Luglio 2020

Schrems II: la sentenza della Corte UE sul Privacy Shield e gli effetti sui trasferimenti extra-UE dei dati personali

Massimiliano Masnada, Partner, Hogan Lovells Studio Legale

1. Breve excursus

A seguito delle rivelazioni di Edward Snowden sulla partecipazione di Facebook ed altri provider di servizi statunitensi al programma di sorveglianza di massa del governo USA denominato "PRISM", nel 2013, Maximillian Schrems, attivista austriaco, presentava denuncia al *Data Protection Commissioner* irlandese sostenendo l'illecito trattamento dei suoi dati personali che sarebbero stati trasferiti negli USA e sottoposti al controllo massivo delle autorità governative statunitensi, insieme a quelli di milioni di cittadini europei. Ciò sarebbe stato facilitato dall'accordo noto come "Safe Harbor", approvato nel 2000 dalla Commissione UE, che consentiva il libero trasferimento, a certe condizioni, dei dati personali tra UE e USA.

Dopo aver deferito la questione alla Corte di giustizia dell'Unione europea, quest'ultima accoglieva le doglianze di Schrems con sentenza C-362/14 del 6 ottobre 2015 (sentenza "Schrems I"), invalidando la decisione 2000/520/CE con cui la Commissione UE aveva giudicato adeguato il livello di protezione assicurato dai *Safe Harbor Privacy Principles* e rinviando la questione al Garante irlandese per una nuova pronuncia.

Nel frattempo, anche su invito del Gruppo di lavoro ex art. 29 (oggi "*European Data Protection Board*" o "EDPB") che raccoglie tutte le autorità privacy degli Stati Membri, a febbraio 2016, la Commissione EU e il Dipartimento del Commercio degli USA trovarono un accordo denominato "*Privacy Shield*" che avrebbe dovuto risolvere i problemi di inadeguatezza sollevati dalla Corte di Giustizia relativamente al *Safe Harbor*. Il *Privacy Shield*, approvato dalla Commissione UE con Decisione 2016/1250 del 16 luglio 2016, tra le altre cose, prevedeva obblighi più severi per le imprese statunitensi che importano dati personali di cittadini europei, un controllo periodico del rispetto di tali obblighi con conseguente applicazione di sanzioni e la previsione di garanzie e obblighi di trasparenza per l'accesso del governo e delle autorità pubbliche USA ai dati personali trasferiti per fini di contrasto e sicurezza nazionale.

Anche a seguito dell'avvento del Regolamento (UE) n. 679/16 ("GDPR") – che ha sostituito la Direttiva 95/46/CE e tutte le normative locali di recepimento – era inevitabile

che il giudizio di rinvio pendente innanzi al *Data Protection Commissioner* irlandese implicasse una nuova valutazione di adeguatezza della tutela prevista dal citato Privacy Shield e, più in generale, delle cd. "clausole contrattuali standard" ("SCCs"), anch'esse approvate dalla Commissione UE come valida misura di garanzia contrattuale per garantire la protezione dei dati personali dei cittadini UE in caso di trasferimento fuori dal territorio comunitario.

Infatti, nel maggio 2018, l'High Court irlandese, investita del caso, deferiva alla Corte di Giustizia diverse questioni concernenti la validità dei trasferimenti effettuati con le SCCs e del Privacy Shield, ponendo l'accento sulla possibile violazione degli articoli 7, 8, 47 e 52 della Carta dei diritti fondamentali dell'UE.

2. Decisione Schrems II

Con la sentenza del 16 luglio 2020 (sentenza "Schrems II"), la Corte di Giustizia ha dichiarato invalida la Decisione 2016/1250 con cui la Commissione UE aveva certificato l'adeguatezza della protezione dei dati personali offerta dal *Privacy Shield* per i trasferimenti tra UE e USA.

