ISSN 2384-9169

Eurojus.it

LA TUTELA DEI DATI PERSONALI UE A SEGUITO DELLA SENTENZA SCHREMS

1. I fatti alla base del rinvio pregiudiziale *Schrems*.

La vicenda oggetto del rinvio pregiudiziale *Schrems* (C-362/14) trae origine dalla doglianza presentata dal sig. Schrems, cittadino austriaco, davanti alla autorità garante della protezione dei dati irlandese volta a ottenere la sospensione del trasferimento negli USA dei dati personali immessi dallo stesso sulla sua pagina *Facebook*. Al riguardo, il sig. Schrems ha sostenuto che, da un lato, tutti i cittadini dell'Unione che usino *Facebook* sono tenuti a concludere un contratto con la filiale UE della società USA Facebook Inc., localizzata in Irlanda (Facebook Irland) e, dall'altro lato, che le informazioni immesse in *Facebook* sono quotidianamente trasferite verso *servers* appartenenti a Facebook Inc., e dunque situati negli USA, dove essi sono trattati e conservati. Il sig. Schrems afferma inoltre che, come dimostrato dalle rivelazioni del sig. Edward Snowden concernenti l'attività di sorveglianza della *National Security Agency* (NSA), il sistema nordamericano non garantisce una protezione adeguata dei dati personali degli individui avverso le illegittime ingerenze di autorità pubbliche USA. In effetti, a seguito delle predette rivelazioni, è stato accertato che la NSA, invocando la necessità di lottare contro il terrorismo e dunque per motivi di sicurezza nazionale, ha ripetutamente avuto accesso ai dati personali non solo USA ma anche UE raccolti tramite Internet (incluso *Facebook*), in tal modo dando vita a programmi di sorveglianza massiccia e apparentemente indiscriminata. A fronte di ciò e al fine di tutelare i diritti UE avverso tali illegittime ingerenze USA, il sig. Schrems ha così domandato al garante per la protezione dei dati irlandese, ove è ubicata la filiale europea della società nordamericana Facebook Inc. responsabile del trattamento dei dati, come imposto dall'articolo 4, paragrafo 1, lettera *a-c*, dalla direttiva 95/46(*GUCE* L 281 del 1995) relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali (sui criteri per determinare il diritto applicabile e l'autorità competente di cui all'articolo 4, sentenza 1 ottobre 2015, *Weltimmo*, C-230/14; sull'ampliamento dell'applicazione territoriale della disciplina UE sulla protezione dei dati personali, v. articolo 3, paragrafo 2, proposta di regolamento della Commissione europea COM(2012)11, e la comunicazione del 27 novembre 2013 COM(2013)846, p. 6) di sospendere il trasferimento dei dati dall'Irlanda agli USA, in tal modo usando la facoltà di controllo loro riconosciuta dagli articoli 25 e 28 dalla predetta direttiva (punti 26-29).

L'autorità garante irlandese ha tuttavia rigettato la denuncia del sig. Schrems ritenendo di non avere competenza a sindacare l'adeguatezza del regime USA di tutela dei dati personali (punto 29), essendo stato quest'ultimo già giudicato adeguato dalla Commissione europea mediante la decisione 520 del 2000 (c.d. Approdo Sicuro o *Safe Harbour*, *GUCE* L 215 del 25 agosto 2000). Tale decisone, adottata sulla base dell'articolo 25 della direttiva 95/46, produce effetti vincolanti in tutti gli Stati

membri e dunque anche per ogni autorità garante nazionale. In particolare, l'articolo 25 della direttiva 95/46, pur prevedendo al primo paragrafo che gli Stati membri hanno il potere di disporre «il trasferimento verso un paese terzo di dati personali…soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato», stabilisce ai successivi paragrafi che qualora la Commissione constati che un paese terzo *non garantisce* un livello di protezione adeguato (paragrafo 4) o viceversa che tale paese *garantisce* un livello di protezione adeguato (paragrafo 6), essa adotta una decisione. Ai sensi del secondo periodo del paragrafo 6 dell'articolo 25 della direttiva 95/46, «gli Stati membri adottano le misure necessarie per conformarsi alla decisione [di adeguatezza] della Commissione». Secondo l'autorità irlandese, il carattere imperativo del paragrafo in esame («gli Stati membri *adottano*») e l'assenza di eccezioni al riguardo sottintende la mancanza in tali casi di discrezionalità dei paesi membri. Il fatto poi che questi ultimi debbano necessariamente conformarsi alla decisione UE di adeguatezza impone alle autorità garanti nazionali di respingere le doglianze di cittadini UE senza neppure valutare l'adeguatezza dello Stato terzo.

Ora, la decisione c.d. Approdo sicuro è per l'appunto una decisione adottata dalla Commissione sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46. Mediante tale decisione, quest'ultima, pur ritenendo che il sistema USA non tuteli i dati personali allo stesso livello dell'Unione (gli Stati Uniti, a differenza della UE, non prevedono tale diritto a livello costituzionale e regolano per lo più tale materia mediante norme solo settoriali (*Financial Services Modernisation Act* del 1999 e *Health Insurance Portability and Accountability Act* del 1996), spesso solo regolamentari o attraverso atti di autoregolamentazione, applicate da una pluralità di autorità differenti come la *Federal Trade Commission* o l'*Office of Consumers Affairs*, *Department of Health*), ha subordinato la concessione dell'adeguatezza al rispetto da parte delle imprese USA che vogliano operare nell'Unione e accedere ai dati UE (c.d. sistema di autocertificazione) di regole – i c.d. principi approdo sicuro e le domande frequenti – allegati alla predetta decisione, i quali sono il frutto della negoziazione tra UE e USA. Posta la diversa sensibilità dei due sistemi in esame nei riguardi del diritto alla tutela dei dati personali ma al fine di favorire in ogni caso lo sviluppo del commercio internazionale tra UE e USA, la decisione Approdo sicuro stabilisce, in buona sostanza, che le imprese USA possano accedere e usare i dati personali UE quando rispettino le sette condizioni elencate all'allegato I (Principi di Approdo sicuro). In particolare, (*i*) le imprese devono informare i singoli in merito alle finalità per cui i dati personali vengono raccolti e utilizzati, alle modalità per presentare reclami, alla tipologia di terzi a cui vengono fornite le informazioni (condizioni di notifica); (*ii*) deve essere offerta la possibilità di rifiutare che le informazioni personali siano rivelate a terzi o utilizzate per fini incompatibili con quelli per cui esse sono state raccolte, in particolare nel caso di dati a carattere delicato (condizioni mediche o sanitarie, origine etnica, opinioni politiche, credenze filosofiche e/o religiose, appartenenza a sindacati, vita sessuale) (c.d. facoltà di rifiuto e di consenso, le quali costituiscono le condizioni di scelta); (*iii*) le imprese che comunicano informazioni a terzi, oltre ad applicare i predetti principi di notifica e di scelta, devono accertarsi che detti terzi aderiscano ai principi dell'approdo sicuro e, in caso contrario, devono stipulare con essi un accordo scritto che comporti l'obbligo di offrire almeno lo stesso livello di protezione della riservatezza richiesto da tali principi (condizioni sul trasferimento successivo); (*iv*) le imprese devono prendere ragionevoli precauzioni per proteggere i dati personali dalla perdita e da abusi, nonché dall'accesso, dalla rivelazione, dall'alterazione e dalla distruzione non autorizzati

(condizioni sulla sicurezza); (*v*) le informazioni personali devono risultare pertinenti ai fini per cui vengono raccolte, nonché accurate, complete e aggiornate (condizioni circa l'integrità dei dati); (*vi*) gli individui devono poter accedere alle informazioni personali che li riguardano per poterle correggere, emendare o cancellare (condizioni di accesso); (*vii*) infine, per tutelare efficacemente la riservatezza dei dati personali occorre disporre meccanismi volti a garantire il rispetto dei principi Approdo sicuro, quali la possibilità di *ricorso* per gli individui cui si riferiscono i dati, *procedure di controllo* per verificare l'effettivo rispetto degli impegni, nonché *meccanismi per evitare l'impunità* di una impresa che non rispetti i predetti principi mediante la previsione tra l'altro di sanzioni sufficientemente rigorose (garanzie di applicazione).

