INTERNAZIONALIZZAZIONE DELLE IMPRESE, COME TRASFERIRE I DATI PERSONALI: IL CASO DEL REGNO UNITO

di Paola Zambon

La crisi spinge sempre più spesso a ricercare mercati nei quali i propri prodotti ed i propri servizi siano ancora appetibili e sempre più spesso l'internazionalizzazione non è più un'alternativa di investimento ma una vera e propria esigenza. È utile notare che il Regno Unito, oltre ad essere un mercato interessante sia per le opportunità che offre a livello commerciale, che a livello di tassazione, risulta essere anche ai fini delle multinazionali, il più appetibile a livello di normativa sulla privacy. L'analisi comprende anche riflessioni aggiornate al recente DL 93/13 in tema di delitti privacy.

❶ *Premessa normativa*

La normativa europea prevede che il trasferimento di dati personali oggetto di un trattamento (o destinati a essere oggetto di un trattamento dopo il trasferimento) verso un paese terzo possa aver luogo solo quando il paese terzo in questione garantisca un livello di protezione adeguato, prendendo in particolare considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo stesso, nonché le regole professionali e le misure di sicurezza applicabili.

In particolare, la Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Gazzetta ufficiale n. L 281 del 23/11/1995 pag. 31 – 50) prevede che un trasferimento di dati personali verso un paese terzo che non garantisce una tutela adeguata possa avvenire, in sintesi, in una delle seguenti condizioni:

- la persona interessata abbia manifestato il proprio consenso in maniera inequivocabile al trasferimento previsto;
- il trasferimento sia necessario per l'esecuzione di un contratto tra la persona interessata ed il responsabile del trattamento, oppure tra questi ed un terzo;
- il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante;
- il trasferimento sia necessario per la salvaguardia dell'interesse vitale della persona interessata, oppure
- il trasferimento avvenga a partire da un registro pubblico.

In ragione della normativa europea sul trattamento dei dati personali, dunque, in Europa i dati personali possono circolare nei ventisette paesi membri nonché nei tre membri EEA (Norvegia, Liechtenstein e Islanda). La Commissione europea ha inoltre il potere di determinare, sulla base dell'articolo 25 della direttiva 95/46/CE, se un paese terzo garantisca o meno un livello di protezione adeguato in ragione della propria legislazione domestica o dei impegni internazionali assunti.

Pertanto la Commissione ha definito una lista dei Paesi terzi che devono essere considerati tra quelli che applicano un adeguato livello di protezione ai fini del trattamento dei dati personali alla stregua di quello europeo, senza dover espletare ulteriori formalità. Tali Paesi risultano essere al momento: Andorra, Argentina, Autralia, Canada, Svizzera, Isole Faeroe, Guernsey, Stato di Israele, Isola di Man, Jersey, Stati Uniti (per quanto riguarda il trincio del *safe harbor* ed i trasferimenti di dati relativi ai passeggeri aerei), Nuova Zelanda, Repubblica Est Uruguay. Qualora il Paese nel quale vengono esportati i dati non sia presente in questa lista o non faccia parte dell'elenco europeo alla quale si applica la normativa europea, sono previsti alcuni meccanismi (es. "Clausole contrattuali tipo"[(1)]) al fine di esportare i dati personali.

❷ *Le novità del 2013*

Dal 2013 i Garanti per la privacy dei Paesi europei riuniti nel Gruppo "Articolo 29" (istituito dall'art. 29 della Dr. 95/46/Ce), organo consuntivo indipendente dell'Unione Europea per la privacy, hanno previsto ed approvato in particolare una procedura al fine di permettere la circolazione dei dati personali per le imprese che fanno parte di gruppi multinazionali anche al di fuori di questi Paesi per i quali non sia prevista un'adeguata protezione.

