafo 1, lettera b), della decisione 2000/520.

46 — Secondo il sig. Schrems, la prima condizione, secondo la quale «sia molto probabile che i principi vengano violati», non sarebbe soddisfatta. Orbene, non viene dedotto che Facebook USA, quale organismo autocertificato al quale vengono trasferiti dati, avrebbe essa stessa violato i principi dell'approdo sicuro a causa dell'accesso massiccio e indifferenziato da parte delle autorità americane ai dati da essa detenuti. Infatti, i principi dell'approdo sicuro sono espressamente limitati dal diritto americano, che l'allegato I, quarto comma, della decisione 2000/520 definisce rimandando alle disposizioni legislative o regolamentari e alle decisioni giurisdizionali.

119. Inoltre, in forza del loro potere di promuovere azioni giudiziarie in caso di violazioni delle disposizioni nazionali di attuazione della direttiva 95/46 ovvero del loro potere di adire per dette violazioni le autorità giudiziarie, ai sensi dell'articolo 28, paragrafo 3, di tale direttiva, le autorità nazionali di controllo, qualora vengano a conoscenza di fatti che dimostrano che un paese terzo non assicura un livello di protezione adeguato, dovrebbero poter adire un giudice nazionale il quale potrà esso stesso decidere, se del caso, di effettuare un rinvio pregiudiziale alla Corte ai fini della valutazione della validità di una decisione sull'adeguatezza della Commissione.

120. Risulta dall'insieme di tali elementi che l'articolo 28 della direttiva 95/46, in combinato disposto con gli articoli 7 e 8 della Carta, deve essere interpretato nel senso che l'esistenza di una decisione adottata dalla Commissione sulla base dell'articolo 25, paragrafo 6, di tale direttiva non produce l'effetto di impedire ad un'autorità nazionale di controllo di istruire una denuncia con la quale si lamenta che un paese terzo non assicura un livello di protezione adeguato ai dati personali trasferiti e, se del caso, di sospendere il trasferimento di tali dati.

121. Anche se la Corte d'appello sottolinea, nella sua decisione di rinvio, che il sig. Schrems non ha formalmente contestato, nel ricorso principale, né la validità della direttiva 95/46 né quella della decisione 2000/520, si evince da tale decisione di rinvio che la censura principale mossa dal sig. Schrems è intesa a rimettere in discussione l'affermazione secondo la quale gli Stati Uniti assicurano, nell'ambito del regime dell'approdo sicuro, un livello di protezione adeguato ai dati personali trasferiti.

122. Emerge parimenti dalle osservazioni del commissario che la denuncia del sig. Schrems è volta a mettere direttamente in discussione la decisione 2000/520. Depositando tale denuncia, quest'ultimo ha inteso attaccare i termini e il funzionamento del regime dell'approdo sicuro in quanto tale, sulla base del rilievo che la sorveglianza di massa dei dati personali trasferiti negli Stati Uniti dimostrerebbe l'inesistenza di una protezione effettiva di tali dati nel diritto e nella prassi in vigore in tale paese terzo.

123. Inoltre, il giudice del rinvio osserva esso stesso che la garanzia offerta dall'articolo 7 della Carta e dai valori fondamentali comuni alle tradizioni costituzionali degli Stati membri sarebbe compromessa qualora si ammettesse che le comunicazioni elettroniche possano essere oggetto di accesso da parte delle autorità statali su base casuale e generalizzata, senza che sia richiesta una motivazione oggettiva in base a considerazioni di sicurezza nazionale o prevenzione di crimini specificamente riguardanti i singoli soggetti interessati, e senza la previsione di garanzie adeguate e verificabili[47]. Il giudice del rinvio esprime pertanto indirettamente dei dubbi sulla validità della decisione 2000/520.

124. Per valutare se, nell'ambito del regime dell'approdo sicuro, gli Stati Uniti garantiscano un livello di protezione adeguato ai dati personali trasferiti è quindi necessario esaminare la validità di tale decisione.

125. A tal riguardo, occorre rilevare che, nell'ambito dello strumento di cooperazione fra la Corte e i giudici nazionali istituito dall'articolo 267 TFUE, la Corte, pur investita in via pregiudiziale esclusivamente di una questione di interpretazione del diritto dell'Unione, può, in talune circostanze particolari, essere indotta ad esaminare la validità di disposizioni di diritto derivato.

126. Pertanto, la Corte ha dichiarato d'ufficio, a più riprese, l'invalidità di un atto del quale le era stata chiesta soltanto l'interpretazione[48]. Essa ha parimenti statuito che «qualora risulti che le questioni deferite da un giudice nazionale abbiano in realtà ad oggetto la validità di atti [dell'Unione], la Corte è tenuta a pronunciarsi, senza imporre al giudice proponente un formalismo che servirebbe unicamente

47 — Punto 24 della decisione di rinvio.

48 — V., segnatamente, sentenze Strehl (62/76, EU:C:1977:18, punti da 10 a 17); Roquette Frères (145/79, EU:C:1980:234, punto 6), nonché Schutzverband der Spirituosen-Industrie (C-457/05, EU:C:2007:576, punti da 32 a 39).

a ritardare il procedimento a norma dell'articolo [267 TFUE] e che sarebbe incompatibile con lo spirito dello stesso» [49]. La Corte ha inoltre già dichiarato che i dubbi sollevati da un giudice del rinvio in merito alla compatibilità di un atto di diritto derivato con le norme volte alla tutela dei diritti fondamentali concernono la legittimità di tale atto sotto il profilo del diritto dell'Unione [50].

127. Ricordo parimenti che risulta dalla giurisprudenza della Corte che gli atti delle istituzioni, degli organi e degli organismi dell'Unione godono di una presunzione di validità, il che implica che essi producano effetti giuridici finché non siano stati revocati, annullati nel contesto di un ricorso per annullamento oppure dichiarati invalidi a seguito di un rinvio pregiudiziale o di un'eccezione di illegittimità. La Corte è competente in via esclusiva a dichiarare l'invalidità di un atto dell'Unione, competenza che ha lo scopo di garantire la certezza del diritto assicurando l'applicazione uniforme del diritto dell'Unione. In mancanza di una declaratoria di invalidità, di modifica o di abrogazione da parte della Commissione, la decisione rimane obbligatoria in tutti i suoi elementi e direttamente applicabile in ogni Stato membro [51].

128. Al fine di fornire una risposta completa al giudice del rinvio e di fugare i dubbi espressi nel corso del presente procedimento in ordine alla validità della decisione 2000/520, ritengo che la Corte debba procedere ad una valutazione di validità di tale decisione.

129. Ciò premesso, occorre parimenti precisare che l'esame della questione se la decisione 2000/520 sia valida o meno deve essere circoscritto alle censure che sono state oggetto di discussione nell'ambito del presente procedimento. Infatti, in tale contesto non sono stati dibattuti tutti gli aspetti relativi al funzionamento del regime dell'approdo sicuro; per questo motivo, non mi sembra possibile dedicarmi in questa sede ad un esame esaustivo delle carenze di tale regime.

130. Per contro, la questione se l'accesso generalizzato e non mirato dei servizi americani di intelligence ai dati trasferiti sia idoneo ad incidere sulla legittimità della decisione 2000/520 è stata oggetto di discussione dinanzi alla Corte nell'ambito del presente procedimento. La validità di tale decisione può pertanto essere valutata sotto questo profilo.