A seguito della decisione dell'autorità garante irlandese di considerare infondate le pretese del sig. Schrems, quest'ultimo ha proposto ricorso davanti alla *High Court* (punto 30). Tale possibilità è garantita dalla stessa direttiva 95/46, la quale prevede proprio che «è possibile un ricorso giurisdizionale avverso le decisioni dell'autorità di controllo recanti pregiudizio» (articolo 28, paragrafo 3, ultimo periodo). Al fine di risolvere la controversia nazionale tra la predetta autorità garante e il sig. Schrems, il giudice irlandese ha deciso di rinviare in via pregiudiziale alla Corte di giustizia al fine di chiarire la portata dell'articolo 25, paragrafo 6, della direttiva 95/46 anche alla luce dell'articolo 8 della Carta UE dei diritti fondamentali sulla tutela dei dati personali UE. La *High Court* ha, in altri termini, chiesto ai giudici di Lussemburgo di precisare se le autorità garanti nazionali possano valutare, istruendo una propria inchiesta, l'adeguatezza di un sistema extra-UE (nel caso di specie USA) quando sollecitate in tal senso dai cittadini UE, e ciò anche quando la Commissione europea abbia, in virtù dell'articolo 25, paragrafo 6, della direttiva 95/46, già considerato adeguato tale sistema straniero e dunque autorizzato il trasferimento di dati UE verso tale sistema (punto 36). Al riguardo, si può inoltre già rilevare come tale quesito si fondasse su una lettera sbagliata o quantomeno parziale delle norme UE applicabili in quanto la stessa decisione di adeguatezza Approdo sicuro prevedeva espressamente l'intervento delle autorità garanti nazionali, nonché la possibile sospensione provvisoria dei trasferimenti di dati ad opera delle stesse (articolo 3) anche se alle condizioni restrittive ivi indicate (lettere *a* e *b*).

2. Sul potere delle autorità garanti nazionali di controllare il rispetto dei requisiti posti dalla direttiva 95/46 in materia di trasferimenti internazionali di dati…

Nel rispondere al quesito pregiudiziale, la Corte, seguendo le conclusioni dell'avvocato generale Bot del 23 settembre 2015 (rispetto ai normali tempi intercorrenti tra conclusioni e sentenza, le conclusioni *Scherms* sono state presentate solo due settimane prima della sentenza del 6 ottobre 2015), ha affermato innanzitutto che le autorità garanti degli Stati membri hanno, in virtù dell'articolo 28 della direttiva 95/46 interpretata alla luce dell'articolo 8 della Carta UE dei diritti fondamentali, il potere di valutare se un trasferimento internazionale di dati dalla UE verso uno Stato terzo rispetti le condizioni della direttiva 95/46 poste agli articoli 25 e 26 in materia di trasferimenti internazionali di dati (punto 47).

I giudici di Lussemburgo sono giunti a tale conclusione valorizzando i poteri e l'indipendenza delle autorità garanti nazionali (punti 38-39). Secondo la Corte, l'istituzione di tali autorità indipendenti è un

elemento essenziale del regime europeo di protezione dei dati personali. La conformità alle regole di diritto comune dell'uso dei dati personali raccolti e conservati anche mediante Internet da parte di ogni autorità pubblica è, in altri termini, assicurata proprio attribuendo ad autorità *indipendenti* il potere di controllare le condizioni e le modalità di uso di tali dati. L'importanza assegnata dai giudici di Lussemburgo al controllo dei garanti nazionali in quanto enti indipendenti non sorprende. Il ruolo centrale di queste ultime nel sistema UE di protezione dei dati personali non solo è espressamente richiamato all'articolo 8, paragrafo 3, della Carta UE, ma è anche alla base della sentenza *Digital Rights Irland ltd (8 aprile 2014, C-293/12 e C-594/12*). In tale pronuncia, i giudici di Lussemburgo hanno dichiarato invalida la direttiva 2006/24 sulla raccolta, la conservazione e l'utilizzo dei dati di una persona fisica residente nell'Unione mediante comunicazioni telefoniche o elettroniche da parte di un'autorità pubblica di uno degli Stati membri (*GUUE* L 105 del 13 aprile 2006) proprio in quanto essa non stabiliva regole chiare, limiti o eccezioni all'accesso e all'uso dei dati personali da parte delle autorità pubbliche dei paesi membri in grado di ridurre il rischio di abusi o usi illeciti dei dati raccolti e conservati, sui quali i garanti nazionali avrebbero dovuto vigilare. La mancanza di regole chiare sull'uso da parte delle autorità pubbliche nazionali dei dati accolti e conservati nell'Unione avrebbe di fatto reso impossibile il controllo su tale uso da parte di autorità indipendenti, ossia una operazione che, riprendendo le parole della stessa Corte, «costituisce un elemento essenziale del rispetto della tutela delle persone riguardo al trattamento dei dati personali» (sentenze *Digital Rights Irland ltd* cit., punto 68; 16 ottobre 2012, *Commissione c. Austria, C-614/10*, punto 37; 9 marzo 2010, *Commissione c. Germania, C-518/07*, punto 23).

Il ruolo centrale ricoperto dalle autorità garanti nazionali nel tutelare i diritti UE emerge inoltre anche dal tenore della stessa direttiva 95/46. Il considerando 62 della direttiva 95/46 prevede, infatti, 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». E in effetti, proprio al fine di consentire che le autorità garanti degli Stati membri possano esercitare la predetta funzione di vigilanza sull'uso dei dati personali UE, la direttiva 95/46 attribuisce loro i più ampi poteri di controllo, i quali sono enumerati, in modo peraltro non esaustivo, all'articolo 28 della direttiva in esame. Quest'ultima norma stabilisce in particolare che le autorità nazionali di controllo, nell'assolvere alla funzione di «sorvegliare, nel proprio territorio, l'applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri» (paragrafo 1), dispongono: (i) di poteri investigativi; (ii) di poteri effettivi d'intervento, quali quello di formulare pareri prima dell'avvio di trattamenti, di ordinare il congelamento, la cancellazione o la distruzione dei dati, o di vietare a titolo provvisorio o definitivo un trattamento dei dati; (iii) del potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva (paragrafo 3).

