Cristina Vicarelli
Avvocato

Invalidazione del Safe Harbor e cloud computing

Il Safe Harbor, il 6 ottobre 2015, è stato protagonista di una delle più importanti sentenze in tema di trattamento dei dati personali rese dalla Corte di Giustizia dell'Unione Europea, che, polverizzandolo, ha colpito al cuore uno dei ponti più utilizzati per trasferire dati personali negli Stati Uniti. Cos'era esattamente il Safe Harbor e quale impatto ha questa sentenza sui sistemi cloud?

Per rispondere a questa domanda occorrerà, da una parte, fare un breve riepilogo delle regole che presiedono al trasferimento dei dati all'estero, in modo da collocare la pronuncia in un quadro coerente, ma, dall'altra, preliminarmente, occorre precisare che perché la sentenza spieghi i suoi effetti su di un servizio cloud, occorre che vi sia trattamento di dati personali. Prima di preoccuparsi degli effetti della sentenza, pertanto, è necessario determinare se il servizio cloud utilizzato comporti o meno un trattamento di dati personali e, in seconda battuta, se il servizio comporti un trasferimento dei dati all'estero. Occorrerà anche tener presente che sono dati personali, per la normativa europea (e da qualche anno anche per quella italiana), **solo** le informazioni concernenti una **persona fisica** identificata o identificabile. Se, infatti, il servizio non comporta un trattamento di dati personali (la definizione di dato personale è molto ampia, essendo tale anche il dato pseudonomizzato) o, pur comportando tale trattamento i dati personali non vengono trasferiti in paesi terzi (ovvero non apparenti all'Unione Europea), rispetto agli effetti della sentenza in commento, non si pone alcun problema.

Non è un manierismo: il Garante Privacy, infatti, già in "Cloud computing: indicazioni per l'uso consapevole dei servizi" nel 2011, invitava gli utenti di servizi cloud a evitare di trasferire sui tale tipologia di infrastrutture determinati tipi di dati, che richiedono stringenti misure di sicurezza, e, negli altri casi, li invitava a informarsi su dove risiedessero,

concretamente, i dati, evitando o minimizzando, per quanto possibile, il trattamento dei dati personali nell'uso di tali servizi.

Se si utilizza un servizio cloud che comporta il trattamento di dati personali, sarà bene appurare ora, se non lo si è fatto prima, ove questi vengano trattati, risalendo la catena dei trattamenti che spesso li caratterizza, attraverso la stratificazione di architetture e subfornitori.

Per l'Autorità, infatti : "Non è (…) indifferente per l'utente sapere se i propri dati si trovino in un server in Italia, in Europa o in un imprecisato Paese extraeuropeo. In ogni caso, l'utente, prima di inserire i dati nella nuvola informatica, dovrebbe assicurarsi che il trasferimento tra i diversi paesi in cui risiedono le cloud avvenga nel rispetto delle cautele previste a livello di Unione europea in materia di protezione dei dati personali, che esigono particolari garanzie in ordine all'adeguatezza del livello di tutela previsto dagli ordinamenti nazionali per tale tipo di informazioni".

In questi casi, qualora i servizi cloud fossero basati in paesi terzi, e segnatamente, negli Stati Uniti, occorrerà prestare molta attenzione.

E' altresì importante comprendere che molti servizi di condivisione di documenti, di messaggistica o di posta elettronica possono essere cloud based. La sentenza sul Safe Harbor potrebbe interessare anche i fornitori di questi servizi: è bene, pertanto, verificare se, nei termini di servizio o nelle condizioni generali di contratto si faccia riferimento al Safe Harbor.

Sarà utile a questo punto, e prima di commentare la pronuncia, tratteggiare rapidamente il quadro normativo.