B – *Sulla validità della decisione 2000/520*

1. Sugli elementi da prendere in considerazione per valutare la validità della decisione 2000/520

131. Occorre richiamare la giurisprudenza secondo la quale, «nell'ambito del ricorso per annullamento, la legittimità di un atto deve essere valutata in base alla situazione di fatto e di diritto esistente al momento in cui l'atto è stato adottato, e la valutazione della Commissione può essere criticata solo se essa risulta manifestamente erronea alla luce degli elementi di cui la stessa disponeva al momento dell'adozione dell'atto in questione» [52].

49 — Sentenza Schwarze (16/65, EU:C:1965:117, pag. 1094).

50 — V. sentenza Hauer (44/79, EU:C:1979:290, punto 16).

51 — V., segnatamente, sentenza CIVAD (C-533/10, EU:C:2012:347, punti da 39 a 41 e la giurisprudenza ivi citata).

52 — V., segnatamente, sentenza BVGD/Commissione (T-104/07 e T-339/08, EU:T:2013:366, punto 291), che richiama la sentenza IECC/Commissione (C-449/98 P, EU:C:2001:275, punto 87).

132. Nella sentenza Gaz de France – Berliner Investissement [53], la Corte ha richiamato il principio secondo il quale «la valutazione della validità di un atto, che la Corte è tenuta ad effettuare nell'ambito di un rinvio pregiudiziale, deve normalmente essere fondata sulla situazione di fatto e di diritto esistente al momento in cui l'atto è stato adottato» [54]. Sembra tuttavia che essa abbia ammesso che «la validità di un atto possa, in taluni casi, essere valutata in relazione ad elementi nuovi intervenuti dopo la sua adozione» [55].

133. Tale apertura così abbozzata dalla Corte mi sembra particolarmente rilevante nell'ambito della presente causa.

134. Infatti, le decisioni adottate dalla Commissione sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46 presentano caratteristiche particolari. Esse sono destinate a valutare se il livello di protezione dei dati personali offerto da un paese terzo presenti o meno un carattere adeguato. Si tratta, in tal caso, di una valutazione destinata a mutare in funzione del contesto di fatto e di diritto vigente nel paese terzo.

135. Alla luce del fatto che la decisione di adeguatezza costituisce un tipo particolare di decisione, la regola secondo la quale la valutazione di validità della medesima potrebbe essere effettuata solo in funzione degli elementi esistenti al momento della sua adozione deve essere, nella specie, attenuata. Una siffatta regola comporterebbe altrimenti che, diversi anni dopo l'adozione di una decisione di adeguatezza, la valutazione sulla validità alla quale la Corte deve procedere non possa prendere in considerazione eventi che si sono verificati successivamente, e ciò sebbene un rinvio pregiudiziale per esame di validità non sia limitato nel tempo e il suo avvio possa appunto essere la conseguenza di fatti posteriori che rivelano le carenze dell'atto in questione.

136. Nella specie, il mantenimento in vigore della decisione 2000/520 da circa quindici anni dimostra che la Commissione ha implicitamente confermato la sua valutazione effettuata nel 2000. Quando, nell'ambito di un rinvio pregiudiziale, la Corte è indotta a vagliare la validità di una valutazione mantenuta nel tempo dalla Commissione, è dunque non solo possibile, ma anche appropriato, che essa possa rapportare tale valutazione alle circostanze nuove che sono intervenute dall'adozione della decisione di adeguatezza.

137. Tenuto conto della natura particolare della decisione di adeguatezza, quest'ultima deve essere oggetto di un riesame regolare da parte della Commissione. Se, a seguito di nuovi eventi verificatisi nel frattempo, la Commissione non modifica la propria decisione, essa conferma implicitamente, ma inevitabilmente, la valutazione effettuata all'inizio. Essa ribadisce pertanto la sua constatazione secondo la quale il paese terzo di cui trattasi assicura un livello di protezione adeguato ai dati personali trasferiti. Spetta alla Corte esaminare se tale constatazione continui ad essere valida malgrado le circostanze intervenute successivamente.

138. Al fine di assicurare un controllo giurisdizionale effettivo su questo tipo di decisione, la valutazione della sua validità deve pertanto essere effettuata, a mio avviso, tenendo conto del contesto di fatto e di diritto attuale.

53 — C-247/08, EU:C:2009:600.

54 — Punto 49 e la giurisprudenza ivi citata.

55 — Punto 50 e la giurisprudenza ivi citata. V., in tal senso, Lenaerts, K., Maselis, I., e Gutman, K., *EU Procedural Law*, Oxford University Press, 2014, che enunciano che «in certain cases, the validity of the particular Union measure can be assessed by reference to new factors arising after that measure was adopted, depending on the determination of the Court» (punto 10.16, pag. 471).

2. Sulla nozione di livello di protezione adeguato

139. L'articolo 25 della direttiva 95/46 poggia interamente sul principio secondo il quale il trasferimento di dati personali verso un paese terzo può aver luogo soltanto se tale paese terzo garantisce un livello di protezione adeguato a tali dati. L'obiettivo di detto articolo consiste dunque nell'assicurare la continuità della protezione conferita da tale direttiva in caso di trasferimento di dati personali verso un paese terzo. Occorre rammentare, a tal riguardo, che detta direttiva offre un livello di protezione elevato dei cittadini dell'Unione con riguardo al trattamento dei loro dati personali.

140. Tenuto conto del ruolo importante svolto dalla protezione dei dati personali alla luce del diritto fondamentale al rispetto della vita privata, un siffatto livello elevato di protezione deve pertanto essere garantito, anche in caso di trasferimento di dati personali verso un paese terzo.

141. È per questo motivo che ritengo che la Commissione possa constatare, sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, che un paese terzo assicura un livello di protezione adeguato solo qualora, al termine di una valutazione di insieme del diritto e della prassi nel paese terzo in questione, essa sia in grado di dimostrare che tale paese offre un livello di protezione sostanzialmente equivalente a quello offerto da tale direttiva, anche se le modalità di tale protezione possono essere diverse da quelle generalmente vigenti all'interno dell'Unione.

142. Benché il termine inglese «adequate» possa essere inteso, dal punto di vista linguistico, nel senso che esso designa un livello di protezione appena soddisfacente o sufficiente, ed avere pertanto un campo semantico diverso dal termine francese «adéquat», si deve osservare che il solo criterio che deve guidare l'interpretazione di tale termine è l'obiettivo consistente nel conseguimento di un livello elevato di protezione dei diritti fondamentali, come richiesto dalla direttiva 95/46.

143. L'esame del livello di protezione offerto da un paese terzo deve prendere in considerazione due elementi fondamentali, ossia il contenuto delle norme applicabili e i mezzi per assicurare il rispetto di tali norme[56].

144. A mio avviso, per conseguire un livello di protezione sostanzialmente equivalente a quello in vigore all'interno dell'Unione, il regime dell'approdo sicuro, il quale poggia in gran parte sull'autocertificazione e sull'autovalutazione da parte delle imprese che partecipano volontariamente a tale regime, dovrebbe essere accompagnato da garanzie adeguate e da un meccanismo di controllo sufficiente. Pertanto, i trasferimenti di dati personali verso paesi terzi non dovrebbero beneficiare di una protezione inferiore rispetto ai trattamenti effettuati all'interno dell'Unione.