Ora, secondo la Corte, i poteri previsti all'articolo 28 della direttiva 95/46 possano applicarsi anche nel caso in esame, il quale ha ad oggetto un *trasferimento* di dati (e non dunque solo un trattamento di dati) *verso uno Stato terzo* (e quindi al di fuori di un certo territorio nazionale dell'UE). Quanto al primo profilo, i giudici di Lussemburgo hanno correttamente rilevato che, ai sensi dell'articolo 2, lettera *b*, della direttiva 95/46, il "trattamento" dei dati personali, ossia «l'insieme di operazione compiute con o senza l'ausilio di processi automatizzati applicate ai dati personali», comprende «la comunicazione

mediante trasmissione» e dunque anche il "trasferimento" dei dati personali dal proprio territorio nazionale a un diverso Stato (punti 44-45). Con riferimento al secondo profilo, essi hanno inoltre precisato che, come espressamente affermato al considerando 60 della direttiva 95/46, il trasferimento dei dati personali verso uno Stato terzo deve essere effettuato nel pieno rispetto delle norme adottate in applicazione della direttiva (punto 46). Se anche i trasferimenti di dati personali verso Stati terzi devono rispettare il regime UE di tutela dei dati stabilito dalla direttiva 95/46, le autorità garanti nazionali possono allora esercitare i poteri elencati all'articolo 28 della direttiva 95/46 per valutare non solo il trattamento dei dati effettuato all'interno del proprio Stato membro, ma anche il trasferimento degli stessi dal proprio paese membro verso Stati terzi. Il potere delle autorità garanti nazionali di valutare se un trasferimento di dati UE verso un paese terzo rispetti le esigenze poste dalla direttiva 95/46 trova peraltro conferma anche all'articolo 25 della direttiva 95/46. Come anzi detto, tale norma riconosce proprio agli Stati membri, e dunque alle autorità garanti nazionali in quanto organi degli stessi, il potere di disporre «il trasferimento verso un paese terzo di dati personali…*soltanto se* il paese terzo di cui trattasi garantisce *un livello di protezione* [quantomeno] *adeguato*».

Tutto ciò posto, e considerato il ruolo centrale svolto dalle autorità garanti nazionali nel sistema UE di protezione dei dati personali di cui all'articolo 8, paragrafo 3, della Carta dei diritti fondamentali, queste ultime hanno, in virtù degli articoli 25 e 28 della direttiva 95/46, il potere di verificare se un trasferimento di dati personali dal proprio territorio nazionale verso uno Stato terzo rispetti le esigenze poste dalla direttiva 95/46 e sia dunque adeguato ai sensi della stessa (punti 47-48). Al riguardo, si rileva già ora come la Corte, pur affermando ripetutamente che le autorità garanti hanno il potere *di controllare l'adeguatezza* del sistema extra-UE, non precisi, quantomeno espressamente, se le autorità di controllo possano anche adottare provvedimenti interni che vietino o sospendano il trasferimento dei dati UE verso Stati terzi considerati inadeguati. Ciò è particolarmente importante allorché la Commissione, come nel caso *Scherms*, abbia adottato una decisione di adeguatezza di un sistema extra-UE e dunque autorizzato i trasferimenti di dati UE verso quest'ultimo Stato, in tal caso potendosi creare un contrasto tra un atto comune di adeguatezza e un provvedimento nazionale di inadeguatezza.

Tale silenzio dei giudici di Lussemburgo si potrebbe spiegare affermando che il riconoscimento di pieni poteri alle autorità garanti nazionali nel caso di trasferimenti di dati personali UE in Stati terzi di cui ai punti 38-49 della sentenza in esame, pur se parte del capoverso relativa ai "poteri delle autorità di controllo di cui all'articolo 28 della direttiva 95/46 *in presenza di una decisione della Commissione* adottata ai sensi dell'articolo 25, paragrafo 6, della detta direttiva", sembri in realtà riguardare il caso, diverso da quello alla base del rinvio pregiudiziale in esame, in cui *manchi una decisione dell'esecutivo UE*. Come risulta dall'*incipit* del paragrafo 40, l'interpretazione dei giudici UE dell'articolo 28 della direttiva 95/46 di cui ai punti 40-49 della sentenza è relativa ai "poteri di cui dispongono le autorità di controllo nazionali con riferimento ai trasferimenti di dati personali verso paesi terzi" e dunque *in generale* ai poteri di cui esse dispongono in tale ambito a prescindere dalla sussistenza di una previa decisione di adeguatezza della Commissione. Il fatto inoltre che la Corte di giustizia menzioni tale possibilità solo a partire dal punto 50 della sentenza *Schrems* (in particolare punti 50-66) sembra confermare *a contrario* che il ragionamento dei giudici di Lussemburgo di cui ai punti

precedenti (ossia 38-49) sia volto solo a delimitare in generale i poteri delle autorità nazionali nel caso di trasferimento di dati in Stati terzi. In realtà, come si avrà modo di vedere, la Corte non ha *espressamente* attribuito alle autorità garanti nazionali il potere di vietare o sospendere, con un provvedimento interno, i trasferimenti di dati UE verso sistemi terzi considerati inadeguati neppure ai successivi punti 50-66 della sentenza, il che lascia un margine di incertezza sugli esatti poteri delle autorità garanti nazionali in presenza di una decisione UE.

3. (segue): … anche quando la Commissione europea abbia già adottato una decisione di adeguatezza di un certo sistema extra-UE di tutela dei dati personali

Una volta stabilito che le autorità garanti nazionali hanno il potere di controllare che il trasferimento dei dati personali UE anche verso Stati terzi garantisca un adeguato livello di tutela degli stessi, la Corte di giustizia ha accertato se queste ultime dispongano di tale potere anche nel caso in cui la Commissione europea, in virtù del paragrafo 6 dell'articolo 25 della direttiva 95/46, abbia adottato una decisione di adeguatezza di un certo Stato terzo e dunque autorizzato il trasferimento dei dati personali UE verso quest'ultimo sistema giuridico (punti 50-66).

Punto di partenza dell'analisi dei giudici di Lussemburgo è stato il fatto che il potere di accertare l'adeguatezza di un certo sistema extra-UE, ossia di una delle condizione per poter autorizzare il trasferimento dei dati personali di cittadini dell'Unione verso Stati terzi, è condiviso dai paesi membri e dalle autorità garanti degli stessi con la Commissione europea. Anzi, come rilevato dagli stessi giudici UE (punti 50-52), l'articolo 25 della direttiva 95/46 pare assegnare la prevalenza della valutazione in merito alla Commissione su quelle unilaterali delle autorità nazionali. Come già osservato, infatti, gli Stati membri sono tenuti ad adottare le misure necessarie per conformarsi alla decisione della Commissione ai sensi del paragrafo 6 della dispostone in esame, la quale è così vincolante per tutti gli Stati membri (e le autorità garanti nazionali) cui è rivolta.

