A chi interessa Schrems II?

Perché la sentenza Schrems II sta avendo un impatto significativo sulla gestione dei dati personali effettuati dalle aziende dell'Unione Europea? Chi si deve preoccupare di questa sentenza? Quali azioni dovranno essere intraprese dalle aziende, soprattutto le piccole e medie, per capire se e come adeguarsi? In questo articolo faremo il punto della situazione dopo circa sei mesi dalla sentenza Schrems II.

Una breve premessa per chi non conoscesse la sentenza Schrems II.

Lo scorso luglio la Corte di Giustizia Europea ha giudicato non valido il c.d. *Privacy Shield*, ovvero l'adeguatezza della protezione offerta dalle condizioni previste nel suddetto accordo, detto anche "Scudo per la Privacy", relativamente ai trasferimenti di dati personali tra la UE e gli Stati Uniti. Poiché moltissimi trasferimenti di dati personali fra UE ed USA – di base, ricordiamo, sono possibili solo sotto determinate condizioni – erano basati sul *Privacy Shield*, capite che tutti questi trasferimenti extra UE verso gli USA, dopo la sentenza Schrems II, in assenza di altre condizioni di adeguatezza, diverrebbero illegali.

Il tutto, infatti, è disciplinato dal Capo V (artt. Da 46 a 50) del Regolamento UE 679/2016 (GDPR) che, come principio, sancisce il divieto di "esportare" dati personali fuori UE, salvo il soddisfacimento di determinate condizioni. Tra queste ultime, le **decisioni di adeguatezza della Commissione Europea** (cfr. art. 45 del GDPR), ovvero esportazioni di dati in Paesi per i quali la Commissione Europea ha giudicato adeguate le garanzie sulla protezione dei dati personali del Paese "importatore" di dati personali (tra cui ad es. la Svizzera). Nel momento in cui – a causa di Schrems II – è "saltata" la condizione di adeguatezza stabilita dal *Privacy Shield*, si è reso necessario identificare un'altra base giuridica valida per il trasferimento dei dati fra UE e Stati Uniti d'America.

Ma perché il Privacy Shield è stato invalidato?

Secondo la Corte, 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 inquadrate in modo 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. Fondandosi sulle constatazioni che compaiono in tale decisione, la Corte rileva che, per taluni programmi di sorveglianza, da detta regolamentazione non emerge 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 possono esserne potenzialmente oggetto. La Corte aggiunge che la stessa normativa, pur se prevede requisiti che devono essere rispettati dalle autorità statunitensi nell'attuare i programmi di sorveglianza considerati, non conferisce agli interessati diritti nei confronti delle autorità statunitensi azionabili dinanzi ai giudici.

Se non fosse chiaro quanto asserito dalla Corte UE si consiglia la visione del film "Snowden" per capire meglio di cosa stiamo parlando. In sintesi, ricordiamo che il "Cloud Act" emanato dagli USA consente alle autorità statunitensi, forze dell'ordine e agenzie di intelligence, di acquisire dati informatici dagli operatori di servizi di *cloud computing* a prescindere dal luogo dove questi dati si trovano; quindi, anche se sono su server fuori dagli USA. La sola condizione è che questi operatori siano sottoposti alla giurisdizione degli Stati Uniti, oppure anche siano società europee che hanno una filiale negli Stati Uniti o che operano nel mercato americano.

In realtà la questione di esportazione dei dati personali extra UE va distinta nei seguenti punti:

1. Trasferimenti di dati personali – in formato digitale o analogico – fra UE e USA
2. Trasferimenti di dati personali – esclusivamente in formato elettronico – fra UE ed aziende statunitensi o comunque aventi una sede in USA
3. Trasferimenti di dati personali fra UE e Paesi extra UE diversi dagli USA per i quali non esiste una decisione di adeguatezza.