Il gruppo di lavoro ha prodotto diversi documenti nell'ottica di pervenire a linee guida utili per le imprese a partire dal 2003 in avanti. Ha fornito, inoltre, un documento esplicativo, datato 19 aprile 2013, per far comprendere sostanzialmente come una multinazionale si debba comportare nel trattamento dei dati personali per conto dei propri clienti facendoli circolare anche al di fuori dell'Unione europea.

Le "Norme vincolanti d'impresa" (*Binding Corporate Rules*, BCR) sono particolarmente adatte nel caso in cui il responsabile del trattamento (impresa di un gruppo multinazionale) intenda effettuare il trasferimento di dati personali ad un platea grande di altre imprese che fanno parte dello stesso gruppo con sedi in qualsiasi parte del mondo. Un tipico caso è quello dei servizi di *outsourcing* o di *cloud computing* offerti dalle imprese internazionali. Tali regole consentono, sostanzialmente, ad una particolare impresa del gruppo di venire delegata a responsabile del trattamento per conto di titolari (clienti) stabiliti in un Paese dell'Unione europea, sulla base di un adeguato contratto di servizi. Con le proprie regole di condotta ("*BCR for Processors*") potrà trattare e comunicare i dati personali all'interno del proprio gruppo, sia per le unità locali o per le sedi e che extra-europee. Per l'Italia la procedura dovrà essere approvata dall'Autorità Garante per la privacy ed in generale dall'Autorità del paese della società capogruppo. Le BCR fungono sostanzialmente da regole di condotta all'interno di un gruppo multinazionale per spostare dati personali in paesi che non garantiscano una protezione adeguata.

Attualmente risultano essere quarantadue le multinazionali che

hanno adottato tali regole. Nessuno ha scelto l'Italia come sede per il proprio gruppo multinazionale ai fini privacy e la ragione è alquanto lapalissiana. Si pensi ad esempio all'introduzione dei delitti in tema di privacy, frode informatica e carte di credito falsificate previsti dall'art. 9 c. 2 DL 93/13[2] che hanno introdotto di fatto la fattispecie delittuale della privacy anche nella responsabilità amministrativa delle società e degli enti (ai sensi e per gli effetti del D.Lgs. 231/01 e successive modifiche ed integrazioni).
In Italia, in sostanza, una società per dimostrare la propria innocenza ai fini di non essere ritenuto responsabile per i delitti privacy commessi nel proprio interesse o a proprio vantaggio da persone rientranti in posizione apicali (o sottoposti) dovrà provare di avere adottato un modello organizzativo atto ed idoneo a prevenire il compimento del reato.
In tema di trattamento illecito di dati personali, il Testo Unico sulla privacy Italiano, prevede che, salvo che il fatto costituisca più grave reato chiunque, al fine di trarne per sè o per altri profitto o di recare ad altri un danno, proceda al trattamento di dati personali in violazione della norma debba essere punito, se dal fatto derivi "nocumento", in particolare, secondo diversi orientamenti giurisprudenziali, il nocumento sarebbe da intendersi "come perdita patrimoniale o di mancato guadagno derivante dalla circolazione non autorizzata di dati personali", e non sempre "esclusivamente riferibile a quello derivato alla persona fisica o giuridica cui si riferiscono i dati, ma anche a quello causato a soggetti terzi quale conseguenza dell'illecito trattamento" quando si concretizzi in un pregiudizio sostanziale alla parte offesa.
Anche per le società quotate in borsa in Italia dunque i principi generali ed internazionali di controllo interno dovranno essere riletti ed aggiornati onde valutare il proprio allineamento con il profilo di rischio che caratterizza la stessa società.

In Italia l'art. 44, comma 1, lett. a) del Codice Privacy (D.Lgs. 196/03), stabilisce che il trasferimento di dati personali diretto verso un paese non appartenente all'Unione europea è consentito quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, individuate dall'Autorità anche in relazione a regole di condotta esistenti nell'ambito di società appartenenti a un medesimo gruppo, ovvero proprio le "norme vincolanti di impresa", garantendo all'interessato la possibilità di far valere i propri diritti nel territorio dello Stato, secondo le regole fissate dal Codice, anche in caso di mancata osservanza delle garanzie individuate nelle norme vincolanti d'impresa stesse.
Tra le sedi più gettonate come sede per il proprio gruppo multinazionale ai fini privacy invece si evidenzia e svetta con il 38% il Regno Unito, seguito al 36% circa dalla Francia e dal 24% circa dai Paesi Bassi.