Tale conclusione trova peraltro fondamento anche nei principi generali del diritto UE. Ai sensi dell'articolo 288 TFUE, le decisioni della Commissione che hanno come destinatari gli Stati membri, quale è per l'appunto quella c.d. Approdo sicuro, vincolano questi ultimi e tutti gli organi nazionali alle regole e alle valutazione ivi contenute. Da tale principio, la Corte deduce correttamente che le autorità nazionali non possono, nel valutare l'adeguatezza di un certo sistema extra-UE e anche quando esse siano persuase dell'inadeguatezza dello stesso, adottare un provvedimento contrario a una decisione dell'esecutivo europeo che invece ne abbia già stabilito l'adeguatezza (punti 51-52). Il principio di supremazia del diritto comune su quelli interni esclude, in altri termini, che le autorità garanti nazionali possano adottare atti opposti a quelli della Commissione europea. Tale effetto preclusivo vincolante si produce inoltre fino a quando l'atto UE non sia stato annullato o dichiarato illegittimo mediante ricorso in annullamento (articolo 263 TFUE), rinvio pregiudiziale (articolo 267 TFUE) o eccezione di invalidità (articolo 277 TFUE). In virtù di una giurisprudenza parimenti consolidata (sentenze 15 giugno 1994, C-137/92, *Commissione c. BASF*, punto 48; 8 luglio 1999, C-245/92, *Chemie Linz c. Commissione*, punto 93; 5 ottobre 2004, C-475/01, *Commissione c. Grecia*, punto 18), infatti, gli atti UE – e tra questi anche le decisioni della Commissione europea quale è quella oggetto di esame – godono di una presunzione di legalità, la quale è superabile solo ricorrendo alla Corte di giustizia dell'Unione

europea. Quest'ultima è in effetti l'unico organo a poter dichiarare l'invalidità di un atto UE (sentenze 22 ottobre 1987, 314/85, *Foto-Frost*, punti 15 ss., e più di recente 22 giugno 2010, C-188-189/10, *Melki e Abdeli*, punto 54). In tal modo, giudici di Lussemburgo confermano peraltro la facoltà della Commissione di introdurre, in tutti gli Stati membri mediante decisione, regole armonizzate per il trasferimento dei dati personali UE in Stati terzi, delle quali ne sancisce anche la prevalenza sulle valutazioni unilaterali delle autorità garanti nazionali. Il fatto che la Corte di giustizia, a differenza dell'avvocato generale, abbia valorizzato l'efficacia vincolate della decisione di adeguatezza della Commissione europea per tutti gli Stati membri e la sua prevalenza sulle valutazioni unilaterali delle autorità garanti è particolarmente opportuna in quanto tali aspetti sembravano invece essere stati fortemente ridimensionati dall'analisi dell'avvocato generale (punti 53-130, spec. 81 ss. delle conclusioni).

L'esistenza di una previa decisione di adeguatezza della Commissione europea, nonché i principi della prevalenza degli atti UE su quelli interni e l'impossibilità per gli Stati membri e le autorità nazionali di adottare provvedimenti contrari a quelli comuni in quanto ciò equivale a dichiarare questi ultimi invalidi, pur impedendo alle autorità garanti nazionali di adottare decisioni contrarie a quelle della Commissione, non eliminano tuttavia la facoltà dei cittadini UE i cui dati personali siano o possano essere trasferiti in uno Stato terzo di domandare alle autorità garanti nazionali, come accaduto in *Schrms*, di controllare l'adeguatezza del sistema extra-UE perché nutrano dei dubbi al riguardo (punto 53). Tale facoltà è in effetti loro riconosciuta dal paragrafo 4 dell'articolo 28 della direttiva, 95/46, il quale prevede che «qualsiasi persona…può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti». Inoltre, secondo la Corte di giustizia, l'adozione di una precedente decisione di adeguatezza della Commissione non impedisce neppure alle autorità garanti nazionali di valutare («*le contrôle des transferts des données*»), perché sollecitate in tal senso da un cittadino UE, l'adeguatezza di un certo sistema extra-UE ai sensi della direttiva 95/46 (punto 54). Tale potere è, infatti, espressamente riconosciuto ai garanti nazionali dagli articoli 25 e 28 della direttiva 95/46 come interpretati alla luce dell'articolo 8, paragrafo 3, della Carta dei diritti fondamentali.

A seguito della sentenza in esame, le autorità garanti nazionali non possono allora più respingere le doglianze dei cittadini UE sul trasferimento di dati UE in sistemi extra-UE senza di fatto esaminarle per il solo fatto che esiste una decisione di adeguatezza della Commissione europea. Tale approccio, il quale è stata seguito dall'autorità irlandese nel caso di specie, è, in altri termini, contraria al diritto UE. Anche in tali casi, i garanti degli Stati membri sono dunque tenuti, in virtù della direttiva 95/46 e dell'articolo 8 della Carta, a valutare con la dovuta diligenza («*avec tout la diligence requise*» punto 63) la domanda di cittadini UE che sostengano la violazione dei dati per effetto del loro trasferimento in un paese terzo, nonché a usare tutti gli strumenti a disposizione (ad esempio quelli investigativi) per formarsi un convincimento sulla adeguatezza o inadeguatezza del sistema extra-UE verso cui i dati UE siano trasferiti.

Al riguardo, la Corte, pur affermando ripetutamente che una previa decisione di adeguatezza della Commissione europea non elimina o riduce il potere di *esaminare* la domanda del cittadino e/o l'adeguatezza di un sistema extra-UE perché sollecitate in tal senso da un cittadino UE (punti 54, 56-

57), non attribuisce tuttavia mai espressamente a queste ultime il potere di vietare o sospendere, mediante un provvedimento interno, i trasferimenti di dati UE verso sistemi terzi reputati inadeguati (così invece espressamente l'avvocato generale Bot al punto 81 delle sue conclusioni). Pur se è vero che il giudice di rinvio ha domandato ai giudici di Lussemburgo solo di precisare se le autorità garanti avrebbero potuto in tali casi «*mener la propre enquête*», questi ultimi ben avrebbero potuto riformulare il quesito pregiudiziale e, al fine di offrire una risposta realmente utile, chiarire anche se queste ultime possano, al termine della predetta inchiesta, adottare un provvedimento interno che vieti o sospenda il trasferimento di dati UE verso sistemi terzi considerati inadeguati. Ciò a maggior ragione vero posto che, come si avrà modo di vedere nel prosieguo, la Corte non ha esitato a riformulare il quesito pregiudiziale sottopostole al fine di accertare la validità della decisione Approdo sicuro, in tal modo trasformando il rinvio pregiudiziale da (solo) interpretativo a rinvio (anche) di validità.

A favore del potere delle autorità garanti nazionali di adottare atti interni di sospensione dei trasferimenti dei dati UE verso Stati terzi considerati inadeguati anche a fronte di una previa decisione di adeguatezza della Commissione milita il fatto che la Corte abbia deciso di annullare la decisione Approdo sicuro perché l'articolo 3, paragrafo 1, della stessa riconosceva alle autorità garanti nazionali la facoltà di valutare l'adeguatezza di un sistema extra-UE anche in presenza di una precedente decisione UE, nonché di sospendere con provvedimenti provvisori interni i trasferimenti dei dati dal proprio Stato membro a uno Stato terzo *solo a condizioni specifiche*. Al riguardo, l'articolo 3 della decisione Approdo sicuro riconosce tali potere delle autorità garanti nazionali solo qualora *a*) gli enti governativi degli Stati Uniti abbiano accertato che una impresa USA viola i principi Approdo sicuro, oppure *b*) è molto probabile che tali principi siano violati, o vi siano ragionevoli motivi per ritenere che l'organismo di esecuzione competente non stia adottando o non adotterà misure adeguate e tempestive per risolvere un caso concreto, o ancora la continuazione del trasferimento dei dati potrebbe determinare un rischio imminente di gravi danni per gli interessati. Tali limiti, secondo la Corte, sarebbero incompatibili con il ruolo centrale svolto dalle stesse nella tutela dei dati UE di cui, tra l'altro, all'articolo 8, paragrafo 3, della Carta UE dei diritti fondamentali. Da tale conclusione sembra allora possibile dedurre *a contrario* che i giudici di Lussemburgo autorizzino le autorità garanti nazionali a un controllo *incondizionato* e *incomprimibile* (punti 99-106), nonché a sospendere in ogni caso i trasferimenti di dati UE verso Stati terzi inadeguati.

