Il perimetro del GDPR

Author : Francesco Maldera

Date : 19 dicembre 2018

L’art. 3 del GDPR

L’art. 3 del Regolamento Europeo 2016/679, meglio noto come GDPR, delinea i confini della sua applicazione. Si tratta di confini fisici ma non solo. Ad una prima lettura, il testo appare chiarissimo: in sintesi, si potrebbe dire che devono adeguarsi al GDPR tutti i titolari ed i responsabili

- che hanno sede (principale o secondaria) nel territorio UE;
- che offrono prodotti o servizi destinati al mercato europeo;
- che monitorano il comportamento di persone fisiche all’interno della UE.

Tuttavia, la questione è un po’ più complessa e lo European Data Protection Board (EDPB)[i], cioè il Comitato Europeo dei Garanti nazionali, nella riunione plenaria del 16 novembre scorso, ha ritenuto di sottoporre a consultazione pubblica le linee guida n. 3/2018 *Guidelines on the territorial scope of the GDPR*[ii]. Le linee guida rimarranno in consultazione al pubblico, così come previsto dal comma 4 dell’art. 70, fino al 18 gennaio 2019; questo significa che chiunque può offrire il proprio contributo per il miglioramento delle indicazioni fornite dal documento.

Le linee guida si concentrano proprio sull’art. 3 del GDPR ed esordiscono ribadendo che esistono due criteri per stabilire l’ambito territoriale della sua applicazione: il criterio della *sede* (stabilimento) ed il criterio del *bersaglio*. I due criteri sono dettati, rispettivamente, dai commi 1 e 2 dell’art. 3.

Quanto conta la sede

Le linee guida n. 3/2018 sottolineano che se il titolare (o il responsabile) ha sede legale in uno dei paesi UE certamente sarà assoggettato al GDPR.

Il problema sorge quando titolare o responsabile non hanno sede legale in uno stato membro UE ma, per esempio, hanno un cosiddetto “stabilimento” ovvero una sede secondaria dalle

caratteristiche stabili. La presenza della sede secondaria, tuttavia, non è sufficiente ad obbligare il titolare (o il responsabile) a conformarsi alle previsioni del GDPR. Il comma 1 dell'art. 3, infatti, richiede che il regolamento deve essere applicato quando il processo di trattamento è sviluppato nell'ambito delle attività svolte in quella sede.

Un esempio: un'azienda coreana vende t?shirt online solo nel mercato asiatico. Tuttavia, ha i suoi fornitori nel nord Italia: tessuti, colori naturali, bottoni sono acquistati tra Lombardia e Piemonte. Quindi, decide di avvalersi di una sede dotata di foresteria che ospita, periodicamente, i buyer provenienti dalla Corea e dove opera stabilmente un *tuttofare* (autista, maggiordomo, ecc.). La sede può dirsi stabile ma l'attività che vi si svolge non riguarda il processo di trattamento di dati personali dell'azienda coreana che, quindi, non è obbligata ad adeguarsi al GDPR. Se nella sede operasse, invece, una segretaria per la registrazione dei contatti dei fornitori e per la definizione degli appuntamenti con loro sarebbe obbligatorio l'adeguamento al GDPR.

Questo chiarisce cosa vuol dire "stabilimento" ma le linee guida si occupano di approfondire gli *incroci* tra il titolare ed il suo responsabile del trattamento (ex art. 28) con riferimento alle rispettive sedi. Le possibili combinazioni sono le seguenti:

	TITOLARE	**RESPONSABILE**
1	Entro UE	Entro UE
2	Entro UE	Fuori UE
3	Fuori UE	Entro UE
4	Fuori UE	Fuori UE

dove

- la dicitura "Entro UE" significa che hanno sede legale o stabilimento con attività connessa al processo di trattamento di dati personali in uno dei paesi UE;
- la dicitura "Fuori UE" significa che non hanno sede legale né stabilimento con attività connessa al processo di trattamento di dati personali in uno dei paesi UE.

Il caso 1 ed il caso 4 non richiedono particolari approfondimenti: nel caso 1 entrambi sono soggetti al GDPR mentre nel caso 4 nessuno dei due è soggetto al regolamento.

Il caso 2 richiede, invece, che il titolare (che deve operare conformemente alla normativa europea), applicando l'art. 28, induca il suo responsabile a rispettare il GDPR. Questo significa che l'accordo contrattuale esistente debba essere piuttosto puntuale rispetto alle previsioni del regolamento e che i controlli previsti dal punto h, coma 3 dell'art. 28 siano abbastanza intensi. Esiste, in pratica, un obbligo *indiretto* di applicazione del GDPR da parte del responsabile del trattamento.

