Diritti privacy in Cina. Nuove regole per le imprese. Cosa cambia?

DIRITTI PRIVACY IN CINA. NUOVE REGOLE PER LE IMPRESE. COSA CAMBIA? CON L'ARRIVO DELLA NUOVA LEGGE SULLA PROTEZIONE DEI DATI CINESE "PERSONAL INFORMATION PROTECTION LAW" (PIPL) LE AZIENDE INTERNAZIONALI CHE RACCOLGONO DATI E FANNO AFFARI CON LA CINA DEVONO PREPARARSI CONSAPEVOLMENTE.

Federico Corti
Dicembre 27, 2021
Scarica PDF dell'articolo

La nuova legge sulla protezione dei dati cinese "*Personal Information Protection Law*" (PIPL), è stata promulgata ufficialmente, con lo scopo di **proteggere i diritti e gli interessi degli individui**, regolare le attività di trattamento delle informazioni personali e facilitare un uso ragionevole delle stesse.

La norma, divenuta a tutti gli effetti applicabile a partire dal primo novembre, si configura come un tassello fondamentale del quadro giuridico della Cina, andando ad affiancarsi alla "*Cybersecurity Law*" (CSL) e alla "*Data Security Law*" (DSL), nel delineare il framework normativo in materia di data protection per gli anni a venire. Oltre a PIPL, CSL e DSL, nel 2021 l'ordinamento giuridico cinese è stato arricchito da una serie di regolamenti di attuazione e di nuovi standard nazionali, che si aggiungono ad altre disposizioni sparse in una pluralità di leggi e codici (dal "*Civil Code*" alla "*E-commerce Law*", solo per citarne alcune).

Nell'articolo di oggi cerchiamo di fare chiarezza rispetto alla **molteplicità di fonti**, vediamo quali progressi sono stati fatti dalla legislazione cinese e dove invece risulta ancora carente e poco garantista rispetto ai diritti degli interessati. L'obiettivo non è solo quello di spiegare le caratteristiche della normativa, ma anche di aiutare le aziende internazionali che raccolgono dati e fanno affari in e con la Cina a **prepararsi consapevolmente**, impostando un approccio risk-based verso la conformità alla normativa della Repubblica Popolare Cinese.

LA DATA SECURITY LAW: COSA CAMBIA

Il 2021 è stato un **anno ricco di novità per la Cina**. A giugno il Comitato permanente del Congresso Nazionale del Popolo, ha promulgato la "*Data Security Law*" (DSL), che è entrata in vigore il 1° settembre 2021.

A differenza della CSL e della PIPL, che impongono obblighi dettagliati in materia di cyber security e protezione dei dati personali alle imprese e ad altre organizzazioni, la DSL si concentra principalmente sulla **sicurezza nazionale** e stabilisce regole di gestione di alto livello per agenzie governative, associazioni industriali, imprese e altre organizzazioni.

La DSL governa non solo l'**elaborazione dei dati e le attività di gestione** condotte all'interno della Cina, ma anche quelle al di fuori della Cina, che hanno il potenziale per danneggiare la sicurezza nazionale. Rimane poco chiaro come questa ampia discrezionalità normativa sarà applicata (l'effetto extraterritoriale dovrebbe dipendere da prossimi trattati o accordi internazionali).

La DSL, inoltre, conferisce poteri di supervisione a diverse Autorità governative, e definisce un sistema gerarchico di categorizzazione dei dati in base all'importanza degli stessi per l'economia cinese. Mentre la CSL richiedeva solo agli "operatori di infrastrutture informatiche critiche" ("CIIOs") di conformarsi a una regolamentazione rafforzata per i dati "importanti", la DSL **espande questo requisito a tutte le imprese che elaborano questo tipo di informazioni.**

Gli adempimenti includono: la localizzazione dei database sul territorio cinese; la necessità di identificare e assegnare le rispettive responsabilità di protezione della sicurezza ad un soggetto responsabile ("*Data Security Officer*") e ad un organo di gestione ("*Data Security Management Department*"); la realizzazione di regolari valutazioni del rischio sulle attività di trattamento dei dati, da presentare in rapporti di valutazione alle Autorità competenti.

Le aziende che fanno affari in e con la Cina devono quindi necessariamente considerare la Data Security Law e conformare i trattamenti agli obblighi e alle restrizioni da questa imposti (spesso più severi di quelli previsti dal GDPR).

Le entità che violano le disposizioni in materia di sicurezza, o subiscono data breach di grave rilevanza, **vanno incontro a multe** fino a 2 milioni di yuan (poco meno di 300.000 Euro), alla potenziale sospensione dei processi aziendali e alla revoca della licenza commerciale.

Le entità che non seguono le disposizioni di CSL e DSL in materia di trasferimenti transfrontalieri di "dati importanti" provocando "gravi conseguenze" rischiano fino a 10 milioni di yuan (quasi 1,5 milioni di Euro) oltre alla sospensione dei processi aziendali e alla revoca della licenza commerciale.

LA PERSONAL INFORMATION PROTECTION LAW

La "*Personal Information Protection Law*" (PIPL), entrata ufficialmente in vigore a novembre 2021, rappresenta il caposaldo, nell'ordinamento giuridico cinese, per la **regolamentazione delle attività di trattamento delle informazioni personali**, con l'obiettivo di proteggere i diritti e gli interessi degli individui e di facilitare un uso ragionevole delle informazioni stesse.

Molti concetti, principi ed istituti, sono stati ripresi dal GDPR, altri sono stati integrati per garantire un maggiore livello di protezione (della sicurezza nazionale cinese). Il tema del trasferimento internazionale dei dati (disciplinato di concerto con CSL e DSL) include degli obblighi specifici per l'esportatore, non previsti all'interno del Capo V del Regolamento europeo.

