il Quotidiano Giuridico

IP & IT

PRIVACY

Il trattamento dei dati personali nell'ambito dei gruppi di società internazionali

giovedì 24 febbraio 2022di Pellicanò Gerolamo Avvocato, Of Counsel CBA
Iorio Anna Avvocato, CBA

Il trattamento dei dati personali nell'ambito dei gruppi societari internazionali presenta profili di complessità, che derivano dalla governance societaria, dai diversi ordinamenti giuridici con cui essi si devono confrontare e dalle non comuni sensibilità rispetto a temi anche importanti.

I gruppi internazionali sono costituiti da una società capogruppo a cui fanno riferimento varie società, tutte direttamente o indirettamente controllate dalla stessa e che sono stabilite in diversi stati. Sono caratterizzati al loro interno da un legame di tipo gestionale, economico e finanziario. La capogruppo esercita la direzione unitaria e coordina l'attività delle controllate per il conseguimento dell'interesse comune ulteriore rispetto a quello realizzabile dalle singole società.

Come anche l'esperienza fin qui acquisita conferma, questo assetto comporta una complicata gestione dell'attività di compliance alla normativa sulla protezione dei dati personali (in particolare, per quanto ci riguarda, il Regolamento Generale sulla protezione dei dati personali (UE) 679/2916, noto come "GDPR"), specie quando l'attività di direzione e coordinamento è esercitata da una capogruppo stabilita in uno stato al di fuori della UE che non sia dotato in materia di una normativa che offra un grado equivalente di protezione dei dati. Può accadere quindi che, nell'esecuzione della direzione unitaria del business del gruppo, la capogruppo stabilita al di fuori dell'UE si proponga di imporre alle controllate attività, procedure e linee guida la cui applicazione integrale potrebbe esporre le società al mancato rispetto della legge nazionale ed europea alla quale sono soggette.

Le difficoltà in concreto più frequentemente riscontrate nell'attività di consulenza legale a società italiane che fanno parte di gruppi internazionali possono essere ricondotte ai seguenti casi:

1) la capogruppo, stabilita in uno stato non facente parte dell'UE, nell'ambizione di uniformare a livello globale le normative del gruppo impone alle controllate

policies senza tenere conto delle legislazioni nazionali incompatibili;

---

2) la capogruppo, stabilita in uno stato dell'UE, non provvede a normare le attività di trattamento del gruppo nel rispetto del GDPR;

---

3) la capogruppo, stabilita in uno stato dell'UE, si mostra renitente ad accettare le specificità applicative - dovute alla normativa locale di riferimento e alle interpretazioni della autorità garante – rispetto a quanto proposto a livello di gruppo.

Nella attività di compliance al GDPR la prima criticità riguarda la mappatura dei flussi dei dati personali a livello di gruppo. È un processo fondamentale che richiede la piena comprensione e collaborazione di tutte le entità e risorse del gruppo. Spesso i flussi dei dati personali seguono percorsi anche territoriali che è problematico ricostruire. È importante che il management apicale sia consapevole dell'importanza di una appropriata identificazione dei flussi. Questa attività comporta l'individuazione dell'attività di trattamento che coinvolgono le diverse società, delle categorie dei dati trattati, delle finalità e della base giuridica che legittima la condivisione dei dati all'interno del gruppo, dei trasferimenti dei dati dentro e fuori l'UE.

Si deve prestare adeguata attenzione all'effettivo ruolo svolto da ciascuna società nelle attività di trattamento dei dati personali e, in particolare, se ciascuna di esse operi in qualità di titolare del trattamento (in quanto ne determini singolarmente finalità e mezzi), ovvero come contitolare del trattamento (quando finalità e mezzi siano determinati insieme ad una o più altre società del gruppo), ovvero, infine, come responsabile del trattamento (quando tratti i dati per conto di altra o altre società del gruppo).