145. A tal riguardo, rilevo, anzitutto, che all'interno dell'Unione prevale la concezione secondo la quale un dispositivo di controllo esterno sotto forma di un'autorità indipendente costituisce un elemento necessario di ogni sistema inteso ad assicurare il rispetto delle norme relative alla protezione dei dati personali.

146. Inoltre, al fine di assicurare l'effetto utile dell'articolo 25, paragrafi da 1 a 3, della direttiva 95/46, occorre tenere conto del fatto che l'adeguatezza del livello di protezione offerto da un paese terzo costituisce una situazione evolutiva che può mutare nel tempo in funzione di una serie di fattori. Gli Stati membri e la Commissione devono pertanto essere costantemente attenti ad ogni mutamento di circostanze idoneo a rendere necessaria una rivalutazione dell'adeguatezza del livello di protezione

56 — V. pag. 5 del documento di lavoro WP 12 della Commissione, intitolato «Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati», adottato dal Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali il 24 luglio 1998.

offerto da un paese terzo. Una valutazione dell'adeguatezza di tale livello di protezione non può affatto essere fissata ad un momento determinato e, poi, essere mantenuta indefinitamente, a prescindere da qualsiasi mutamento di circostanze che mostri che, in realtà, il livello di protezione offerto non è più adeguato.

147. L'obbligo del paese terzo di assicurare un livello di protezione adeguato costituisce pertanto un obbligo di durata. Pur se la valutazione è effettuata in un momento determinato, il mantenimento della decisione di adeguatezza presuppone che nessuna circostanza intervenuta successivamente sia in grado di rimettere in discussione la valutazione iniziale effettuata dalla Commissione.

148. Infatti, non si deve perdere di vista il fatto che l'obiettivo dell'articolo 25 della direttiva 95/46 consiste nell'evitare che i dati personali vengano trasferiti verso un paese terzo che non assicura un livello di protezione adeguato, in violazione del diritto fondamentale alla protezione dei dati personali garantito dall'articolo 8 della Carta.

149. Occorre sottolineare che il potere conferito dal legislatore dell'Unione alla Commissione all'articolo 25, paragrafo 6, della direttiva 95/46, di constatare che un paese terzo assicura un livello di protezione adeguato, è espressamente subordinato alla necessità che tale paese terzo assicuri un tale livello ai sensi del paragrafo 2 di tale articolo. Qualora circostanze nuove siano idonee a rimettere in discussione la valutazione iniziale della Commissione, quest'ultima dovrebbe adeguare di conseguenza la propria decisione.

3. Valutazione

150. Ricordo che, ai sensi dell'articolo 25, paragrafo 6, della direttiva 95/46, «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». Letto in combinato con l'articolo 25, paragrafo 2, di tale direttiva, l'articolo 25, paragrafo 6, della medesima significa che, per constatare che un paese terzo assicura un livello di protezione adeguato, la Commissione deve procedere ad una valutazione di insieme delle norme di diritto in vigore in tale paese terzo, nonché della loro applicazione.

151. Si è visto che il mantenimento, da parte della Commissione, della sua decisione 2000/520, malgrado il sopravvenire di elementi di fatto e di diritto nuovi, deve essere considerato espressione della volontà della medesima di confermare la sua valutazione iniziale.

152. Non spetta alla Corte, nell'ambito di un rinvio pregiudiziale, valutare i fatti all'origine della controversia che ha portato il giudice nazionale ad effettuare tale rinvio [57].

153. Mi baserò pertanto sui fatti indicati dal giudice del rinvio nella sua domanda di pronuncia pregiudiziale, fatti che, del resto, sono ampiamente considerati dimostrati dalla Commissione stessa [58].

154. Gli elementi che sono stati dedotti dinanzi alla Corte per contestare la valutazione della Commissione secondo la quale il regime dell'approdo sicuro assicura un livello di protezione adeguato ai dati personali trasferiti dall'Unione verso gli Stati Uniti possono essere così descritti.

57 — V., segnatamente, sentenza Fallimento Traghetti del Mediterraneo (C-140/09, EU:C:2010:335, punto 22 e la giurisprudenza ivi citata).

58 — V. comunicazione della Commissione menzionata alla nota a piè di pagina 2 e comunicazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento del regime «Approdo sicuro» dal punto di vista dei cittadini dell'UE e delle società ivi stabilite [COM(2013) 847 final].

155. Nella sua domanda di pronuncia pregiudiziale, il giudice del rinvio parte dalle due constatazioni di fatto seguenti. Da un lato, i dati personali trasferiti da imprese quali Facebook Ireland alla loro società madre stabilita negli Stati Uniti possono, successivamente, essere consultati dalla NSA nonché da altre agenzie di sicurezza americane nel corso di operazioni di sorveglianza e di intercettazioni massicce e indiscriminate. Infatti, a seguito delle rivelazioni del sig. Snowden, gli elementi di prova disponibili non ammettono attualmente altre conclusioni plausibili [59]. Dall'altro, i cittadini dell'Unione non disporrebbero di un diritto effettivo di essere sentiti sulla questione della sorveglianza e dell'intercettazione dei loro dati da parte della NSA e di altre agenzie di sicurezza americane [60].

156. Le constatazioni di fatto effettuate in tali termini dalla Corte d'appello sono suffragate dalle constatazioni effettuate dalla Commissione stessa.

157. Così, nella sua summenzionata comunicazione sul funzionamento del regime dell'approdo sicuro dal punto di vista dei cittadini dell'Unione e delle società ivi stabilite, la Commissione ha preso le mosse dalla constatazione che, nel corso del 2013, informazioni relative all'ampiezza e alla portata dei programmi di controllo americani hanno suscitato preoccupazioni sulla continuità della protezione dei dati personali lecitamente trasferiti negli USA nell'ambito del regime dell'approdo sicuro. Essa ha rilevato che tutte le imprese partecipanti al programma PRISM, e che consentono alle autorità americane di avere accesso a dati conservati e trattati negli Stati Uniti, risultano certificate nel quadro dell'approdo sicuro. A suo avviso, tale sistema è diventato così una delle piattaforme di accesso delle autorità americane di intelligence alla raccolta di dati personali inizialmente trattati nell'Unione [61].

158. Risulta da tali elementi che il diritto e la prassi degli Stati Uniti consentono di raccogliere su larga scala i dati personali di cittadini dell'Unione che vengono trasferiti nell'ambito del regime dell'approdo sicuro, senza che questi ultimi beneficino di una protezione giurisdizionale effettiva.

159. Tali constatazioni di fatto dimostrano, a mio avviso, che la decisione 2000/520 non contiene garanzie sufficienti. A causa di tale carenza di garanzie, detta decisione è stata attuata in un modo che non soddisfa i requisiti richiesti dalla Carta, nonché dalla direttiva 95/46.

160. Orbene, una decisione adottata dalla Commissione sul fondamento dell'articolo 25, paragrafo 6, della direttiva 95/46 è intesa alla constatazione che un paese terzo «garantisce» un livello di protezione adeguato. Il termine «garantisce», coniugato al presente, implica che, per potere essere mantenuta, una siffatta decisione deve riguardare un paese terzo che continua, successivamente all'adozione di detta decisione, a garantire un livello di protezione adeguato.

