



Bruxelles, 6.11.2015
COM(2015) 566 final

**COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL
CONSIGLIO**

**relativa al trasferimento di dati personali dall'UE agli Stati Uniti d'America in
applicazione della direttiva 95/46/CE a seguito della sentenza della Corte di giustizia
nella causa C-362/14, (Schrems)**

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

relativa al trasferimento di dati personali dall'UE agli Stati Uniti d'America in applicazione della direttiva 95/46/CE a seguito della sentenza della Corte di giustizia nella causa C-362/14, (Schrems)

1. INTRODUZIONE: L'ANNULLAMENTO DELLA DECISIONE "APPRODO SICURO"

La sentenza della Corte di giustizia dell'Unione europea (in appresso: "la Corte di giustizia" o "la Corte"), del 6 ottobre 2015, nella causa C-362/14, (Schrems)¹ ribadisce l'importanza del diritto fondamentale alla protezione dei dati personali, come sancito nella Carta dei diritti fondamentali dell'UE, anche quando i dati sono trasferiti al di fuori dell'UE.

I trasferimenti di dati personali costituiscono un elemento fondamentale delle relazioni transatlantiche. L'UE è il più importante partner commerciale degli Stati Uniti, così come gli Stati Uniti sono il più importante partner commerciale dell'UE e i trasferimenti di dati, sempre più spesso, fanno parte integrante dei loro scambi commerciali.

Al fine di facilitare i flussi di dati, pur garantendo un elevato livello di protezione dei dati personali, la Commissione ha riconosciuto l'adeguatezza del quadro di "Approdo sicuro" (Safe Harbour) con l'adozione della decisione 2000/520/CE della Commissione del 20 luglio 2000 (in appresso: "la decisione Approdo sicuro"). Nella decisione, basata sull'articolo 25, paragrafo 6, della direttiva 95/46/CE², la Commissione ha riconosciuto che i principi di approdo sicuro e le domande più frequenti (FAQ) pubblicate sull'argomento dal Dipartimento del commercio degli Stati Uniti offrono una protezione adeguata ai fini del trasferimento dei dati personali dall'UE³. Di conseguenza, i dati personali potevano essere liberamente trasferiti dagli Stati membri dell'UE a società stabilite negli Stati Uniti che avevano sottoscritto i principi, nonostante l'assenza di una legge generale sulla protezione dei dati negli Stati Uniti. Il funzionamento degli accordi del tipo "Approdo sicuro" si fonda sull'autocertificazione del rispetto degli impegni da parte delle imprese aderenti. Benché l'adesione ai principi di approdo sicuro e alle domande più frequenti (FAQ) sia volontaria, tali impegni sono vincolanti ai sensi del diritto statunitense per le entità che li hanno sottoscritti e il loro rispetto può essere imposto dalla Federal Trade Commission statunitense⁴.

¹ Sentenza del 6 ottobre 2015 nella causa C-362/14, Maximilian Schrems/Commissario per la protezione dei dati, EU:C:2015:650 (in appresso anche: la "sentenza" o la "sentenza Schrems").

² 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 (GUL 281 del 23.11.95, pag. 31 ("direttiva 95/46/CE" o "la direttiva").

³ Ai fini della presente comunicazione, l'espressione "Unione europea" comprende anche il SEE. Di conseguenza, i riferimenti agli "Stati membri" devono essere intesi in modo da coprire anche gli Stati membri del SEE.

⁴ Per un approfondimento degli accordi del tipo "Approdo sicuro", si veda la comunicazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento dell'approdo sicuro dal punto di vista dei cittadini dell'UE e delle società stabilite nell'UE (COM/2013/847 final).

Nella sentenza del 6 ottobre 2015, la Corte ha dichiarato l'invalidità della decisione "Approdo sicuro". È in tale contesto che la presente comunicazione mira a fornire una panoramica degli strumenti alternativi che consentono i trasferimenti transatlantici di dati ai sensi della direttiva 95/46/CE in mancanza di una decisione di adeguatezza. Inoltre essa descrive in sintesi le conseguenze della sentenza per altre decisioni di adeguatezza della Commissione. Nella sentenza, la Corte ha chiarito che una decisione di adeguatezza a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE è subordinata all'accertamento da parte della Commissione dell'esistenza nel paese terzo interessato di un livello di protezione dei dati personali che, pur non necessariamente identico, è "sostanzialmente equivalente" a quello garantito nell'UE in virtù della direttiva, letta alla luce della Carta dei diritti fondamentali. Per quanto riguarda specificamente la decisione "Approdo sicuro", la Corte ha stabilito che essa non conteneva riscontri sufficienti da parte della Commissione sulle limitazioni in materia di accesso delle autorità pubbliche degli Stati Uniti ai dati trasferiti ai sensi di tale decisione e sull'esistenza di un'efficace tutela giuridica contro tali interferenze. In particolare, la Corte ha chiarito che si deve ritenere che una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata. Inoltre, la Corte ha confermato che, anche in caso di una decisione di adeguatezza a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE, le autorità degli Stati membri in materia di protezione dei dati (DPA) continuano ad avere il potere e il dovere di verificare, con assoluta indipendenza, se il trasferimento di dati verso un paese terzo rispetta i requisiti stabiliti dalla direttiva 95/46/CE, letto alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali. Tuttavia, la Corte ha anche affermato che soltanto la Corte di giustizia può dichiarare invalido un atto dell'Unione - qual è una decisione di adeguatezza della Commissione.

La sentenza della Corte si basa sulla comunicazione della Commissione del 2013 sul funzionamento del regime dell'approdo sicuro dal punto di vista dei cittadini dell'Unione e delle società ivi stabilite⁵, in cui la Commissione ha identificato una serie di carenze e ha proposto 13 raccomandazioni. Sulla base di tali raccomandazioni, la Commissione ha condotto trattative con le autorità statunitensi, a partire dal gennaio 2014, con l'obiettivo di mettere in atto un accordo rinnovato e rafforzato per gli scambi transatlantici di dati.

A seguito della sentenza, la Commissione ribadisce il proprio impegno a raggiungere l'obiettivo di un nuovo e solido quadro per i trasferimenti transatlantici di dati personali. A tale riguardo, essa ha immediatamente ripreso e intensificato i colloqui con il governo degli Stati Uniti per garantire che ogni nuovo accordo per i trasferimenti transatlantici di dati personali sia pienamente in linea con le norme stabilite dalla Corte. Tale quadro deve quindi disporre di sufficienti limitazioni, garanzie e meccanismi di controllo giurisdizionale volti a garantire la continuità della protezione dei dati personali dei cittadini dell'UE anche per

⁵ 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, del 27.11.2013). Cfr. anche la comunicazione della Commissione al Parlamento europeo e al Consiglio, "Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA" COM(2013) 846 final, del 27.11.2013, e il relativo memorandum "Restoring Trust in EU-US data flows – Frequently Asked Questions" (ripristinare la fiducia nei flussi di dati tra UE e Stati Uniti — Domande più frequenti, MEMO/13/1059, 27.11.2013).