La normativa

Occorre rammentare, in estrema sintesi, come la normativa europea (e anche quella italiana, che ricalca la Direttiva 95/46/CE), ponga un **generale divieto di trasferire dati personali in paesi terzi,** a meno che non ricorra una di queste 3 condizioni:

1. il paese terzo garantisca ai dati personali un **livello di protezione "adeguato**";
2. l'interessato abbia manifestato il proprio **consenso** in maniera inequivocabile;
3. sussistano **idonee garanzie contrattuali**, ossia:

- o sono state adottate delle **clausole standard** (citate dagli addetti ai lavori anche come "Model Clauses") elaborate dalla Commissione Europea che garantiscano la tutela dei dati personali degli interessati,
- oppure sono state adottate le cosiddette **BCR (Binding Corporate Rules**), ossia norme privatistiche elaborate da gruppi di imprese che vengono sottoposte a un peculiare processo di approvazione da parte delle Data Protection Autority europee e sono finalizzate a regolamentare gli scambi di dati personali che coinvolgono il gruppo stesso, con riguardo alle tutele che assistono il trasferimento di dati personali in paesi terzi.

Altre condizioni che giustificano il trasferimento verso paesi terzi sono elencate al comma 1 dell'articolo 26 della Direttiva 95/46/CE, ma si tratta di ipotesi specifiche che cadono di lato rispetto alla presente disamina trattandosi di fattispecie relative a trasferimenti motivati da rapporti (anche pre) contrattuali tra titolare e interessato, o autorizzati dalla legge per la salvaguardia di un interesse pubblico rilevante, per la difesa in giudizio o la salvaguardia della vita o dell'integrità fisica, o in riferimento al caso in cui, nel rispetto delle norme previste per la consultazione, il trasferimento avvenga da parte di un registro pubblico.

Il Gruppo ex Articolo 29 della Direttiva 95/46/CE ha affermato nel Documento di lavoro 12/1998 che le esenzioni di cui al primo comma dell'art. 26, compresa quella inerente la prestazione del consenso inequivocabile da parte dell'interessato, si applicano **solo quando i trasferimenti non sono ricorrenti, né massicci o strutturali** ribadendo nel 2012

(v. oltre) che sulla base di tali interpretazioni è quasi impossibile applicare quelle deroghe nel contesto del cloud computing.

La Sentenza della Corte di Giustizia del 6 ottobre 2015, a una prima lettura, riguarda il trasferimento verso un paese terzo che garantisce (rectius, nel caso del Safe Harbor, garantiva) un livello adeguato di protezione. Come si determina l'adeguatezza? Essa è rimessa alla Commissione Europea. La Commissione, infatti, può stabilire, sulla base di un procedimento che prevede, fra l'altro, il parere favorevole del Gruppo ex Articolo 29 della Direttiva 95/46/CE (d'ora innanzi WP ART 29), che il livello di protezione offerto in un determinato Paese è adeguato (articolo 25, comma 6, della Drettiva 95/46/CE), e che, pertanto, è possibile trasferirvi dati personali.

I trasferimenti, una volta stabilita con tali modalità l'adeguatezza del paese terzo, avvengono senza ulteriori adempimenti, previo recepimento della decisione nell'ordinamento del Paese Membro da parte dell'Autorità nazionale (In Italia è prevista l'autorizzazione del Garante ex art. 44 Codice Privacy).

La decisione di adeguatezza della Commissione adottata il 26 luglio 2000, nei confronti degli Stati Uniti, basata su determinati standard ai quali le imprese statunitensi destinatarie dei trattamenti dichiaravano spontaneamente di aderire, era, appunto, individuata come "Safe Harbor", o, nella traduzione italiana, "Approdo Sicuro". Il termine veniva usato, infatti, sia in riferimento al protocollo (più che altro di principio) seguito dalla imprese aderenti, sia per indicare la decisione della Commissione che ne accalcava l'adeguatezza: qui viene usato principalmente per individuare la decisione della Commissione.

Safe Harbor e Cloud Computing

Nel 2012 il WP ART 29 era intervenuto con il parere 5/2012 (WP 196) sul Cloud Computing, allo scopo di orientare i titolari dei trattamenti sulle criticità connesse a tali servizi. Nell'occasione, il Gruppo dimostrava una certa diffidenza nei confronti delle decisioni di adeguatezza, osservando che tali decisioni, ivi compresi i principi Safe Harbor

("approdo sicuro"), hanno un ambito di applicazione geografica limitata e quindi non coprono tutti i trasferimenti all'interno del cloud.