In breve, secondo la Corte, la normativa interna degli USA in materia di accesso e di utilizzo, da parte delle autorità statunitensi, di dati trasferiti dall'UE non soddisfa i principi alla base del GDPR, tra cui quello di proporzionalità, in quanto esiste la possibilità da parte delle autorità pubbliche e di controllo degli USA di accedere e trattare i dati personali trasferiti senza limitazioni a quanto sia strettamente necessario per le ragioni di sorveglianza.

In pratica, la carenza osservata dalla Corte si traduce in una mancanza di diritti effettivi degli interessati nei confronti delle autorità statunitensi. A tale riguardo, la Corte ha ritenuto, tra le altre cose, che il meccanismo del difensore civico (il cd. "*Ombudsperson*" ossia il "Mediatore dello Scudo") previsto dal Privacy Shield non fornisce effettivamente garanzie equivalenti a quelle richieste dal diritto dell'UE, come ad esempio assicurare l'indipendenza del difensore civico e l'esistenza di norme che conferiscono al difensore civico il potere di adottare decisioni vincolanti per i servizi di intelligence e per le altre autorità pubbliche statunitensi.

Al contrario, la sentenza non impatta direttamente sulla validità delle SCCs approvate dalla Commissione UE per il trasferimento di dati a Paesi extra-UE, sebbene la Corte abbia chiarito che, salvo il caso in cui esista una valida decisione di adeguatezza della legge privacy del Paese importatore dei dati adottata dalla Commissione UE, l'autorità di controllo di ciascuno Stato Membro è tenuta a sospendere o vietare un trasferimento di dati personali verso un Paese extra-UE quando ritenga, alla luce delle circostanze specifiche, che le SCCs 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.

Ciononostante, alcune autorità di controllo come quella irlandese, intervenendo con un commento ufficiale sulla sentenza Schrems II, hanno messo in dubbio la legittimità dei trasferimenti effettuati sulla base delle SCCs verso gli Stati Uniti e invitato le altre autorità a raggiungere una posizione comune sulla questione. Il Garante per la protezione dei dati personali italiano non si è espresso sul punto.

3. Le FAQ pubblicate dall'EDPB

Raccogliendo l'invito del Garante irlandese, l'EDPB ha pubblicato le FAQ sul caso Schrems II che, tuttavia, non sembrano fornire elementi utili a tradurre in concreto la decisione del Corte. In sostanza, l'EDPB sottolinea che le parti, intese come esportatore UE e importatore extra-UE di dati personali, hanno l'obbligo di effettuare le proprie valutazioni sui trasferimenti esistenti nell'ambito di SCCs (la FAQ includono anche le *Binding Corporate Rules* - BCR che regolano di solito i trasferimenti infragruppo) alla luce delle preoccupazioni espresse dalla Corte.

Le FAQ chiariscono, infatti, che la possibilità o meno di trasferire i dati personali sulla base delle SCC dipenderà dal risultato della valutazione effettuata dall'esportatore dei dati sulle garanzie offerte nel Paese importatore (segnatamente, gli USA) rispetto all'adeguatezza dei meccanismi di tutela. La valutazione dovrà tenere conto delle circostanze del trasferimento e di eventuali misure contrattuali supplementari adottate per fare fronte alle preoccupazioni espresse dalla Corte. Tali misure dovrebbero garantire che il trasferimento oltre il territorio UE non pregiudichi il livello di protezione conforme al GDPR e alle normative locali europee. In buona sostanza, se, all'esito della valutazione, si dovesse concludere che, tenendo conto delle circostanze del trasferimento e di eventuali misure supplementari, non vi fossero adeguate garanzie, le società esportatrici sarebbero costrette a sospendere o a porre fine al trasferimento dei dati personali.