quanto riguarda l'eventuale accesso da parte delle autorità pubbliche ai fini dell'applicazione della legge e della sicurezza nazionale. Nel frattempo, sono state espresse preoccupazioni da parte dell'industria per quanto riguarda le possibilità di proseguire i trasferimenti di dati⁶. È pertanto necessario chiarire le condizioni in base alle quali tali trasferimenti possano continuare. Ciò ha indotto il Gruppo di lavoro "Articolo 29" — l'organo consultivo indipendente che riunisce i rappresentanti di tutte le autorità di protezione dei dati degli Stati membri e il garante europeo della protezione dei dati — a rendere pubblica, il 16 ottobre, una dichiarazione⁷ riguardante le prime conclusioni da trarre dalla sentenza. Tra l'altro, tale dichiarazione contiene i seguenti orientamenti per il trasferimento dei dati:

- l'accordo sull'approdo sicuro ("Safe Harbour") non può più costituire la base giuridica per i trasferimenti di dati personali;
- le clausole contrattuali tipo e le norme vincolanti d'impresa possono nel frattempo essere utilizzate come base per i trasferimenti di dati, anche se il Gruppo di lavoro "Articolo 29" ha dichiarato, tra l'altro, che continuerà ad analizzare l'impatto della sentenza su tali strumenti alternativi.

La dichiarazione invita altresì gli Stati membri e le istituzioni dell'UE ad avviare discussioni con le autorità statunitensi al fine di trovare soluzioni tecniche e giuridiche per i trasferimenti di dati; i negoziati per un nuovo accordo "Approdo sicuro" potrebbero, a parere del Gruppo di lavoro "Articolo 29", essere parte di tale soluzione.

Il Gruppo di lavoro "Articolo 29" ha annunciato che, qualora entro la fine di gennaio 2016, non si trovasse una soluzione concordata con le autorità statunitensi, e in base alla valutazione di strumenti alternativi per i trasferimenti di dati, le autorità di protezione dei dati adotterà tutti i provvedimenti necessari e opportuni, compresa un'azione di contrasto coordinata.

Infine, il Gruppo di lavoro "Articolo 29" ha sottolineato la responsabilità condivisa delle autorità di protezione dei dati, le istituzioni dell'UE, gli Stati membri e le imprese nella ricerca di soluzioni sostenibili per dare esecuzione alla sentenza della Corte. In particolare, il Gruppo di lavoro ha esortato le imprese a valutare la possibilità di introdurre qualsiasi soluzione tecnica e giuridica per attenuare eventuali rischi che corrono quando trasferiscono i dati.

⁶ I rappresentanti delle associazioni industriali hanno espresso queste preoccupazioni, tra l'altro, a un incontro organizzato poco dopo la sentenza Schrems dal Vicepresidente Anspic e i Commissari Oettinger e Jourová in data 14 ottobre. Cfr. Daily News del 14.10.2015 (MEX/15/5840). Si veda anche: "Lettera aperta sull'attuazione della sentenza della Corte di giustizia nella causa C-362/14 Maximilian Schrems/Data Protection Commissioner", datata 13 ottobre 2015, inviata al presidente della Commissione, Jean-Claude Juncker, e firmato da varie associazioni e società dell'industria dell'UE e degli Stati Uniti: http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=1045&PortalId=0&TabId=353.

⁷ Dichiarazione del Gruppo di lavoro "Articolo 29", disponibile al seguente indirizzo Internet: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

La presente comunicazione lascia impregiudicati i poteri e i compiti dell'autorità di protezione dei dati di esaminare la legittimità di tali trasferimenti in piena indipendenza⁸. Essa non stabilisce regole vincolanti e rispetta pienamente il potere dei giudici nazionali di interpretare il diritto applicabile e, se necessario, di operare un rinvio alla Corte di giustizia per una pronuncia in via pregiudiziale. Né può la presente comunicazione costituire la base per qualsiasi diritto individuale o collettivo o una domanda di risarcimento.

2. BASI ALTERNATIVE PER I TRASFERIMENTI DI DATI PERSONALI VERSO GLI STATI UNITI.

Le norme in materia di trasferimenti internazionali di dati, di cui alla direttiva 95/46/CE sono basate su una chiara distinzione tra, da un lato, i trasferimenti di dati verso paesi terzi che garantiscono un livello di protezione adeguato (articolo 25 della direttiva) e, dall'altro, i trasferimenti verso paesi terzi che non garantiscono in modo accertato una tutela adeguata (articolo 26 della direttiva).

La sentenza Schrems verte sulle condizioni alle quali, ai sensi dell'articolo 25, paragrafo 6, della direttiva 95/46/CE, la Commissione può decidere che un paese terzo garantisce un livello di protezione adeguato.

Se il paese terzo verso il quale i dati personali devono essere esportati dall'UE non garantisce - in modo accertato - un tale livello adeguato di protezione, l'articolo 26 della direttiva 95/46/CE prevede una serie di motivi alternativi sulla base dei quali il trasferimento può avvenire ugualmente. In particolare il trasferimento può essere effettuato se il soggetto competente a determinare le finalità e i mezzi del trattamento di dati personali (il "responsabile del trattamento"):

- fornisce adeguate garanzie, ai sensi dell'articolo 26, paragrafo 2, della direttiva 95/46/CE, relative alla protezione della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché all'esercizio di tali diritti. Dette garanzie possono segnatamente essere fornite mediante clausole contrattuali che vincolano l'esportatore e l'importatore dei dati (cfr. sezioni 2.1 e 2.2). Queste includono le clausole contrattuali tipo emesse dalla Commissione e, riguardo ai trasferimenti tra le diverse entità di un gruppo societario multinazionale, le norme vincolanti d'impresa autorizzate dalle autorità di protezione dei dati; oppure
- si basa su una delle deroghe espressamente elencate alle lettere da a) a f) dell'articolo 26, paragrafo 1, della direttiva 95/46/CE (cfr. sezione 2.3).

Rispetto alle decisioni di adeguatezza risultanti dalla valutazione globale del sistema di un determinato paese terzo e che possono in linea di principio contemplare tutti i trasferimenti verso tale sistema, queste basi alternative per i trasferimenti hanno entrambe un campo di

⁸ Cfr. articolo 8, paragrafo 3 della Carta dei diritti fondamentali dell'UE e articolo 16, paragrafo 2, del TFUE. Tale indipendenza è stata evidenziata anche dalla Corte nella sua sentenza Schrems.

applicazione più limitato (dato che si applicano soltanto a specifici flussi di dati) e una più ampia copertura (in quanto non sono necessariamente confinate a un paese specifico). Esse si applicano ai flussi di dati effettuati da particolari entità che hanno deciso di avvalersi di una delle possibilità offerte dall'articolo 26 della direttiva 95/46/CE. Inoltre, quando fondano i loro trasferimenti su tali motivi, e poiché non possono basarsi su un accertamento di adeguatezza del paese terzo contenuto in una decisione della Commissione, gli esportatori e gli importatori di dati hanno la responsabilità di garantire che i trasferimenti sono conformi ai requisiti della direttiva.