Più specificamente, in ordine al Safe Harbor, pur ammettendo che i trasferimenti verso organizzazioni USA che aderissero a tali principi potessero avvenire legalmente ai sensi della legislazione UE, il Gruppo di lavoro rilevava che la sola autocertificazione di conformità al Safe Harbor poteva non essere considerata sufficiente in assenza di una solida applicazione dei principi di protezione dei dati nel contesto del sistema cloud.

Il Gruppo di lavoro riteneva, in buona sostanza, che le società che esportano dati dovessero ottenere le prove dell'esistenza delle autocertificazioni Safe Harbor e richiedere che venisse dimostrata l'osservanza dei relativi principi. Aspetto importante, soprattutto in ordine alle informazioni fornite ai soggetti interessati dal trattamento dei dati.

Non solo: il Gruppo di lavoro riteneva anche che il cliente cloud dovesse verificare che i contratti tipo offerti dai fornitori cloud fossero conformi ai requisiti nazionali concernenti le clausole contrattuali sul trattamento dei dati, ritenendo che spesso mancassero elementi richiesti dalle citate normative, e che tali elementi non potessero essere sostituiti dalla mera adesione al Safe Harbor. In questi casi, l'esportatore era incoraggiato a utilizzare altri strumenti giuridici disponibili, come le clausole contrattuali standard o le norme vincolanti d'impresa (BCR).

Soprattutto l'adesione al Safe Harbor appariva del tutto carente in merito alle misure di sicurezza: anche sotto questo primario aspetto apparivano necessarie integrazioni.

Nella pratica, tuttavia, anche a causa dello squilibrio tra la forza contrattuale del fornitore e quella del cliente titolare dei dati, molti rapporti si sono appianati sulla mera adesione al Safe Harbor, dichiarata dal fornitore stesso.

Degli aspetti privacy rilevanti da inserire nella contrattazione dei servizi cloud avevo già parlato in altro post, al quale rinvio.

La Sentenza della Corte di Giustizia

In questo quadro, già complesso, deflagra la pronuncia della Corte di Giustizia, su una causa avviata dal signor Maximilian Schrems, un cittadino austriaco utilizzatore di Facebook dal 2008. Come accadeva per gli altri iscritti residenti nell'Unione, i dati forniti dal signor Schrems a Facebook erano trasferiti, in tutto o in parte, a partire dalla filiale irlandese di Facebook, su server situati nel territorio degli Stati Uniti, dove erano oggetto di trattamento. Il signor Schrems, alla luce delle rivelazioni fatte nel 2013 dall'ormai noto whistleblower Edward Snowden in merito alle attività dei servizi di intelligence negli Stati Uniti (in particolare della National Security Agency, o «NSA»), ha adito l'autorità irlandese di controllo ritenendo che il diritto e le prassi statunitensi non offrissero una tutela adeguata contro la sorveglianza svolta dalle autorità pubbliche sui dati trasferiti verso tale paese. L'autorità irlandese ha respinto la denuncia, segnatamente con la motivazione che, in una decisione del 26 luglio 2000, la Commissione aveva ritenuto che, nel contesto del cosiddetto regime di "Safe Harbor", gli Stati Uniti garantissero un livello adeguato di protezione dei dati personali trasferiti.

La High Court of Ireland (Alta Corte di giustizia irlandese), investita della causa, ha adito la Corte di Giustizia, per conoscere se questa decisione della Commissione producesse l'effetto di impedire a un'autorità nazionale di controllo di indagare su una istanza con cui si lamenti che un paese terzo non assicuri un livello di protezione adeguato e, se necessario, di sospendere il trasferimento di dati contestato.

La Corte di Giustizia rende una sentenza storica:

Innanzi tutto afferma che l'esistenza di una decisione della Commissione che dichiara che un paese terzo garantisce un livello di protezione adeguato dei dati personali trasferiti non può sopprimere e neppure ridurre i poteri di cui dispongono le autorità nazionali di controllo in forza della Carta dei diritti fondamentali dell'Unione europea e della Direttiva 95/46/CE. La Corte sottolinea, a questo proposito, il diritto alla protezione dei dati

personali garantito dalla Carta e la missione di cui sono investite le autorità nazionali di controllo in forza della Carta medesima.