Né invero a una diversa conclusione sembra dover indurre il paragrafo 103 della sentenza in esame, secondo cui i poteri di esecuzione attribuiti dal legislatore UE alla Commissione europea mediante l'articolo 25, paragrafo, 6 della direttiva 95/46 non conferiscono a quest'ultima istituzione la competenza a restringere i poteri delle autorità nazionali di controllo di cui all'articolo 28 della direttiva stessa. Almeno letteralmente, tale paragrafo potrebbe essere interpretato nel senso che l'articolo 3 della decisione Approdo sicuro è incompatibile con l'articolo 8 della Carta UE non tanto perché esso limita dei poteri fondamentali delle autorità garanti nazionali, ma in quanto tali limiti sono stati introdotti dalla Commissione (e non dal legislatore UE) mediante un atto solo di esecuzione (e non legislativo). *A contrario* si potrebbe allora affermare che i poteri di controllo delle autorità garanti potrebbero essere limitati dal legislatore UE attraverso un atto legislativo comune. Posto tuttavia che la Carta UE dei diritti fondamentali è parte del diritto primario, l'introduzione di condizioni analoghe a quelle di cui

all'articolo 3 della decisione Approdo sicuro anche attraverso un atto legislativo UE dovrebbe essere parimenti considerata contraria all'articolo 8 della Carta UE dei diritti fondamentali.

Non è chiaro tuttavia in che modo tali poteri delle autorità garanti nazionali si coordini con la prevalenza della decisione della Commissione europea su quelle unilaterali delle autorità nazionali e la conseguente impossibilità di queste ultime di adottare provvedimenti contrari alla decisione comune (punti 50-52, 61-66). In particolare, non è facile comprendere come le autorità nazionali, le quali a seguito della predetta sentenza devono certamente valutare seriamente la domanda di cittadini UE che sostengano la violazione dei dati per effetto del loro trasferimento in un certo paese terzo e possono usare tutti gli strumenti a disposizione (ad esempio quelli investigativi) per formarsi un convincimento sulla adeguatezza o inadeguatezza del sistema extra-UE verso cui i dati UE siano trasferiti, possano spingersi fino ad adottare un provvedimento interno che vieti o sospenda unilateralmente tale trasferimento verso un sistema extra-UE considerato inadeguato anche in presenza di una decisione UE contraria, senza per questo violare il principio di supremazia del diritto comune su quelli interni e la competenza esclusiva dei giudici di Lussemburgo a dichiarare invalido un atto UE. Al riguardo, e seppur un po' artificiosamente, si potrebbe affermare che tale provvedimento interno non rimetterebbe in realtà in discussione la decisione di adeguatezza della Commissione in quanto il primo è volto solo a impedire il trasferimento dei dati personali da un *certo paese membro* (ad esempio l'Irlanda) verso uno Stato terzo (ad esempio gli USA) mediante *una determinata impresa* (ad esempio *Facebook*) e non invece *ogni trasferimento* di dati UE (e dunque di tutti gli Stati membri) verso uno Stato terzo anche attraverso altre società, come invece previsto dalla decisione della Commissione europea. Inoltre, e probabilmente proprio al fine di ovviare a decisioni di inadeguatezza di autorità garanti nazionali anche in presenza di una previa decisione di adeguatezza UE, la Corte di giustizia ha imposto in tali casi alle autorità di controllo nazionali di agire in giustizia davanti ai giudici interni, i quali hanno a propria volta il dovere di effettuare rinvio pregiudiziale ai giudici di Lussemburgo quanto alla validità della decisione UE. Come si avrà modo di vedere, il meccanismo ivi previsto dalla Corte sembra tuttavia particolarmente complesso e lascia qualche perplessità.

4. Il dovere delle autorità garanti nazionali di agire in giustizia.

A seguito del controllo di adeguatezza del sistema extra-UE, le autorità garanti nazionali possono (i) ritenere le doglianze dei cittadini UE sprovviste di fondamento e concordare così con la Commissione europea, o invece (ii) considerare fondate le doglianze del cittadino europeo, in tal modo giungendo a conclusioni opposte da quelle dell'esecutivo UE. Nel primo caso, la Corte rileva che il cittadino la cui domanda sia stata respinta ha la possibilità di impugnare la decisione dell'autorità garante davanti a un giudice nazionale (punto 64). L'articolo 28, paragrafo 3, seconda frase, della direttiva 95/46, a maggior ragione se interpretato alla luce dell'articolo 47 della Carta che riconosce tra i diritti fondamentali UE quello di una tutela giurisdizionale effettiva, attribuisce proprio ai cittadini UE il diritto di presentare ricorso davanti ai giudici nazionali avverso la decisione dei garanti nazionali ritenute lesive dei propri diritti. Qualora poi i giudici interni giungano alle medesime conclusioni dell'autorità garante e della Commissione europea, essi respingeranno il ricorso. Viceversa, tutte le volte in cui il giudice nazionale ritenga fondate le doglianze del cittadino UE, esso è obbligato, anche quando le sue

sentenze siano impugnabili davanti a un organo giurisdizionale nazionale superiore, a rinviare in via pregiudiziale alla Corte (sentenza *Foto-Frost*, cit.), la quale è l'unica a poter dichiarare invalida la decisione della Commissione e la valutazione di adeguatezza ivi contenuta del sistema extra-UE.

La situazione si complica tuttavia nel caso inverso, ossia qualora l'autorità garante nazionale, chiamata a valutare l'adeguatezza del sistema extra-UE di tutela dei dati personali perché sollecitata in tal senso, consideri tale sistema *inadeguato* e giunga così a conclusioni opposte a quelle della Commissione. Al fine di risolvere il contrasto tra un atto nazionale che, presupponendo l'inadeguatezza di un certo sistema extra-UE, sospenda il trasferimento di dati personali UE verso quest'ultimo e una decisione della Commissione europea di adeguatezza, la Corte afferma che in tali casi l'autorità nazionale *deve poter agire in giustizia* (punto 65). Pur in mancanza di indicazioni specifiche al riguardo, l'obbligo di agire davanti ai giudici interni sembra preordinato a effettuare il rinvio pregiudiziale ai giudici UE al fine di esaminare la validità della decisione di adeguatezza della Commissione europea (in tal senso invece espressamente l'avvocato generale al punto 119 delle sue conclusioni). Come anzi detto, infatti, questi ultimi sono gli unici a poter dichiarare invalido un atto dell'Unione, qual è per l'appunto la decisione in esame.

Il dovere imposto alle autorità garanti nazionali di proporre ricorso alle autorità giurisdizionali del proprio Stato membro sottintende inoltre che, secondo gli stessi giudici UE, le prime autorità, a differenze delle seconde, non sono neppure abilitate a proporre rinvio pregiudiziale di validità ai sensi dell'articolo 267 TFUE. Il dovere UE delle autorità garanti nazionali di agire in giustizia di cui al punto 65 della sentenza *Schrems* si spiega, in altri termini, solo presupponendo che lo strumento del rinvio pregiudiziale sia indisponibile alle stesse. In effetti, e seppur se con riferimento alle autorità garanti nazionali della concorrenza, la giurisprudenza UE ha proprio escluso che enti di questo tipo siano «giurisdizioni» abilitate a effettuare rinvio pregiudiziale ai sensi dell'articolo 267 TFUE (sentenze 31 maggio 2005, C-53/03, *Syfait*; 10 dicembre 2010, C-439/08, *VEBIC*).