2.1. Soluzioni contrattuali

Come sottolineato dal Gruppo di lavoro "Articolo 29", al fine di offrire garanzie sufficienti ai fini dell'articolo 26, paragrafo 2, della direttiva 95/46/CE, le clausole contrattuali devono "compensare in modo soddisfacente la mancanza di un livello generale di protezione adeguata e comportare gli elementi essenziali di tutela che possono mancare in una qualsiasi situazione particolare"⁹. Al fine di facilitare l'uso di tali strumenti nei trasferimenti internazionali, la Commissione ha approvato, a norma dell'articolo 26, paragrafo 4, della direttiva, quattro serie di clausole contrattuali tipo ritenute conformi alle prescrizioni dell'articolo 26, paragrafo 2, della direttiva. Due serie di clausole tipo si riferiscono a trasferimenti tra responsabili del trattamento¹⁰, mentre le altre due serie di clausole tipo trattano i trasferimenti tra il responsabile del trattamento e l'incaricato del trattamento che agiscono sotto le sue istruzioni¹¹. Ciascuna di tali serie di clausole tipo stabilisce i rispettivi obblighi degli esportatori e degli importatori di dati. Sono compresi gli obblighi per quanto riguarda, tra l'altro, le misure di sicurezza, le informazioni della persona interessata in caso di trasferimento di dati sensibili, la notifica all'esportatore di dati di richieste di accesso da parte delle autorità di contrasto dei paesi terzi o di qualsiasi accesso accidentale o non autorizzato e i diritti delle persone interessate all'accesso, rettifica e cancellazione dei propri dati personali, nonché le norme in materia di compensazione per la persona interessata in caso di danni derivanti da una violazione di una delle parti delle clausole contrattuali tipo. Le clausole tipo stabiliscono anche che le persone interessate dell'UE hanno la possibilità di far valere dinanzi un'autorità di protezione dei dati e/o un organo giurisdizionale dello Stato membro in cui è stabilito l'esportatore di dati i diritti che loro derivano dalle clausole contrattuali in qualità di

⁹ Cfr. Gruppo di lavoro "Articolo 29", "Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla protezione dei dati" (WP12), 24 luglio 1998, pag. 16.

¹⁰ Decisione 2001/497/CE della Commissione, del 15 giugno 2001, relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/CE (GU L 181 del 4.7.2001, pag. 19), e decisione 2004/915/CE della Commissione, del 27 dicembre 2004, che modifica la decisione 2001/497/CE per quanto riguarda l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi (GU L 385 del 29.12.2004, pag. 74).

¹¹ Decisione 2002/16/CE della Commissione, del 27 dicembre 2001, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio (GU L 6 del 10.1.2002, pag. 52), e decisione 2010/87/UE della Commissione, del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio (GU L 39 del 12.2.2010, pag. 5). La prima decisione, che è stata abrogata dalla seconda, si applica esclusivamente ai contratti conclusi prima del 15 maggio 2010.

terzo beneficiario¹². Tali diritti e obblighi sono necessari nelle clausole contrattuali perché, contrariamente alla situazione in cui la Commissione ha compiuto un accertamento di adeguatezza, non si può presumere che l'importatore di dati del paese terzo rientri in un adeguato sistema di sorveglianza e esecuzione delle norme sulla protezione dei dati.

Poiché le decisioni della Commissione sono obbligatorie in tutti i loro elementi per gli Stati membri, inserire le clausole contrattuali tipo in un contratto implica che le autorità nazionali sono in linea di principio tenute all'obbligo di accettare tali clausole. Di conseguenza, esse non possono rifiutare il trasferimento dei dati verso un paese terzo unicamente sulla base del fatto che queste clausole contrattuali tipo non offrono sufficienti garanzie. Ciò lascia impregiudicato il loro potere di esaminare tali clausole alla luce dei requisiti stabiliti dalla Corte nella sentenza Schrems. In caso di dubbi, esse dovrebbero intentare una causa dinanzi a un tribunale nazionale, il quale a sua volta può presentare una domanda di pronuncia pregiudiziale alla Corte di giustizia. Benché non vi sia alcun obbligo di preventiva autorizzazione nazionale per procedere al trasferimento nella legislazione che recepisce la direttiva 95/45/CE della maggior parte degli Stati membri, alcuni Stati membri mantengono un sistema di notifica e/o di autorizzazione preventiva per l'utilizzo delle clausole contrattuali tipo. In tal caso, l'autorità nazionale di protezione dei dati deve confrontare le clausole effettivamente contenute nel contratto in questione con le clausole contrattuali tipo e verificare che non sia stata apportata alcuna modifica¹³. Se le clausole sono state utilizzate senza modifiche¹⁴, in linea di principio¹⁵, l'autorizzazione è concessa automaticamente¹⁶. Come ulteriormente precisato infra (cfr. sezione 2.4), ciò non pregiudica misure supplementari che l'esportatore di dati potrà essere indotto a prendere, in particolare in seguito a informazioni ricevute dall'importatore dei dati sui cambiamenti intervenuti nel sistema giuridico del paese terzo che possono impedire all'importatore dei dati di adempiere i propri obblighi ai sensi del contratto. Nell'applicazione delle clausole contrattuali tipo, sia gli

¹² Cfr. ad esempio, il considerando 6 della decisione 2004/915/CE della Commissione e la clausola V del relativo allegato; la clausola 7 dell'allegato della decisione 2010/87/UE della Commissione.

¹³ Giova ricordare che la proposta di regolamento generale sulla protezione dei dati (COM(2012) 11 final) prevede che i trasferimenti basati sulle clausole contrattuali tipo o sulle norme vincolanti d'impresa, nella misura in cui questi sono state adottate dalla Commissione o in conformità con il previsto meccanismo di coerenza, non richiedono ulteriori autorizzazioni.

¹⁴ L'uso delle clausole contrattuali tipo, tuttavia, non impedisce alle parti di concordare di aggiungere altre clausole, nella misura in cui non contraddicono, direttamente o indirettamente, le clausole approvate dalla Commissione o pregiudicano i diritti o le libertà fondamentali delle persone interessate. Cfr. Commissione europea, "Domande frequenti relative ai trasferimenti di dati personali dall'UE/SEE verso paesi terzi" (FAQ B. 1.9), pag. 28 (disponibile al seguente indirizzo Internet: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf).

¹⁵ Se dubita della compatibilità delle clausole contrattuali tipo con i requisiti della direttiva, un'autorità di protezione dei dati dovrebbe rinviare la questione a un giudice nazionale che può allora presentare una domanda di pronuncia pregiudiziale alla Corte di giustizia (cfr. punti 51, 52, 64 e 65 della sentenza Schrems).

¹⁶ Il Gruppo di lavoro "Articolo 29" ha istituito un'apposita procedura di cooperazione tra le autorità di protezione dei dati per l'approvazione delle clausole contrattuali che una società cerca di utilizzare nei diversi Stati membri. Cfr. Gruppo di lavoro "Articolo 29", "Documento di lavoro che istituisce una procedura di cooperazione per emettere pareri comuni sulle "clausole contrattuali" considerate conformi alla clausola tipo CE" (WP 226), 26 novembre 2014. Cfr. anche la clausola VII dell'allegato della decisione 2004/915/CE della Commissione, e clausola 10 dell'allegato alla decisione 2010/87/UE della Commissione.

esportatori di dati sia, se si assoggettano al contratto, gli importatori di dati rientrano sotto la supervisione delle autorità di protezione dei dati.

