Dottorato di ricerca in Ordine internazionale e diritti umani, Sapienza, Università di Roma - Intercenter, Università di Messina

Ordine internazionale e diritti umani

International Legal Order and Human Rights
Ordenamiento Jurídico Internacional y Derechos Humanos
Ordre juridique international et Droits de l'Homme

OSSERVATORIO SU COMMERCIO INTERNAZIONALE E DIRITTI UMANI N. 4/2020

1. IL TRASFERIMENTO DEI DATI PERSONALI AL DI FUORI DELL'UE ALLA LUCE DEL DIRITTO FONDAMENTALE ALLA PROTEZIONE DEI DATI NELLA RECENTE GIURISPRUDENZA DELLA CORTE DI GIUSTIZIA

1. La Grande Sezione della Corte di Giustizia dell'Unione europea, in data 16 luglio 2020, si è pronunciata su una domanda pregiudiziale proposta dalla *High Court* irlandese in merito all'interpretazione e alla validità della normativa UE sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali e, in particolare, dell'art. 3, par. 2, primo trattino, degli artt. 25 e 26, nonché dell'art. 28, par. 3, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati alla luce dell'art. 4, par. 2, TUE e degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea, della decisione 2010/87/UE della Commissione, del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46, come modificata dalla decisione di esecuzione (UE) 2016/2297 della Commissione, del 16 dicembre 2016 (in seguito «decisione CPT»), nonché della decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46 (*C-311/18, Data Protection Commissioner c. Facebook Ireland Ltd e Maximilliam Schrems*).

Ricordiamo che questa controversia è collegata a quella già decisa dalla Corte di giustizia con la *sentenza del 6 ottobre 2015, causa C-362/14 Maximillian Schrems c. Data Protection Commissioner*, che aveva già invalidato il regime UE-USA di c.d. «approdo sicuro» (con cui la Commissione, senza averne le competenze, aveva privato le autorità di sorveglianza degli Stati membri dei loro poteri nel caso in cui una persona avesse contestato la compatibilità dei principi di approdo sicuro con la tutela della vita privata e delle libertà e diritti fondamentali delle persone; in dottrina si veda M. NINO, *La Corte di giustizia UE dichiara l'invalidità del sistema di Safe Harbour: la sentenza Schrems*).

A seguito di questa sentenza e del successivo annullamento, ad opera del giudice irlandese, della decisione di rigetto di una precedente denuncia del sig. Schrems, l'autorità di controllo irlandese aveva infatti invitato quest'ultimo a riformulare la sua precedente denuncia, tenendo conto della dichiarazione di invalidità della decisione 2000/520. Nella sua riformulazione, che è all'origine del procedimento che ha generato la sentenza del 2020, il sig. Schrems ha sostenuto che gli Stati Uniti non offrono ancora una protezione sufficiente per i dati ivi trasferiti, e ha chiesto quindi di sospendere o vietare, per il futuro, i trasferimenti dei suoi dati personali dall'Unione verso gli Stati Uniti, trasferimenti che Facebook Ireland Ltd.

effettua invece sistematicamente in applicazione di «clausole tipo» di protezione contenute nell'allegato della decisione 2010/87/UE.

Il Commissario irlandese per la protezione dei dati personali, ritenendo che la sua decisione sulla denuncia del sig. Schrems dipendesse dalla validità della decisione 2010/87/UE, nell'ambito del procedimento instaurato in sede nazionale, ha sollecitato la High Court affinché presentasse alla CGUE una domanda di pronuncia pregiudiziale.

Va pure detto che, successivamente all'avvio di detto procedimento, la Commissione ha adottato la decisione (UE) 2016/1250 sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy.

2. Prima di passare all'analisi delle motivazioni della Corte di Giustizia, è opportuno fare un breve *excursus* sul quadro giuridico di riferimento.