La Corte considera che nessuna disposizione della direttiva osta a che le autorità nazionali controllino i trasferimenti di dati personali verso paesi terzi oggetto di una decisione della Commissione. Anche quando esiste una decisione della Commissione, quindi, le autorità nazionali di controllo, investite di una domanda, devono poter esaminare in piena indipendenza se il trasferimento dei dati di una persona verso un paese terzo rispetti i requisiti stabiliti dalla direttiva. Tuttavia, la Corte ricorda che solo essa è competente a dichiarare invalida una decisione della Commissione, così come qualsiasi atto dell'Unione. Pertanto, qualora un'autorità nazionale o una persona ritenga che una decisione della Commissione sia invalida, tale autorità o persona deve potersi rivolgere ai giudici nazionali affinché, nel caso in cui anche questi nutrano dubbi sulla validità della decisione della Commissione, essi possano rinviare la causa dinanzi alla Corte di giustizia. **Pertanto, in ultima analisi è alla Corte che spetta il compito di decidere se una decisione della Commissione è valida o no.**

La Corte passa quindi a verificare la validità della decisione della Commissione del 26 luglio 2000. A questo proposito, la Corte ricorda che la Commissione era tenuta a constatare che gli Stati Uniti garantiscano effettivamente, in considerazione della loro legislazione nazionale o dei loro impegni internazionali, un livello di protezione dei diritti fondamentali **sostanzialmente equivalente** a quello garantito nell'Unione a norma della Direttiva, interpretata alla luce della Carta. La Corte osservava che la Commissione non ha proceduto a una constatazione del genere, ma si è limitata a esaminare il regime dell'approdo sicuro.

Orbene, senza che alla Corte occorra verificare se questo sistema garantisce un livello di protezione sostanzialmente equivalente a quello assicurato nell'Unione, la Corte rileva che esso è esclusivamente applicabile alle imprese americane che lo sottoscrivono e che, invece, **le autorità pubbliche degli Stati Uniti non vi sono assoggettate**. Inoltre, le

esigenze afferenti alla sicurezza nazionale, al pubblico interesse e all'osservanza delle leggi statunitensi prevalgono sul regime del Safe Harbor, cosicché le imprese americane sono tenute a disapplicare, senza limiti, le norme di tutela previste da tale regime laddove queste ultime entrino in conflitto con tali esigenze. Il regime statunitense del Safe Harbor rende così possibili **ingerenze da parte delle autorità pubbliche americane nei diritti fondamentali delle persone,** e la decisione della Commissione non menziona l'esistenza, negli Stati Uniti, di norme intese a limitare queste eventuali ingerenze, **né l'esistenza di una tutela giuridica efficace contro tali ingerenze.**

Per quanto attiene al livello di tutela **sostanzialmente equivalente** alle libertà e ai diritti fondamentali garantiti all'interno dell'Unione, la Corte dichiara che, nel diritto dell'Unione:

- una normativa non è limitata allo stretto necessario se autorizza in **maniera generalizzata** la conservazione di tutti i dati personali di tutte le persone i cui dati sono trasferiti dall'Unione verso gli Stati Uniti
- **senza che sia operata alcuna differenziazione, limitazione o eccezione** in funzione dell'obiettivo perseguito
- e senza che siano fissati **criteri oggettiv**i intesi a circoscrivere l'accesso delle autorità pubbliche ai dati e la loro successiva utilizzazione.

La Corte soggiunge che una normativa che consenta alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche deve essere considerata **lesiva del contenuto essenziale del diritto fondamentale al rispetto della vita privata.**

Parimenti, la Corte osserva che una normativa che **non preveda alcuna facoltà per il singolo di esperire rimedi giuridici diretti ad accedere ai dati personali che lo riguardano o ad ottenerne la rettifica o la cancellazione viola il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva,** facoltà, questa, che è connaturata all'esistenza di uno Stato di diritto.