Oltre ai punti relativi alle valutazioni individuali, a mio modo di vedere, gli aspetti più significativi delle FAQ sono i seguenti:

a) Le FAQ riconoscono espressamente che SCC e BCR possono essere ancora considerati strumenti adeguati ove vengano inserite misure supplementari in grado di recepire le preoccupazioni espresse dalla Corte di Giustizia. In particolare, dopo aver ribadito che è responsabilità delle parti valutare i trasferimenti, hanno dichiarato: "*L'EDPB sta attualmente analizzando la sentenza della Corte per determinare il tipo di misure supplementari che potrebbero essere fornite in aggiunta ai SCCs e ai BCR, che si tratti di misure legali, tecniche o organizzative, per trasferire dati verso paesi terzi in cui i SCCs o i BCR non forniranno da soli il livello sufficiente di garanzie. L'EDPB sta esaminando ulteriormente in che cosa potrebbero consistere queste misure supplementari e fornirà maggiori indicazioni*". A tal riguardo, conversazioni informali con alcune autorità europee rivelano che in seno all'EDPB si stia discutendo su quali potrebbero essere queste misure, e sarebbero già emerse alcune raccomandazioni riguardo le misure tecniche

di salvaguardia come la crittografia. Si sta pensando, infatti, di coinvolgere tecnici e ingegneri per esaminare le implicazioni tecniche e le potenziali soluzioni.

b) Le FAQ richiamano, più in generale, le deroghe di cui all'Art. 49 del GDPR relative al trasferimento dei dati personali oltre il territorio comunitario. Nel ribadire la loro validità, tuttavia, l'EDPB richiama l'attenzione sul consenso come base giuridica per i singoli trasferimenti sulla base di circostanze specifiche. In particolare, le FAQ stabiliscono che il linguaggio del consenso deve informare gli interessati sui possibili rischi del trasferimento verso gli Stati Uniti e altre giurisdizioni non adeguate. In tal caso, tuttavia, occorre precisare che il consenso deve essere "liberamente espresso" e non può costituire la condizione necessaria per l'utilizzo del servizio. Ciò non funzionerebbe nemmeno per i dati relativi alle risorse umane, data la posizione delle autorità di protezione dei dati, secondo cui i dipendenti non possono fornire un consenso libero ed effettivo al trattamento dei dati nella maggior parte dei casi. Ma se il consenso è l'unico modo per utilizzare un servizio basato negli Stati Uniti (è il caso di servizi online che sono forniti un tutto il mondo da un unico provider avente sede negli USA), a mio parere sarebbe inaccettabile (e con evidenti profili di incostituzionalità) che un'autorità amministrativa neghi a un residente dell'UE il diritto di utilizzare il servizio basato negli Stati Uniti, andando ad incidere sull'autonomia contrattuale delle parti e sulla libertà di scelta dell'individuo. Altra cosa sarebbe pretendere la massima trasparenza, ossia che l'individuo sia correttamente informato sulla possibilità che i suoi dati personali trasferiti negli USA siano a loro volta messi a disposizione dell'autorità pubblica USA per finalità di sorveglianza e sicurezza nazionale. A quel punto, la questione rientra nella libera e consapevole facoltà di scelta dell'interessato.

4. Cosa succede adesso? Vademecum per le imprese italiane

L'EDPB non ha ufficialmente annunciato una moratoria rispetto alle investigazioni circa la legittimità dei trasferimenti dei dati personali fuori dall'UE e, in particolare, negli USA. Anche se questa sembra essere la strada intrapresa, anche memori di quanto accadde dopo la prima pronuncia della Corte di giustizia sul caso Schrems che dichiarò invalido l'allora Safe Harbour. Appare, infatti, francamente poco plausibile un'azione nei confronti di quelle società che hanno avviato una rinegoziazione dei loro contratti in base alla decisione della Corte di Giustizia. Ciò che emerge dalle FAQ è l'invito delle autorità di protezione dei dati alle imprese a prendere immediati provvedimenti per conformarsi alla decisione, come l'analisi dei loro flussi di dati verso l'estero e l'avvio di una valutazione di adeguatezza delle SCCs.

