Digeat N.1 - 19 Marzo 2024

Trasferire dati personali oltre i confini europei: un’analisi complessa da fare per i DPO di organizzazioni pubbliche e private

Di Andrea Lisi

Abstract

Fornire precisi parametri per legittimare trasferimenti di dati personali extra SEE laddove non sia intervenuta una decisione di adeguatezza da parte della Commissione europea è un’attività molto delicata e complessa per chi si occupa di protezione dei dati personali. Per orientarsi occorre prima di tutto comprendere bene come si articola il principio di accountability in questi contesti.

Indice

Premessa

Ha senso ancora oggi porsi problematiche legate al trasferimento dei nostri dati personali fuori dai confini europei? Non possiamo non chiedercelo se siamo Data Protection Officer o anche semplici cultori della protezione dei dati personali. Effettivamente dai tempi dell’Internet siamo ormai in un mondo globalizzato, anazionale, privo di confini, collegato da nervi che sembrano appartenere a un unico cervello. Eppure, già molti anni prima di ciò che stiamo vivendo adesso, Nathaniel Hawthorne scriveva che “*il mondo della materia è diventato un grande nervo, vibrante migliaia di miglia in un impetuoso punto del tempo*”. Ma non poteva ovviamente riferirsi all’internet, al web, o all’avvento dei social o dell’intelligenza artificiale, ma all’avvento dell’energia elettrica.

Ogni rivoluzione tecnologica ci scuote nel profondo e sembra mettere radicalmente in discussione i nostri principi etici e le nostre certezze giuridiche.

> “*Nel Fedro di Platone, Socrate diceva che la scrittura era una minaccia per la cultura perché a un libro non si possono fare domande. A Socrate mancava Internet*”, ci ricordava ironicamente Luciano De Crescenzo. E oggi in questo suo pensiero avrebbe senz’altro citato l’IA che ha invaso ogni discorso relativo all’innovazione digitale che ci riguarda.

I grandi pensatori hanno sempre saputo essere visionari e sono riusciti così a porci dubbi, domande, che riescono a proiettarci verso il futuro, astraendoci dal presente. Obiettivi simili si pone la normativa generale e, cioè, elabora fattispecie astratte in grado di piegarsi e adattarsi anche alle più incredibili

rivoluzioni tecnologiche, ovviamente anche grazie all'interpretazione giuridica.

I principi generali ci aiutano da sempre a trovare una chiave di lettura e documentare una scelta responsabile. Ed è questo, del resto, ciò che si chiede a chi oggi si occupa di "compliance digitale", a maggior ragione nell'applicazione della normativa sulla protezione dei dati personali che è governata – come ben sappiamo – dal fondamentale principio di ***accountability***.

E il principio di *accountability* anima anche le scelte che titolari e responsabili del trattamento dei dati personali – magari coadiuvati da preparati DPO – devono compiere in caso di trasferimenti di dati extra SEE.

I trasferimenti di dati personali fuori dai confini europei nel GDPR: le finalità del legislatore

Le ragioni per le quali in un mondo totalmente globalizzato e interconnesso sia ancora necessario **verificare la legittimità di un trasferimento di dati** da un territorio a un altro sono ben illustrate nel considerando 101 del GDPR che afferma in particolare che "*i flussi di dati personali verso e da paesi al di fuori dell'Unione e organizzazioni internazionali sono necessari per l'espansione del commercio internazionale e della cooperazione internazionale. L'aumento di tali flussi ha posto nuove sfide e problemi riguardanti la protezione dei dati personali. È opportuno però che, quando i dati personali sono trasferiti dall'Unione a titolari del trattamento e responsabili del trattamento o altri destinatari in paesi terzi o a organizzazioni internazionali, il livello di tutela delle persone fisiche assicurato nell'Unione dal presente regolamento non sia compromesso, anche nei casi di trasferimenti successivi dei dati personali dal paese terzo o dall'organizzazione internazionale verso titolari del trattamento e responsabili del trattamento nello stesso o in un altro paese terzo o presso un'altra organizzazione internazionale. In ogni caso, i trasferimenti verso paesi terzi e organizzazioni internazionali potrebbero essere effettuati soltanto nel pieno rispetto del presente regolamento. Il trasferimento potrebbe aver luogo soltanto se, fatte salve le altre disposizioni del presente regolamento, il titolare del trattamento o il responsabile del trattamento rispetta le condizioni stabilite dalle disposizioni del presente regolamento in relazione al trasferimento di dati personali verso paesi terzi o organizzazioni internazionali*".