Infine, la Corte dichiara che la decisione della Commissione del 26 luglio 2000 priva le autorità nazionali di controllo dei loro poteri nel caso in cui una persona contesti la compatibilità della decisione con la tutela della vita privata e delle libertà e diritti fondamentali delle persone. La Corte afferma che la Commissione non aveva la competenza di limitare in tal modo i poteri delle autorità nazionali di controllo.

Per questo complesso di motivi, la Corte dichiara invalida la decisione della Commissione del 26 luglio 2000.

Si tratta di una pronuncia pregiudiziale, ed è importante ricordarlo perché la sentenza interpretativa della Corte pronunciata su rinvio pregiudiziale non solo vincola il giudice a quo, che è tenuto ad applicare la norma dell'Unione secondo l'interpretazione offerta dalla Corte, e gli altri giudici e le amministrazioni nazionali che sono tenuti a fare applicazione delle norme così come interpretate dalla Corte, ma obbliga anche gli Stati Membri ad adottare tutte le misure idonee ad adeguare il proprio ordinamento alla norma dell'Unione così come interpretata dalla Corte, pena la violazione del principio di leale cooperazione e conseguente obbligo di risarcire i danni .

Gli effetti della sentenza

Il primo, evidente, effetto della sentenza è l'invalidazione del Safe Harbor. Ciò ha comportato un'evidente ricaduta: l'illiceità dei trasferimenti di dati personali basati sul Safe Harbor stesso.

In Italia, il 22 ottobre 2015 Il Garante emetteva il provvedimento "Trasferimento dati personali verso gli USA: caducazione provvedimento del Garante del 10.10.2001 di riconoscimento dell'accordo sul c.d. "Safe Harbor" Pubblicato sulla Gazzetta Ufficiale n. 271 del 20 novembre 2015.

Il Garante sottolineava che, venuto meno il presupposto di liceità del trasferimento di dati, e in attesa delle prossime decisioni che sarebbero state assunte in sede europea, le imprese avrebbero potuto dunque trasferire lecitamente i dati delle persone solo

avvalendosi di altri strumenti quali, ad esempio, le clausole contrattuali standard o le regole di condotta adottate all'interno di un medesimo gruppo (le cosiddette BCR, Binding Corporate Rules).

Il provvedimento del Garante seguiva, senza ricalcarla, la posizione comune assunta dai Garanti Europei. Il WP ART 29, infatti, si era riunito il 16 ottobre 2015 pubblicando una dichiarazione volta a dettare una linea comune in ordine alla attuazione della sentenza resa dalla Corte di Giustizia.

Il WP ART 29 da una parte evidenziava come le problematiche connesse alla sorveglianza di massa fossero un elemento chiave della decisione della Corte, esplicitando ciò che nella pronuncia restava implicito: se il problema è la sorveglianza di massa senza limiti e tutele, **nessuno degli strumenti di trasferimento a disposizione può superare l'incompatibilità tra la normativa europea e quella statunitense.**

Dall'altra parte poneva in evidenza come, a fronte dei profili di inadeguatezza delineati in sentenza, il giudizio di adeguatezza avrebbe dovuto essere molto cauto.

Nonostante i rilievi ora sommariamente accennati invitava la Commissione ad aprire un dialogo con gli Stati Uniti al fine di raggiungere un nuovo protocollo, un Safe Harbor 2, che potesse ricondurre i trasferimenti verso gli USA entro standard di adeguatezza.

Fissava un termine, il 30 gennaio 2016, entro il quale rimpiazzare la decisione di adeguatezza, riservandosi di procedere nel frattempo alla disamina delle ricadute della sentenza sugli altri strumenti di trasferimento, dei quali, medio tempore, consentiva l'utilizzo: clausole standard e BCR.

Ad oggi l'accordo sul Safe Harbor 2 non è ancora stato raggiunto, e il WP ART 29 si riunirà il 2 febbraio 2016, e scioglierà le riserve assunte.