La sentenza Schrems II, con la conseguente invalidazione del Privacy Shield, riguarda strettamente il punto 1 sopra elencato, mentre il **CLOUD Act** (*Clarifying Lawful Overseas Use of Data Act*, approvato a marzo 2018) è relativo al punto 2 e per il momento è soggetto a Schrems II solo la parte riguardante i dati trasferiti dalla UE verso Società statunitensi nel territorio degli USA.

Non vorrei scendere in ulteriori considerazioni su altri aspetti oltre a quelli strettamente inerenti Schrems II, se non altro per motivi di spazio, sebbene da un lato sia auspicabile che non si ripetano situazioni in cui la digitalizzazione di consistenti archivi cartacei contenenti dati personali (anche della P.A.) venga svolta – essenzialmente per motivi di costo – in Paesi dell'Est Europa o dell'Africa, dall'altro comunque bisogna pensare anche alle aziende europee che svolgono attività commerciali e di assistenza in Paesi del Medio Oriente o del Sud

Est Asiatico dove la privacy è considerata l'ultimo dei problemi.

Una scappatoia alla cancellazione del *Privacy Shield*, per consentire il trasferimento di dati personali, potrebbe essere costituita dall'applicazione delle c.d. **Clausole Contrattuali Tipo** (*Standard Contractual Clause* o SCC, in base all'art. 46 del GDPR), approvate dalla Commissione Europea prima dell'avvento del GDPR e confermate successivamente, ma purtroppo le SCC sono affette dal medesimo vizio del *Privacy Shield*:. Infatti, essendo clausole contrattuali fra il titolare (o responsabile) del trattamento entro la UE e l'importatore (titolare o responsabile del trattamento) negli USA, non possono prevedere garanzie sui diritti degli interessati che impediscano a enti governativi USA di accedere – per motivi di sicurezza – a dati personali memorizzati in *datacenter* del proprio territorio (e non solo, come abbiamo visto a causa del CLOUD Act).

Perché Schrems II ha una portata così estesa? Occorre considerare che l'oggetto del trasferimento dati non riguarda solo archivi cartacei, ma naturalmente anche dati in formato digitale memorizzati in *cloud* presso *datacenter* ubicati fuori UE, nello specifico negli USA. Poiché questa è la situazione in cui ricadono i più importanti provider di servizi *cloud* del mondo, ovvero Microsoft, Google, Amazon e così via (Apple non ha propri datacenter ma si rivolge agli altri *provider* noti) è chiaro che la problematica riveste una grandissima quantità di dati gestiti in cloud da numerose aziende europee.

La prima risposta di molti *Provider* è stata l'adesione alle Clausole Contrattuali Tipo, che però, come abbiamo visto, hanno il medesimo problema che ha invalidato il *Privacy Shield*, per cui sarebbero necessarie ulteriori garanzie di sicurezza nel trasferimento di dati (Le Linee Guida EDPB 02/2020 citano …«*a condizione che siano messe in atto misure tecniche e organizzative adeguate per salvaguardare i diritti e le libertà degli interessati, come misure tecniche supplementari (ad esempio misure di sicurezza, pseudonimizzazione e restrizioni di accesso*»).

Secondo le opinioni di molti esperti a livello internazionale tali ulteriori garanzie potrebbero essere fornite da misure di sicurezza ulteriori quali la **pseudonimizzazione** e la **cifratura**. Da un punto di vista concettuale è chiaro che se il titolare o responsabile del trattamento che desidera esportare i dati personali in un *cloud* negli Stati Uniti, attraverso la pseudonimizzazione o la cifratura degli stessi si garantirebbe contro ingerenze di apparati governativi degli Stati Uniti, poiché i dati a cui avrebbero eventualmente accesso sarebbero non identificabili, ovvero non sarebbe comunque possibile identificare le persone fisiche proprietarie

dei dati in questione. Soluzione giuridicamente valida, ma poco applicabile dal punto di vista pratico.

