Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

# Dopo la sentenza della Corte di Giustizia UE sulla invalidità della *Decisione Safe Harbour* per il trasferimento dei dati verso gli USA: l'impatto pratico sulla esportazione dei dati personali.

***di:***
***Prof. Avv. Alessandro del Ninno***
***Studio Legale Tonucci & Partners***
***adelninno@tonucci.com***

---

**Indice**



---

## § 1. Introduzione: brevi cenni al caso C-362/14 *Maximillian Schrems vs. Data Protection Commissioner.*

Sta facendo parlare – e molto (qualcuno ha parlato di "*terremoto digitale con epicentro Bruxelles*") – la recente sentenza della Corte di Giustizia UE con la quale è stato deciso che l'accordo c.d. del *Safe Harbour*, cioè la norma sull'approdo sicuro dei dati personali trasferiti verso gli USA che ha certificato 15 anni fa i rapporti di fiducia tra Bruxelles e gli Stati Uniti, non è valido.

Il caso è presto riassunto: Maximilian Schrems è un cittadino austriaco che fin dal 2008 è titolare di un account Facebook. Come per molti altri utenti titolari di un account Facebook, alcuni dei dati personali forniti da Schrems a Facebook vengono trasferiti dai *servers* della società irlandese controllata da Facebook verso *servers* ubicati negli Stati Uniti d'America, dove sono oggetto di trattamento. Lo studente austriaco propone ricorso all'Autorità per la protezione dei dati personali irlandese (il "*Data Protection Commissioner*") sostenendo che in base alle rivelazioni fatte da Edward Snowden nel 2013 circa le attività dei servizi di intelligence USA (in particolare la National Security Agency – NSA e il programma di controllo *Prism*), il quadro giuridico degli Stati Uniti non offrirebbe quell'"*adeguato livello di protezione dei dati*

*personali*" (con particolare riferimento alle attività di sorveglianza delle autorità pubbliche) che è presupposto ineliminabile (tanto nella Direttiva UE sulla tutela dei dati personali, quanto nelle legislazioni nazionali di recepimento degli Stati Membri) per rendere lecito il trasferimento dei dati verso gli USA. Il Garante privacy irlandese respinge il ricorso richiamando in particolare la Decisione 26 Luglio 2000 n. 520 della Commissione UE, secondo la quale i "*Principi di approdo sicuro in materia di riservatezza*" allegati alla medesima decisione, applicati in conformità agli orientamenti forniti da talune "*Domande più frequenti*" (FAQ) parimenti allegate, garantiscono un livello adeguato di protezione dei dati personali trasferiti dalla Unione Europea ad organizzazioni aventi sede negli Stati Uniti sulla base della documentazione pubblicata dal Dipartimento del commercio statunitense. In base dunque alla c.d. *Decisione Safe Harbour*, la Commissione UE considerava gli Stati Uniti come Paese che assicura un adeguato livello di protezione dei dati personali ivi trasferiti.

L'Alta Corte irlandese, alla quale Maximilian Schrems si rivolge per impugnare la deliberazione del *Data Protection Commissioner,* decide quindi di coinvolgere la Corte di Giustizia UE sollevando una questione interpretativa preliminare per accertare se in la *Decisione Safe Harbour* determina l'effetto di impedire che una Autorità privacy nazionale possa decidere su un ricorso che contesti che un paese terzo non assicura un adeguato livello di protezione dei dati e – ove appropriato – sospenda il trasferimento dei dati.

### § 2. La sentenza della Corte di Giustizia UE e l'annullamento della *Decisione Safe Harbour*.

Nella sua sentenza del 6 ottobre 2015, la Corte di Giustizia UE ha chiarito che l'esistenza di una decisione della Commissione che stabilisce che un paese terzo (ovviamente extra UE) assicura un adeguato livello di protezione dei dati personali trasferiti in quel Paese non può eliminare - e nemmeno ridurre o limitare - i poteri delle Autorità di controllo nazionali ai sensi sia della Carta Fondamentale dei Diritti dell'Unione Europea che della Direttiva sulla protezione dei dati (la Direttiva 95/46/CE). In particolare la Corte di Giustizia richiama il diritto alla protezione dei dati personali garantito dalla Carta e i compiti di tutela demandati sempre dalla Carta alle Autorità nazionali di garanzia.