A pochi giorni dalla data fissata per la riunione, è ancora impossibile determinare quale sarà la sorte non solo del Safe Harbor 2, che ormai pare essere il problema minore, ma

anche di model clauses e BCR, dato che potrebbero essere bloccati anche i trasferimenti basati su questi strumenti.

Nel lasso di tempo accordato dal WP ART 29 alla Commissione, le dichiarazioni di talune autorità nazionali non sono state sempre rassicuranti: una DPA tedesca ha mostrato di non considerare le model clauses uno strumento adeguato, in contrasto con altre; sempre in Germania anche il Governo è intervenuto di recente a illustrare la propria posizione in ordine all'adeguatezza delle clausole standard e delle BCR.

Anche l'Autorità francese si è mostrata molto scettica, paventando il blocco dei trasferimenti verso gli USA se non interverranno novità entro la fine di Gennaio, mentre il Garante Italiano, profilando la pesante ricaduta economica che avrebbero le imprese italiane da quella che viene definita da più parti come la balcanizzazione dell'internet, ha fatto appello al Presidente del Consiglio per far pressioni politiche allo scopo di non polverizzare anche i trasferimenti basati su BCR e clausole standard.

Non solo: se davvero non si avrà un nuovo Safe Harbor nel termine assegnato, e il WP ART 29 spazzasse via anche gli altri strumenti sulla scorta dell'insufficiente livello di adeguatezza degli USA, quante delle decisioni di adeguatezza resterebbero in piedi?

I commentatori più attenti hanno rilevato come lo standard di adeguatezza sia stato fissato dalla Corte di Giustizia su un piano molto alto: occorre garantire una protezione sostanzialmente identica a quella che garantisce l'UE.

Un simile standard, unito alla possibilità riconosciuta alle autorità nazionali di investigare circa il livello di protezione offerto dagli stati, e al potere della Corte di Giustizia di invalidare le decisioni che non garantiscano livelli di protezione adeguati potrebbe innescare un effetto domino in grado di **travolgere tutte le (poche) decisioni di adeguatezza già adottate**.

Le ricadute sui servizi cloud

Per quanto appena detto è evidente come la sentenza Schrems sia potenzialmente in grado di impattare profondamente sui sistemi cloud.

Non solo per la natura del cloud, che comporta una copertura territoriale atipica destinata a restare sotto lo scacco dalla possibile caducazione delle altre decisioni di adeguatezza già adottate, effetto che potrebbe scaturire in un prossimo futuro, ma anche per l'effetto immediato della sentenza.

Come sopra si è evidenziato, gli strumenti a disposizione del cloud per trasferire dati in paesi terzi sono mutilati rispetto alla rosa prevista dalla direttiva e ristretti solo a BCR, model clauses e decisioni di adeguatezza.

Tuttavia la scalabilità dei servizi e la riduzione dei costi rendono i servizi cloud appetibili anche alle PMI e ai professionisti, che non possono utilizzare le BCR, strumento pensato e misurato sulle multinazionali (e non si tratta certo di un procedimento in grado di esaurirsi nel breve lasso temporale definito dal WP ART 29, necessitando di tempistiche ben più ampie).

Lo scompenso di potere contrattuale tra fornitore e utente PMI fa sì che le clausole standard (che comunque avrebbero bisogno di essere aggiornate / integrate per rispettare la decisione della Corte di Giustizia) non possano essere adottate su istanza del cliente, ma solo su iniziativa del fornitore.

In assenza di una decisione di adeguatezza, non residuano strumenti concretamente utilizzabili, di fronte ai colossi americani.

Alcuni fornitori, per mettersi al riparo dalle conseguenze pregiudizievoli della sentenza hanno aperto data center in UE, provando a bypassare il trasferimento di dati all'estero. Se, però, il criterio di inadeguatezza è tarato sulla sorveglianza di massa rivelata da Snowden, ciò potrebbe non essere sufficiente. Le imprese sono statunitensi e sono sottoposte alla normativa nazionale e per ragioni di sicurezza il Governo americano può anche chiedere l'accesso a dati conservati all'estero.