Immaginiamo, infatti, applicazioni in cloud utilizzate da tempo che memorizzano i loro database in piattaforme *cloud* ospitate in *datacenter* in USA: a parte il fatto che i contratti con i fornitori sono stati sottoscritti pre GDPR e pre Schrems II, e dunque difficilmente emendabili a costi contenuti, come possiamo pensare di cifrare il database che non è stato predisposto in tale ottica? Oggi parleremmo di *privacy-by-design*, ma il discorso potrebbe essere valido per i nuovi applicati, fermo restando che la scelta si riduce molto se imponiamo questo vincolo.

Tantomeno parlare di pseudonimizzazione degli archivi digitali, ubicando tabelle diverse in *datacenter* diversi. Occorrerebbe una riprogettazione di tutto il sistema informatico… certamente si può fare tutto, ma a quali costi? E poi su campi anagrafici come ci si deve comportare? Se la mail è del tipo nome.cognome@dominio.it il dato personale resta, i campi contenenti *nome* e *cognome* non è che li possiamo dividere a piacimento.

Personalmente ho assistito a diversi eventi (naturalmente rigorosamente "*webinar*" on line in questo periodo) nei quali alcuni esperti giuristi hanno fornito indicazioni su come le aziende dovrebbero procedere per adeguarsi al post Schrems II e, francamente, ho sentito anche molti pareri e risposte alle domande dei partecipanti, per così dire, "poco pragmatiche" e di non semplice applicazione, soprattutto per le piccole e medie organizzazioni del nostro Paese.

Tra le risposte più paradossali ricordo la seguente: "*se un collaboratore di un'azienda sita nella UE con dati in cloud nella UE accede, da una postazione di lavoro negli USA, a dati (personali) memorizzati negli archivi digitali dell'azienda, si tratta di trasferimenti di dati extra UE*?" La risposta è stata "*si, perché il collaboratore accedendo ai dati tratta dati personali*".

Ora, chiaramente non si può estrapolare una domanda dal contesto in cui avviene l'elaborazione dei dati, che presuppone probabilmente un'azienda multinazionale che magari dovrebbe aver stabilito delle c.d. "norme vincolanti d'impresa" (o *binding corporate rules*) come disciplinato dall'art. 47 del GDPR, ma prescindiamo da ciò (l'argomento meriterebbe una trattazione separata più ampia) e facciamo un ragionamento. Se la mia organizzazione – sita nella UE con Server nella UE – pubblica, attraverso un portale web ad accesso riservato (tralasciamo per un momento le misure di sicurezza implementate per il controllo degli accessi), alcune informazioni contenenti anche dati personali, probabilmente il portale web sarà accessibile anche fuori dallo Spazio Economico Europeo, salvo aver implementato particolari controlli (comunque aggirabili accedendo attraverso VPN che geolocalizzano l'indirizzo IP in Europa). Si tratta di trasferimento di dati personali extra UE? Non può essere, perché in tal caso qualunque dipendente o collaboratore di un'azienda ubicata nella UE che va in trasferta in un Paese terzo, per il quale non esistono decisioni di adeguatezza sulla regolamentazione a

protezione dei dati personali, e che accede anche semplicemente alla posta elettronica di lavoro tramite dispositivo mobile effettuerebbe un trattamento di dati personali con trasferimento extra UE! Allora bisogna guardare soltanto a dove i dati sono conservati, anche se questo principio non è stato definito in modo preciso e se qualche esperto di privacy vi dicesse che è sufficiente una visualizzazione dei dati su un dispositivo in U.S. per rientrare nel trasferimento dei dati extra UE o ha interpretato male il Regolamento oppure c'è una falla nel regolamento UE 679/2016 stesso.

Ma torniamo al problema del *cloud* negli Stati Uniti, che si estende a tutti i *cloud* gestiti da società americane (ma qui non siamo nell'ambito di trasferimenti extra-UE).