Il fatto poi che i giudici di Lussemburgo non facciano alcun riferimento nella sentenza in esame al ricorso in annullamento, pare sottintendere che la Corte non ritenga neppure percorribile la strada di sindacare la validità della predetta decisione mediante il ricorso di cui all'articolo 263 TFUE. In effetti, al fine di garantire la stabilità giuridica, tale ricorso può essere proposto solo entro il termine di due mesi dalla pubblicazione dell'atto e dunque esclusivamente nell'immediatezza dell'adozione dello stesso. Il termine perentorio di cui all'articolo 263 TFUE, il quale è peraltro di ordine pubblico (sentenza Trib. 18 settembre 1997, T-121/96, *Mutual Aid Administration Services NV c. Commissione*), impedisce, in altri termini, di sottoporre ai giudici di Lussemburgo la questione della legittimità della decisione della Commissione europea quando, come nel caso in esame, sia trascorso molto tempo dall'adozione e dalla pubblicazione dell'atto comune che si intenda impugnare (la decisione Approdo sicuro è stata adottata e pubblicata nel 2000 e il sig. Schrems ha depositato la sua doglianza davanti all'autorità garante irlandese nel 2013).

Inoltre, le autorità garanti nazionali, in quanto organi di uno Stato membro, sono ricorrenti non privilegiati, cosicché esse potrebbero impugnare un atto analogo a quello in esame che ha come destinatari (solo) i paesi membri (ad esempio la nuova decisione Approdo sicuro al momento oggetto

di negoziazione tra la UE e gli USA), solo provando di essere "direttamente e individualmente riguardati" dalla stessa. Anche considerato che tali condizioni di ricevibilità sono applicate dalla giurisprudenza UE in modo restrittivo e particolarmente severo, pare tuttavia difficile che le autorità garanti nazionali siano in particolare in grado di dimostrare di essere "individualmente" riguardate da una decisione UE di questo tipo, ossia che quest'ultima, in virtù di particolari caratteristiche di fatto o di diritto, le individui come destinatari formali dell'atto. Al fine di sostenere la ricevibilità di tale (eventuale e futuro) ricorso, le autorità garanti nazionali potrebbero però far valere, ad esempio, il fatto di essere espressamente nominate nell'atto oggetto di impugnazione (Trib. 21 settembre 2005, T-315/01, *Kadi* e Corte 3 settembre 2008, C□402/05 e C□415/05, spec. punto 241) o invece di essere titolari del diritto di partecipare alla formazione dell'atto (attraverso il c.d. Gruppo di lavoro "Articolo 29") (17 gennaio 2002, T-47/00, *Rica Foods c. Commissione*). Come noto, tali ragioni hanno indotto in passato i giudici di Lussemburgo a ritenere ricevibili ricorsi proposti da ricorrenti non privilegiati avverso atti a portata generale o indirizzati agli Stati membri. Né invero la decisione della Commissione pare poter essere qualificata come un atto regolamentare, ossia un atto non legislativo a portata generale (sentenze Trib. 25 ottobre 2011, *Microban*, T-262/10; Corte 3 ottobre 2013, C-583/11 P, *Inuit Tapiriit Kanatami*), il che ne permetterebbe l'impugnazione provando di essere solo direttamente riguardate dall'atto. Pur se la decisione in esame non è adotta mediante la procedura legislativa, tale atto (di esecuzione) ha come destinatari gli Stati membri e non è quindi a "portata generale".

Qualora si ritenga che le autorità garanti nazionali non siano "direttamente e individualmente" riguardate dalla (nuova) decisione di adeguatezza della Commissione europea, quest'ultima potrebbe allora essere impugnata, in ogni caso nel termine di due mesi dalla pubblicazione, dagli Stati membri (e in particolare dal paese membro di appartenenza dell'autorità garante nazionale), i quali sono ricorrenti privilegiati. Viceversa, nel caso in cui si concluda nel senso di ritenere tali autorità come destinatarie *sostanziali* dell'atto, potrebbe essere messa in discussione la loro facoltà, alla base invece della sentenza *Schrems*, di contestare la legittimità dell'atto UE in via indiretta davanti ai giudici nazionali. Secondo una giurisprudenza UE costante (Trib. 13 settembre 1995, T-244/93 e T-486/93, *TWD*; Corte 23 febbraio 2006, C-346/03 e C-529/03, *Atzeni e a.*), infatti, qualora i destinatari sostanziali di un atto comune non abbiano agito in via diretta davanti ai giudici di Lussemburgo mediante ricorso in annullamento nei limiti temporali previsti dall'articolo 263 TFUE, essi non possono eccepirne l'illegittimità davanti ai giudici interni, chiedendo a questi ultimi di sollevare una questione di validità ai sensi dell'articolo 267 TFUE, in quanto ciò equivarrebbe a riconoscere loro la possibilità di eludere il carattere definitivo dell'atto UE dopo la scadenza del termine di cui all'articolo 263 TFUE.

La soluzione proposta dai giudici UE nel caso in cui le autorità garanti nazionali ritengano un certo sistema extra-UE inadeguato nonostante una previa decisione comune di adeguatezza e abbiano dunque dei dubbi sulla validità di una decisione dell'esecutivo UE suscita tuttavia alcune perplessità. Innanzitutto, non è chiaro mediante quale strumento giurisdizionale di diritto interno le predette autorità possano agire *personalmente* davanti i giudici nazionali. L'uso da parte della Corte dell'espressione "l'autorità deve poter agire in giustizia" sottintende che sia quest'ultima (e non il cittadino UE o la singola impresa USA e in ogni caso a prescindere dalla loro iniziativa in merito) a dover agire davanti al giudice interno. Anche considerato che, come rilevato dalla Corte (punto 65), il

legislatore nazionale ha il compito di prevedere delle vie di ricorso interne in grado di permettere alle autorità di controllo di far valere davanti ai giudici nazionali le doglianze dei cittadini UE che esse ritengano fondate, gli Stati membri dovranno allora istituire una specifica via di ricorso, la quale permetta in casi del genere alle autorità garanti nazionali di agire in giustizia, così come richiesto dalla Corte. Posto inoltre che l'azione proposta dall'autorità garante davanti ai giudici interni è preordinata a effettuare rinvio pregiudiziale di validità, tale ricorso dovrà possedere le caratteristiche alle quali la giurisprudenza UE subordina la ricevibilità di tali rinvii e in particolare essere una controversia (i) reale (ii) tra più parti opposte tra loro (sentenze 11 marzo 1980, 104/79, *Foglia c. Novello*; 19 ottobre 1995, C-111/94, *Job Center*; ordinanza 6 ottobre 2005, C-256/05, *Telekom Austria*). La sussistenza di tali condizioni può tuttavia porre difficoltà nel caso in esame. Nella ricostruzione della Corte, il predetto giudizio sembra in effetti volto non tanto a risolvere una controversia reale tra parti opposte, ma solo a effettuare il rinvio pregiudiziale di validità ai giudici UE al fine di preservare i principi di supremazia del diritto UE su quelli interni e il monopolio della Corte nel valutare la validità degli atti comuni.