Più in particolare, La Corte di Giustizia UE precisa che nessuna disposizione della Direttiva europea sulla Tutela dei Dati Personali vieta alle Autorità nazionali di garanzia di sovrintendere o valutare i trasferimenti di dati personali verso Paesi terzi extra UE che sono stati oggetto di una Decisione della Commissione UE. Di conseguenza, anche ove la Commissione abbia adottato una decisione, le Autorità nazionali di supervisione, se investite di un ricorso, devono e possono esaminare in completa indipendenza se un trasferimento di dati personali verso un Paese terzo rispetta i requisiti contenuti nella Direttiva UE sulla protezione dei dati. Non di meno, la Corte evidenzia che essa sola ha il potere di dichiarare che un atto comunitario –

come una decisione della Commissione – è invalido. Di conseguenza, ove una autorità nazionale o la persona che ha avviato un ricorso davanti all'autorità nazionale considerino che una decisione della Commissione è invalida, tale autorità o quella persona devono avere la facoltà di portare il ricorso e il relativo procedimento avanti ai tribunali nazionali affinchè questi possano deferire il caso alla Corte di Giustizia se vi sono dubbi circa la validità dell'atto comunitario.

Chiariti questi presupposti, la Corte esamina poi se la Decisione *Safe Harbour* possa essere considerata invalida. In tale prospettiva, i giudici europei partono dal presupposto che la Commissione UE era stata richiesta di verificare se gli Stati Uniti d'America di fatto assicurassero, in base alle leggi nazionali o in base ad impegni discendenti da impegni assunti da quel Paese a livello internazionale, un livello di protezione dei diritti fondamentali (quale è quello alla protezione delle informazioni personali) essenzialmente equivalente a quello garantito all'interno dell'Unione Europea dalla Direttiva sulla protezione dei dati letta – però - alla luce della Carta Fondamentale dei Diritti UE. Conclude la Corte, tuttavia, che la Commissione non effettuò tale verifica, limitandosi ad esaminare semplicemente il c.d. "*schema di approdo sicuro*" (cioè un insieme di principi relativi alla protezione dei dati ai quali le organizzazione con sede negli Stati Uniti dovevano aderire su base volontaristica).

Senza approfondire gli aspetti se tale schema garantisca o meno un livello di protezione dei dati trasferiti essenzialmente equivalente a quello in vigore nella UE, la Corte osserva che lo "*schema di approdo sicuro*" è applicabile esclusivamente alle imprese americane che ad esso aderiscono, mentre le stesse autorità pubbliche USA non sono invece soggette a tale schema. Inoltre, esigenze sovrane quali la sicurezza nazionale, il pubblico interesse e le necessità di applicazione di principi normativi dell'ordinamento degli Stati Uniti d'America prevalgono sullo "*schema di approdo sicuro*", con la oggettiva conseguenza che le organizzazioni con sede negli USA sono addirittura obbligate, senza limitazione alcuna, a disapplicare i principi di tale schema cui pure abbiano aderito se essi entrano in conflitto che le superiori esigenze pubbliche appena segnalate. Lo schema di approdo sicuro come applicato negli USA rende dunque possibile l'interferenza – da parte delle autorità pubbliche americane – con i diritti fondamentali delle persone e la *Decisione Safe Harbour* della Commissione non solo non fa riferimento alla esistenza negli Stati Uniti d'America di regole che possano limitare tale interferenza, ma neanche alla esistenza di effettive tutele legali che proteggano da una tale interferenza.

Tra l'altro, la Corte integra la propria analisi sullo "*schema di approdo sicuro*" facendo riferimento al quadro che emerso da due Comunicazioni della Commissione UE: la Comunicazione "*Ricostruire la fiducia UE-USA nello scambio dei dati personali*" (COM2013/846 del 27 Novembre 2013) e la *Comunicazione della Commissione europea al Parlamento europeo sul funzionamento del Safe Harbour dalla prospettiva dei cittadini europei e delle imprese con sede nell'Unione Europea* (COM2013/847 del 27 Novembre 2013).