Altre differenze riguardano l'assenza, fra le basi giuridiche che legittimano la gestione dei dati, dell'interesse legittimo, e la più corposa elencazione delle attività di trattamento che fanno scattare l'obbligo di una valutazione di impatto privacy (definita "*personal information protection impact assessment*").

Il PIPL prevede anche importanti sanzioni (seppure meno severe rispetto a quelle previste dal GDPR): se un "*personal information handler*" (l'equivalente del Titolare del trattamento) viola i requisiti della PIPL, le Autorità regolatrici possono imporre azioni correttive, emettere avvertimenti, confiscare i redditi illegali, sospendere i servizi o emettere sanzioni pecuniarie. Queste ultime vanno fino a 50 milioni di Yuan (circa 6,9 milioni di Euro) o al 5% del reddito dell'anno precedente. Resta da capire, all'atto pratico, come e se queste sanzioni verranno applicate.

ALTRE FONTI E CONSIDERAZIONI

A corredo dei tre pilastri del regime giuridico generale di protezione dei dati e di sicurezza informatica della Cina (CSL, DSL, PIPL), troviamo tutta una serie di recenti regolamenti di attuazione correlati.

Fra questi, di sicuro rilievo, sono le regole sulla portata delle informazioni personali necessarie per i tipi comuni di *mobile web applications* ("*App Rules*"). Già nel primo mese di applicazione delle regole (maggio-giugno 2021) il *Cyberspace Administration of China* (CAC) ha pubblicato quattro annunci su un numero totale di 351 app per il loro mancato rispetto degli obblighi di protezione delle informazioni personali.

Le principali violazioni includono: la raccolta eccessiva di informazioni personali non correlate ai servizi forniti dalle app, e l'elaborazione delle stesse senza ottenere il consenso degli utenti.

"*Negli ultimi anni*" ha dichiarato il CAC, "*le applicazioni internet mobili sono state ampiamente utilizzate e hanno giocato un ruolo importante nel promuovere lo sviluppo economico e sociale e nel servire il sostentamento delle persone. Allo stesso tempo, è comune che le applicazioni raccolgano informazioni personali oltre il loro scopo, e gli utenti non possono installarle e usarle se rifiutano di accettare*".

Possiamo quindi ritenere che la Cina, rispetto alla disciplina vigente fino a pochi mesi fa (di fatto recepibile volontariamente), stia facendo importanti passi avanti.

Il quadro giuridico è delineato, resta da capire come si comporteranno le Autorità incaricate dell'applicazione della PIPL nei vari dipartimenti, e come le aziende accoglieranno i nuovi adempimenti.

AFFARI CON LA CINA E PRIVACY: COME COMPORTARSI

In primo luogo, le aziende internazionali che fanno affari in Cina dovrebbero valutare se, ed in che modo, le nuove norme della Repubblica Popolare Cinese si applicano alle loro attività di trattamento dei dati. Per conformarsi è necessario considerare che CSL, DSL e PIPL impongono diversi obblighi per le imprese:

- L'implementazione di specifiche misure di sicurezza per prevenire accessi non autorizzati ed il verificarsi di furti, perdite o modifiche dei dati trattati
- La gestione di eventuali violazioni ("personal information leak, distortion, or loss") in conformità all'art. 57 del PIPL
- La nomina, nei casi previsti, di un "*personal information protection officers*"
- La nomina, per le aziende ubicate al di fuori della Cina, di un rappresentante
- La realizzazione di periodici audit di conformità normativa
- La realizzazione, nei casi previsti, di un "*personal information protection impact assessment*"

Questi adempimenti si affiancano alle regole ordinarie per la gestione delle informazioni personali (capitolo II del PIPL), e ad altre importanti considerazioni, fra cui:

- La necessità di valutare se i dati trattati possono essere considerati come "dati importanti" secondo la DSL
- La necessità di creare, nei casi previsti, procedure interne e un comitato di gestione per la sicurezza e la conformità dei dati
- La necessità di condurre regolari valutazioni del rischio sulle attività di trattamento e presentare tali rapporti di valutazione alle Autorità competenti
- La necessità di stabilire piani di emergenza per rispondere agli incidenti di sicurezza
- La necessità di mappare dati e trattamenti, avendo cura di identificare eventuali esportazioni (soggette ad un regime particolarmente rigoroso)

La complessità del regime giuridico, così come la pluralità di adempimenti, impongono alle aziende che hanno rapporti con la Cina (o che operano in Cina) di effettuare una approfondita valutazione degli obblighi applicabili, in modo da non incorrere in sanzioni, sia ai sensi del PIPL, che ai sensi del GDPR.

Labor Project, oltre ad offrire consulenza sul tema, realizza corsi che affrontano anche tematiche delicate, come il trasferimento dei dati o la gestione degli stessi da parte di "*personal information handlers*" ubicati nella Repubblica Popolare Cinese.

Per un approfondimento sui fondamenti di diritto privacy comparato e un'analisi delle norme internazionali a confronto segui il corso di formazione dedicato di LPA.

Labor Project®
consulenza operativa per l'impresa

Labor Project S.r.l.
Iscrizione Ufficio Registro Imprese
di Como con n. 02725120139
Cap. Soc. € 100.000 i.v.
P.I. 02725120139

CANTU'
Via Brianza, 65
22063 Cantù (CO)
Tel. +39 031 704381
info@laborproject.it

ROMA
Via Lima, 7
00198 Roma (RM)
roma@laborproject.it

MILANO
Viale Monza, 347
20126 Milano (MI)
milano@laborproject.it

LUGANO
Via Luigi Canonica,11
6900 Lugano (Svizzera)
info@privacydesk.ch