Il contesto normativo in cui la vicenda in esame va inquadrata è costituito dalla direttiva 95/46/CE del 24 ottobre 1995, poi abrogata dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (*General Data Protection Regulation*, «GDPR»). Con la direttiva 95/46 il legislatore europeo intendeva fissare alcuni criteri comuni al fine di garantire un'omogenea protezione dei dati personali nel territorio europeo. Tuttavia, la diversa interpretazione delle norme comunitarie da parte degli Stati membri ha impedito un'effettiva armonizzazione normativa in materia. Il legislatore europeo ha così deciso di sostituire lo strumento della direttiva con quello del regolamento al fine di introdurre un quadro normativo in materia di protezione dei dati più coerente e omogeneo (*v.* C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*)

Ricordiamo che nell'ordinamento dell'Unione europea la protezione delle persone fisiche con riguardo al trattamento dei dati personali è espressamente elevata al rango di diritto fondamentale dall'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea e dall'art. 16, par. 1, del Trattato sul funzionamento dell'Unione europea («TFUE»), i quali riconoscono il diritto di ogni persona alla protezione dei dati di carattere personale che la riguardano, come riportato anche nel considerando 1 del GDPR (sul tema in dottrina *v.* F. ROSSI DEL POZZO, *La giurisprudenza della Corte di giustizia sul trattamento dei dati personali*, pag 11).

Peraltro, l'art. 45, par. 1, GDPR in parte corrispondente al precedente art. 25, par. 2, della direttiva abrogata, rubricato «Trasferimento sulla base di una decisione di adeguatezza», riconosce il potere della Commissione di decidere se un paese terzo, un territorio, un settore specifico di un territorio o un'organizzazione internazionale offrono un livello adeguato di protezione dei dati. In tal caso, i trasferimenti di dati personali verso tale paese terzo od organizzazione internazionale possono avere luogo senza ulteriori autorizzazioni; allo stesso modo la Commissione può decidere di revocare una tale decisione.

A tale riguardo ricordiamo che nei punti 139 e seguenti delle Conclusioni dell'Avvocato generale Yves Bot presentate il 23 settembre 2015 nella già citata causa C-362/14 *Maximillian Schrems c. Data Protection Commissioner*, relativamente alla «nozione di livello di protezione adeguato», è chiarito come tale espressione debba essere intesa nel senso di «un livello di protezione sostanzialmente equivalente a quello offerto» nell'UE «anche se le modalità di tale protezione possono essere diverse da quelle generalmente vigenti all'interno dell'Unione». Tuttavia, continua l'Avvocato generale, l'adeguatezza del livello di protezione offerto da un paese terzo è una situazione in continua evoluzione, che può mutare nel tempo a seconda 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 offerto da un paese terzo. E la Commissione, con la decisione del 12 luglio 2016, riconosceva che gli Stati Uniti, mediante lo «scudo», garantivano un livello di protezione adeguato dei dati personali ivi trasferiti, poiché era assicurato, nel complesso, un livello di protezione sostanzialmente equivalente a quello dei principi fondamentali stabiliti nella direttiva 95/46/CE, ed erano altresì previsti efficaci meccanismi interni di vigilanza e di ricorso.

Il meccanismo del *Privacy Shield* entrava in vigore il 1 agosto 2016, colmando il vuoto temporaneamente lasciato dal *Safe Harbor* («Approdo sicuro»), il sistema volontario di autocertificazione a cui in passato erano tenute ad uniformarsi le organizzazioni americane che ricevevano dati personali dall'Unione europea, ritenuto illegittimo (*v.* G. SCHARCHILLO, *Dal Safe Harbor al Privacy Shield. Il trasferimento di dati personali verso gli Stati Uniti dopo la sentenza Schrems*).

Inoltre occorre ricordare che, ai sensi dell'art. 288, quarto comma, TFUE, una decisione di adeguatezza della Commissione ha carattere vincolante per gli Stati membri destinatari (C-69/13, Mediaset SpA c. Ministero dello Sviluppo economico punto 23). Pertanto, i loro organi, fra i quali figurano le autorità di controllo, e nel caso specifico il *Data Protection Commissioner*, l'autorità di supervisione irlandese, non possono adottare misure contrarie a dette decisioni, come ad esempio sospendere o vietare trasferimenti di dati personali verso enti ritenuti idonei. D'altro canto una decisione di tale natura non può né elidere né ridurre i poteri espressamente riconosciuti alle autorità nazionali di controllo dall'art. 8, par. 3 della Carta, nonché dall'art. 28 della direttiva 95/46, oggi sostituito dall'art. 51 del RGPD (C-362/14, *Maximillian Schrems c. Data Protection Commissioner* punto 53).

Ricordiamo pure che la Corte ha competenza esclusiva nel dichiarare l'invalidità di un atto dell'Unione, e nel caso anche di una decisione della Commissione adottata in applicazione dell'art. 25, par. 6, della direttiva 95/46, al fine di garantire il primato del diritto dell'Unione (giurisprudenza richiamata in C-188/10 e C-189/10, Melki e Abdeli punto 52 e 53).