L'adozione delle clausole contrattuali tipo non impedisce alle imprese di ricorrere ad altri strumenti, come accordi contrattuali *ad hoc*, per dimostrare che i loro trasferimenti avvengono con garanzie sufficienti ai sensi dell'articolo 26, paragrafo 2, della direttiva 95/46/CE. A norma dell'articolo 26, paragrafo 2, della direttiva, essi devono essere approvati caso per caso dalle autorità nazionali. Talune autorità di protezione dei dati hanno elaborato linee guida in questo campo, anche sotto forma di contratti standardizzati o le modalità dettagliate da seguire nella redazione delle clausole di trasferimento dei dati. La maggior parte dei contratti attualmente utilizzati dalle imprese per effettuare i loro trasferimenti internazionali di dati, tuttavia, sono basati su clausole contrattuali tipo approvate dalla Commissione¹⁷.

2.2. I trasferimenti intragruppo

Un'impresa multinazionale può adottare norme vincolanti d'impresa per trasferire dati personali dall'UE a consociate estere situate al di fuori dell'Unione in conformità con i requisiti di cui all'articolo 26, paragrafo 2, della direttiva 95/46/CE. Questo tipo di codice di buone prassi fornisce la base soltanto per i trasferimenti effettuati all'interno del gruppo societario.

L'uso di norme vincolanti d'impresa consente quindi ai dati personali di circolare liberamente tra le varie entità di un gruppo societario a livello mondiale — senza bisogno di disporre di accordi contrattuali tra ogni entità societaria — garantendo al contempo che lo stesso elevato livello di protezione dei dati personali sia rispettato in tutto il gruppo, per mezzo di un'unica serie di norme vincolanti ed esecutive. Avere un'unica serie di regole crea un sistema più semplice e più efficace per il personale, che è più facile da attuare e da comprendere per le persone interessate. Al fine di aiutare le imprese nell'elaborazione delle norme vincolanti d'impresa, il Gruppo di lavoro "Articolo 29" ha specificato gli elementi sostanziali (ad esempio la limitazione delle finalità, la sicurezza del trattamento, informazioni trasparenti alle persone interessate, restrizioni ai successivi trasferimenti al di fuori del gruppo, i diritti individuali di accesso, rettifica e opposizione) e procedurali (ad es. audit, controllo di conformità, trattamento dei reclami, la cooperazione con le autorità di protezione dei dati, la responsabilità e la giurisdizione) per le norme d'impresa vincolanti basate sulle norme UE sulla protezione dei dati¹⁸. Queste regole sono non solo vincolanti per i membri del gruppo societario ma, analogamente alle clausole contrattuali tipo, sono anche esecutive nell'UE: le persone i cui dati sono oggetto di trattamento da parte di un'entità del gruppo sono autorizzate in quanto terzi beneficiari a far rispettare le norme vincolanti d'impresa, presentando un

¹⁷ Cfr. Gruppo di lavoro "Articolo 29", "Documento di lavoro che istituisce una procedura di cooperazione per emettere pareri comuni sulle "clausole contrattuali" considerate conformi alla clausola tipo CE" (WP 226), 26 novembre 2014, pag. 2.

¹⁸ Cfr. Gruppo di lavoro "Articolo 29", "Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules" (WP 153), 24 giugno 2008. "Working Document setting up a framework for the structure of Binding Corporate Rules" (WP 154), 24 giugno 2008; e "Working document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules" (WP 155), 24 giugno 2008.

reclamo ad un'autorità di protezione dei dati e intentando un'azione dinanzi ad un giudice di uno Stato membro. Inoltre, le norme vincolanti d'impresa devono designare un'entità all'interno dell'UE che assume la responsabilità per le violazioni delle norme da parte di uno dei membri del gruppo al di fuori dell'UE che è vincolato da tali norme.

In base alla legislazione che recepisce la direttiva della maggior parte degli Stati membri, il trasferimento dei dati sulla base delle norme vincolanti d'impresa deve essere autorizzato dalle autorità di protezione dei dati in ciascuno Stato membro dal quale la società multinazionale intende trasferire dati. Al fine di agevolare e accelerare il processo, nonché ridurre gli oneri per i richiedenti, il Gruppo di lavoro "Articolo 29" ha introdotto un modulo standard di domanda¹⁹ e stabilito una specifica procedura di cooperazione tra le autorità di protezione di dati competenti²⁰ che include la designazione di una "autorità capofila" responsabile per la gestione della procedura di approvazione.

2.3. Deroghe

In mancanza di una decisione di adeguatezza ai sensi dell'articolo 25, paragrafo 6, della direttiva 95/46/CE e a prescindere dall'uso delle clausole contrattuali tipo e/o delle norme vincolanti d'impresa, i dati personali possono essere trasferiti a entità stabilite in un paese terzo, nella misura in cui trova applicazione una delle deroghe alternative di cui all'articolo 26, paragrafo 1, della direttiva 95/46/CE²¹:

- la persona interessata ha fornito, in modo inequivocabile, il proprio consenso al trasferimento proposto;
- il trasferimento è necessario all'esecuzione di un contratto concluso tra la persona interessata ed il responsabile del trattamento ovvero all'esecuzione di misure precontrattuali prese a richiesta di tale persona,
- il trasferimento è necessario per la conclusione o l'esecuzione di un contratto, concluso o da concludere nell'interesse della persona interessata, tra il responsabile del trattamento e un terzo;

¹⁹ Gruppo di lavoro "Articolo 29", "Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data" (WP 133), 10 gennaio 2007.

²⁰ Cfr. Gruppo di lavoro "Articolo 29", "Documento di lavoro che istituisce una procedura di cooperazione per emettere pareri comuni sulle garanzie sufficienti offerte dalle "norme vincolanti d'impresa" (WP 107), 14 aprile 2005.

²¹ Come sottolineato dal Gruppo di lavoro "Articolo 29", nella misura in cui le altre disposizioni della direttiva 95/46/CE contengono requisiti aggiuntivi pertinenti per l'utilizzo di tali deroghe (ad esempio le limitazioni dell'articolo 8 per il trattamento di dati sensibili), essi devono essere rispettati. Cfr. Gruppo di lavoro "Articolo 29", "Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE, del 24 ottobre 1995" (WP 114), 25 novembre 2005, pag. 8. Cfr. anche Commissione europea, "Domande frequenti relative ai trasferimenti di dati personali dall'UE/SEE verso paesi terzi" (FAQ D.2), pag. 50.

- il trasferimento è necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante²², ovvero per accertare, esercitare o difendere un diritto in via giudiziale,
- il trasferimento è necessario per la salvaguardia di interessi vitali della persona interessata,
- il trasferimento avviene a partire da un registro pubblico il quale, in forza di disposizioni legislative o regolamentari, è predisposto per l'informazione del pubblico ed è aperto alla consultazione del pubblico o di chiunque possa dimostrare un interesse legittimo, nella misura in cui nel caso specifico siano rispettate le condizioni che la legge prevede per la consultazione.