La Commissione europea aveva difatti suggerito nel 2013 le azioni da intraprendere per ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA a seguito delle profonde preoccupazioni sulle rivelazioni di programmi di raccolta di intelligence su larga scala degli Stati Uniti, che hanno avuto un impatto negativo sulle relazioni fra le due sponde dell'Atlantico. La risposta della Commissione si articolava: 1) in un documento strategico (comunicazione) sui flussi di dati transatlantici, che indica le sfide e i rischi emersi a seguito delle rivelazioni dei programmi di raccolta di intelligence statunitensi, e le misure da prendere per affrontare queste preoccupazioni; 2) in un'analisi del funzionamento della *Decisione Safe Harbour*; 3) una relazione sui risultati del gruppo di lavoro UE-USA (cfr. MEMO/13/1059) sulla protezione dei dati, costituito nel luglio 2013; 4) una revisione degli accordi esistenti sui dati del codice di prenotazione (*Passenger Name Record, PNR*) (cfr. MEMO/13/1054) e sul programma di controllo delle transazioni finanziarie dei terroristi (*Terrorist Finance Tracking Programme, TFTP)* che regolano gli scambi di dati in questi settori a fini di contrasto (cfr. MEMO/13/1164).

Vi è da dire che la stessa Commissione UE già nel 2013 – al fine di rendere più sicuro il regime "*Approdo sicuro*" – aveva suggerito 13 raccomandazioni correttive alla *Decisione Safe Harbour* per migliorarne il funzionamento, evidenziando come essa fosse carente sotto parecchi aspetti. E inoltre, la stessa Commissione – a conclusione dell'analisi condotta nel 2013 dopo lo scandalo successivo alle rivelazioni di Snowden – aveva riconosciuto che le autorità degli Stati Uniti d'America erano in grado di accedere ai dati personali trasferiti negli USA dall'UE e di trattarli in modalità incompatibili sia con gli scopi del trasferimento sia oltre quanto necessario e proporzionato alla luce della necessità di preservare la sicurezza nazionale. Inoltre, la Commissione osservò che le persone e le organizzazioni non avevano mezzi amministrativi o giurisdizionali per l'esercizio dei propri diritti di accesso ai dati, di rettifica o di cancellazione.

Con riguardo alle valutazioni sul livello di protezione essenzialmente equivalente a quello garantito a tutela dei diritti e delle libertà fondamentali nella UE – continua la Corte di Giustizia UE nella sua sentenza – i giudici europei affermano che ai sensi della legislazione UE, ove essa autorizzi (come nella *Decisione Safe Harbour*), in via generale, la conservazione di tutti i dati personali di tutti i soggetti le cui informazioni sono trasferite dall'Europa agli Stati Uniti, tale legislazione non limita i trattamenti a quanto strettamente necessario ed inoltre non prescrive la necessità di individuare differenziazioni, limitazioni o eccezioni alla luce delle finalità perseguite né pone un criterio oggettivo per determinare i limiti di accesso ai dati da parte delle autorità pubbliche e il conseguente uso dei dati trasferiti. Di conseguenza, continua la Corte UE, una regolamentazione che consenta alle autorità pubbliche l'accesso in via generalizzata al contenuto di dati e comunicazioni elettroniche deve essere valutata come in grado di compromettere l'essenza del diritto fondamentale al rispetto della

vita privata. D'altro canto, la Corte osserva che una regolamentazione che non preveda alcuna possibilità per i soggetti interessati di avvalersi di rimedi legali per accedere ai propri dati personali o di ottenere la rettifica o la cancellazione di tali dati compromette l'essenza del diritto fondamentale alla effettiva protezione giudiziale, diritto connaturato allo stesso principio di legalità.

