Europa-USA: così vicini, così lontani quando si parla di privacy

Guido Scorza
Funzionario presso il Garante per la Protezione dei Dati Personali*

L'ecosistema digitale e gli USA

Il web batte bandiera americana.
È un dato di fatto difficilmente controvertibile.
I più grandi fornitori di servizi *cloud* globali hanno sede negli Stati Uniti in una striscia di terra compresa tra Seattle, San Francisco e dintorni.
Basti pensare a Amazon, Google e Microsoft.
Certo non esiste solo il *cloud*.
Ma se si voltano le spalle ai servizi *cloud* destinati a aziende e pubbliche amministrazioni e si rivolge lo sguardo al mercato dei servizi digitali rivolti ai consumatori, la situazione non cambia.
Google, YouTube, Facebook, Whatsapp, Instagram, Twitter, Linkedin, Netflix, Amazon, E-Bay hanno tutte sede negli Stati Uniti, nella stessa striscia di terra e sono, indiscutibilmente, i *brand* che soddisfano la più parte del fabbisogno digitale quotidiano di qualche miliardo di utenti nel mondo, diverse centinaia di milioni nell'Unione Europea.
Il combustibile che garantisce il funzionamento di questi servizi – tanto quelli business to business che quelli business to consumer e consumer to consumer – sono i dati, personali e non, perché i dati rappresentano, a seconda dei servizi, l'oggetto del servizio o il suo corrispettivo indiretto.

Interrompere il flusso di dati tra vecchio e nuovo continente, pertanto, equivarrebbe, nella sostanza, a spegnere il web e l'ecosistema digitale.
Questo, almeno, nell'immediato.
Si tratta di uno scenario rispetto al quale i mesi della pandemia e il progressivo trasferirsi di una fetta importante della popolazione globale – inclusa evidentemente quella europea – nell'ecosistema digitale hanno rappresentato fattori di amplificazione straordinari.
Oggi il mondo è enormemente più digitale di quanto non lo fosse meno di dodici mesi fa e i dati scambiati in ventiquattro ore nella dimensione globale dei servizi online, non sono neppure lontanamente paragonabile a quelli all'inizio della pandemia.
Basta leggere i bilanci e i rendiconti economico-finanziari delle big tech americane relativi a questi, ormai quasi, dodici mesi di pandemia per averne conferma.
Mentre la tenuta economico-finanziaria di un intero sistema di mercato è stata messa a dura prova dal Covid, società come Zoom, Amazon, E-Bay, Google, Facebook o Microsoft – ma solo per citarne alcuni – hanno fatto registrare risultati positivi imprevedibili e, infatti, imprevisti nelle loro previsioni 2019 (per il 2020).
Ecco perché la Sentenza resa dalla Corte di Giustizia dell'Unione Europea il 16 luglio 2020 nel caso ormai ribattezzato Schrems II rischia di innescare un terremoto senza precedenti nell'ecosistema digitale.

La sentenza Schrems II

Come è noto con la Sentenza resa nella causa C-311/18 la Corte di Giustizia dell'Unione europea ha dichiarato invalida la decisione 2016/1250 della Commissione sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy [nda quella nota come Privacy Shield] ritenendo che gli Stati Uniti d'America continuino a non poter essere considerati un ordinamento capace di offrire garanzie adeguate sotto il profilo della protezione dei dati personali ovvero equivalenti a quelle previste dalla disciplina europea della materia.
A tal proposito la Corte ha rilevato che la predetta decisione, al pari della precedente decisione 2000/520 [Safe Harbour] già dichiarata invalida con la Sentenza del 6 ottobre 2015 [nda la c.d. Sentenza Schrems I] sancirebbe il primato delle esigenze attinenti alla sicurezza nazionale, all'interesse pubblico e al rispetto della normativa statunitense, rendendo così possibili ingerenze nei diritti fondamentali delle persone i cui dati sono trasferiti verso tale Paese terzo.