Viceversa, il caso 3 prevede che il responsabile del trattamento rispetti il GDPR ma non presenta gli stessi obblighi per il titolare. Quindi, quest'ultimo non ha gli obblighi che il GDPR prevede per i titolari del trattamento sempre che non ricada nelle previsioni del comma 2 dell'art. 3 che approfondiremo più avanti.

Un esempio: un rivenditore di auto (titolare) con sede legale in Marocco e nessun'altra sede ha deciso di rivolgersi ad un call center francese (responsabile) per rilevare la customer satisfaction dei propri clienti che sono esclusivamente soggetti residenti in Marocco. In questo caso, il titolare non ha l'obbligo di rispettare il GDPR mentre il call center, essendo nel territorio UE, deve rispettare gli *obblighi del responsabile del trattamento* previsti dal GDPR.

E quanto conta l'attività che si svolge

Il criterio del *bersaglio*, dettato dal comma 2 dell'art. 3, fornisce le condizioni di applicazione rispetto all'attività che, in concreto, svolgono titolare o responsabile e le persone interessate da tale attività.

Proprio rispetto agli *interessati* vale una premessa fondamentale: è l'insieme delle persone che "sono nell'Unione Europea" e non solo quelli che hanno la cittadinanza in uno dei Paesi membri. Questo vuol dire che se l'attività svolta dal titolare "Fuori UE" (con il significato introdotto in precedenza) coinvolge il trattamento di dati personali di un immigrato in Italia, è necessario l'adeguamento al GDPR se la stessa attività rientra nell'offerta di beni o servizi o in un monitoraggio dei comportamenti.

Un esempio: un'organizzazione umanitaria con sede legale in Israele (e nessuna sede in Europa) intercetta i migranti in mare aperto e regala loro uno smartwatch per monitorare i loro spostamenti ed alcuni valori biologici (battito cardiaco, pressione sanguigna, ecc.) al fine di poter avviare interventi di primo soccorso in caso di necessità. Al momento dello sbarco in Italia, la società israeliana diventa *debitrice di privacy* nei confronti dei migranti che "sono nell'Unione Europea" e deve, quindi, rispettare il GDPR.

Le linee guida, quindi, approfondiscono i punti a) e b) del comma 2, art. 3.

Il punto a) è relativo all'offerta di beni e servizi a soggetti che "sono nell'Unione Europea" e le linee guida approfondiscono il percorso logico che ogni titolare (o responsabile) deve seguire per capire se è obbligato a conformarsi al GDPR con riferimento, soprattutto, all'attività di vendita online. In particolare, l'EDPB ritiene che debbano essere valutati i seguenti aspetti sintomatici di un sito web:

- esplicita citazione di un paese membro UE (o dell'intera UE) nell'ambito del proprio sito web;
- esistenza di campagne pubblicitarie, tradizionali o tramite social network o tramite motori di ricerca, dirette a paesi membri;
- intrinseca natura dell'attività, per esempio l'attività turistica;
- esistenza di elementi di contatto (numeri di telefono o indirizzi email dedicati) raggiungibili da paesi dell'UE;
- utilizzo di un dominio web esplicitamente riconducibile a paesi membri UE (.eu, .it, ecc.);
- presenza di specifiche istruzioni per lo svolgimento del servizio o per l'ottenimento del prodotto all'interno dell'Unione Europea;
- citazione di precedenti clienti europei;
- presenza dei prezzi espressi in euro;

- possibilità di consegna in paesi membri UE.

Naturalmente, l'EDPB precisa che la presenza di uno solo di questi aspetti sintomatici non può indurre a pensare che il titolare che offre questi beni o servizi sia obbligato a rispettare il GDPR. Tuttavia, la presenza di più sintomi e la loro intensità deve essere attentamente valutata dagli interessati oltre che, naturalmente, dalle autorità di controllo.

Il punto b) del comma 2, art. 3, invece, si focalizza sul monitoraggio. L'attività di monitoraggio che comporta il rispetto del GDPR deve essere diretta *intenzionalmente* a predire i comportamenti successivi degli interessati o alla loro profilazione. Le linee guida fanno rientrare in questo tipo di attività:

- le pubblicità online mirate;
- le attività di geolocalizzazione;
- le attività di tracciamento tramite cookie o altri sistemi (p.e. impronte digitali);
- l'offerta di diete personalizzate o, comunque, interventi sulla salute basati su dati raccolti da precedenti comportamenti degli interessati;
- la ripresa tramite TV a circuito chiuso;
- lo svolgimento di indagini di mercato sistematiche.

Conclusioni

Il documento prodotto dall'EDPB aggiunge, quindi, ulteriori elementi di riflessione ai trattamenti che, più o meno intensamente, superano i confini *fisici* e *politici* dell'Unione Europea. Confini che, per l'applicazione del GDPR, raramente possono considerarsi stabili nel tempo.

Note:

[i] https://edpb.europa.eu/

[ii] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf

Articolo a cura di **Francesco Maldera**