Infine la Corte UE evidenzia che la *Decisione Safe Harbour* impedisce alle autorità nazionali di controllo (es: i Garanti privacy) di valutare i reclami di soggetti che richiedono ad esse di valutare se la Decisione è compatibile con la protezione della privacy e dei diritti e libertà fondamentali degli individui. E' in tale prospettiva che la Corte severamente dichiara che la Commissione non aveva competenza per restringere in tal modo tali poteri in capo alle autorità nazionali di supervisione e controllo.

Per tutte tali argomentazioni, la Corte di Giustizia ha dichiarato invalida la *Decisione Safe Harbour.*

**§ 3. Le conseguenze pratiche dell'annullamento della *Decisione Safe Harbour*: gli altri presupposti di liceità per il trasferimento dei dati personali negli USA.**

In primo luogo, la sentenza è destinata ad avere rilevanti impatti pratici non solo per quanto concerne aspetti relativi alla vita privata delle persone (e il caso nasce appunto dalla contestazione di un privato cittadino circa il trasferimento dei suoi dati Facebook negli USA). Gli effetti sono altresì destinati a riverberarsi anche sulle organizzazioni aziendali che – per i più svariati motivi – trasferiscono dati personali negli USA per fini commerciali o gestionali: si pensi ai grandi gruppi con Holding controllanti con sede in USA che impongono il trasferimento e la conservazione centralizzata negli Stati Uniti dei dati dei dipendenti delle sedi europee ed estere; oppure si pensi a società che offrono servizi di comunicazione elettronica che sempre più spesso si avvalgono di *server farms* in USA per la conservazione dei dati degli utenti; o si pensi, ancora, ai contratti di *outsourcing* con imprese USA. Insomma, la questione non è solo rappresentata dai rischi per la vita privata del passeggero di aerei o dell'utente Facebook (ma anche Apple, Google e Microsoft) i cui dati vengono trasferiti negli USA: la questione attiene ora anche alla necessità di impostare corrette politiche aziendali in tutti quei casi ove i dati dei soggetti interessati (dipendenti, clienti, fornitori, etc) sono trasferiti in USA.

Va detto che la *Decisione Safe Harbour* non è e non era l'unico presupposto di liceità del trasferimento dei dati personali negli Stati Uniti, anche se – da un certo punto di vista – rappresentava la via più comoda e meno "burocratica" per fondare la liceità del trasferimento, essendo sufficiente la c.d. *certificazione Safe Harbour* (cioè la iscrizione volontaristica dell'impresa a tale sistema in un registro detenuto dal Ministero per il Commercio Estero USA) da parte dell'organizzazione americana destinataria dei dati.

Il Codice della privacy italiano, ad esempio (così come la Direttiva UE sulla protezione dei dati, all'art. 26) disciplina il trasferimento dei dati all'estero (non solo negli USA) distinguendo tra trasferimento intra-comunitario e trasferimenti dei dati verso Paesi extra UE. Il trasferimento dei dati intra-comunitario – proprio per l'esistenza di un adeguato livello di protezione discendente dalla implementazione della Direttiva sulla *data protection* in tutti i 28 Paesi membri – non pone alcun problema: anzi, l'impostazione del Legislatore è altamente "liberale" visto che le disposizioni del Codice privacy non possono essere applicate in modo tale da restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione europea, fatta salva l'adozione eventuali provvedimenti in caso di trasferimenti di dati effettuati al fine di eludere le medesime disposizioni (art. 42). In sostanza nemmeno è del tutto corretto parlare di "trasferimento", visto che lo spazio UE (e lo Spazio Economico Europeo: Norvegia, Islanda, Liechtenstein) è considerato un unico territorio.

Nel caso invece di trasferimenti di dati verso Paesi extra-UE, vige un principio del tutto opposto, che è quelle del divieto: il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è vietato quando l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato. Sono valutate anche le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza.