Tali motivi costituiscono una deroga al divieto generale di trasferire dati personali a soggetti stabiliti in un paese terzo senza un adeguato livello di protezione. In effetti, l'esportatore di dati non deve garantire che l'importatore di dati fornirà una protezione adeguata e, di solito, non deve ottenere l'autorizzazione preventiva per il trasferimento da parte delle pertinenti autorità nazionali. Tuttavia, a causa del loro carattere eccezionale, il Gruppo di lavoro "Articolo 29" ritiene che tali deroghe devono essere interpretate in senso restrittivo²³.

Il Gruppo di lavoro "Articolo 29" ha pubblicato diversi documenti di orientamento non vincolanti sull'applicazione dell'articolo 26, paragrafo 1, della direttiva 95/46/CE²⁴, tra cui una serie di norme in materia di "migliori pratiche" concepite per orientare l'azione di esecuzione dell'autorità di protezione dei dati²⁵. In particolare, il Gruppo di lavoro raccomanda che i trasferimenti di dati a carattere personale che possono essere considerati ripetuti, voluminosi o abituali siano effettuati, se possibile, in un quadro giuridico specifico, come ad esempio un contratto o norme vincolanti d'impresa²⁶.

²² Ciò può includere, ad esempio, i trasferimenti di dati tra amministrazioni fiscali o doganali oppure tra servizi competenti per la sicurezza sociale (cfr. considerando 58 della direttiva 95/46/CE). Anche i trasferimenti fra organismi di vigilanza nel settore dei servizi finanziari possono beneficiare della deroga. Cfr. Gruppo di lavoro "Articolo 29", "Documento di lavoro: Trasferimenti di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla protezione dei dati" (WP12), 24 luglio 1998, pag. 25.

²³ Cfr. Gruppo di lavoro "Articolo 29", "Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE, del 24 ottobre 1995" (WP 114), 25 novembre 2005, pagg. 7 e 17.

²⁴ Cfr. Gruppo di lavoro "Articolo 29", "Documento di lavoro: Trasferimenti di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati" (WP12), 24 luglio 1998. "Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE, del 24 ottobre 1995" (WP 114), 25 novembre 2005. Cfr. anche Commissione europea, "Domande frequenti relative ai trasferimenti di dati personali dall'UE/SEE verso paesi terzi" (FAQ da D.1 a D.9), pagg. 48-54.

²⁵ Cfr. Gruppo di lavoro "Articolo 29", "Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE, del 24 ottobre 1995" (WP 114), 25 novembre 2005, pagg. 8-10.

²⁶ Cfr. Gruppo di lavoro "Articolo 29", "Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE, del 24 ottobre 1995" (WP 114), 25 novembre 2005, pag. 9. Secondo il Gruppo di lavoro, trasferimenti voluminosi o ripetuti possono essere effettuati solo sulla base di una deroga quando sia impossibile nella pratica ricorrere alle clausole contrattuali tipo o a norme vincolanti d'impresa e quando il rischio per le persone interessate è modesto (ad esempio i trasferimenti internazionali di denaro). Cfr. anche Commissione europea, "Domande frequenti relative ai trasferimenti di dati personali dall'UE/SEE verso paesi terzi" (FAQ D.1), pag. 49.

Nella presente comunicazione, la Commissione tratterà solo quelle deroghe che risultano particolarmente pertinenti per i trasferimenti nell'ambito commerciale a seguito della constatazione che la decisione sull'approdo sicuro è stata invalidata.

2.3.1. Trasferimenti necessari per l'esecuzione di un contratto o per l'esecuzione di misure precontrattuali prese a richiesta della persona interessata (articolo 26, paragrafo 1, lettera b))

La presente deroga può essere pertinente, ad esempio, nel contesto di una prenotazione alberghiera, o nel caso in cui siano trasferite ad un paese terzo informazioni su un pagamento al fine di effettuare un bonifico bancario. Tuttavia, in ciascuno di questi casi il Gruppo di lavoro "Articolo 29" ritiene che vi sia un "nesso stretto e sostanziale", un "collegamento diretto ed obiettivo" tra la persona interessata e lo scopo del contratto o della misura precontrattuale (criterio di necessità)²⁷. Inoltre, la deroga non può essere applicata ai trasferimenti di ulteriori informazioni non necessarie ai fini del trasferimento o dei trasferimenti per un fine diverso dall'esecuzione del contratto (ad esempio, il seguito di un'operazione di marketing)²⁸. Per quanto riguarda le misure precontrattuali, il Gruppo di lavoro "Articolo 29" ha ritenuto che solo i contatti avviati dalla persona interessata (ad esempio, una richiesta di informazioni su un determinato servizio) sarebbero coperti ma non quelli derivanti da approcci di marketing effettuati dal responsabile del trattamento dei dati²⁹.

2.3.2. Trasferimenti necessari per la conclusione o l'esecuzione di un contratto, concluso nell'interesse della persona interessata, tra il responsabile del trattamento o un terzo (articolo 26, paragrafo 1, lettera c))

Questa deroga può essere pertinente, ad esempio, quando la persona interessata è il beneficiario di un bonifico bancario internazionale, o quando un'agenzia di viaggi trasmette i dati della prenotazione di un volo ad una compagnia aerea. Anche in questo caso si applica il criterio di necessità e deve sussistere un nesso stretto e sostanziale tra l'interesse della persona interessata e lo scopo perseguito con il contratto.

2.3.3. Trasferimenti necessari o prescritti dalla legge per constatare, esercitare o difendere un diritto per via giudiziaria (articolo 26, paragrafo 1, lettera d))

Questa deroga potrebbe essere applicabile, ad esempio, nei casi in cui una società abbia necessità di trasferire dati per difendersi in un'azione legale, o per presentare un reclamo davanti a un giudice o un'autorità pubblica. Come per le due precedenti deroghe, ciò è

²⁷ Cfr. Gruppo di lavoro "Articolo 29", "Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE, del 24 ottobre 1995" (WP 114), 25 novembre 2005, pag. 13. Cfr. anche "parere 6/2002 relativo alla trasmissione da parte delle compagnie aeree di informazioni sugli elenchi dei passeggeri e di altri dati agli Stati Uniti" (WP 66), 24 ottobre 2002.

²⁸ Cfr. Gruppo di lavoro "Articolo 29", "Documento di lavoro: Trasferimenti di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati" (WP12), 24 luglio 1998, pag. 24. "Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE, del 24 ottobre 1995" (WP 114), 25 novembre 2005, pag. 13.

²⁹ Cfr. Gruppo di lavoro "Articolo 29", "Documento di lavoro: Trasferimenti di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla protezione dei dati" (WP12), 24 luglio 1998, pag. 24.

subordinato al criterio di necessità³⁰: deve sussistere una stretta connessione con il contenzioso o il procedimento giudiziario (anche di natura amministrativa).

Secondo il Gruppo di lavoro "Articolo 29", la deroga può essere applicata solo se sono state rispettate le norme sulla cooperazione internazionale nei procedimenti penali o civili che disciplinano il tipo di trasferimento, segnatamente perché derivanti dalle disposizioni della convenzione dell'Aia del 18 marzo 1970 ("la convenzione sull'assunzione delle prove")³¹.