È sulla base di queste norme che la Corte, con la sentenza del 16 luglio 2020, ha potuto esaminare e quindi dichiarare invalida la decisione in esame di adeguatezza già adottata dalla Commissione.

3. Passando all'analisi delle motivazioni, la Corte, cumulando una serie di questioni, ha affrontato il delicato profilo della conformità della decisione «scudo per la privacy» in rapporto alle norme del GDPR, lette alla luce della Carta.

In particolare, la Corte ha dovuto verificare se gli Stati Uniti garantissero effettivamente un livello adeguato di protezione in rapporto all'articolo 45 del GDPR, in base agli artt. 7, 8 e 47 della Carta.

In primo luogo, è necessario evidenziare che la Carta tutela distintamente il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali, rispettivamente negli articoli 7 e 8. Inoltre, nonostante l'art. 8 abbia avuto il merito di aver inizialmente codificato il diritto alla privacy, quest'ultimo è ormai concettualmente distinto da quello al trattamento dei dati personali (in dottrina I. A. GAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale*, pag. 8). Richiamando le parole di Rodotà nel Discorso conclusivo della Conferenza internazionale sulla protezione dei dati, esso peraltro si proietta ben al di là della sfera privata, divenendo elemento costitutivo della cittadinanza del nuovo millennio.

Alla luce di una giurisprudenza consolidata della Corte, il diritto alla protezione dei dati personali ha natura relativa, cioè esso non costituisce un diritto assoluto, ma va considerato sulla base della sua funzione sociale: ne consegue che possono essere apportate restrizioni all'esercizio di tale diritto, a condizione che le stesse rispondano effettivamente ad obiettivi di interesse generale e non costituiscano, rispetto allo scopo perseguito, un intervento sproporzionato, tale da ledere la sostanza stessa dei diritti tutelati (cfr. la sentenza C-112/00, *Eugen Schmidberger, Internationale Transporte und Planzüge e Repubblica d'Austria,* punto 80).

L'art. 8, par. 2, della Carta, infatti, autorizza, a determinate condizioni, il trattamento dei dati personali, nel rispetto del «principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge».

L'art. 52, par. 1, della Carta, che tratta delle limitazioni ai diritti ivi contemplati, utilizza poi una formula ispirata alla giurisprudenza costante della Corte di Giustizia, secondo la quale le restrizioni all'esercizio dei diritti fondamentali possono essere operate purché rispondano effettivamente a finalità di interesse generale perseguite dalla Comunità (C-292/97, *Kjell Karlsson e a.,* punto 45). Secondo l'articolo in questione, le limitazioni all'esercizio di questi diritti sono consentite purché siano previste dalla legge, rispettino il contenuto essenziale di detti diritti e libertà, il principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

L'Avvocato generale Henrik Saugmandsgaard Øe, nelle conclusioni presentate il 19 dicembre 2019 sulla causa C-311/18, ha pure chiarito come qualsiasi ingerenza nell'esercizio dei diritti garantiti dagli artt. 7 e 8 della Carta debba essere soggetta a un rigoroso controllo di proporzionalità. Richiamando la giurisprudenza costante della Corte, il principio di proporzionalità esige che gli atti delle istituzioni dell'Unione siano idonei a realizzare obiettivi legittimi e non superino i limiti di ciò che è necessario e idoneo e al conseguimento di tali obiettivi (*v.* C-293/12 e C-594/12, Digital Rights Ireland Ltd e Kärntner Landesregierung punto 46). Il test di proporzionalità è spesso rivendicato dalla Corte al fine di valutare la compatibilità delle scelte del legislatore europeo con i principi sanciti dalla Carta. La costante applicazione di questa tecnica decisionale ha portato ad una riflessione di carattere generale sulla tendenza della Corte ad impiegare la Carta come parametro di giudizio (*v.* V. FIORILLO, *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali*).