Al riguardo, pare inoltre opportuno rilevare come in *Schrems* la Corte di giustizia non ha imposto alle autorità garanti nazionali che, chiamate a valutare l'adeguatezza del sistema extra-UE di tutela dei dati, giungano a conclusioni opposte a quelle della Commissione, a comunicare a quest'ultima i loro dubbi sull'adeguatezza dei sistemi extra-UE o l'adozione di misure provvisorie di sospensione dei flussi di dati UE verso sistemi di paesi terzi ritenuti inadeguati. Tali obblighi erano invece prescritti ai paragrafi 2 e 3 dell'articolo 3 della decisione Approdo sicuro del 2000. Il silenzio della Corte di giustizia sul punto e il fatto che, come si avrà modo di vedere, essa abbia annullato l'*intera* decisione Approdo sicuro (tra l'altro per incompatibilità all'articolo 8, paragrafo 3, della Carta del paragrafo 1 dell'articolo 3 della decisione) sembra dover indurre a escludere la possibilità di prevedere analoghi obblighi nella nuova decisione Approdo sicuro, attualmente oggetto di revisione da parte della Commissione europea. E ciò nonostante misure di questo tipo favorirebbero la cooperazione tra autorità garanti nazionali e Commissione europea quanto all'adeguatezza di un certo sistema extra-UE soprattutto in presenza di una previa decisione di adeguatezza UE.

5. L'invalidità della decisione Approdo sicuro

Sebbene il rinvio pregiudiziale effettuato dalla Corte irlandese fosse volto solo a ottenere l'interpretazione di talune norme della direttiva 95/46, i giudici di Lussemburgo, invocando la necessità di fornire una risposta completa alla giurisdizione di rinvio, hanno scelto di spingersi oltre il quesito pregiudiziale, accertando anche la validità della decisione Approdo sicuro. In tal modo la Corte ha peraltro riformulato il quesito sottopostole, trasformando di fatto il rinvio pregiudiziale (solo) di interpretazione in rinvio pregiudiziale (anche) di validità (si tratta di una operazione assai rara: così ad esempio sentenze 1° dicembre 1965, 16/65, *Schwarze*; viceversa 12 novembre 1969, 29/69, *Stauder*). In effetti, sia la giurisdizione di rinvio sia il sig. Schrems nella procedura principale hanno sostenuto che il sistema USA di protezione dei dati non fosse "adeguato" ai sensi dell'articolo 25 della direttiva 95/46, in tal modo mettendo in discussione la validità della decisione della Commissione europea che, al contrario, aveva considerato il sistema USA come adeguato.

Ora, la direttiva 95/46 non contiene una definizione di "livello di tutela adeguato". Al riguardo, l'articolo

25, paragrafo 2, della direttiva in esame si limita a stabilire che l'adeguatezza del regime extra-UE ove vengano trasferiti i dati UE sia accertata «avendo riguardo [al]la natura dei dati, [al]le finalità del trattamento, [a]l paese di origine e [a]l paese di destinazione finale, [al]le norme di diritto, generali o settoriali, [al]le regole professionali e [al]le misure di sicurezza vigenti nel paese terzo di cui trattasi, nonché [a]gli impegni internazionali assunti» dallo stesso. Posta la mancanza di una nozione condivisa di "adeguatezza", e nonostante la Corte stessa ammetta che l'uso dell'espressione "adeguato" impedisca di esigere che lo Stato terzo tuteli i dati personali in modo *identico* a quanto previsto dalla UE (punti 70-73), i giudici di Lussemburgo hanno richiesto che quest'ultimo garantisca un livello di protezione particolarmente elevato. L'espressione "livello di tutela adeguato" esige in particolare che il sistema extra-UE assicuri effettivamente, in ragione della propria legislazione interna o di accordi internazionali, un livello di tutela *sostanzialmente equivalente* a quello garantito nell'Unione in virtù della direttiva 95/46, così come peraltro interpretata alla luce della Carta UE dei diritti fondamentali (punto 73). Invocando l'applicazione della Carta, i giudici di Lussemburgo hanno, in altri termini, imposto un'interpretazione particolarmente rigorosa della norma in esame, andando oltre il dettato legislativo ("adeguato" rispetto "equivalente").

A fronte di un livello di adeguatezza così elevato non sorprende allora che i giudici UE abbiano concluso per l'invalidità, peraltro totale, della decisione della Commissione europea. Ciò è a maggiore ragione vero considerato che la tutela dei dati personali è un principio fondamentale dell'Unione, cosicché il potere discrezionale dell'esecutivo UE quanto all'adeguatezza del livello di tutela assicurato da uno Stato terzo è ridotto, nonché sottoposto al controllo particolarmente severo della Corte (punto 78). Al riguardo, i giudici di Lussemburgo hanno ribadito principi già alla base della sentenza *Digital Rights Irland* (punti 47-48), la quale ha parimenti condotto all'annullamento totale della direttiva 2006/24 sulla raccolta, la conservazione e l'utilizzo dei dati di una persona fisica residente nell'Unione da parte di un'autorità pubblica di uno degli Stati membri.

La scelta di annullare la decisione Approdo sicuro trova fondamento innanzitutto nel fatto che quest'ultima consente di derogare ai principi ivi enunciati per motivi di sicurezza nazionale (articoli 1-2 della decisione e allegati I, II e IV alla stessa). Secondo la Corte (punti 79-98), tale deroga costituisce un'interferenza illegittima nel diritto UE della protezione dei dati *in quanto prevista in modo incondizionato*. In particolare, la predetta decisione *non conteneva alcuna spiegazione* relativamente all'esistenza di (i) misure, legislative interne o di diritto internazionale, mediante le quali gli USA assicurano un livello di protezione adeguato avverso le illegittime ingerenza di autorità pubbliche USA (punti 83-88), e (ii) appositi strumenti giurisdizionali per reagire alle eventuali illegittime ingerenze delle autorità USA (punto 89). Tale silenzio della decisione Approdo sicuro è ancora più rilevante per il fatto che è lo stesso esecutivo UE, nelle sue comunicazioni del 2013 (COM(2013)846, punti 2-3; COM(2013)847, punti 7-8), ad aver rilevato che il sistema USA non premette di limitare l'accesso per motivi di sicurezza nazionale a quanto necessario e proporzionato, né prevede vie di ricorso al fine di ottenere l'accesso, la rettifica o la cancellazione dei dati UE (punto 90). La stessa Commissione avrebbe in un certo senso ammesso le lacune delle decisione di adeguatezza Approdo sicuro. E in effetti il negoziato, attualmente in corso e ormai a uno stadio avanzato, tra UE e USA sulla decisione Approdo Sicuro è proprio volto al rafforzamento di tali aspetti.

