Desk "Assistenza e Tutela della Proprietà Intellettuale e Ostacoli al Commercio"

ICE Pechino

Rapporto di approfondimento sul trasferimento di dati personali tra Unione Europea e Repubblica Popolare Cinese

La crescente digitalizzazione dei processi economici ha reso i flussi transfrontalieri di dati personali un elemento strutturale dell'attività delle imprese multinazionali. Gruppi societari con sedi in più giurisdizioni, piattaforme digitali, servizi cloud, sistemi HR centralizzati e attività di marketing a livello globale comportano, sempre più frequentemente, trasferimenti di informazioni personali tra Unione Europea (UE) e Repubblica Popolare Cinese (RPC).

Tali trasferimenti si collocano all'intersezione di due sistemi normativi complessi: da un lato il Regolamento (UE) 2016/679 (GDPR), dall'altro la *Personal Information Protection Law* (PIPL), in vigore dal novembre del 2021. Pur condividendo l'obiettivo comune di tutelare i diritti degli interessati e garantire un utilizzo lecito e sicuro dei dati personali, le due discipline si fondano su logiche regolatorie differenti, con rilevanti conseguenze pratiche per le imprese.

Il presente rapporto fornisce un inquadramento sintetico, ma sistematico delle regole applicabili ai trasferimenti di dati personali tra UE e RPC, evidenziando le aree di potenziale rischio e gli adempimenti richiesti alle organizzazioni che operano in entrambe le giurisdizioni.

Principi comuni, modelli regolatori differenti

Sia il GDPR sia la PIPL hanno una portata extraterritoriale. Entrambe le normative possono infatti applicarsi a trattamenti effettuati al di fuori del territorio di riferimento quando riguardano dati personali di soggetti situati nell'UE o nella RPC. Questo elemento di estensione territoriale rende inevitabile, per molte imprese, una doppia conformità.

Tuttavia, le similitudini terminano, in larga parte, sul piano dei principi generali.

Il GDPR si fonda su un modello di *accountability* del titolare del trattamento: è l'organizzazione che deve dimostrare la conformità alle regole, adottando misure tecniche e organizzative adeguate, effettuando valutazioni d'impatto (DPIA) e mantenendo aggiornata la documentazione necessaria.

La PIPL, pur introducendo concetti analoghi (tra cui, liceità, minimizzazione e trasparenza), si inserisce in un quadro normativo più ampio che comprende la *Data Security Law* e la *Cybersecurity Law*, riflettendo un'impostazione maggiormente orientata alla governance statale dei dati e alla sovranità digitale. La supervisione fa capo, in particolare, alla *Cyberspace Administration of China* (CAC), con un ruolo centrale dell'autorità amministrativa nel processo autorizzativo.

Il trasferimento di dati personali dalla Cina verso l'estero

La PIPL disciplina il trasferimento transfrontaliero con un'impostazione differente. In linea generale, qualsiasi organizzazione che trasferisca informazioni personali al di fuori del territorio cinese potrebbe essere tenuta, al ricorrere di determinate soglie o condizioni, a:

- sottoporsi a una valutazione di sicurezza effettuata dalla CAC;
- sottoscrivere un contratto standard per il trasferimento di dati personali e depositarlo presso la CAC;
- ottenere una certificazione rilasciata da un ente accreditato.

Il meccanismo applicabile dipende dal volume dei dati trattati, dalla natura dell'operatore e dalla tipologia di dati coinvolti. Inoltre, per talune categorie di soggetti – in particolare gli operatori di infrastrutture informatiche critiche (CII) o le organizzazioni che trattano grandi quantità di dati personali – può permanere un obbligo di localizzazione dei dati, ossia di conservazione delle informazioni personali all'interno del territorio cinese, salvo specifiche eccezioni.

Sono previste altresì, in alcuni casi, esenzioni o procedure semplificate, ad esempio per trasferimenti infragruppo limitati a finalità di gestione delle risorse umane o di amministrazione interna. Tuttavia, tali esenzioni devono essere valutate caso per caso e non possono essere applicate automaticamente.

Intersezioni e criticità operative per le società che operano in entrambi gli Stati

Per le imprese che operano sia nell'UE sia nella RPC, la gestione dei flussi di dati personali richiede, pertanto, un'attenta armonizzazione dei due sistemi normativi.

Le organizzazioni devono coordinare *(i)* il proprio modello di governance privacy; *(ii)* le informative agli interessati; *(iii)* le basi giuridiche del trattamento; *(iv)* i contratti infragruppo, nonché con i fornitori esterni; *(v)* le misure tecniche e organizzative di sicurezza; *(vi)* le procedure di gestione dei *data breach*.

Non di rado, ciò comporta la creazione di sistemi documentali paralleli, con adempimenti distinti per ciascuna giurisdizione. Il rischio derivante da eventuali situazioni di non conformità, infatti, non è soltanto sanzionatorio, ma anche reputazionale, specie in caso di incidenti di sicurezza che coinvolgano trasferimenti transfrontalieri.

Allo stesso tempo, si osserva una progressiva convergenza attorno a principi comuni quali trasparenza, sicurezza e responsabilizzazione del titolare del trattamento. Le imprese già strutturate secondo il modello GDPR possono disporre di una base solida per adeguarsi anche ai requisiti della PIPL, purché integrino gli specifici obblighi autorizzativi e di localizzazione previsti dal diritto cinese.

Conclusioni

Il trasferimento di dati personali tra UE e RPC rappresenta un tema complesso del diritto della protezione dei dati a livello globale. L'assenza di una decisione di adeguatezza tra le due giurisdizioni e la diversa impostazione dei rispettivi sistemi normativi impongono alle imprese un approccio prudente, documentato e integrato.

In un contesto caratterizzato da crescente attenzione alla sovranità digitale e alla sicurezza nazionale, la conformità non può essere considerata un mero adempimento formale, ma rappresenta un elemento strategico della governance aziendale. Un'analisi preventiva dei flussi di dati, lo svolgimento di valutazioni d'impatto adeguatamente documentate e una gestione strutturata dei rapporti con fornitori, cloud provider e partner tecnologici coinvolti nei trattamenti di dati rappresentano presidi fondamentali per garantire operatività conforme, sicurezza giuridica e competitività su scala internazionale.

***

Il presente rapporto è frutto della libera interpretazione e sintesi delle fonti ivi menzionate da parte dell'Avv. Carlo D'Andrea, in qualità di Avvocato responsabile del Desk "Assistenza e Tutela della Proprietà Intellettuale e Ostacoli al Commercio" costituito presso l'Agenzia ICE di Pechino e non costituisce in ogni caso un parere legale sulle questioni trattate, né può dar luogo a legittimi affidamenti o fondare iniziative di natura legale. Per eventuali richieste di chiarimenti, vi invitiamo a fare riferimento all'indirizzo e-mail ipr.pechino@ice.it e/o al sito web https://www.ice.it/it/mercati/cina/pechino/desk-tutela-proprieta-intellettuale