Tale divieto è soggetto ad eccezionali deroghe. Una prima deroga consente il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, se diretto verso un Paese non appartenente all'Unione europea, in base a specifica autorizzazione del Garante oppure se si verificano i seguenti presupposti fissati dall'art. 43 del Codice della privacy:

a) l'interessato ha manifestato il proprio consenso espresso o, se si tratta di dati sensibili, in forma scritta;

b) il trasferimento è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;

c) il trasferimento è necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento;

d) il trasferimento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo;

e) il trasferimento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

f) il trasferimento è effettuato in accoglimento di una richiesta di accesso ai documenti amministrativi, ovvero di una richiesta di informazioni estraibili da un pubblico registro, elenco, atto o documento conoscibile da chiunque, con l'osservanza delle norme che regolano la materia;

g) il trasferimento è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico.

La seconda deroga al divieto di trasferimento dei dati verso Paesi extra UE è rappresentato dalle cosiddette "*decisioni di adeguatezza*". Difatti, la Commissione europea può stabilire, sulla base di un procedimento che prevede, fra l'altro, il parere favorevole del Gruppo dei Garanti privacy UE, che il livello di protezione offerto in un determinato Paese è adeguato (articolo 25, comma 6, della Direttiva 95/46/CE), e che pertanto è possibile trasferirvi dati personali. Sulla base di questo meccanismo, ad oggi gli Stati extra-UE che seguono sono stati ritenuti – con apposita "*decisione di adeguatezza*"ratificata da altrettanti provvedimenti dei Garanti nazionali – come offrire un adeguato livello di protezione nella rispettive legislazioni, con la conseguenza che trasferire i dati in tali Paesi è come trasferirli all'interno della UE:

1. Andorra
2. Argentina
3. Australia – PNR
4. Canada
5. Faer Oer
6. Guernsey
7. Isola di Man
8. Israele
9. Jersey
10. Nuova Zelanda
11. Svizzera
12. Uruguay

Tra questi Paesi ci sarebbero ancora (come anche riportato sul sito del Garante privacy, dal quale è stata prontamente eliminata la sezione sul Safe Harbour..) gli USA, sulla base dell'accordo del Safe Harbour (ora dichiarato invalido dalla Corte di

Giustizia) e dell'accordo PNR - (*Passenger Name Record, PNR*) sul trasferimento dei dati dei passeggeri degli aerei…

La terza deroga al divieto è rappresentata dalle cosiddette "*clausole contrattuali standard*". La Commissione europea, ai sensi dell'articolo 26(4) della Direttiva 95/46/CE, può stabilire che determinati strumenti contrattuali consentono di trasferire dati personali verso Paesi terzi. In pratica, incorporando il testo delle clausole contrattuali in questione in un contratto utilizzato per il trasferimento (*Data Transfer Agreement*), l'esportatore dei dati garantisce che questi ultimi saranno trattati conformemente ai principi stabiliti nella Direttiva anche nel Paese terzo di destinazione. Sinora la Commissione ha adottato quattro decisioni in materia.

Infine, la quarta deroga al divieto è rappresentata dalla procedura cosiddetta delle *BCR – Binding Corporate Rules*. Si tratta di uno strumento volto a consentire il trasferimento di dati personali dal territorio dello Stato verso Paesi terzi (extra-UE) tra società facenti parti dello stesso gruppo d'impresa. Le BCR si concretizzano in un documento contenente una serie di clausole (*rules*) che fissano i principi vincolanti (*binding*) al cui rispetto sono tenute tutte le società appartenenti ad uno stesso gruppo (*corporate*).

Le BCR costituiscono un meccanismo in grado di semplificare gli oneri amministrativi a carico delle società di carattere multinazionale con riferimento ai flussi intragruppo di dati personali.

Il rilascio di un'autorizzazione al trasferimento di dati personali tramite BCR consente alle filiali della multinazionale che ne abbia fatto richiesta, anche se stabilite in diversi Paesi, di trasferire, all'interno del gruppo d'impresa, i dati personali oggetto delle BCR, senza ulteriori adempimenti (quali ad esempio la sottoscrizione di clausole contrattuali tipo, il rilascio di specifiche autorizzazioni ai sensi del Codice, etc).

La procedura per la definizione del testo delle BCR prevede una fase "europea" ed una fase "nazionale"; quest'ultima è finalizzata al rilascio dell'autorizzazione nazionale (ove necessaria, come in Italia).