Al fine di evitare possibili sanzioni e, soprattutto, di scongiurare provvedimenti di blocco dei trasferimenti dei dati personali da parte dell'autorità di controllo, le imprese dovrebbero adottare misure appropriate e idonee a dimostrare che i trasferimenti di dati fuori dal territorio comunitario avvengano in conformità al GDPR e tengono in considerazione le preoccupazioni espresse dalla Corte di giustizia nella sentenza Schrems

II. A tal fine, è auspicabile che le imprese che esportano dati personali adottino alcuni comportamenti virtuosi che sarebbero senza dubbio apprezzati dalle autorità di controllo, quali:

1) Laddove per il trasferimento di dati personali negli USA è stato utilizzato come base giuridica il Privacy Shield, verificare se sia possibile la modifica della base giuridica del trasferimento, prendendo ad esempio in considerazione le ipotesi elencate dall'art. 49 del GDPR, tra cui:

    a. consenso informato dell'interessato (tenendo presente le precisazioni sopra descritte dell'EDPB in tema di validità del consenso);

    b. trasferimento necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;

    c. trasferimento necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato (es. contratto a favore di terzo);

    d. trasferimento necessario per importanti motivi di interesse pubblico. Questa eccezione è molto ampia. Normalmente l'interesse pubblico è stabilito da una legge ovvero da un provvedimento amministrativo e non è lasciato alla discrezionalità del singolo. Tuttavia, la presenza dell'interesse pubblico va valutata di volta in volta;

    e. trasferimento necessario per accertare, esercitare o difendere un diritto in sede giudiziaria. E' il caso in cui il titolare europeo debba difendersi ovvero affermare un proprio diritto dinnanzi alle corti di un Paese terzo per cui è necessario il trasferimento (magari ad un consulente, ad un difensore e poi all'autorità giudiziaria del Paese terzo) di alcuni dati personali per consentire lo svolgimento delle attività difensive. Vale in ogni caso il vincolo della proporzionalità sia con riferimento al contenuto dei dati trasferiti che al tempo di conservazione;

    f. trasferimento necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso. E' il classico esempio di un malato che viene curato all'estero.

2) Se le ipotesi sopra elencate non possono essere adottate come valida base giuridica del trasferimento, occorre verificare anzitutto le decisioni della Commissione UE sull'adeguatezza delle leggi sulla protezione dei dati personali di alcuni Paesi terzi e, soprattutto, le eventuali dichiarazioni dell'EDPB relative alla legalità dei trasferimenti di dati verso determinati Paesi sulla base delle SCCs, con particolare

attenzione ai trasferimenti di dati verso gli Stati Uniti. E' probabile, infatti (e senz'altro auspicabile) che le autorità di controllo pubblichino un vademecum o delle linee guida sull'utilizzo delle SCCs e delle eventuali ulteriori misure contrattuali di salvaguardia rispetto ai singoli Paesi. Inoltre, è possibile che la Commissione UE anticipi ogni eventuale decisione dell'EDPB, pubblicando una nuova versione di SCCs aggiornate per affrontare i rischi individuati dalla Corte di giustizia in relazione alle attività delle autorità pubbliche statunitensi.

3) Nel breve periodo, tuttavia, laddove nessun'altra base giuridica sia percorribile (ovvero siano già state stipulate tra le parti le SCCs), è auspicabile negoziare con l'importatore dei dati la stipula di SCCs con l'aggiunta di ulteriori misure di garanzia per gli interessati coinvolti nel trasferimento nel senso auspicato dalla Corte di giustizia nella sentenza Schrems II. Tale attività dovrà essere preceduta da una sorta di *due diligence* rispetto alle garanzie offerte dal Paese importatore:

    a. identificare i flussi di dati personali trasmessi e il grado di rischio per gli interessati in caso di trasferimenti successivi alle autorità di sorveglianza;

    b. analizzare le leggi locali del Paese destinatario e gli obblighi ivi contenuti di trasmissione dei dati alle autorità pubbliche: a questo proposito, per i trasferimenti di dati verso gli Stati Uniti, sarà particolarmente rilevante verificare in che misura il destinatario dei dati è soggetto alla Sezione 702 FISA e all'E.O. 12333.