161. In realtà, le menzionate rivelazioni relative ai comportamenti della NSA, la quale utilizzerebbe dati trasferiti nell'ambito del regime dell'approdo sicuro, hanno evidenziato le debolezze della base giuridica costituita dalla decisione 2000/520.

162. Le carenze messe in evidenza nel corso del presente procedimento figurano più in particolare all'allegato I, quarto comma, di tale decisione.

163. Ricordo che, ai sensi di tale disposizione, «[l]'adesione [ai] principi [dell'approdo sicuro] può essere limitata: a) se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia; b) da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione».

59 — Punto 7, lettera c), della decisione di rinvio.

60 — Punto 7, lettera b), della decisione di rinvio.

61 — Pag. 19 della sua comunicazione.

164. Il problema deriva sostanzialmente dall'impiego che le autorità americane fanno delle deroghe previste da detta disposizione. A causa della loro formulazione eccessivamente generica, l'attuazione di tali deroghe da parte di dette autorità non è limitata a quanto strettamente necessario.

165. A tale formulazione eccessivamente generica si somma la circostanza che i cittadini dell'Unione non dispongono di mezzi di ricorso adeguati avverso il trattamento dei loro dati personali per fini diversi da quelli per cui essi sono stati inizialmente raccolti e poi trasferiti verso gli Stati Uniti.

166. Le deroghe previste dalla decisione 2000/520 all'applicazione dei principi dell'approdo sicuro, segnatamente per esigenze legate alla sicurezza nazionale, avrebbero dovuto essere corredate dall'attuazione di un meccanismo di controllo indipendente idoneo ad evitare le violazioni al diritto alla vita privata accertate.

167. In tal senso, le rivelazioni sulla prassi dei servizi di intelligence americani quanto alla sorveglianza generalizzata dei dati trasferiti nell'ambito del regime dell'approdo sicuro hanno messo in luce talune carenze proprie della decisione 2000/520.

168. Le asserzioni nell'ambito della presente causa non integrano una violazione, da parte di Facebook, dei principi dell'approdo sicuro. Se un'impresa certificata, come Facebook USA, concede alle autorità americane l'accesso ai dati che le sono stati trasferiti da uno Stato membro, può ritenersi che essa lo faccia per conformarsi alla legislazione statunitense. Alla luce del fatto che una situazione del genere è espressamente ammessa dalla decisione 2000/520, a causa della formulazione ampia delle deroghe che essa contiene, è in realtà la questione della compatibilità di tali deroghe con il diritto primario dell'Unione a porsi nell'ambito della presente causa.

169. Occorre sottolineare, a tal riguardo, che si evince da una giurisprudenza costante della Corte che il rispetto dei diritti dell'uomo rappresenta una condizione di legittimità degli atti dell'Unione e che nell'Unione non possono essere consentite misure incompatibili con il rispetto di questi ultimi [62].

170. Risulta peraltro dalla giurisprudenza della Corte che la comunicazione dei dati personali raccolti a terzi, pubblici o privati, costituisce un'ingerenza nel diritto al rispetto della vita privata «quale che sia l'ulteriore utilizzazione delle informazioni così comunicate» [63]. Ancora, nella sentenza Digital Rights Ireland e a. [64], la Corte ha confermato che il fatto di autorizzare le autorità nazionali competenti ad avere accesso a siffatti dati costituisce un pregiudizio supplementare a tale diritto fondamentale [65]. Inoltre, qualsiasi forma di trattamento dei dati personali è prevista all'articolo 8 della Carta e costituisce un'ingerenza nel diritto alla protezione di tali dati [66]. L'accesso di cui dispongono i servizi di intelligence americani ai dati trasferiti integra pertanto parimenti un'ingerenza nel diritto fondamentale alla protezione dei dati personali garantito dall'articolo 8 della Carta, in quanto un siffatto accesso costituisce un trattamento di tali dati.

171. Come constatato dalla Corte in tale sentenza, l'ingerenza così individuata è di vasta portata e va considerata particolarmente grave, alla luce del numero significativo di utenti interessati e delle quantità di dati trasferiti. Tali elementi, sommati alla segretezza dell'accesso da parte delle autorità americane ai dati personali trasferiti verso le imprese stabilite negli Stati Uniti, rendono l'ingerenza estremamente seria.

62 — V., segnatamente, sentenza Kadi e Al Barakaat International Foundation/Consiglio e Commissione (C-402/05 P e C-415/05 P, EU:C:2008:461, punto 284, nonché la giurisprudenza ivi citata).

63 — Sentenza Österreichischer Rundfunk e a. (C-465/00, C-138/01 e C-139/01, EU:C:2003:294, punto 74).

64 — C-293/12 e C-594/12, EU:C:2014:238.

65 — Punto 35.

66 — Punto 36.

172. A ciò si aggiunge la circostanza che i cittadini dell'Unione utenti di Facebook non sono informati del fatto che i loro dati personali saranno accessibili in maniera generale per le agenzie di sicurezza americane.

173. Occorre parimenti porre l'accento sul fatto che il giudice del rinvio ha constatato che, negli Stati Uniti, i cittadini dell'Unione non hanno alcun diritto effettivo ad essere sentiti sulla questione della sorveglianza e dell'intercettazione dei loro dati. La FISC esercita una supervisione, ma il procedimento dinanzi alla medesima è segreto e si svolge inaudita altera parte [67]. Ritengo che si sia in presenza, in tal caso, di un'ingerenza nel diritto dei cittadini dell'Unione ad un ricorso effettivo, tutelato dall'articolo 47 della Carta.

174. Sussiste pertanto un'ingerenza nei diritti fondamentali tutelati dagli articoli 7, 8 e 47 della Carta resa possibile dalle deroghe ai principi dell'approdo sicuro di cui all'allegato I, quarto comma, della decisione 2000/520.

175. Occorre adesso verificare se tale ingerenza sia giustificata o meno.

176. Conformemente all'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti da quest'ultima devono essere previste dalla legge e devono rispettare il contenuto essenziale di tali diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni a detti diritti e libertà solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

177. Alla luce delle condizioni così fissate per poter ammettere limitazioni all'esercizio dei diritti e delle libertà protetti dalla Carta, dubito fortemente che si possa ritenere che le limitazioni oggetto della presente causa rispettino il contenuto essenziale degli articoli 7 e 8 della Carta. Infatti, l'accesso dei servizi di intelligence americani ai dati trasferiti sembra estendersi al contenuto delle comunicazioni elettroniche; ciò arrecherebbe pregiudizio al contenuto essenziale del diritto fondamentale al rispetto della vita privata e degli altri diritti sanciti all'articolo 7 della Carta. Inoltre, nella misura in cui la formulazione ampia delle limitazioni previste all'allegato I, quarto comma, della decisione 2000/520 consente potenzialmente di disapplicare l'insieme dei principi dell'approdo sicuro, si potrebbe ritenere che tali limitazioni pregiudichino il contenuto essenziale del diritto fondamentale alla protezione dei dati personali [68].

178. Quanto alla questione se l'ingerenza constatata risponda ad un obiettivo di interesse generale, ricordo, anzitutto, che, ai sensi dell'allegato I, quarto comma, lettera b), della decisione 2000/520, l'adesione ai principi dell'approdo sicuro può essere limitata «da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione».