Con riferimento alla procedura a livello europeo, e dal momento che le BCR hanno ad oggetto i flussi di dati personali tra società appartenenti a un unico gruppo di impresa e dislocate in diversi paesi del mondo, l'autorizzazione al trasferimento transfrontaliero di dati trova una sua utilità esclusivamente se rilasciata da tutte le Autorità di protezione dei dati competenti negli Stati Membri da cui hanno origine i trasferimenti.

Per questo motivo, il Gruppo dei Garanti UE ha elaborato una procedura di cooperazione a livello europeo in grado di assicurare la predisposizione di un testo di BCR condiviso da tutte le Autorità e valevole per tutti i trasferimenti oggetto delle BCR medesime. Tale procedura è condotta da una sola Autorità (c.d. "*lead Authority*") la quale dialoga, in rappresentanza di tutte le altre Autorità privacy, con la società capogruppo. In particolare, la *lead Authority* esamina la bozza di BCR presentata dalla

società (c.d. "*consolidated draft*"), la invia alle altre Autorità per riceverne eventuali commenti (Fase 1) e dialoga con la società per la predisposizione di un testo che accolga tutte le osservazioni formulate (c.d. "*final draft*" - Fase 2).

Il documento così redatto è inviato alle Autorità partecipanti alla procedura, al fine di ottenerne una valutazione positiva in termini di adeguatezza del livello di protezione dei dati personali.

Di recente, alcune Autorità (fra cui il Garante) hanno aderito ad una dichiarazione di intenti, c.d. "*Dichiarazione di Mutuo riconoscimento*", al fine di semplificare la procedura di approvazione del testo di BCRa livello europeo, velocizzandone la relativa tempistica.

Ai sensi di tale nuovo modello, la lead Authority, con il supporto di altre due Autorità, dialoga con la società capogruppo al fine di giungere alla predisposizione di un testo ritenuto in linea con i principi fissati dai documenti in materia di BCR emanati dai Garanti privacy UE.

Il parere con il quale la *lead Authority* attesta la conformità del testo di BCR ai principi sopra indicati è considerato dalle altre Autorità aderenti al sistema di Mutuo riconoscimento quale fondamento sufficiente al rilascio della rispettiva autorizzazione nazionale.

Qualora la singola Autorità si esprima a favore del testo di BCR, ovvero una volta raggiunta la definizione di un testo di BCR giudicato conforme dalla lead Authority in base alla procedura semplificata sopra descritta, l'Autorità nazionale potrà procedere al rilascio di un'autorizzazione nazionale al trasferimento dei dati personali oggetto del testo medesimo, ove prevista.

* * * * *

## § 4. Valutazioni conclusive: gli scenari del *cross-border data flow*.

Dunque i titolari del trattamento non potranno più fondare il trasferimento dei dati personali verso gli USA appellandosi alla certificazione Safe Harbour dell'organizzazione statunitense destinataria.

Tra l'altro, appare opportuno ricordare che l'effetto dell'annullamento della Decisione da parte della Corte di Giustizia UE non ha determinato affatto il divieto automatico di trasferimento verso gli USA: la sentenza ha l'effetto di "restituire" al Garante privacy irlandese (che aveva respinto il reclamo di Schrems sulla base della mera esistenza della *Decisione Safe Harbour*) il potere-dovere di riesaminare il ricorso e di verificare, alla conclusione della istruttoria, se il trasferimento dei dati personali dei titolari europei di account Facebook verso gli Stati Uniti d'America sia conforme alla Direttiva UE sulla tutela dei dati personali o – in caso contrario – se debba essere sospeso perché quel Paese non offre un livello di protezione dei dati adeguato ed equivalente a quello vigente nella UE.

Ma è ovvio che comunque l'effetto pratico dell'annullamento della Decisione Safe Harbour è quello di non potere più fondare il trasferimento dei dati verso gli USA sulla base dell'accordo di approdo sicuro. Ciò per le altre motivazioni che la Corte di Giustizia ha lucidamente illustrato e per le quali ha ritenuto invalido il sistema dell'Approdo Sicuro (interferenza delle autorità pubbliche non soggette all'accordo, dovere delle organizzazioni USA aderenti all'accordo di subire tali interferenze per superiori principi normativi, inesistenza di rimedi legali per gli interessati, come il diritto di accesso, rettifica, cancellazione dei dati, etc).