Tornando al caso in esame, la Corte ha evidenziato come l'accesso ai dati personali da parte di un'autorità pubblica, e nello specifico di quelle autorità che gestiscono i programmi di sorveglianza degli Stati Uniti, costituisca un'ingerenza nei diritti fondamentali sanciti dagli artt. 7 e 8 della Carta e quindi non garantisca un livello di protezione sostanzialmente equivalente a quello richiesto dall'art. 52, par. 1, seconda frase, della stessa Carta (punto 185). La Corte europea fa riferimento alla *Foreign Intelligence Surveillance Court* (FISC), la Corte federale degli Stati Uniti istituita sotto il *Foreign Intelligence Surveillance Act* (FISA) del 1978, che ai sensi dell'articolo 702 FISA, non incontra limitazioni nell'autorizzare i programmi di sorveglianza, né l'esercizio dell'attività della FISC è accompagnato da garanzie per i cittadini stranieri potenzialmente oggetto del programma, e all'Executive Order 12333 (E.O. 12333) che ha lo scopo di ampliare i poteri e le responsabilità delle agenzie d'intelligence degli Stati Uniti, senza tuttavia conferire diritti nei confronti delle autorità statunitensi. Per questi motivi, tali articoli non garantiscono un livello di tutela equivalente a quello richiesto all'interno dell'Unione.

In secondo luogo, l'art. 47 della Carta esige che ogni individuo, i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati, abbia diritto ad un ricorso effettivo dinanzi ad un giudice, nel rispetto di determinate condizioni: ciò è espressione del principio generale del diritto ad un sindacato giurisdizionale (*v. C-222/84, Marguerite Johnston e Chief Constable of The Royal Ulster Constabulary* punto 18).

Ora, va detto che la giurisprudenza europea sviluppatasi intorno al diritto affermato nell'articolo 47 della Carta è molto vasta: limitandoci ad alcuni cenni, ricordiamo come la sentenza Les Verts riconosca quale «elemento fondante lo stato di diritto dell'Union europea la possibilità di sindacare la validità degli atti delle istituzioni europee». Ed è in applicazione di questo principio che il considerando 104 del RGPD sostiene che i Paesi terzi dovrebbero riconoscere ai soggetti interessati «diritti effettivi e azionabili e un mezzo di ricorso effettivo in sede amministrativa e giudiziale al fine di garantire un adeguato livello di protezione sostanzialmente equivalente a quello assicurato all'interno dell'Unione».

Inoltre, la «decisione scudo per la privacy» prevede l'istituzione di un meccanismo di mediazione da parte delle autorità statunitensi, inizialmente considerato dalla Commissione sufficiente a garantire un mezzo di ricorso effettivo per coloro i cui dati personali fossero stati oggetto di trasferimento ai sensi dell'articolo 45, paragrafo 2, lettera a) del GDPR. Tuttavia, l'indipendenza del Mediatore rispetto al potere esecutivo è stata messa in discussione, poiché tale organo viene designato dal Segretario di Stato ed è tenuto a riferire direttamente a quest'ultimo. La Corte è giunta quindi alla conclusione che questo meccanismo non offre una garanzia sostanzialmente equivalente a quella richiesta dall'art. 47 della Carta; né i programmi fondati sull' E.O 12333 né quelli sull'articolo 702 FISA garantiscono il diritto ad un ricorso effettivo.

Per i motivi elencati, la Corte ha ritenuto che il livello di protezione offerto dagli Stati Uniti non è tale da giustificare una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, del GDPR.

4. L'invalidità sancita dalla Corte, comunque, non pare creare un vero e proprio vuoto giuridico, in quanto gli articoli 46 e 49 del GDPR stabiliscono comunque a quali condizioni possano avere luogo trasferimenti dei dati personali verso paesi terzi in assenza di una decisione della Commissione (punto 202).

In primo luogo, ai sensi dell'art. 46, parr. 1 e 2, che riprende l'ormai abrogato art. 26, par. 2, della direttiva 95/46, in assenza di una decisione di adeguatezza, il titolare può autorizzare il trasferimento dei dati personali ad un paese terzo «solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi».

Il par. 2, lett. c) dell'art. 46 del GDPR riconosce quali garanzie adeguate «le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2».

Tra queste rientrano le clausole contrattuali tipo allegate alla decisione 2010/87.

Merita di essere sottolineato che «la decisione CPT» non è una decisione di adeguatezza ai sensi dell'art. 45, par. 3, del GDPR, in quanto la Commissione non giunge a constatare se un paese terzo, un territorio o uno o più settori di quest'ultimo offrano un livello adeguato di protezione. Le clausole tipo ad essa allegate, difatti, data la loro natura contrattuale, non vincolano le autorità pubbliche dei paesi terzi, ma mirano a fornire ai titolari o ai responsabili del trattamento stabiliti nell'Unione garanzie contrattuali uniformemente applicabili. Inoltre, non è escluso che possano adottarsi misure supplementari al fine di garantire il livello di protezione richiesto dall'Unione. A tal riguardo, il considerando 109 del regolamento prevede

che i titolari o i responsabili del trattamento possano includere «tali clausole tipo in un contratto più ampio» o «aggiungere altre clausole o garanzie supplementari, purché non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo adottate dalla Commissione o da un'autorità di controllo o ledano i diritti o le libertà fondamentali degli interessati».