2.3.4. Previo consenso inequivocabile della persona interessata al trasferimento previsto (articolo 26, paragrafo 1, lettera a))

Benché il consenso possa essere utilizzato come base per i trasferimenti di dati, si impongono alcune considerazioni. Poiché il consenso deve essere accordato al trasferimento "previsto", ciò richiede un previo consenso preventivo al trasferimento in questione (o a una particolare categoria di trasferimenti). Se la richiesta è fatta online, il Gruppo di lavoro "Articolo 29" ha raccomandato l'uso di caselle da contrassegnare (anziché caselle preselezionate)³². Perché il consenso deve essere inequivocabile, il minimo dubbio sull'effettiva manifestazione del consenso renderebbe inapplicabile la deroga. Ciò significa probabilmente che molte situazioni in cui il consenso è, nel migliore dei casi, implicito (ad esempio, quando una persona è stata informata di un trasferimento e non ha sollevato obiezioni) non sarebbero ammissibili. Per contro, la deroga può essere utilizzata nei casi in cui l'entità trasferente disponga di un contatto diretto con la persona interessata, possano essere facilmente fornite le informazioni necessarie e possa essere ottenuto il consenso inequivocabile³³.

Inoltre, ai sensi dell'articolo 2, lettera h), della direttiva 95/46/CE, il consenso deve essere libero, specifico e informato. Secondo il Gruppo di lavoro "Articolo 29", il primo requisito implica che un'eventuale "pressione" può inficiare la validità del consenso. Ciò è particolarmente importante nel contesto lavorativo, in cui il rapporto di subordinazione e di dipendenza insito nella condizione di personale dipendente è tale, in linea di principio, da far rimettere in discussione il ricorso al consenso³⁴. Più in generale, il consenso accordato da una

³⁰ Cfr. Gruppo di lavoro "Articolo 29", "Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE, del 24 ottobre 1995" (WP 114), 25 novembre 2005, pag. 15. Ad esempio, in un contesto lavorativo la deroga non può essere utilizzata per trasferire i fascicoli di tutti i dipendenti alla società madre stabilita in un paese terzo a motivo di eventuali futuri procedimenti giudiziari.

³¹ Convenzione dell'Aia sull'assunzione delle prove all'estero in materia civile e commerciale, *aperta alla firma* il 18 marzo 1970, 23 U.S.T. 2555, 847 U.N.T.S. 241. La convenzione si applica, ad esempio, alla presentazione del materiale probatorio prima del processo (pre-trial discovery) o alle richieste da parte dell'autorità giudiziaria di uno Stato membro all'autorità competente di un altro Stato membro volte a ottenere prove destinate ad essere utilizzate in procedimenti giudiziari nello Stato richiedente.

³² Gruppo di lavoro "articolo 29", "documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE, del 24 ottobre 1995" (WP 114), 25 novembre 2005, pag. 10, con riferimento al "Parere 5/2004 relativo alle comunicazioni indesiderate a fini di commercializzazione diretta ai sensi dell'articolo 13 della direttiva 2002/58/CE" (WP 90), 27 febbraio 2004, punto 3.2.

³³ Cfr. Gruppo di lavoro "Articolo 29", documento di lavoro: Trasferimenti di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla protezione dei dati" (WP12), 24 luglio 1998, pag. 24.

³⁴ Gruppo di lavoro "Articolo 29", "Parere 8/2001 sul trattamento dei dati personali nel contesto dell'occupazione" (WP 48), 13 settembre 2001, pag. 3, 23 e 26. Secondo il Gruppo di lavoro, il ricorso al consenso dovrebbe limitarsi ai casi in cui il lavoratore abbia l'effettiva possibilità di scelta libera e possa

persona interessata che non abbia avuto la possibilità di operare un'effettiva scelta o si è trovata davanti a un fatto compiuto non può essere considerato valido³⁵.

È di fondamentale importanza che le persone interessate siano adeguatamente informate in anticipo del fatto che i dati possono essere trasferiti al di fuori dell'UE, verso quale paese terzo e a quali condizioni (la finalità, l'identità e le coordinate del destinatario, ecc.). Tali informazioni dovrebbero vertere anche sul rischio specifico che i loro dati siano trasferiti a un paese terzo che non garantisce un'adeguata protezione³⁶. Inoltre, come rilevato dal Gruppo di lavoro "Articolo 29", la revoca del consenso della persona interessata, pur non essendo retroattiva, dovrebbe, in linea di principio, impedire qualsiasi ulteriore trattamento dei dati personali³⁷. Alla luce di tali limitazioni, il Gruppo di lavoro "Articolo 29" ritiene che il consenso non sia tale da garantire un adeguato quadro di lungo termine per i responsabili del trattamento dei dati in caso di trasferimenti strutturali³⁸.

2.4. Le basi alternative per i trasferimenti di dati personali in sintesi

Dalle considerazioni sopra esposte consegue che le imprese possono utilizzare una serie di diversi strumenti alternativi per effettuare i trasferimenti internazionali di dati verso paesi terzi che non si ritiene garantiscano un livello adeguato di protezione ai sensi dell'articolo 25, paragrafo 2, della direttiva 95/46/CE. A seguito della sentenza Schrems, il Gruppo di lavoro "Articolo 29" ha in particolare chiarito che, pur proseguendone la valutazione e fatte salve le competenze delle autorità di protezione dei dati di esaminare casi particolari, le clausole contrattuali tipo e le norme vincolanti d'impresa possono essere utilizzate per il trasferimento di dati verso gli Stati Uniti³⁹. Da parte sua, l'industria ha reagito in modi diversi alla sentenza, anche facendo ricorso a tali strumenti alternativi come base dei trasferimenti di dati⁴⁰.

Tuttavia, vanno sottolineate due importanti condizioni. In primo luogo, si deve ricordare che, a prescindere dalla specifica base giuridica invocata, il trasferimento di dati verso un paese terzo può essere legittimamente effettuato solo se i dati sono stati originariamente raccolti e

successivamente ritirare il proprio consenso senza subire pregiudizio. Cfr. anche Gruppo di lavoro "Articolo 29", "Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE, del 24 ottobre 1995" (WP 114), 25 novembre 2005, pag. 11.

³⁵ Cfr. Gruppo di lavoro "Articolo 29", "Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE, del 24 ottobre 1995" (WP 114), 25 novembre 2005, pag. 11. Cfr. anche "Parere 6/2002 relativo alla trasmissione da parte delle compagnie aeree di informazioni sugli elenchi dei passeggeri e di altri dati agli Stati Uniti" (WP 66), 24 ottobre 2002.

³⁶ Cfr. Gruppo di lavoro "Articolo 29", "Documento di lavoro: Trasferimenti di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla protezione dei dati" (WP12), 24 luglio 1998, pag. 24.

³⁷ Gruppo di lavoro "Articolo 29", "Parere 15/2011 sulla definizione di consenso" (WP 187), 13 luglio 2011, pag. 10.