❸ *Altre considerazioni in tema di Binding Corporate Rules*

Le "Norme vincolanti d'impresa" devono prevedere alcune clausole formate in modo che tutte le società all'interno del gruppo sia tenute a rispettarle. È fondamentale dunque la pianificazione della nomina di soggetti in posizione apicale che garantiscano la conformità normativa, la formazione adeguata per i dipendenti delle società ed la definizione di un modo in cui diffondere le norme vincolanti d'impresa, nonché l'obbligo per tutte le società del gruppo di rispettare i dettami del titolare del trattamento (in particolare le istruzioni sulla sicurezza contenute nel contratto).
È utile nominare altresì un soggetto collettore di tutte le istanze

Confronto della procedura per il trasferimento dei dati

	Italia	Regno Unito
Autorizzazione preventiva al trasferimento di dati personali	Richiesta all'Autorità Garante	Nessuna richiesta formale
Documenti da presentare alle Autorità Garanti per ottenere l'autorizzazione al trasferimento	Modello Wp 133[3], Testo delle norme vincolanti d'impresa e connessi allegati	Modello Wp 133[3], Testo delle norme vincolanti d'impresa e connessi allegati
Tempistica prevista ai fini dell'ottenimento dell'autorizzazione (se tutti i documenti sono considerati conformi)	45 giorni	Al massimo 1 mese
Richiesta la traduzione in lingua locale	Sì con traduzione giurata. La traduzione in forma semplice va comunque fatta per il modello Wp 133[3]	Sì ma solo per l'Autorità capofila
Richieste addizionali	Pagamento di diritti al Garante (1.000 euro)	Nessuna
Diffusione delle norme vincolanti d'impresa	Solo su richiesta	Pubblicazione nel sito del Garante Privacy britannico del permesso ottenuto. I documenti devono essere conformi al "Freedom of Information Act 2000" e sono generalmente comunicati solo su richiesta con eccezioni nel caso contengano dati sensibili.

da parte delle società del gruppo in modo che lo stesso sia in grado di fornire un'armonica ed aggiornata informativa delle eventuali problematiche sollevate al titolare del trattamento, che sarà così facilitato nell'individuare aggiustamenti o ridisegni del modello organizzativo adottato. È altresì fondamentale chiarire i profili di responsabilità del gruppo rispetto al titolare del trattamento ed agli interessati. A questi ultimi ovviamente dovrebbe essere consentita la scelta del foro di competente in caso di controversia. La vigilanza del modello organizzativo adottato dovrà inoltre ripercuotersi ovviamente in controlli periodici, sia da parte di *auditors* interni che esterni alla società in modo che il titolare del trattamento possa adottare le migliori misure preventive sulla base anche dell'analisi delle relazioni da essi stilate. Il controllo potrà avvenire ovviamente anche da parte delle Autorità Garanti competenti.
Una volta implementata la bozza delle BCR, al fine di nominare la società che rappresenterà il gruppo ai fini privacy e gli obblighi in esse indicate alle autorità competenti, si dovrà compilare la domanda *standard* per l'approvazione delle norme vincolanti d'impresa (WP 133)[3]. ©

NOTE

1. Si veda in particolare la Decisione della Commissione 2004/915/CE, del 27 dicembre 2004.
2. Per approfondimento si veda anche http://www.taxlawplanet.it/societa-nuove-responsabilita-per-i-delitti-in-tema-di-privacy-sostituzione-di-identita-digitale-e-carte-di-credito-falsificate-modelli-organizzativi-231-da-aggiornare/
3. Per il Testo delle norme: http://www.garanteprivacy.it/documents/10160/10704/1607333 ◊