Inoltre, la «decisione CPT» prevede dei meccanismi efficaci che permettono di garantire il rispetto del livello di protezione adeguato richiesto dall'Unione.

Essa impone infatti all'esportatore e all'importatore di dati di verificare, prima del trasferimento, se il livello di protezione è rispettato nel paese terzo: la clausola 5, lettera *a)*, richiede, in particolare, che l'importatore si impegni a informare prontamente l'esportatore qualora non possa ottemperare per qualsiasi ragione agli obblighi che incombono in forza del contratto concluso. In questo caso «l'esportatore ha facoltà di sospendere il trasferimento e/o risolvere il contratto». Ai sensi della lettera b) del medesimo articolo, l'importatore è poi tenuto ad informare l'esportatore se la legislazione del paese terzo gli impedisce di uniformarsi alle clausole tipo in questione. In ogni caso, ai sensi della clausola 6, qualora l'interessato abbia subito un pregiudizio può ottenere il risarcimento del danno sofferto.

È alla luce di queste considerazioni, quindi, che la Corte ha fatto salva la «decisione CPT» così come modificata dalla decisione di esecuzione (UE) 2016/2297 della Commissione, in quanto questa prevede dei meccanismi efficaci di sospensione o divieto del trasferimento qualora il destinatario non abbia rispettato dette clausole o si sia trovato nell'impossibilità di rispettarle.

Per quanto riguarda ulteriori modalità residue di trasferimento dei dati personali verso paesi terzi, nello specifico nei confronti degli Stati Uniti, in attesa di un nuovo accordo quadro, è necessario utilizzare i mezzi forniti dal GDPR.

A tal fine ricordiamo che l'art. 46, par. 2, lett. *b),* del regolamento riconosce come garanzie adeguate le norme vincolanti d'impresa (*Binding Corporate Rules*, BCR) di cui all'art. 47 del GDPR, cioè le norme approvate dall'autorità di controllo competente in base al meccanismo di conformità dell'arti. 63 del regolamento. Alle norme aziendali vincolanti possono aderire le società stabilite nell'UE che intendano trasferire i dati personali all'interno di un gruppo di imprese o imprese al di fuori dell'UE, fornendo la base per i trasferimenti effettuati solo all'interno del gruppo societario.

Il Gruppo di lavoro "Articolo 29" (*Article 29 Working Party*), gruppo di lavoro europeo indipendente che si occupava delle questioni relative alla protezione dei dati prima dell'entrata in vigore del GDPR e che ha cessato di esistere il 25 maggio 2018 per essere sostituito dallo European Data Protection Board (EDPB), ha elaborato una serie di documenti al fine di aiutare le imprese nell'elaborazione delle norme vincolanti d'impresa. In particolare, per agevolare il trasferimento dei dati sulla base delle norme vincolanti d'impresa, che necessita di un'autorizzazione delle autorità di protezione dei dati di ciascuno Stato membro dal quale la società multinazionale intende trasferire dati, il Gruppo ha predisposto una procedura di cooperazione che facilita l'approvazione delle "Binding Corporate Rules" in base al GDPR.

L'EDPB ha adottato, il 23 luglio 2020, delle Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18, in cui ha specificato che la possibilità di trasferire o meno dati personali sulla base delle BCR dipenderà dall'esito di una valutazione, tenuto conto delle circostanze del trasferimento e delle misure supplementari eventualmente messe in atto. Tali misure supplementari dovrebbero garantire, unitamente alle BCR e alla luce di un'analisi caso per caso delle circostanze del trasferimento,

che la normativa statunitense non interferisca con l'adeguato livello di protezione richiesto dal diritto UE.

E, come stabilito al punto 145 della sentenza «Schrems II», qualora si giungesse alla conclusione che, tenuto conto delle circostanze del trasferimento e delle eventuali misure supplementari, non vi siano adeguate garanzie, occorrerà sospendere o vietare il trasferimento di dati personali o, in alternativa, informare l'autorità interna competente.