³⁸ Cfr. Gruppo di lavoro "Articolo 29", "Documento di lavoro su un'interpretazione comune dell'articolo 26, paragrafo 1, della direttiva 95/46/CE, del 24 ottobre 1995" (WP 114), 25 novembre 2005, pag. 11.

³⁹ Cfr. la dichiarazione del gruppo di lavoro "articolo 29" del 16 ottobre 2015 (cit. alla nota 8).

⁴⁰ Alcune multinazionali hanno dichiarato che esse fondano i propri trasferimenti di dati verso gli Stati Uniti su strumenti alternativi. Cfr. ad esempio le dichiarazioni della Microsoft (<http://blogs.microsoft.com/on-the-issues/2015/10/06/a-message-to-our-customers-about-eu-us-safe-harbor/>) or Salesforce (<http://www.salesforce.com/company/privacy/data-processing-addendum-faq.jsp>). Altre società statunitensi quali Oracle hanno dichiarato di offrire ai clienti cloud la possibilità di conservare i propri dati in Europa, di modo che non siano trasmessi altrove: <http://www.irishtimes.com/business/technology/oracle-keeps-european-data-within-its-eu-based-data-centres-1.2408505?mode=print&ot=example.AjaxPageLayout.ot>

successivamente trattati dal responsabile del trattamento dei dati stabilito nell'UE in conformità della normativa nazionale che recepisce la direttiva 95/46/CE applicabile. La direttiva chiarisce espressamente che le attività di trattamento che hanno luogo prima del trasferimento, così come il trasferimento stesso, devono rispettare pienamente le norme adottate dagli Stati membri conformemente alle altre disposizioni della direttiva⁴¹. In secondo luogo, in mancanza di un accertamento di adeguatezza della Commissione, spetta ai responsabili del trattamento garantire che i trasferimenti di dati avvengano con garanzie sufficienti ai sensi dell'articolo 26, paragrafo 2, della direttiva. Questa valutazione deve essere effettuata alla luce di tutte le circostanze relative al trasferimento in questione. In particolare, sia le clausole contrattuali tipo che le norme vincolanti d'impresa prevedono che, se l'importatore di dati ha motivo di ritenere che la legislazione applicabile nel paese di destinazione può impedirgli di assolvere i suoi obblighi, ne informa prontamente l'esportatore di dati nell'UE. In tale situazione, spetta all'esportatore prendere le misure appropriate, necessarie per garantire la protezione dei dati personali⁴². Tali misure possono variare da misure tecniche, organizzative, giuridiche o connesse al modello aziendale⁴³ fino alla possibilità di sospendere il trasferimento dei dati o di risolvere il contratto. Tenuto conto di tutte le circostanze del trasferimento, gli esportatori di dati possono quindi dover porre in essere salvaguardie supplementari per integrare quelle previste ai sensi della base giuridica applicabile al trasferimento per soddisfare le prescrizioni dell'articolo 26, paragrafo 2 della direttiva.

Il rispetto di tali obblighi deve essere valutato, in ultima analisi, dalle autorità di protezione dei dati caso per caso nell'ambito dell'esercizio delle loro funzioni di controllo e applicazione, anche nel contesto dell'approvazione di accordi contrattuali e norme d'impresa vincolanti o sulla base di ricorsi individuali. Benché talune autorità di protezione dei dati abbiano espresso dubbi circa la possibilità di utilizzare gli strumenti di trasferimento, quali le clausole contrattuali tipo e le norme vincolanti d'impresa, per i flussi di dati transatlantici⁴⁴, nella dichiarazione rilasciata a seguito della sentenza Schrems, il Gruppo di lavoro "Articolo 29" ha

⁴¹ Cfr. considerando 60 e articolo 25, paragrafo 1, della direttiva 95/46/CE.

⁴² Cfr. ad esempio, clausola 5 dell'allegato della decisione 2010/87/UE della Commissione, e Gruppo di lavoro "Articolo 29", "Working document setting up a framework for the structure of Binding Corporate Rules" (WP 154), 24 giugno 2008, pag. 8.

⁴³ Cfr. ad esempio gli orientamenti pubblicati dall'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA): https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf.

⁴⁴ Cfr. ad esempio il documento programmatico pubblicato dalla Conferenza sulla protezione dei dati delle autorità tedesche di protezione dei dati a livello federale e statale del 26.10.2015: <https://www.datenschutz.hessen.de/ft-europa.htm#entry4521>. Sottolineando che la sentenza Schrems contiene "rigorosi requisiti sostanziali" che sia la Commissione sia le autorità di protezione dei dati sono tenute a rispettare, il documento indica che l'autorità di protezione dei dati tedesca valuterà la liceità dei trasferimenti di dati basati su strumenti alternativi (clausole contrattuali tipo, norme vincolanti d'impresa) e non rilascerà più nuove autorizzazioni per l'uso di detti strumenti. In parallelo, le singole autorità di protezione dei dati tedesche hanno emanato chiari avvertimenti del fatto che gli strumenti alternativi di trasferimento sono oggetto di esame giuridico. Cfr. ad esempio i documenti di sintesi delle posizioni pubblicati dalle autorità di protezione dei dati di Schleswig-Holstein: <https://www.datenschutzzentrum.de/artikel/981-ULD-Position-Paper-on-the-Judgment-of-the-Court-of-Justice-of-the-European-Union-of-6-October-2015,-C-36214.html> e della Renania-Palatinato: https://www.datenschutz.rlp.de/de/aktuell/2015/images/20151026_Folgerungen_des_LfDI_RLP_zum_EuG_H-Urteil_Safe_Harbor.pdf.

annunciato che continuerà la sua analisi dell'impatto della sentenza su altri strumenti di trasferimento⁴⁵. Ciò non pregiudica i poteri delle autorità di protezione dei dati di indagare casi particolari e di esercitare i loro poteri in modo da proteggere le persone.

3. LE CONSEGUENZE DELLA SENTENZA SCHREMS SULLE DECISIONI DI ADEGUATEZZA

Nella sua sentenza, la Corte di giustizia non rimette in questione le competenze della Commissione a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE di accertare che un paese terzo garantisca un livello di protezione adeguato, a condizione che i requisiti stabiliti dalla Corte di giustizia siano rispettati. In linea con questi requisiti, la proposta del 2012 di un regolamento generale sulla protezione dei dati⁴⁶ volta a sostituire la direttiva 95/46/CE, chiarisce e precisa le condizioni alle quali possono essere adottate decisioni di adeguatezza. Nella sentenza Schrems, la Corte ha anche chiarito che, quando la Commissione adotta una decisione di adeguatezza, essa è vincolante per tutti gli Stati membri e i loro organismi, comprese le autorità di protezione dei dati, fintantoché non venga revocata, annullata o dichiarata invalida dalla Corte di giustizia, che è il solo organo competente al riguardo. Le autorità di protezione dei dati continuano ad essere competenti a esaminare le domande ai sensi dell'articolo 28, paragrafo 4, della direttiva 95/46/CE, relative alla conformità del trasferimento dei dati con i requisiti stabiliti dalla direttiva (come interpretata dalla Corte), ma non possono svolgere un accertamento definitivo. Piuttosto, gli Stati membri devono prevedere la possibilità di portare il caso dinanzi ad un giudice nazionale, che a sua volta può adire la Corte di giustizia mediante una domanda di pronuncia pregiudiziale ai sensi dell'articolo 267 del trattato sul funzionamento dell'Unione europea (TFUE).