Alcuni autorevoli esperti della materia indicano questi passi per affrontare e gestire il problema a livello aziendale:

1. Identificare gli archivi contenenti dati personali conservati e/o gestite da fornitori al di fuori dello Spazio Economico Europeo (SEE); ma questo avrebbe dovuto essere già stato fatto.
2. Fra questi vanno identificati gli archivi che attualmente sono gestiti negli Stati Uniti sfruttando, come base giuridica, il *Privacy Shield*.
3. Esaminare i relativi contratti di gestione dei dati in *cloud* con i fornitori coinvolti e richiedere ai medesimi su quali nuove condizioni sono resi possibili i trattamenti di dati personali fuori dallo SEE.
4. Contrattare con i fornitori nuove condizioni contrattuali per rendere lecito il trasferimento di dati extra UE (es. SCC integrate con misure di garanzia aggiuntive, ecc.).
5. In alternativa al punto precedente migrare il *cloud storage* in *datacenter* nella UE.
6. Adeguare le informative privacy ed il Registro delle attività di trattamento di dati personali nei punti relativi al trasferimento dei dati in un Paese Terzo o Organizzazione internazionale.

In generale, se il trasferimento dei dati non riguarda gli Stati Uniti, ma un altro Paese per il quale non è presente una decisione di adeguatezza della Commissione Europea, si consiglia – prima del punto 4 – di approfondire quali requisiti legislativi relativi alla protezione dei dati personali sono in vigore nel Paese ove vengono esportati i dati, al fine di decidere se il trasferimento può essere adeguatamente tutelato da clausole contrattuali stipulate con il fornitore.

Le procedure indicate sono formalmente corrette, ma alcune di queste attività sono estremamente difficoltose ed onerose per le nostre PMI. Oltre ad un eventuale *cloud* nel quale può essere "appoggiato" un sistema informatico, occorrerebbe valutare:

- l'eventuale piattaforma web utilizzata dal consulente del lavoro per elaborare le paghe (che difficilmente quest'ultimo ha gestito in conformità al GDPR con

una gestione in qualità di sub-responsabile del trattamento);
- i servizi di *office automation* in cloud forniti da Microsoft (Office 365, ora Microsoft 365 e OneDrive) o Google /Gmail, GDrive, ecc.), ma anche le tanto diffuse piattaforme di web-*meeting* o videoconferenza quali Microsoft Teams o Skype, Google Meet, GoToMeeting, ecc. che si servono di *datacenter* collocati negli USA ed altrove.
- Io servizi di invio mail e newsletter basati sul web.

Alcuni di questi servizi possono essere "spostati" su *datacenter* in Europa, altri no. Ma sono servizi che molte aziende utilizzano da tempo!

Ad aggravare la situazione occorre notare che le piattaforme *Google Classroom* e *Microsoft for Education*, tanto importanti in questo periodo di Didattica A Distanza e che hanno parzialmente salvato l'istruzione scolastica in questi mesi, sono state ufficialmente approvate dall'AGID (Agenzia per l'Italia Digitale) in quanto ritenute "sicure", soprattutto rispetto ad altre che hanno registrato violazioni di dati importanti (es. Zoom). Ma non solo: il Ministero della Giustizia ha autorizzato lo svolgimento di udienze dei processi civili e penali in modalità "a distanza", durante l'emergenza Covid-19, attraverso la piattaforma Microsoft Teams. Cosa facciamo? Cambiamo tutto in questo momento particolare di emergenza?

Tra le risposte che ho sentito fornire da diversi legali in alcuni webinar è che i *provider* – quali Microsoft e Google – forniscono la possibilità di scegliere l'ubicazione del *datacenter* in Europa… ma a quale prezzo? Gli abbonamenti, ad es. a *Google Workspace Enterprise*, che consentono di scegliere l'ubicazione del *datacenter* costano molto di più della semplice licenza *business* per i medesimi servizi!

Perché una piccola o media organizzazione, che probabilmente sta facendo fatica a reggere l'effetto devastante di questa pandemia, dovrebbe sostenere questi ulteriori costi? Solo perché esiste la recondita possibilità che l'FBI o l'NSA vadano un domani a leggere i dati personali trattati da società statunitensi? Al proposito il Dipartimento del Commercio degli Stati Uniti ha pubblicato, a settembre 2020, un *Whitepaper* denominato "*Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*" dove la portata del problema viene significativamente sminuita, possono essere reperiti altri articoli sul web che minimizzano la possibilità che enti governativi USA possano violare diritti sulla protezione dei dati dei cittadini dell'Unione. Come in altre

questioni bisogna “sentire tutte le campane”.