179. È giocoforza constatare che i «legittimi interessi» menzionati in tale disposizione non vengono precisati. Ne risulta un'incertezza quanto all'ambito di applicazione, potenzialmente estremamente ampio, di tale deroga all'applicazione dei principi dell'approdo sicuro da parte delle imprese aderenti.

67 — Punto 7, lettera b), della decisione di rinvio.

68 — V., a tal riguardo, sentenza Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238, punti 39 e 40).

180. La lettura delle spiegazioni contenute al titolo B dell'allegato IV della decisione 2000/520, intitolato «Autorizzazioni legali esplicite», conferma tale impressione, in particolare l'affermazione secondo la quale «[è] ovvio che quando la legge statunitense impone un'obbligazione conflittuale, le organizzazioni statunitensi, che aderiscano o no ai principi "approdo sicuro", devono osservare la legge». Viene inoltre indicato, per quanto attiene alle autorizzazioni esplicite, che «sebbene i principi "approdo sicuro" intendano colmare le differenze tra il sistema americano e quello europeo relativamente alla tutela della privacy, siamo tenuti al rispetto delle prerogative legislative dei legislatori eletti».

181. Ne risulta che, a mio avviso, tale deroga è contraria agli articoli 7, 8 e 52, paragrafo 1, della Carta, nella misura in cui essa non persegue un obiettivo di interesse generale definito in maniera sufficientemente precisa.

182. In ogni caso, la facilità e la genericità con le quali la stessa decisione 2000/520, ai suoi allegati I, quarto comma, lettera b), e IV, B, prevede che i principi dell'approdo sicuro possano essere esclusi in applicazione di norme di diritto americano sono incompatibili con la condizione secondo la quale le deroghe alle norme relative alla protezione dei dati personali devono essere limitate a quanto strettamente necessario. Il requisito della necessità viene effettivamente menzionato, ma, a parte il fatto che la dimostrazione di tale requisito è posta a carico dell'impresa di cui trattasi, non vedo come una siffatta impresa potrebbe sottrarsi ad un obbligo di escludere i principi dell'approdo sicuro che discende da norme di diritto che essa è tenuta ad applicare.

183. Ritengo pertanto che la decisione 2000/520 debba essere dichiarata invalida perché l'esistenza di una deroga che consente in maniera talmente generica e imprecisa di escludere i principi del regime dell'approdo sicuro impedisce di per sé di ritenere che tale regime garantisca un livello di protezione adeguato ai dati personali che vengono trasferiti negli Stati Uniti dall'Unione.

184. Passando poi alla prima categoria di limiti previsti all'allegato I, quarto comma, lettera a), della decisione 2000/520, attinenti ad esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia degli Stati Uniti, solo la prima finalità mi sembra essere sufficientemente precisa da essere considerata una finalità di interesse generale riconosciuta dall'Unione ai sensi dell'articolo 52, paragrafo 1, della Carta.

185. Occorre adesso verificare la proporzionalità dell'ingerenza constatata.

186. A questo proposito, si deve ricordare che il «principio di proporzionalità esige, secondo una costante giurisprudenza della Corte, che gli atti delle istituzioni dell'Unione siano idonei a realizzare gli obiettivi legittimi perseguiti dalla normativa di cui trattasi e non superino i limiti di ciò che è idoneo e necessario al conseguimento degli obiettivi stessi» [69].

187. Per quanto riguarda il controllo giurisdizionale del rispetto di tali condizioni, «allorché si tratta di ingerenze in diritti fondamentali, la portata del potere discrezionale del legislatore dell'Unione può risultare limitata in funzione di un certo numero di elementi, tra i quali figurano, in particolare, il settore interessato, la natura del diritto di cui trattasi garantito dalla Carta, la natura e la gravità dell'ingerenza nonché la finalità di quest'ultima» [70].

188. Ritengo che le decisioni adottate dalla Commissione sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46 siano integralmente soggette al controllo della Corte quanto alla proporzionalità della valutazione effettuata da tale istituzione in merito all'adeguatezza del livello di protezione offerto da un paese terzo a causa «della sua legislazione nazionale o dei suoi impegni internazionali».

69 — Sentenza Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238, punto 46, nonché la giurisprudenza ivi citata).

70 — Ibidem (punto 47 e la giurisprudenza ivi citata).

189. Occorre osservare a tal riguardo che, nella sentenza Digital Rights Ireland e a.[71], la Corte ha dichiarato che, «tenuto conto, da un lato, del ruolo importante svolto dalla protezione dei dati personali sotto il profilo del diritto fondamentale al rispetto della vita privata e, dall'altro, della portata e della gravità dell'ingerenza in tale suddetto diritto che la direttiva [in questione] comporta, il potere discrezionale del legislatore dell'Unione risulta ridotto e di conseguenza è necessario procedere ad un controllo stretto»[72].

190. Una siffatta ingerenza deve essere idonea a realizzare l'obiettivo perseguito dall'atto dell'Unione in questione ed essere necessaria a conseguire tale obiettivo.

191. A tal riguardo, «[p]er quel che riguarda il rispetto della vita privata, la protezione di tale diritto fondamentale, secondo la costante giurisprudenza della Corte, richiede (…) che le deroghe e le restrizioni alla tutela dei dati personali debbano operare entro i limiti dello stretto necessario»[73].

192. Nel suo controllo, la Corte tiene parimenti conto della circostanza che «la tutela dei dati personali, risultante dall'obbligo esplicito previsto all'articolo 8, paragrafo 1, della Carta, riveste un'importanza particolare per il diritto al rispetto della vita privata sancito dall'articolo 7 della stessa»[74].

193. Secondo la Corte, la quale richiama, a tal riguardo, la giurisprudenza della Corte europea dei diritti dell'uomo, «la normativa dell'Unione di cui trattasi deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati sono stati conservati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati»[75]. La Corte indica che «[l]a necessità di disporre di siffatte garanzie è tanto più importante allorché (...) i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi»[76].

194. Esiste, a mio avviso, un'analogia fra l'allegato I, quarto comma, lettera a), della decisione 2000/520 e l'articolo 13, paragrafo 1, della direttiva 95/46. Nella prima disposizione, è indicato che l'adesione ai principi dell'approdo sicuro può essere limitata «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]». Nella seconda, viene previsto che 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 di tale direttiva, qualora tale restrizione costituisca una misura necessaria alla salvaguardia, segnatamente, della sicurezza dello Stato, della difesa, della pubblica sicurezza, nonché della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali.

195. Come rilevato dalla Corte nella sua sentenza IPI[77], dal dettato dell'articolo 13, paragrafo 1, della direttiva 95/46 risulta che gli Stati membri possono prevedere le misure contemplate da tale disposizione unicamente quando siano necessarie. La «necessità» delle misure condiziona quindi la facoltà accordata agli Stati membri da detta disposizione[78]. In relazione ai trattamenti di dati personali

71 — C-293/12 e C-594/12, EU:C:2014:238.

72 — Punto 48.

73 — Sentenza Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238, punto 52, nonché la giurisprudenza ivi citata).

74 — Ibidem (punto 53).

75 — Ibidem (punto 54 e la giurisprudenza ivi citata).

76 — Ibidem (punto 55 e la giurisprudenza ivi citata).

77 — C-473/12, EU:C:2013:715.

78 — Punto 32.

all'interno dell'Unione, deve ritenersi che i limiti previsti dall'articolo 13 di tale direttiva siano circoscritti a quanto strettamente necessario al conseguimento dell'obiettivo perseguito. Lo stesso deve valere, a mio avviso, nel caso dei limiti ai principi dell'approdo sicuro che sono previsti all'allegato I, quarto comma, della decisione 2000/520.