La corretta individuazione non è sempre agevole. Si pensi all'attività di trattamento dei dati personali nell'utilizzo degli strumenti IT, quando la gestione è accentrata presso la capogruppo. Questa, in qualità di fornitore dei servizi IT per le controllate, potrebbe trattare i dati personali per conto di ciascuna di esse e sarebbe pertanto configurabile come responsabile del trattamento designata da ciascuna di esse. Diversamente la capogruppo potrebbe acquistare software e altri tool a livello centrale per l'intero gruppo, decidendone finalità e modi del trattamento, lasciando tuttavia alle società autonomia nella gestione dei tool. In tal caso, la definizione dei ruoli e delle competenze delle società nel trattamento dei dati personali risulta più complessa.

Altro aspetto di non poco conto riguarda la legittimità della comunicazione dei dati personali tra le società del gruppo. Frequentemente la controllante si impone come destinataria dei dati trattati dalle società del gruppo senza che vi sia previamente una precisa individuazione delle finalità e della base giuridica che possa legittimare tale comunicazione. Non sempre si può ricorrere come base giuridica al legittimo interesse della capogruppo di coordinare e dirigere le attività del gruppo, in qualità di autonomo titolare del trattamento.

Le criticità crescono se i trasferimenti infragruppo coinvolgono società stabilite al di fuori dell'Unione Europea.

Quando il trattamento dei dati personali ricade nell'ambito di applicazione materiale e territoriale del GDPR e comporta il trasferimento dei dati al di fuori dell'UE, si devono rispettare le condizioni previste dal GDPR perché il trasferimento sia ritenuto legittimo. Il paese destinatario stabilito al di fuori dell'UE deve essere dichiarato adeguato da parte della Commissione europea, oppure devono essere fornite altre garanzie adeguate, come l'adozione di norme vincolanti di impresa o di clausole contrattuali standard approvate dalla Commissione.

Come si vede, è ribadita l'imprescindibilità di una mappatura dei flussi dei dati personali a livello di gruppo.

Nella pratica si verifica la tendenza dei gruppi internazionali a promuovere accordi di gruppo che regolino i flussi dei dati personali sottoscritti dalle società interessate.

È uno strumento utile con cui un gruppo di società stabilite anche al di fuori dell'UE può disciplinare i trasferimenti dei dati personali attraverso la loro previa mappatura e la conseguente indicazione delle garanzie introdotte ai sensi della normativa pertinente. Il contenuto è normalmente il seguente: elenco delle società partecipanti all'accordo; normativa applicabile; categorie di dati trattati con relative finalità e base giuridica; quando le società agiscono come responsabili del trattamento o in contitolarità (con indicazione di quanto previsto dagli artt. 28 e 26 del GDPR); clausole contrattuali standard per i trasferimenti al di fuori dell'UE; misure di sicurezza anche secondo quanto richiesto dalla Corte di Giustizia Europea nel caso "Schrems II".

Gli accordi devono quindi indicare chiaramente le singole attività di trattamento e le società che agiscono per ogni attività e con quale ruolo. Un accordo specifico e completo, pur di complessa definizione in relazione alle situazioni di fatto e ai diversi ordinamenti giuridici in gioco, potrebbe risultare una soluzione appropriata.

Uno strumento che dovrebbe essere maggiormente considerato è infine quello del "rappresentante" che, ai sensi del GDPR e nei casi in esso disposti, deve rappresentare il titolare o il responsabile del trattamento quando questi ultimi non sono stabiliti nell'UE ma trattano i dati personali degli interessati presenti nell'UE.

Un'ultima annotazione, di metodo. Al fine di comprendere i diversi trattamenti, i flussi di condivisione dei dati, i diversi ruoli, le specificità normativa è fondamentale la massima collaborazione tra legali in-house, DPO e consulenti esterni delle società del gruppo. Senza questa collaborazione ci si troverebbe di fronte a muri inespugnabili.