La preoccupazione del legislatore europeo, quindi, non è di certo quella di paralizzare il commercio internazionale o elettronico, ma di continuare a **salvaguardare i diritti e le libertà fondamentali delle persone fisiche anche nel momento in cui i loro dati si spostano oltre i confini europei**. Del resto, tale preoccupazione si ritrova, nelle sue radici interpretative, anche negli ambiti di applicazione materiale e territoriale del GDPR che mirano a imporre le sue fondamentali garanzie in modo il più ampio possibile. Così vanno interpretati sia il **considerando 14** che afferma con nettezza l'opportunità che "*la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali* " e sia **il considerando 18** che – pur ricordando che il GDPR non possa applicarsi ad attività domestiche e strettamente personali (come l'uso dei social network) – afferma con forza che esso però vada applicato *"ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico*".

> Lo spirito del GDPR in poche parole è proprio quello di costituire un baluardo sostanziale a tutela dei nostri diritti e libertà fondamentali che possono essere calpestati da una digitalità fuori controllo e nelle fauci ingorde di grandi provider anazionali.

I presupposti di legittimità dei trasferimenti extra SEE

Come sappiamo, secondo il GDPR i trasferimenti di dati personali verso Paesi non appartenenti allo Spazio Economico Europeo (SEE, ossia UE + Norvegia, Liechtenstein, Islanda) o verso

un'organizzazione internazionale sono consentiti se l'adeguatezza del Paese terzo o dell'organizzazione sia stata riconosciuta tramite decisione della Commissione europea (art. 45 del Regolamento UE 2016/679). In assenza di tale decisione, il trasferimento è consentito solo qualora il titolare o il responsabile del trattamento forniscano **garanzie adeguate** che prevedano quindi **diritti azionabili e mezzi di ricorso effettivi per gli interessati** (art. 46 del Regolamento UE 2016/679).

Al riguardo, possono costituire garanzie adeguate, **senza autorizzazione da parte del Garante**:

- gli strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici (art. 46, par. 2, lett. a);
- le norme vincolanti d'impresa (art. 46, par. 2, lett. b);
- le clausole tipo (art. 46, par. 2, lett. c e lett. d);
- i codici di condotta (art. 46, par. 2, lett. e);
- i meccanismi di certificazione (art. 46, par. 2, lett. f).

Previa autorizzazione del Garante:

- le clausole contrattuali *ad hoc* (art. 46, par. 3, lett. a);
- gli accordi amministrativi tra autorità o organismi pubblici (art. 46, par. 3, lett. b)[1].

In assenza di ogni altro presupposto, è possibile trasferire i dati personali in base ad **alcune deroghe** (consenso, contratto, interesse pubblico, difesa in giudizio, interesse vitale, registro pubblico, cogente interesse legittimo del titolare) che secondo l'art. 49 del Regolamento UE 2016/679 si verificano in specifiche situazioni.

Tali deroghe vanno, quindi, considerate **residuali e occasionali**, secondo quanto precisato nel considerando 111, laddove si afferma testualmente che "*è opportuno prevedere la possibilità di trasferire dati in alcune circostanze se l'interessato ha esplicitamente acconsentito, se il trasferimento è occasionale e necessario in relazione a un contratto o un'azione legale, che sia in sede giudiziale, amministrativa o stragiudiziale, compresi i procedimenti dinanzi alle autorità di regolamentazione. È altresì opportuno prevedere la possibilità di trasferire dati se sussistono motivi di rilevante interesse pubblico previsti dal diritto dell'Unione o degli Stati membri o se i dati sono trasferiti da un registro stabilito per legge e destinato a essere consultato dal pubblico o dalle persone aventi un legittimo interesse. In quest'ultimo caso, il trasferimento non dovrebbe riguardare la totalità dei dati personali o delle categorie di dati contenuti nel registro; inoltre, quando il registro è destinato a essere consultato dalle persone aventi un legittimo interesse, i dati possono essere trasferiti soltanto se tali persone lo richiedono o ne sono destinatarie, tenendo pienamente conto degli interessi e dei diritti fondamentali dell'interessato*".

> Se la decisione di adeguatezza della Commissione consente sostanzialmente all'esportatore di dati di muoversi nelle sue valutazioni come se si fosse all'interno dello Spazio Economico Europeo, in assenza di tale decisione di adeguatezza occorre fare **analisi supplementari**, pur muovendosi nelle condizioni stabilite (o meglio garanzie ritenute adeguate) dal GDPR. Del resto, questo è lo spirito del principio di *accountability* che anima l'intero Regolamento europeo, come ci ha ricordato l'European Data Protection Board (EDPB) nella sua **Raccomandazione 01/2020**.