196. Orbene, è giocoforza constatare che non tutte le versioni linguistiche menzionano il criterio della necessità nel testo dell'allegato I, quarto comma, lettera a), della decisione 2000/520. Ciò vale, segnatamente, per la versione in lingua francese, la quale indica che «[l]'adhésion aux principes peut être limitée par (...) les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis», mentre, a titolo di esempio, le versioni in lingua spagnola, tedesca e inglese indicano che le limitazioni istituite devono essere necessarie per conseguire gli obiettivi summenzionati.

197. In ogni caso, gli elementi di fatto dedotti dal giudice del rinvio, nonché dalla Commissione nelle sue summenzionate comunicazioni mostrano chiaramente che, nella prassi, l'attuazione di tali limitazioni non è circoscritta a quanto strettamente necessario al conseguimento degli obiettivi previsti.

198. Osservo, a tal proposito, che l'accesso ai dati personali trasferiti di cui dispongono i servizi di intelligence americani copre in maniera generale qualsiasi persona e qualsiasi mezzo di comunicazione elettronica, nonché l'insieme dei dati trasferiti, compreso il contenuto delle comunicazioni senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di interesse generale perseguito [79].

199. Infatti, l'accesso dei servizi di intelligence americani ai dati trasferiti riguarda in maniera globale l'insieme delle persone che fanno uso dei servizi di comunicazione elettronica, senza che sia richiesto che le persone interessate presentino una minaccia per la sicurezza nazionale [80].

200. Una siffatta sorveglianza massiccia e indifferenziata è sproporzionata per natura e costituisce un'ingerenza ingiustificata nei diritti garantiti dagli articoli 7 e 8 della Carta.

201. Come rilevato giustamente dal Parlamento nelle sue osservazioni, poiché è impossibile, per il legislatore dell'Unione o per gli Stati membri, adottare disposizioni legislative che, in violazione, della Carta, prevedano una sorveglianza massiccia e indifferenziata, ne consegue inevitabilmente e a maggior ragione che non si può ritenere in alcuna circostanza che paesi terzi garantiscano un livello di protezione adeguato ai dati personali dei cittadini dell'Unione allorché la loro normativa autorizza effettivamente la sorveglianza e l'intercettazione massicce e indifferenziate di questo tipo di dati.

202. Occorre inoltre sottolineare che il regime dell'approdo sicuro, come definito dalla decisione 2000/520, non contiene le garanzie idonee ad evitare un accesso massiccio e generalizzato ai dati trasferiti.

203. Osservo, a tal riguardo, che la Corte ha messo in evidenza, nella sentenza Digital Rights Ireland e a. [81], l'importanza di prevedere «norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta» [82]. Secondo la Corte, una siffatta ingerenza deve essere «regolamentata con precisione da disposizioni che permettano di garantire che essa sia

79 — V., per analogia, sentenza Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238, punto 57 e la giurisprudenza ivi citata).

80 — Ibidem (punti 58 e 59).

81 — C-293/12 e C-594/12, EU:C:2014:238.

82 — Punto 65.

effettivamente limitata a quanto strettamente necessario» [83]. La Corte ha parimenti posto l'accento, in questa sentenza, sulla necessità di prevedere «garanzie sufficienti, come richieste dall'articolo 8 della Carta, che permettano di assicurare una protezione efficace dei dati [personali] conservati contro i rischi di abuso nonché contro eventuali accessi e usi illeciti dei suddetti dati» [84].

204. Orbene, è giocoforza constatare che i meccanismi di arbitrato privato e la FTC, a causa del suo ruolo limitato alle controversie di natura commerciale, non costituiscono strumenti di contestazione dell'accesso dei servizi di intelligence americani ai dati personali trasferiti dall'Unione.

205. La competenza della FTC è limitata agli atti e alle pratiche sleali o ingannevoli in materia commerciale o collegata al commercio, ed essa non si estende pertanto alla raccolta e all'impiego di informazioni personali a fini non commerciali [85]. L'ambito di competenza limitato della FTC restringe il diritto dei singoli alla protezione dei loro dati personali. La FTC è stata creata non già per assicurare la protezione del diritto individuale alla vita privata, come avviene in seno all'Unione per le autorità nazionali di controllo, bensì per garantire un commercio leale ed affidabile per i consumatori, il che limita, de facto, le sue capacità di intervento nella sfera relativa alla protezione dei dati personali. La FTC non svolge pertanto un ruolo equiparabile a quello delle autorità nazionali di controllo previste all'articolo 28 della direttiva 95/46.

206. I cittadini dell'Unione i cui dati sono stati trasferiti possono rivolgersi ad organismi arbitrali specializzati stabiliti negli Stati Uniti, come TRUSTe e BBBOnline, per chiedere precisazioni sulla questione se l'impresa che detiene i loro dati personali violi i requisiti del regime di autocertificazione. L'arbitrato privato assicurato da organismi come TRUSTe non può trattare le violazioni del diritto alla protezione dei dati personali commesse da organismi o autorità diverse dalle imprese autocertificate. Tali organismi arbitrali non hanno alcuna competenza a statuire sulla legittimità delle attività delle agenzie di sicurezza americane.

207. Né la FTC né gli organismi arbitrali privati sono pertanto competenti a controllare le possibili violazioni dei principi di protezione dei dati personali commesse da operatori pubblici come le agenzie di sicurezza americane. Una siffatta competenza sarebbe tuttavia essenziale per garantire pienamente il diritto alla protezione effettiva di tali dati. La Commissione non poteva pertanto constatare, adottando la decisione 2000/520 e mantenendola in vigore, che per l'insieme dei dati personali trasferiti verso gli Stati Uniti sussistesse una protezione adeguata del diritto conferito dall'articolo 8, paragrafo 3, della Carta, ossia che un'autorità indipendente esercitasse un controllo effettivo sul rispetto dei requisiti di protezione e sicurezza di tali dati.

208. Occorre pertanto rilevare l'assenza, nel regime dell'approdo sicuro previsto dalla decisione 2000/520, di un'autorità indipendente che possa controllare che l'attuazione delle deroghe ai principi dell'approdo sicuro venga limitata allo stretto necessario. Orbene, si è visto che un siffatto controllo da parte di un'autorità indipendente costituisce, sotto il profilo del diritto dell'Unione, un elemento essenziale del rispetto della tutela delle persone con riguardo al trattamento dei dati personali [86].

209. Occorre sottolineare, a tal riguardo, il ruolo svolto, nel sistema di protezione dei dati personali in vigore all'interno dell'Unione, dalle autorità nazionali di controllo in sede di controllo delle limitazioni previste all'articolo 13 della direttiva 95/46. Ai sensi dell'articolo 28, paragrafo 4, secondo comma, di tale direttiva, «[q]ualsiasi persona può, in particolare, chiedere a un'autorità di controllo di verificare la liceità di un trattamento quando si applicano le disposizioni nazionali adottate a norma

83 — Idem.

84 — Ibidem (punto 66).

85 — V., a tal riguardo, allegato II, FAQ 11, della decisione 2000/520, sub «Attività della Commissione federale per il commercio (Federal Trade Commission, FTC)», e allegati III, V e VII alla medesima.