Ricordiamo pure che l'art. 49, rubricato «Deroghe in specifiche situazioni», elenca una serie di casi eccezionali in cui, anche in assenza di una decisione di adeguatezza ai sensi dell'art. 45, par. 3, o delle garanzie adeguate ai sensi dell'articolo 46 del GDPR, può avvenire il trasferimento dei dati personali verso un paese terzo.

A riguardo, l'EPDB ha adottato le linee guida 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679, in data 25 maggio 2018. Nel caso in cui, ad esempio, il trasferimento avvenga sulla base del par. 1, lettera a) dell'articolo, cioè nel caso in cui il soggetto interessato abbia esplicitamente acconsentito a tale trasferimento, il consenso in questione dovrà essere esplicito, specifico al tipo di trasferimento, e l'interessato dovrà essere informato sui possibili rischi del trasferimento. Nell'ipotesi del par. 1, lettera d), cioè «quando il trasferimento sia necessario per importanti motivi di interesse pubblico», le linee guida precisano che una discriminante fondamentale affinché operi la deroga è l'importanza dell'interesse e non la natura dell'organizzazione. Inoltre, nonostante in quest'ultimo caso il trasferimento possa non essere "occasionale", ciò non vuol dire che possa avvenire in maniera sistematica e generale.

Precisa ancora il Comitato che le deroghe di cui all'art. 49 rappresentano delle eccezioni al principio generale secondo cui i dati personali sono preferibilmente trasferiti verso paesi terzi in presenza di adeguate garanzie offerte da questi, oppure qualora siano state prodotte garanzie adeguate, e l'interessato goda quindi di diritti effettivi e azionabili. Per tali motivi, esse devono essere interpretate in maniera restrittiva, in modo che l'applicazione dell'art. 49 non diventi "la regola" ma rimanga limitata a specifiche situazioni.

Infine, il Comitato europeo per la protezione dei dati dovrà valutare le conseguenze della sentenza sugli strumenti di trasferimento diversi dalle clausole tipo e dalle norme vincolanti d'impresa.

5. Una prima valutazione sull'impatto della sentenza «Schrems II» è desumibile dal commento del Garante europeo per la protezione dei dati (*European data protection supervisor,* EPDS), il quale ha accolto positivamente le soluzioni della Corte di Giustizia, le quali hanno confermato l'importanza di un elevato livello di protezione nel trasferimento dei dati dall'UE verso Paesi terzi. Il Garante ha pure riconosciuto come i notevoli sviluppi legislativi fatti in tutto il mondo nell'ambito della protezione dei dati personali e della privacy elevino il livello di protezione dei dati personali da diritto fondamentale "europeo" a diritto fondamentale universalmente riconosciuto. Data la sua natura legata alla crescente centralità dello sviluppo delle tecnologie e dall'informazione, questo diritto è stato anche definito come un diritto dell'età tecnologica (*v.* M. GAMBINI, *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*).

Da un punto di vista pratico, poi, va detto che la dichiarazione di invalidità dell'accordo quadro «scudo per la privacy» non è accompagnata da alcun periodo di transizione. Dall'entrata in vigore dalla sentenza della Corte, qualsiasi trasferimento di dati verso gli Stati Uniti dovrà avvenire esclusivamente sulla base degli strumenti giuridici che abbiamo illustrato.

Ad esempio, qualora un soggetto, come ad es. *Facebook Ireland Ltd*, intenda trasferire dati personali negli Stati Uniti, nel caso di specie a *Facebook Inc.,* dovrà servirsi delle SCC o delle BCR, e ciò comunque con esiti incerti: infatti, la possibilità di trasferire dati personali sulla base di questi mezzi dipende da una valutazione che le parti ed eventualmente l'autorità di sorveglianza o i giudici degli stati membri o europei dovranno compiere, tenendo conto delle circostanze del trasferimento e delle misure supplementari eventualmente messe in atto.

Ad ogni modo la sentenza in commento conferma la centralità del ruolo delle autorità di sorveglianza degli Stati membri (*Data Protection Authority*, DPA), istituite ai sensi dell'art. 51 del GDPR, quale garanzia di difesa degli interessi dei singoli individui e del loro diritto fondamentale alla protezione dei dati in rapporto alle grandi compagnie situate nel mondo e vincolate a regole che variano da Stato a Stato.

PIETRO MATTIOLI