Tale impostazione interpretativa non deve sorprenderci, perché la semplice lettura del considerando 104 del GDPR ci indirizza in questa direzione, laddove si precisa che "*in linea con i valori fondamentali su cui è fondata l'Unione, in particolare la tutela dei diritti dell'uomo, è opportuno che la Commissione, nella sua valutazione del paese terzo, o di un territorio o di un settore specifico all'interno di un paese terzo, tenga conto del modo in cui tale paese rispetta lo stato di diritto, l'accesso alla giustizia e le norme e gli standard internazionali in materia di diritti dell'uomo, nonché la legislazione generale e settoriale riguardante segnatamente la sicurezza pubblica, la difesa e la sicurezza nazionale, come pure l'ordine pubblico e il diritto penale. L'adozione di una decisione di adeguatezza nei confronti di un territorio o di un settore specifico all'interno di un paese terzo dovrebbe prendere in considerazione*

criteri chiari e obiettivi come specifiche attività di trattamento e l'ambito di applicazione delle norme giuridiche e degli atti legislativi applicabili in vigore nel paese terzo. Il paese terzo dovrebbe offrire garanzie di un adeguato livello di protezione sostanzialmente equivalente a quello assicurato all'interno dell'Unione, segnatamente quando i dati personali sono trattati in uno o più settori specifici. In particolare, il paese terzo dovrebbe assicurare un effettivo controllo indipendente della protezione dei dati e dovrebbe prevedere meccanismi di cooperazione con autorità di protezione dei dati degli Stati membri e agli interessati dovrebbero essere riconosciuti diritti effettivi e azionabili e un mezzo di ricorso effettivo in sede amministrativa e giudiziale".

In poche parole, laddove questa puntuale valutazione di adeguatezza non sia stata fatta dalla Commissione, **devono essere i titolari e i responsabili del trattamento a provvedere direttamente a compensare tale carenza** di protezione dei dati personali in un paese terzo attraverso l'utilizzo di adeguate garanzie a tutela dell'interessato[2].

Conclusioni

In estrema sintesi, l'EDPB ha precisato che, in assenza di decisione di adeguatezza rispetto al paese terzo in cui si intende effettuare il trasferimento, **il titolare del trattamento può adottare una delle misure di garanzia previste dall'art. 46 del GDPR, ma deve anche assicurarsi che il livello di protezione del paese terzo sia sostanzialmente equivalente a quello offerto dall'ordinamento europeo**, anche favorendo l'implementazione le cd. **misure supplementari** riportate nella Raccomandazione 01/2020 dell'EDPB.

Si richiede a titolari e responsabili, cooperando con i propri DPO, di sviluppare il cd. ***transfer impact assesment***, un modello organizzativo ben documentato che di fatto consenta una valutazione concreta e approfondita dello **strumento scelto dal titolare per legittimare il trasferimento** dei dati personali nel Paese Terzo.

> Tale valutazione va fatta anche alla luce del quadro giuridico e dell'applicazione concreta della legge di riferimento del paese terzo di destinazione. Si tratta di un *assessment* che dovrà essere, quindi, effettuato in modo calzante al contesto di riferimento, attraverso particolareggiate mappature sui flussi di dati e monitorando costantemente l'adeguatezza offerta dalle misure tecniche e organizzative individuate nell'analisi.

Come sappiamo bene, la Raccomandazione dell'EDPB 01/2020 è stata motivata dalla **sentenza C-311/18** (cd. «Schrems II») con la quale la Corte di giustizia dell'Unione europea ha dichiarato l'invalidità della decisione 2016/1250 della Commissione europea sull'adeguatezza della protezione offerta dal regime del cd. "*Privacy Shield*". Ma gli autorevoli contenuti della sentenza della Corte e della Raccomandazione dell'EDPB hanno una portata generale e devono essere accolti con favore nell'analisi interpretativa di qualsiasi trasferimento dei dati extra SEE.

Tutti i titolari di dati personali che intendono trasferire dati verso Paesi che **non sono stati oggetto di positiva valutazione di adeguatezza da parte della Commissione** (o verso organizzazioni che non rientrano nella "Data Privacy Framework List")[3] devono, quindi, in via preliminare valutare le circostanze concrete dei trasferimenti dei dati e le misure supplementari eventualmente azionabili. **Devono cioè preoccuparsi di garantire un livello adeguato di protezione delle persone fisiche in relazione ai loro diritti e libertà fondamentali**. In ossequio al principio di *accountability*, l'adeguatezza del livello di protezione deve essere verificata e assicurata in modo attivo e continuo, attuando misure legali, tecniche e organizzative che ne garantiscano l'effettività e comprovando il rispetto dei principi di protezione dei dati personali.

NOTE

[1] Utilissimo il riepilogo fornito sul sito del Garante per la protezione dei dati personali e reperibile a questa pagina.

[2] Si veda in proposito il considerando 108 del GDPR.

[3] Si fa ovviamente riferimento all'EU-US Data Privacy Framework (DPF) del 10 luglio 2023 e cioè al nuovo accordo USA-UE sul trasferimento dei dati che in qualche modo ha riattivato la fluidità dei trasferimenti di dati messi in crisi dalla sentenza della Corte di Giustizia del 16 luglio 2020.

APPROFONDISCI L'ARGOMENTO