86 — V. sentenza Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238, punto 68, nonché la giurisprudenza ivi citata).

dell'articolo 13 della presente direttiva». Per analogia, ritengo che la menzione di limiti all'applicazione dei principi dell'approdo sicuro all'allegato I, quarto comma, della decisione 2000/520, avrebbe dovuto essere accompagnata dall'attuazione di un meccanismo di controllo assicurato da un'autorità indipendente specializzata in materia di protezione dei dati personali.

210. L'intervento di autorità di controllo indipendenti si trova, infatti, al centro del sistema europeo di protezione dei dati personali. È pertanto naturale che l'esistenza di siffatte autorità sia stata considerata, anzitutto, una delle condizioni necessarie alla constatazione dell'adeguatezza del livello di protezione offerto dai paesi terzi. Si tratta di una condizione affinché i flussi di dati dal territorio degli Stati membri verso quello di paesi terzi non vengano vietati in conformità all'articolo 25 della direttiva 95/46 [87]. Come rilevato nel documento di discussione adottato dal gruppo di lavoro istituito dall'articolo 29 di tale direttiva, vi è in Europa un ampio consenso sulla necessità di «un sistema di "controllo esterno" sotto forma di autorità' indipendente, atto ad assicurare l'osservanza delle norme di tutela» [88].

211. Rilevo, inoltre, che la FISC non mette a disposizione dei cittadini dell'Unione i cui dati personali sono stati trasferiti negli Stati Uniti un ricorso giurisdizionale effettivo. Infatti, le tutele nei confronti della sorveglianza posta in essere dai servizi governativi nell'ambito dell'articolo 702 della legge del 1978 sulla sorveglianza dei servizi di intelligence stranieri si applicano unicamente ai cittadini americani, nonché ai cittadini stranieri che risiedono legalmente e permanentemente negli Stati Uniti. Come rilevato dalla Commissione stessa, il controllo dei programmi americani di raccolta di intelligence potrebbe essere migliorato rafforzando il ruolo della FISC e introducendo mezzi di ricorso per i singoli. Questi meccanismi potrebbero ridurre il trattamento di dati personali dei cittadini dell'Unione che non sono rilevanti ai fini della protezione della sicurezza nazionale [89].

212. Inoltre, la Commissione ha indicato essa stessa che i cittadini dell'Unione non hanno alcuna possibilità di ottenere l'accesso, la rettifica o la cancellazione dei dati, o rimedi amministrativi o giurisdizionali in relazione alla raccolta e all'ulteriore trattamento dei loro dati personali nell'ambito dei programmi di controllo americani [90].

213. Occorre infine rilevare che le norme americane relative alla protezione della vita privata possono essere oggetto di un'applicazione differenziata fra i cittadini americani e i cittadini stranieri [91].

214. Da quanto precede deriva che la direttiva 2000/520 non prevede norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta. È quindi giocoforza constatare che tale decisione e l'applicazione che ne viene fatta comportano un'ingerenza di vasta portata e di particolare gravità in detti diritti fondamentali, senza che siffatta ingerenza sia regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario.

215. Adottando la decisione 2000/520, e poi mantenendola in vigore, la Commissione ha dunque oltrepassato i limiti imposti dal rispetto del principio di proporzionalità alla luce degli articoli 7, 8 e 52, paragrafo 1, della Carta. A ciò si aggiunge la constatazione di un'ingerenza ingiustificata nel diritto dei cittadini dell'Unione ad un ricorso effettivo, tutelato dall'articolo 47 della Carta.

87 — V. Poullet, Y., «L'autorité de contrôle: "vues" de Bruxelles», *Revue française d'administration publique*, n. 89, gennaio-marzo 1999, pag. 69, specialmente pag. 71.

88 — V. pag. 7 del documento di lavoro WP 12 della Commissione menzionato alla nota a piè di pagina 56.

89 — Pagg. 10 e 11 della comunicazione della Commissione menzionata alla nota a piè di pagina 2.

90 — Punto 7.2, pag. 20, della comunicazione della Commissione menzionata alla nota a piè di pagina a pag. 58.

91 — V., su tale questione, Kuner, C., «Foreign Nationals and Data Protection Law: A Transatlantic Analysis», *Data Protection Anno 2014: How To Restore Trust*? Intersentia, Cambridge, 2014, pag. 213, specialmente pag. 216 e segg.

216. Di conseguenza, tale decisione deve essere dichiarata invalida, dato che, a causa delle violazioni dei diritti fondamentali descritte in precedenza, non può ritenersi che il regime dell'approdo sicuro da essa instaurato garantisca un livello di protezione adeguato ai dati personali che vengono trasferiti dall'Unione verso gli Stati Uniti nell'ambito di tale regime.

217. A fronte di una siffatta constatazione di violazioni dei diritti fondamentali dei cittadini dell'Unione, ritengo che la Commissione avrebbe dovuto sospendere l'applicazione della decisione 2000/520.

218. Tale decisione ha una durata indeterminata. Orbene, la presente causa dimostra che l'adeguatezza del livello di protezione offerto da un paese terzo può evolversi nel tempo in funzione del mutamento delle circostanze sia di fatto che di diritto che hanno fondato detta decisione.

219. Rilevo che la stessa decisione 2000/520 contiene disposizioni che prevedono la possibilità per la Commissione di adeguare la medesima in funzione delle circostanze.

220. In tal senso, risulta dal considerando 9 di tale decisione che «[l]'approdo sicuro creato dai principi e dalle FAQ può richiedere una revisione alla luce dell'esperienza e degli sviluppi riguardanti la tutela della vita privata in un contesto in cui la tecnologia rende sempre più facile il trasferimento e il trattamento dei dati personali, e dei risultati delle attività di applicazione e di esecuzione da parte delle autorità competenti».

221. Analogamente, ai sensi dell'articolo 3, paragrafo 4, di detta decisione, «[o]ve le informazioni di cui ai paragrafi 1, 2 e 3 del presente articolo provino che uno degli organismi incaricati di garantire la conformità ai principi applicati conformemente alle FAQ negli Stati Uniti non svolge la sua funzione in modo efficace, la Commissione ne informa il Dipartimento del commercio degli Stati Uniti e, se necessario, presenta progetti di misure (…) al fine di annullare o sospendere la presente decisione o limitarne il campo d'applicazione».

222. Inoltre, secondo l'articolo 4, paragrafo 1, della decisione 2000/520, essa «può essere adattata in qualsiasi momento alla luce dell'esperienza acquisita nella sua attuazione e/o qualora il livello di protezione offerta dai principi e dalle FAQ sia superato dai requisiti della legislazione degli Stati Uniti. La Commissione valuta in ogni caso l'applicazione della presente decisione tre anni dopo la sua notifica agli Stati membri sulla base delle informazioni disponibili e comunica qualsiasi riscontro al comitato istituito dall'articolo 31 della direttiva 95/46/[...], fornendo altresì ogni indicazione che possa influire sulla valutazione relativa all'adeguata salvaguardia offerta dalla disposizione di cui all'articolo 1 della presente decisione, ai sensi dell'articolo 25 della direttiva 95/46». Ai sensi dell'articolo 4, paragrafo 2, della decisione 2000/520, «[l]a Commissione, se necessario, presenta progetti di opportuni provvedimenti in conformità alla procedura di cui all'articolo 31 della direttiva 95/46».