Ad esempio Microsoft si è opposta alla richiesta di accesso ai dati conservati sui suoi server allocati in Iranda, ma non ha ancora ottenuto una sentenza (che, se a suo favore, potrebbe certamente contribuire al dibattito). Sempre Microsoft ha cercato di proteggere i dati dei cittadini UE, custoditi su server di un sobfornitore europeo attraverso un complesso impianto contrattuale, ma anche questo non è detto che sia un mezzo in grado di resistere alle istanze governative, almeno fino a che non sorga controversia e una sentenza lo sancisca.

Nessuna soluzione?

Dati gli annunci contrastanti in ordine alla possibilità di approdare a un Safe Harbor 2 entro il termine assegnato, non è possibile prevedere quali saranno le misure che adotterà il WP ART 29 il 2 febbraio 2016.

Nella migliore delle ipotesi, si raggiungerebbe un nuovo Safe Harbor nei termini, e verrebbero date indicazioni concrete circa le modalità di adeguamento di model clauses e BCR alle nuove esigenze di protezione, in modo che possano costituire un efficace impianto contrattuale in grado di resistere alle pressioni governative correlate alla sorveglianza di massa, dato che così come sono state implementate sino ad oggi non paiono soddisfare i criteri fissati dalla Corte di Giustizia e non si comprende come lo stesso trattamento possa essere parametrato a standard tanto elevati in caso di decisioni di adeguatezza e privo di guarentigie efficaci negli altri casi. Ciò si attesta in netto contrasto con i principi enunciati dalla Corte, ai quali, invece, occorre attenersi.

Tuttavia, a parere di chi scrive, anche nel peggiore degli scenari possibili (appaia impossibile raggiungere in tempi stretti una decisione sul Safe Harbor 2, vengano inibiti anche gli atri strumenti di trasferimento), ci sono alcuni elementi che potrebbero mitigare le conseguenze della pronuncia salvaguardando al contempo la privacy degli interessati.

In primis, una spinta importante verso una soluzione potrebbe arrivare dalla tempestiva approvazione in seno agli Stati Uniti del Judicial Redress Act of 2015, che estenderebbe

alcune delle tutele previste dal Privacy Act del 1974 anche ai cittadini UE che così potrebbero agire in difesa della propria privacy innanzi ai Giudici delle Corti USA.

In secondo luogo è il WP ART 29 a lasciare aperto uno spiraglio: nella dichiarazione del 16 ottobre 2015, infatti si legge: "Therefore, the Working Party is urgently calling on the Member States and the European institutions to open discussions with US authorities in order to find political, legal and **technical** solutions enabling data transfers to the territory of the United States that respect fundamental rights."

Il riferimento alle soluzioni tecniche è successivamente ribadito nelle conclusioni:

"In conclusion, the Working Party insists on the shared responsibilities between data protection authorities, EU institutions, Member States and businesses to find sustainable solutions to implement the Court's judgment. In particular, in the context of the judgment, businesses should reflect on the eventual risks they take when transferring data and should consider putting in place any legal and **technical solutions** in a timely manner to mitigate those risks and respect the EU data protection acquis."

Il **riferimento alle soluzioni tecniche** che possano comportare tutela dei dati personali pare attagliarsi alla cifratura. Idonee soluzioni di **criptatura end to end** potrebbero quindi consentire il trasferimento di dati in paesi terzi?

Certo allo stato appare una via percorribile, in via prudenziale e ove possibile, per i sistemi cloud e fintanto che non verranno aperte backdoor come richiesto da alcuni governi, anche europei.

Altrimenti, qualora il WP ART 29 non fornisse alternative, occorrerà migrare i servizi verso fornitori che abbiano sede in UE, e server solo sul territorio europeo.

Il che comporterebbe una **balcanizzazione del cloud** assistita da una forte dose di ipocrisia. Come, infatti, non vedere lo sguardo strabico dell'Europa che blocca il trasferimento di dati personali in USA proclamando elevati e sacrosanti standard di protezione contro le ingerenze governative mentre alcuni Stati Membri virano verso la

sorveglianza di massa e giungono a pretendere sistemi privilegiati di accesso nei sistemi di cifratura?