4) Sulla base dei risultati della verifica effettuata, elaborare e negoziare con l'importatore dei dati, una serie di misure contrattuali aggiuntive da inserire nelle SCCs al fine di aumentare le garanzie per gli interessati in caso di trasferimento dei loro dati personali. In attesa che l'EDPB pubblichi linee guida o fornisca chiarimenti sulle misure aggiuntive più idonee per tutelare i diritti degli interessati in caso di trasferimento dei dati personali tramite le SCCs, si possono ipotizzare alcune misure tecniche e organizzative come:

    a. valutazione preventiva di quali dati è necessario trasferire secondo un principio di proporzionalità e privacy by design

    b. uso di tecniche di criptografia

    c. pseudonimizzazione dei dati

    d. modifica delle modalità di accesso: in luogo dell'invio dei dati presso l'importatore, prevedere l'accesso in remoto tramite credenziali fornite a limitate persone dell'importatore presso i sistemi e i database dell'esportatore;

    e. tracciabilità degli accessi;

f. clausole aggiuntive che prevedono l'obbligo di notifica preventiva e di autorizzazione dell'esportatore in caso di richiesta di *disclosure* dal parte dell'autorità pubblica straniera ovvero il diritto dell'esportatore di bloccare il flusso di dati e impedire di fatto il trasferimento ulteriore;

g. la previsione di forme di cooperazione tra esportatore e importatore per consentire all'interessato, oltre che la trasparenza rispetto ai trasferimenti successivi dei suoi dati, anche la possibilità di utilizzare, senza sopportare gli oneri economici e le spese legali, gli strumenti processuali e i diritti di azione previsti dalla legislazione del Paese importatore per opporsi alla *disclosure*

5. Conclusioni

Al di là dei rimedi indicati, è tangibile il rischio di creare delle vere e proprie "*black list*" di Stati extra-UE che non garantiscono la tutela della privacy dei cittadini europei, con evidenti conseguenze sul piano dei commerci internazionali e della geopolitica. La valutazione del cd. "rischio Paese" potrebbe determinare gravi conseguenze sulle transazioni internazionali e sull'offerta globale di servizi, inclusi il *cloud computing*, i servizi bancari, assicurativi e finanziari. Il flusso di dati verso Paesi extra-UE (se consideriamo anche UK come tale) è alla base della gran parte delle transazioni e dei commerci. Se è vero che i dati personali sono il nuovo "oro nero" e che l'accumulo di enormi masse di dati (cd. Big Data), il loro studio e utilizzo ai fini commerciali e di mercato è alla base delle fortune dei *big players* (fornitori di servizi online, *cloud computing*, *social media*, *big tech*), è altrettanto vero che la maggior parte (se non la totalità) di essi si trova in USA o in altri Paesi extra-UE (es. Cina, Corea del Sud).

Viene da chiedersi quindi se la sentenza in commento non sia frutto di una volontà politica di ridisegnare i rapporti futuri nell'ottica di un "neo-sovranismo" europeo rispetto allo strapotere dei fornitori extra-UE; se si voglia forzare la conservazione dei dati all'interno dei confini europei impedendo o rendendo più difficile il flusso verso l'esterno al fine di invogliare gli *stakeholders* ad operare la scelta di optare per fornitori europei, piuttosto che avvalersi di operatori statunitensi per i quali gli adempimenti necessari renderebbero svantaggioso il trasferimento oltreoceano.

Del resto, gli stessi *big players* potrebbero essere, addirittura, spinti da tale decisione prendere in considerazione un processo di "europeizzazione" dei loro servizi, portandoli come molti di loro hanno già fatto prima della sentenza Schrems II, all'interno dell'UE e risolvendo così, a monte, il problema del trasferimento dei dati personali.

Ciò che è sicuro e, in un certo senso, ineludibile è il principio affermato dalla Corte di giustizia secondo cui andrà, d'ora in poi, sempre garantita l'effettiva sovranità dei dati dei cittadini europei a fronte di raccolte di massa di dati da parte di autorità governative straniere celate dal pretesto della sorveglianza a fini di sicurezza. Che sia la fine dell'epopea del Grande Fratello di orwelliana memoria?