Inoltre, la Corte di giustizia ha espressamente confermato che il ricorso da parte di un paese terzo a un sistema di autocertificazione (come nel caso dei principi di "approdo sicuro") non esclude una constatazione di adeguatezza ai sensi dell'articolo 25, paragrafo 6, della direttiva 95/46/CE, purché vi siano efficaci meccanismi di individuazione e di vigilanza che rendano possibile in pratica individuare e sanzionare qualsiasi violazione delle norme in materia di protezione dei dati.

Dato che l'attuale decisione "Approdo sicuro" non conteneva elementi sufficienti a tale riguardo, la Corte di giustizia ha dichiarato l'invalidità della decisione. È quindi evidente che i trasferimenti di dati tra l'UE e gli Stati Uniti non possono più essere effettuati su tale base, vale a dire esclusivamente invocando il rispetto dei principi di approdo sicuro. Atteso che il trasferimento di dati verso un paese terzo che non garantisce un livello di protezione adeguato

⁴⁵ Cfr. Dichiarazione del gruppo di lavoro "Articolo 29" del 16 ottobre 2015 (cit. alla nota 8).

⁴⁶ Commissione europea, Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati); Parlamento europeo, Risoluzione legislativa del 12 marzo 2014 sul progetto di relazione sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), (COM(2012) 011 – C7-0025/2012 – 2012/0011(COD)); Consiglio, Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), Elaborazione di un orientamento generale, 9565/15. La proposta è attualmente nella fase finale della procedura legislativa.

(o almeno nei casi in cui ciò non è stato stabilito in una decisione della Commissione ai sensi dell'articolo 25, paragrafo 6, della direttiva 95/46/CE), è, in linea di principio, vietato⁴⁷, esso è legittimo solo se l'esportatore dei dati può invocare uno degli strumenti alternativi di cui sopra nella sezione 2. In mancanza di una decisione di adeguatezza, è responsabilità dell'esportatore di dati — sotto il controllo delle autorità di protezione dei dati — garantire che le condizioni per ricorrere ad uno di tali strumenti siano soddisfatte con riferimento al trasferimento di dati.

Il campo di applicazione della sentenza è limitato alla decisione "Approdo sicuro" della Commissione. Tuttavia, ciascuna delle altre decisioni di adeguatezza⁴⁸ contiene una limitazione dei poteri delle autorità di protezione dei dati che è identico all'articolo 3 della decisione "Approdo sicuro" e che la Corte di giustizia ha ritenuto invalida⁴⁹. La Commissione intende ora trarre le necessarie conseguenze dalla sentenza elaborando in tempi brevi una decisione, che dovrà essere adottata secondo la procedura di comitatologia applicabile, per sostituire tale disposizione in tutte le decisioni di adeguatezza esistenti. Inoltre, la Commissione procederà a una valutazione periodica delle attuali e delle future decisioni di adeguatezza, anche mediante la periodica revisione congiunta del loro funzionamento in collaborazione con le autorità competenti del paese terzo in questione.

4. CONCLUSIONI

Come confermato dal Gruppo di lavoro "Articolo 29", gli strumenti alternativi che autorizzano i flussi di dati possono ancora essere utilizzati dalle imprese per leciti trasferimenti di dati verso paesi terzi, come gli Stati Uniti. Tuttavia, la Commissione ritiene che un rinnovato e solido quadro per i trasferimenti di dati personali verso gli Stati Uniti rimanga una priorità fondamentale. Un quadro di questo tipo è la soluzione più completa per garantire un'effettiva continuità della protezione dei dati personali dei cittadini europei quando sono trasferiti negli Stati Uniti. Esso offre inoltre la soluzione migliore per il commercio transatlantico, poiché offre un meccanismo di trasferimento più semplice, meno laborioso e quindi meno costoso, in particolare per le PMI.

Già nel 2013 la Commissione aveva avviato negoziati con il governo degli Stati Uniti su un nuovo accordo per i trasferimenti transatlantici di dati basato sulle sue 13 raccomandazioni⁵⁰. Sono stati compiuti notevoli progressi nell'avvicinare le opinioni di entrambe le parti, ad esempio su un monitoraggio e un'applicazione più rigorosi dei principi di approdo sicuro da parte, rispettivamente, del ministero del Commercio degli Stati Uniti e della Federal Trade Commission degli Stati Uniti, una maggiore trasparenza per i consumatori per quanto riguarda i loro diritti alla protezione dei dati, una più facile e meno costosa possibilità di ricorso in caso di reclami e norme più chiare in materia di trasferimenti successivi dalle società che aderiscono ai principi "approdo sicuro" a quelle che non vi aderiscono (ad esempio, ai fini di

⁴⁷ Cfr. considerando 57 della direttiva 95/46/CE.

⁴⁸ Attualmente, sono state adottate decisioni di adeguatezza con riferimento ai seguenti paesi: Andorra, Argentina, Canada, Isole Fær Øer, Guernsey, Israele, Isola di Man, Jersey, Nuova Zelanda, Svizzera e Uruguay. Cfr. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

⁴⁹ Cfr. punti 99-104 della sentenza Schrems.

⁵⁰ Cfr. nota 4 supra.

trattamento diretto e di trattamento affidato in subcontratto). Ora che la decisione "Approdo sicuro" è stata dichiarata invalida, la Commissione ha intensificato il dialogo con il governo degli Stati Uniti per garantire che gli obblighi giuridici formulati dalla Corte di giustizia siano rispettati. La Commissione mira a concludere le discussioni e raggiungere questo obiettivo in tre mesi.

Fino a quando il rinnovato quadro transatlantico non sarà attuato, le imprese hanno bisogno di invocare gli strumenti alternativi di trasferimento disponibili. Tuttavia, tale opzione comporta responsabilità per gli esportatori di dati, sotto la supervisione delle autorità di protezione dei dati.

Contrariamente alla situazione in cui esiste un riscontro da parte della Commissione del fatto che un paese terzo garantisce un livello adeguato di protezione dei dati, che gli esportatori di dati possano invocare ai fini dei trasferimenti di dati dall'UE, questi ultimi rimangono responsabili della verifica che i dati personali siano protetti in modo efficace quando utilizzano strumenti alternativi. Ciò può includere l'obbligo di adottare le misure opportune, ove necessario.

A tale riguardo, le autorità di protezione dei dati hanno un ruolo centrale da svolgere. In quanto principale autorità preposta all'applicazione dei diritti fondamentali delle persone interessate, le autorità di protezione dei dati sono responsabili e hanno il potere di vigilare sui trasferimenti di dati dall'UE verso i paesi terzi, in piena indipendenza. La Commissione invita i responsabili del trattamento a cooperare con le autorità di protezione dei dati, aiutandole così a svolgere efficacemente il loro ruolo di vigilanza. La Commissione continuerà a lavorare a stretto contatto con il Gruppo di lavoro "Articolo 29" per garantire un'applicazione uniforme della normativa UE sulla protezione dei dati.