Come ci si deve allora comportare per impostare correttamente le politiche organizzative di *data transfer* verso gli USA o comunque verso Paesi non appartenenti alla UE, allo Spazio Economico Europeo o alla lista dei 12 Stati considerati "adeguati"?

Premesso che le procedure e le modalità illustrate al paragrafo precedente (autorizzazione al trasferimento specifica del Garante, che ad esempio la ha rilasciata anche per Paesi quali la Confederazione Elvetica o la Nuova Zelanda, presupposti ex art. 43 del Codice della privacy, decisioni di adeguatezza, clausole contrattuali standard, BCR – *Binding Corporate Rules*) sono tra di loro alternative, deve formularsi una prima considerazione proprio alla luce della sentenza della Corte di Giustizia UE.

La Corte ha annullato la Decisione della Commissione UE sul presupposto (anche) che la stessa non è applicabile alle autorità pubbliche e non evita interferenze di queste con i diritti e le libertà fondamentali dei cittadini. Sorge automatico il dubbio che lo stesso principio sarebbe applicabile allora anche ad altre decisioni della Commissione UE: ad esempio alle decisioni con le quali sono stati ritenuti idonei i Paesi sopra elencati (ci si dovrebbe chiedere se la valutazione di adeguatezza delle legislazioni di quei Paesi ha avuto ad oggetto anche norme privacy locali che vietino o regolamentino le interferenze delle autorità pubbliche…). Oppure la Decisione con la quale la Commissione ha approvato la procedura BCR o le clausole contrattuali standard, che pure si applicano sostanzialmente a soggetti privati (anche se non sono vietati *data transfer agreement* con destinatari pubblici).

Al di là di questa considerazione, deve comunque ritenersi che allo stato la via più sicura per impostare corrette politiche del trasferimento dei dati verso Paesi extra UE non dotati di un quadro giuridico privacy che offra un adeguato livello di protezione sia rappresentata – almeno per le imprese che non sono parte di Gruppi multinazionali che possono accedere alla procedura BCR - dalla stipula di appositi *Data Transfer Agreement* con l'importatore estero dei dati che incorporino le clausole contrattuali standard. Ciò perché – solo per fare un esempio – tali clausole prevedono specificatamente obblighi per il destinatario-importatore dei dati di consentire l'esercizio di tutti i diritti privacy degli interessati ai sensi della legislazione nazionale dell'esportatore e fanno salvi i poteri di controllo, intervento e giurisdizione dell'Autorità privacy nazionale cui l'interessato cui si riferiscono i dati può rivolgersi

in caso di violazione dei suoi diritti. Dunque esattamente due aspetti per i quali la Corte di giustizia UE ha invece ritenuto carente e invalida la *Decisione Safe Harbour*.

La Commissione europea ha promesso che "*nelle prossime settimane*" presenterà un piano per dare attuazione alla sentenza e per un quadro normativo più chiaro e con salvaguardie idonee. Dal 2013 l'Unione europea – come detto - sta negoziando con gli Stati Uniti un nuovo accordo per la gestione e lo scambio dei dati personali on-line e l'intenzione è di arrivare alla conclusione dei colloqui il prima possibile. Anche se – a parere di chi scrive – alla luce degli altri accordi USA-UE (es: le negoziazioni segrete in corso sul *Transatlantic Trade and Investment Partnership* - o TTIP, cioè il Trattato di liberalizzazione commerciale transatlantico che ha l'intento dichiarato di abbattere dazi e dogane tra Europa e Stati Uniti rendendo il commercio e lo scambio di dati libero tra le due sponde dell'oceano) il rischio per la protezione dei dati personali dei cittadini appare sempre più elevato, e la vittoria del Sig. Schrems un piccolo episodio di una battaglia molto più grande.