Secondo i Giudici, in particolare, le limitazioni della protezione dei dati personali che risultano dalla normativa interna degli Stati Uniti in materia di accesso e di utilizzo, da parte delle autorità statunitensi, di siffatti dati trasferiti dall'Unione verso tale Paese terzo, e che sono state valutate dalla Commissione nella decisione 2016/1250, non sono tali da da rispondere a requisiti sostanzialmente equivalenti a quelli richiesti, nel diritto dell'Unione, dal principio di proporzionalità, giacché i programmi di sorveglianza fondati sulla suddetta normativa non si limitano a quanto strettamente necessario. La Corte, al riguardo, ha rilevato che, per taluni programmi di sorveglianza, dalla disciplina americana, non emergerebbe in alcun modo l'esistenza di limiti all'autorizzazione, in essa contenuta, dell'attuazione di tali programmi e neppure l'esistenza di garanzie per gli stranieri che si trovino a esserne oggetto.

I Giudici europei, inoltre, hanno aggiunto che la stessa normativa, pur prevedendo requisiti che devono essere rispettati dalle autorità statunitensi nell'attuare i programmi di sorveglianza in questione, non conferisce agli interessati diritti nei confronti delle autorità statunitensi azionabili dinanzi ai giudici.

Quanto al requisito della tutela giurisdizionale, la Corte ha ritenuto che, contrariamente a quanto considerato dalla Commissione nella decisione 2016/1250, il meccanismo di mediazione previsto da tale decisione non fornisce agli interessati un mezzo di ricorso effettivo dinanzi ad un organo che offra garanzie sostanzialmente equivalenti a quelle richieste nel diritto dell'Unione, tali da assicurare tanto l'indipendenza del Mediatore previsto da tale meccanismo quanto l'esistenza di norme che consentano al suddetto Mediatore di adottare decisioni vincolanti nei confronti dei servizi di intelligence statunitensi.

Nella sostanza, dunque, i Giudici del Lussemburgo con la Sentenza del 16 luglio 2020 hanno messo nero su bianco che le leggi americane restano troppo distanti dalla disciplina europea in materia di privacy con particolare riferimento ai poteri che accordano alle agenzie di intelligence e agli scarsi effettivi diritti in termini di tutela giurisdizionale della privacy e che gli accordi internazionali intercorsi tra Europa e Stati Uniti non sono idonei a eliminare tali differenze.

In principio – e la circostanza merita di essere ricordata per quanto si dirà nel prosieguo – la Corte ricorda che un trasferimento di dati personali verso un Paese extra UE può trovare giustificazione, oltre che in una decisione di adeguatezza della Commissione anche in un accordo convenzionale tra l'esportatore e l'importatore e che, dunque, almeno in astratto, i trasferimenti che fossero risultati preclusi in forza della Decisione Privacy Schield invali-

data, avrebbero potuto fondarsi sul perfezionamento delle cc.dd. *Standard contractual clause* di cui alla Decisione 2010/87.

Lo schema di provvedimento dell'EDPB e la situazione attuale

L'European data protection board (EDPB), la commissione che riunisce le Autorità di protezione dei dati personali nazionali che operano in tutta Europa, lo scorso 10 novembre ha lanciato una consultazione pubblica su uno schema di provvedimento che ha un unico obiettivo dichiarato: quello di identificare rimedi e soluzioni capaci di garantire il trasferimento di dati personali dall'Europa agli Stati Uniti nonostante la Sentenza Schrems II e, dunque, nonostante la declaratoria di nullità del c.d. Privacy Shield.
Tale esigenza affonda la sua ragion d'essere nel contesto che si è descritto sopra, un contesto nel quale l'interruzione di ogni trasferimento di dati personali tra Europa e Stati Uniti appare un'opzione difficilmente valida nel breve-medio periodo.
Non vi è, peraltro, dubbio alcuno che, a seguito della citata Sentenza, tale scenario sia concreto e attuale e non possa essere ignorato.
Vale la pena, quindi, formulare qualche breve considerazione allo scopo di chiarire gli esatti termini della questione e provare a fornire ai titolari e responsabili dei trattamenti che hanno l'esigenza di trasferire dati negli Stati Uniti talune prime indicazioni in attesa del varo definitivo del provvedimento del Board dei garanti europei all'esito della consultazione pubblica.
La prima necessaria considerazione, anche per fugare dubbi e opinioni diffuse sulla vicenda è che lo schema di provvedimento posto in consultazione, pur nascendo con l'intenzione di risolvere lo specifico problema del trasferimento dei dati personali lungo la tratta Europa-Stati Uniti ha una portata più ampia – o almeno ambizioni maggiori – giacché intende identificare garanzie e rimedi utili ogni qualvolta ci si trovi davanti all'esigenza di trasferire dati personali dall'Europa a un qualsiasi Paese terzo il cui ordinamento non sia stato riconosciuto dalla Commissione europea come capace di offrire un livello di tutela ai dati personali equivalente rispetto a quella garantita dalla disciplina europea.
Perché – e questo è un dato importante da tenere presente – la situazione che, dopo la Sentenza della Corte di Giustizia, si è venuta a creare tra Bruxelles e Washington non è unica ma è comune a decine di altri Paesi verso i quali i dati personali in partenza dall'Europa possono dover approdare.
Si sbaglierebbe, insomma, a affrontare la questione e a rispondere alla consultazione pubblica guardando solo ai rapporti tra Europa e USA o a far