Se valutiamo correttamente questo rischio per gli interessati (i nostri dipendenti e/o i nostri clienti o persone fisiche che li rappresentano, ad esempio) possiamo facilmente capire che è ampiamente compensato dal fatto che i *datacenter* di Google e Microsoft sono molto più sicuri di un *datacenter* dislocato nella UE, in più le società di Mountain View e di Redmond possono garantire, oltre a svariate certificazioni sulla sicurezza delle informazioni (ISO 27k) e sui *datacenter*, anche una ridondanza dello *storage* ineguagliabile. I nostri dati, infatti, non sono memorizzati in un unico *datacenter*, in Irlanda o negli Stati Uniti, ma sono replicati in altri *datacenter*, magari in Australia o in Sudamerica, garantendoci così la disponibilità dei dati anche in caso di grandi cataclismi localizzati quali terremoti, incendi o alluvioni, o emergenze pandemiche che impediscono al personale di svolgere le normali attività di manutenzione ICT.

Purtroppo, in questo caso, il GDPR non richiede di basarsi su una **valutazione dei rischi**, ma su basi giuridiche che possono essere valide o meno. Infatti, se leggete le FAQ dell’EDPB tradotte dal nostro Garante per la Protezione dei Dati Personali potrete notare asserzioni molto forti, ovvero che **il trasferimento di dati personali negli USA, in assenza di adeguate garanzie, è illegale** e che **non è previsto un periodo di transizione**.

La questione, credo, non sia solo legale ed etica (protezione dei diritti delle persone fisiche relativamente ai loro dati personali), ma anche politica. La UE punta a un *cloud* europeo? Vogliono contrastare lo strapotere delle società americane in questo settore?

Di conseguenza credo che una soluzione – concreta e praticabile da tutti – debba essere trovata a livello politico, fra UE e USA, con la partecipazione di EDPB e/o altri Enti competenti in tema di privacy a livello internazionali. L’importante è che questi enti non perdano il buon senso e si calino nella realtà industriale e dei servizi delle organizzazioni di ogni tipo che operano nell’Unione.

Nel frattempo, quale consiglio dare alle piccole e medie imprese del nostro Paese? Sicuramente quello di percorrere gli step precedentemente indicati guidati dal buon senso. Ossia di fermarsi nel caso emergessero ostacoli insormontabili o comunque si configurassero soluzioni eccessivamente costose, e di aspettare che a livello più alto siano trovate delle soluzioni perseguibili.

Non vorrei che qualche organizzazione, perseguendo le strade più “rigoriste”, decida di abbandonare servizi efficienti e discretamente sicuri a fronte di soluzioni meno efficienti e soprattutto meno sicure, ad esempio eliminando un backup in *cloud* a fronte di un backup in locale.

Da un punto di vista formale *l’escamotage* potrebbe essere quello di ricorrere alle deroghe previste dall’art. 49 del Regolamento UE 679/2016, tra cui ad esempio il

consenso dell’interessato, purché adeguatamente informato sui rischi che corrono i suoi dati personali (difficile far capire come stanno le cose realmente, impraticabile in molti casi) e modificare nel modo più generico possibile Informative privacy e Registro dei trattamenti.

Se nelle realtà di medio-piccole dimensioni al momento si trovano tutte le posizioni possibili, dal non prendere nemmeno in considerazione il problema, a reimpostare i sistemi informatici in modalità più “autarchiche”, nelle Aziende più ci si pone anche la domanda: quali alternative credibili ci sono ai servizi di Microsoft, Google, ecc.? Se dobbiamo lavorare in diversi Paesi del mondo dobbiamo adeguarci anche alla normativa vigente in quel Paese, privacy compresa.

Vedi anche: le FAQ EDPB su Schrems II tradotte dal Garante Privacy, il Whitepaper del Governo USA e le Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.