223. La Commissione ha rilevato, nelle sue osservazioni, che «esiste un'elevata probabilità che l'adesione ai principi dell'approdo sicuro sia stata limitata in un modo che non risponde più alle condizioni strettamente circoscritte dell'esenzione prevista in materia di sicurezza nazionale» [92]. Essa osserva, a tal riguardo, che «[dall]e rivelazioni in questione emerge un grado di sorveglianza indifferenziata su larga scala, il quale non è compatibile con il criterio di necessità previsto in tale esenzione né, in termini più generali, con il diritto alla protezione dei dati personali sancito all'articolo 8 della Carta» [93]. La Commissione ha inoltre constatato essa stessa che «[l]a portata [dei] programmi di controllo, associata alla disparità di trattamento riservata ai cittadini [dell'Unione], mette in questione il livello di protezione offerto dall'accordo Approdo sicuro» [94].

92 — Punto 44.

93 — Idem.

94 — Pag. 5 della comunicazione della Commissione menzionata alla nota a piè di pagina 2.

224. Inoltre, la Commissione ha espressamente riconosciuto, in udienza, che, nell'ambito della decisione 2000/520, come è applicata attualmente, non sussistono garanzie che il diritto dei cittadini dell'Unione alla protezione dei loro dati sarà assicurato. Tale constatazione non è tuttavia idonea, a suo avviso, a rendere invalida tale decisione. Pur se la Commissione condivide l'affermazione secondo la quale essa deve agire a fronte di circostanze nuove, essa ritiene di avere adottato misure adeguate e proporzionate avviando negoziati con gli Stati Uniti al fine di riformare il regime dell'approdo sicuro.

225. Non sono di tale avviso. Infatti, nel frattempo, i trasferimenti di dati personali verso gli Stati Uniti devono poter essere sospesi su iniziativa delle autorità nazionali di controllo o a seguito di denunce depositate presso le medesime.

226. Inoltre, ritengo che, a fronte di tali constatazioni, la Commissione avrebbe dovuto sospendere l'applicazione della decisione 2000/520. Infatti, l'obiettivo di protezione dei dati personali perseguito dalla direttiva 95/46 nonché dall'articolo 8 della Carta fa gravare taluni obblighi non solo sugli Stati membri, ma anche sulle istituzioni dell'Unione, come risulta dall'articolo 51, paragrafo 1, della Carta.

227. Nella sua valutazione del livello di protezione offerto da un paese terzo, la Commissione deve esaminare non solo la normativa interna e gli impegni internazionali di tale paese terzo, ma anche il modo in cui la protezione dei dati personali viene garantita nella prassi. Se l'esame della prassi rivela delle disfunzioni, la Commissione deve reagire e, se del caso, sospendere e/o adeguare senza indugio la propria decisione.

228. Come si è visto nelle considerazioni svolte in precedenza, l'obbligo incombente sugli Stati membri consiste principalmente nell'assicurare, tramite l'azione delle loro autorità nazionali di controllo, il rispetto delle norme previste dalla direttiva 95/46.

229. L'obbligo che grava sulla Commissione consiste nel sospendere l'applicazione di una decisione da essa adottata sulla base dell'articolo 25, paragrafo 6, di tale direttiva in caso di comprovati inadempimenti da parte del paese terzo di cui trattasi fintantoché essa conduce negoziati con tale paese terzo onde porre fine a detti inadempimenti.

230. Ricordo che una decisione adottata dalla Commissione sulla base di tale disposizione è intesa a constatare che un paese terzo «garantisce» un livello di protezione adeguato ai dati personali oggetto di un trasferimento verso tale paese terzo. Il termine «garantisce», coniugato al presente, implica che, per poter essere mantenuta, una siffatta decisione debba riguardare un paese terzo che, successivamente all'adozione di detta decisione, continua a garantire un siffatto livello di protezione adeguato.

231. Secondo il considerando 57 della direttiva 95/46, «deve essere vietato il trasferimento di dati personali verso un paese terzo che non offre un livello di protezione adeguato».

232. Ai sensi dell'articolo 25, paragrafo 4, di tale direttiva, «[q]ualora la Commissione constati, secondo la procedura dell'articolo 31, paragrafo 2, che un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, gli Stati membri adottano le misure necessarie per impedire ogni trasferimento di dati della stessa natura verso il paese terzo in questione». Inoltre, l'articolo 25, paragrafo 5, di detta direttiva dispone che «[l]a Commissione avvia, al momento opportuno, negoziati per porre rimedio alla situazione risultante dalla constatazione di cui al paragrafo 4».

233. Risulta da quest'ultima disposizione che, nel sistema predisposto dall'articolo 25 della direttiva 95/46, i negoziati avviati con un paese terzo sono volti a rimediare ad un'assenza di livello di protezione adeguato constatata in conformità al procedimento previsto all'articolo 31, paragrafo 2, di tale direttiva. Nel caso di specie, la Commissione non ha formalmente constatato, in conformità a tale

procedura, che il regime dell'approdo sicuro non garantiva più un livello di protezione adeguato. Ciò premesso, se la Commissione ha deciso di avviare negoziati con gli Stati Uniti, è proprio perché essa ha ritenuto, in via preliminare, che il livello di protezione assicurato da questo paese terzo non fosse più adeguato.

234. Sebbene fosse a conoscenza di disfunzioni in sede di applicazione della decisione 2000/520, la Commissione non ha né sospeso né adeguato quest'ultima, determinando in tal modo il persistere della violazione dei diritti fondamentali delle persone i cui dati personali sono stati e continuano ad essere trasferiti nell'ambito del regime dell'approdo sicuro.

235. Orbene, la Corte ha già dichiarato, pur se in un altro contesto, che spetta alla Commissione vigilare sull'adeguamento di una normativa ai nuovi dati [95].

236. Una siffatta inerzia della Commissione, che arreca direttamente pregiudizio ai diritti fondamentali tutelati dagli articoli 7, 8 e 47 della Carta, costituisce, a mio avviso, un motivo supplementare per dichiarare invalida la decisione 2000/520 nell'ambito del presente rinvio pregiudiziale [96].

III – **Conclusione**

237. Sulla scorta delle considerazioni sin qui svolte, propongo alla Corte di risolvere nel modo seguente le questioni pregiudiziali sottopostele dalla Corte d'appello:

L'articolo 28 della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in combinato con gli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che l'esistenza di una decisione adottata dalla Commissione europea sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46 non produce l'effetto di impedire ad un'autorità nazionale di controllo di istruire una denuncia con la quale si lamenta che un paese terzo non garantisce un livello di protezione adeguato ai dati personali trasferiti e, se del caso, di sospendere il trasferimento di tali dati.

La decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio 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, è invalida.

95 — V., in tal senso, sentenza Agrarproduktion Staebelow (C-504/04, EU:C:2006:30, punto 40).

96 — Sebbene la Corte abbia dichiarato, nella sentenza T. Port (C-68/95, EU:C:1996:452) che «il Trattato non ha previsto la possibilità di un rinvio con cui il giudice nazionale chieda alla Corte di dichiarare in via pregiudiziale la carenza di un'istituzione» (punto 53), sembra che essa adotti una posizione più favorevole a tale possibilità nella sentenza Ten Kate Holding Musselkanaal e a. (C-511/03, EU:C:2005:625, punto 29).