indossare a questi ultimi la maglia nera della privacy come se, gli Stati Uniti, oltre a non rappresentare un approdo sicuro per i dati personali nei cittadini europei rappresentassero il peggiore tra gli approdi per tali dati personali.
Non si tratta di una difesa d'ufficio degli Stati Uniti né del loro regime giuridico che evidenzia, effettivamente, tutti i limiti e le carenze puntualmente annotati dalla Corte di Giustizia dell'Unione Europea ma di una riflessione che ha lo scopo di evidenziare come, in una società sempre più globale e connessa, è indispensabile – ancorché, per quanto si dirà più avanti, forse insufficiente – accompagnare ogni trasferimento di dati personali verso Paesi terzi non "coperti" da una valida decisione di adeguatezza della Commissione europea, con l'adozione di una serie di misure contrattuali, organizzative e tecnologiche che sono quelle che le Autorità nazionali che siedono nel board hanno, sin qui, identificate come utili a affrontare il problema venutosi a creare a seguito della recente decisione della Corte.
La seconda considerazione non meno importante della precedente richiede uno sforzo di trasparenza e onestà intellettuale.
La Corte di Giustizia dell'Unione europea con la Sentenza Schrems II ha accertato che le leggi americane non riconoscono agli interessati un livello di tutela equivalente rispetto a quello loro riconosciuto dalla disciplina europea in materia di protezione di dati personali.
La questione sollevata, pertanto, riguarda un confronto tra due ordinamenti.
Così stando le cose, pertanto, è evidente – sul piano logico prima ancora che giuridico – che il problema venutosi a creare non può essere in alcun modo integralmente risolto né dal basso, né dall'esterno.
Non c'è nessun provvedimento che possa essere adottato dall' EDPB, né da nessuna altra Autorità nazionale di protezione dei dati personali, né, a maggior ragione, nessuna iniziativa contrattuale, organizzativa o tecnologica adottabile da parte di soggetti privati che possa sgretolare il muro eretto dalla Sentenza dei Giudici del Lussemburgo e garantire una prosecuzione generale, serena e ininterrotta dei dati personali tra i due continenti.
Un problema di disallineamento tra due Ordinamenti si risolve solo intervenendo su uno o entrambi gli ordinamenti.
E la stessa identica situazione si avrebbe – e probabilmente si avrà – in relazione alla circolazione dei dati personali tra l'Europa e altri Paesi extra UE.
Si tratta do una conclusione che appare opportuno tenere presente per evitare di nutrire attese illusorie circa l'adozione di qualsivoglia provvedimento a livello europeo o nazionale che valga a risolvere il problema alla radice.
Meglio, decisamente, rimboccarsi le maniche e ragionare in termini di limitazione, contenimento, minimizzazione dei rischi per quei trasferimenti di dati personali negli USA che appaiono irrinunciabili o il cui contenuto