Ora, pur se la Corte pone l'accento sull'assenza di motivazione della decisione quanto ai due predetti profili («*sans pour autant contenir les constatations*» di cui al punto 83; «*ne fait pas état*» di cui al punto 89), i giudici di Lussemburgo non si sono limitati a rilevare solo una lacuna motivazionale della stessa, ma hanno fornito anche criteri interpretativi (punti 91-95) che dovranno essere seguiti dall'esecutivo europeo nella nuova decisione Approdo sicuro. Riprendendo principi già elaborati nella sentenza *Digital Rights Ireland*, la Corte, dopo aver ricordato che la sicurezza nazionale è un principio fondamentale dell'UE che consente di derogare al diritto, parimenti essenziale, alla tutela dei dati personali (punto 87), ha precisato che i casi nei quali le autorità pubbliche degli Stati tanto membri (*Digital Rights Ireland*) quanto terzi (*Schrems*) possono accedere ai dati personali UE devono essere disciplinate da regole chiare, precise e prevedibili (punto 91), nonché essere ammessi solo quando strettamente necessario (punto 92). Come rileva la stessa Corte di giustizia (punto 94), un sistema di *accesso generalizzato* al contenuto delle comunicazioni, quale sembra essere quello di cui alla decisione in esame, è lesivo dell'*essenza* del diritto fondamentale alla tutela dei dati. Anche considerato il paragrafo 1 dell'art. 52 della Carta UE dei diritti fondamentali, secondo cui «eventuali limitazioni all'esercizio dei diritti…riconosciuti dalla presente Carta devono…*rispettare il contenuto essenziale di detti diritti e libertà*», un'interferenza così ampia nel diritto della protezione dei dati personali UE da parte di autorità pubbliche (UE e a maggior ragione di uno Stato terzo) non sembra allora poter mai essere giustificata.

Il fatto poi che in *Schrems* i giudici di Lussemburgo applichino con riferimento a misure UE giustificate da esigenze di sicurezza nazionale i medesimi principi di *Digital Rights Ireland*, riguardanti invece i limiti che il diritto comune alla tutela dei dati personali può incontrare per lottare contro la criminalità (direttiva 2006/24), sottintende anche che i giudici UE non attribuiscono alcuna specificità alle misure adottate per motivi di sicurezza nazionale rispetto a quelle adottate su un'altra base giuridica. Ciò appare peraltro segnare una differenza tra la giurisprudenza UE e quella CEDU, avendo la Corte di Strasburgo attribuito agli Stati contraenti un margine di discrezionalità più ampio in materia di sicurezza nazionale rispetto ad altri ambiti (ad esempio sentenze CEDU 6 settembre 1978 *Klass e a. c. Germania*, serie A n. 28, par. 49; 26 marzo 1987, *Leander c. Svezia*,Serie A n. 116). Posto inoltre che i principi di cui alle sentenze *Digital Rights Ireland* e *Schrems* sono formulati in modo generale, essi sembrano doversi applicare non solo al diritto derivato UE ma anche a quello degli Stati membri, con la conseguenza che leggi nazionali in materia di sorveglianza, come quelle adottate di recente da Regno Unito e Francia, non prevedrebbero sufficienti limiti e salvaguardie tali da evitare una sorveglianza di massa da parte di autorità pubbliche e potrebbero pertanto non rispondere pienamente ai predetti requisiti.

Tali aspetti, unitamente a quelli già analizzati relativi ai poteri delle autorità garanti degli Stati membri di cui all'articolo 3, paragrafo 1, della decisione 2000/520, hanno indotto la Corte a dichiarare invalida, peraltro totalmente, la decisione Approdo sicuro, in tal modo confermando la soluzione di cui alla già citata pronuncia *Digital Rights Irland*.

Inoltre, e ancora una volta in modo analogo alla sentenza *Digital Rights Irland*, i giudici UE hanno parimenti deciso di annullare la predetta decisione con effetti *ex tunc* (nella causa *Digital Rights Irland*

la proposta di sospendere l'applicazione della direttiva annullata solo per il futuro era invero stata avanzata dell'avvocato generale ai punti 154-158 delle sue conclusioni). La scelta di non limitare gli effetti nel tempo della sentenza, la quale può essere effettuata (i) qualora vi sia un rischio di *gravi ripercussioni economiche* in virtù dell'elevato numero di rapporti giuridici costituiti in buona fede, e (ii) in presenza di una obiettiva e rilevante *incertezza giuridica* (tra le tante, sentenza 8 aprile 1976, 43/75, *Defrenne II*), sorprende un po'. Pur se la limitazione *ex nunc* degli effetti di sentenze pregiudiziali è eccezionale nel sistema UE, le due predette condizioni sembrano integrate nel caso in esame. A seguito della sentenza *Scherms*, i trasferimenti di dati personali a fini commerciali tra UE e USA, ossia un aspetto essenziale degli scambi commerciali, non si possono più basare sulle regole Approdo sicuro. Ciò ha un impatto significativo non solo sulle 4.500 imprese localizzate negli USA destinatarie di dati UE e che, ormai da quindici anni, utilizzano ogni giorno e in buona fede tali principi, ma anche sulle imprese che usano le regole Approdo sicuro per trasferire dati dalla UE. Tutto ciò può quantomeno creare gravi ripercussioni economiche, nonché incertezza giuridica. Posto inoltre che le sentenze pregiudiziali costruiscono dei precedenti, pur se non insuperabili, la pronuncia in esame crea incertezza giuridica anche per trasferimenti di dati UE verso tutti gli altri Stati terzi che negli ultimi anni abbiano, al pari degli USA, ottenuto l'adeguatezza dalla Commissione (ossia Andorra, Argentina, Canada, Isole Faeroe, Guernsey, Israele, Isola di Man, Jersey, Nuova Zelanda, Svizzera, Uruguay). E non solo: a seguito della predetta pronuncia, l'autorità garante della Svizzera, la quale ha un accordo (*US-Swiss Safe Harbor*) sul modello dell'Approdo sicuro UE-USA, ha affermato che, finché la Svizzera non negozierà un nuovo accordo con il governo USA, l'accordo *US-Swiss Safe Harbor* non costituisce più una base legale sufficiente per la trasmissione dei dati personali agli USA compatibile con la legge elvetica sulla protezione dei dati. L'incertezza giuridica determinata dalla sentenza in esame non è, in altri termini, circoscritta solo al territorio dell'Unione o a quelli di Stati terzi che abbiano concluso accordi nella materia in esame con l'UE, ma anche in paesi terzi che abbiano adottato atto anche solo modellati su quelli UE. La decisione della Corte di non limitare gli effetti nel tempo della sentenza si potrebbe allora spiegare solo per il fatto che nel caso di specie essa accerti la violazione di un diritto fondamentale, ossia una violazione del diritto UE di particolare gravità, in tal modo confermando l'approccio già seguito in merito in *Digital Rights Irland*.

La stessa Corte pare tuttavia consapevole delle gravi ripercussioni economiche e delle incertezza giuridica che la sentenza può effettivamente generare. Nonostante i giudici UE, al pari di ogni magistratura, "parlino solo attraverso le proprie pronunce", il 13 ottobre 2015 il nuovo presidente della Corte di giustizia dell'UE, *Koen Lenaerts*, derogando a tale principio generale, ha per la prima volta rilasciato una intervista al *Wall Street Journal* proprio al fine di chiarire la sentenza in esame. Non è quindi esclusivamente per il suo solo contenuto che la sentenza in commento si presenta come un precedente di prima importanza.

Pubblicato il: 02/11/2015
Autore: Serena Crespi
Categorie: articoli ,
Tag: Facebook, privacy, tutela dei dati personali

Editore: Bruno Nascimbene, Milano
Rivista registrata presso il Tribunale di Milano, n. 278 del 9 settembre 2014