specifico non appare tale da sollevare preoccupazioni sostanziali in termini di accesso da parte di eventuali soggetti pubblici americani.
Ma, al tempo stesso, sembra opportuno riflettere sull'opportunità di sospendere autonomamente il trasferimento oltre-oceano di dati personali di particolare rilevanza o *appeal* per soggetti pubblici statunitensi in relazione ai quali non vi sono concrete misure di contenimento o minimizzazione dei rischi adottabili né sul piano tecnologico, né su quello organizzativo, né su quello contrattuale.
Questo perché, come si è anticipato, allo stato e fino all'intervento di novità rilevanti sul piano dell'ordinamento interno americano o sul piano delle relazioni internazionali la decisione della Corte di Giustizia dell'Unione europea non può, evidentemente, essere svuotata completamente di contenuto o ignorata semplicemente perché alza l'asticella del trasferimento dei dati dall'Europa agli USA a un livello, oggettivamente, in molti casi, irraggiungibili.
E anche perché, non può essere dimenticato che i Giudici del Lussemburgo, con la stessa decisione del luglio scorso, hanno messo nero su bianco che incombe sulle autorità di controllo, nel contesto di un trasferimento di dati personali extra UE, il compito, salvo che esista una decisione di adeguatezza validamente adottata dalla Commissione, di sospendere o vietare un trasferimento di dati personali verso un Paese terzo quando ritengano, alla luce delle circostanze proprie di tale trasferimento, che le clausole tipo di protezione dei dati non siano o non possano essere rispettate in tale Paese e che la protezione dei dati trasferiti, richiesta dal diritto dell'Unione, non possa essere garantita con altri mezzi, ove l'esportatore stabilito nell'Unione non abbia esso stesso sospeso tale trasferimento o messo fine a quest'ultimo.
È, pertanto, evidente che, qualora un'autorità di protezione dei dati personali nazionale, domani, si trovasse interessata di una questione relativa a un trasferimento di dati personali verso gli Stati Uniti e dovesse constatare che nessuna delle garanzie contrattuali, tecnologiche o di processo adottate da esportatore e importatore sono idonee a superare le criticità – anche solo a livello potenziale – sollevate dalla Corte di Giustizia, tale Autorità non potrebbe far altro che sospendere o bloccare il trasferimento e, al ricorrere delle condizioni, sanzionare il titolare del trattamento e/o il responsabile.
Un bel problema in una società globalizzata come quella in cui viviamo e in presenza di un mercato digitale nel quale si confrontano centinaia di attori transnazionali.
Una terza e ultima considerazione – che, sfortunatamente non può che aggravare un contesto già critico – suggerisce che è difficile ipotizzare rimedi contrattuali da soli capaci di garantire di risolvere – specie in maniera

generalizzata o anche semplicemente con riferimento a trattamenti di dati personali articolati e complessi – il problema del quale si discute mentre, probabilmente, esistono taluni rimedi tecnologici capaci di attenuare il problema, fino a considerarlo risolto, sebbene, naturalmente, con riferimento sempre a singole e specifiche ipotesi.

Tanto basta a suggerire che, difficilmente, allo stato, si possa pensare di trasferire dati personali verso gli Stati Uniti senza intervenire sui processi e le tecnologie sin qui utilizzate e limitandosi a modificare, in un modo o nell'altro, gli accordi in essere.

Le eccezioni a questa regola sono due e due soltanto: o il destinatario dei dati negli USA gode, *ex lege*, di un regime di segreto tale da porlo al riparo – e porre al riparo i dati che riceve dall'Europa – dal rischio di accessi da parte del Governo di Washington e delle sue Agenzie di intelligence o esportatore e importatore hanno già adottato rimedi tecnologici, organizzativi e contrattuali capaci di fare in modo che sebbene la legge USA abiliti Governo e agenzie di Intelligence a accedere ai dati in questione, tali dati approdino fisicamente o figurativamente sul suolo americano in una forma tale da garantire che chi provasse ad accedervi non riuscirebbe comunque a mettere le mani su dati capaci di essere ricondotti a una o più persone identificate. Due situazioni, oggettivamente, più facili a dirsi che a farsi.

L'unica possibile conclusione è che è urgente che le diplomazie europea e statunitense si mettano alla ricerca di una soluzione più definitiva – anche se difficilmente sarà possibile identificarne una solida nel breve periodo come insegna la brevissima storia del Privacy Shield – mentre la comunità scientifica e quella degli addetti ai lavori deve – in raccordo con le Autorità di protezione dei dati – continuare a esplorare rimedi e soluzioni capaci di identificare il maggior numero di possibili soluzioni temporanee e parziali a un problema con il quale dovremo necessariamente fare i conti ancora a lungo.

Ma, proprio perché oggi il problema riguarda con maggiore urgenza i rapporti tra Europa e USA ma domani potrebbe riguardare quelli tra Europa e decine di altri Paesi, probabilmente, l'unica vera possibile risposta sta nell'avvio di una discussione spedita, nella comunità internazionale, per l'identificazione di uno strumento pattizio capace di garantire la libera circolazione globale dei dati nel rispetto di poche ma insuperabili garanzie per gli interessati.