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

ICE Pechino

Rapporto di approfondimento sulla revisione della Legge sulla cybersicurezza della Repubblica Popolare Cinese

Il 28 ottobre 2025, la 18ª Sessione del Comitato Permanente della 14ª Assemblea Nazionale del Popolo ha approvato la Decisione sull'emendamento della Legge sulla cybersicurezza della Repubblica Popolare Cinese. Si tratta della prima revisione sostanziale della legge dalla sua entrata in vigore nel 2017 e rappresenta un ulteriore passo nel processo di rafforzamento del sistema cinese di governance della cybersicurezza e della sicurezza dei dati.

La nuova disciplina, che è entrata in vigore il 1° gennaio 2026, introduce modifiche rilevanti in diversi ambiti, tra cui l'inclusione delle nuove tecnologie digitali, come l'intelligenza artificiale, nel perimetro regolatorio e il rafforzamento del sistema di responsabilità giuridica per gli operatori di rete.

Il presente rapporto analizza le principali novità introdotte dalla modifica e ne esamina le implicazioni per le imprese, con particolare attenzione agli operatori stranieri che svolgono attività in Cina o che gestiscono infrastrutture digitali e flussi di dati nel mercato cinese.

Obiettivi della riforma e impatto complessivo

La riforma della Legge sulla cybersicurezza comprende complessivamente quattordici disposizioni, distribuite nei capitoli relativi alle disposizioni generali, al supporto e alla promozione della cybersicurezza, alla sicurezza delle operazioni di rete, alla sicurezza delle informazioni di rete e alla responsabilità. Un elemento particolarmente significativo è rappresentato dal rafforzamento della responsabilità: dieci delle modifiche introdotte riguardano infatti direttamente la disciplina sanzionatoria, segnalando la volontà del

legislatore di aumentare l'efficacia del quadro regolatorio attraverso una maggiore chiarezza delle conseguenze giuridiche in caso di violazioni.

Per le imprese straniere operanti in Cina, la revisione non introduce obblighi completamente nuovi, ma rappresenta piuttosto un affinamento e un consolidamento del sistema normativo già esistente. Le modifiche mirano a rendere le disposizioni più operative e prevedibili. In questo contesto, la conformità normativa assume un ruolo sempre più centrale nella governance aziendale, non soltanto come obbligo legale ma anche come strumento per migliorare la gestione del rischio e la sicurezza delle infrastrutture digitali.

Inclusione dell'intelligenza artificiale nel quadro regolatorio

Una delle novità più rilevanti introdotte dalla riforma riguarda l'esplicito inserimento dell'intelligenza artificiale nel perimetro della regolamentazione della cybersicurezza. Il nuovo articolo 20 stabilisce che lo Stato sostiene la ricerca e lo sviluppo delle tecnologie fondamentali legate all'intelligenza artificiale, inclusi gli algoritmi, le risorse di dati utilizzate per l'addestramento dei modelli e la capacità di calcolo necessaria per il loro funzionamento.

La disposizione sottolinea inoltre l'importanza di rafforzare i sistemi di monitoraggio e valutazione dei rischi associati all'intelligenza artificiale, promuovendo al contempo lo sviluppo di standard etici e di meccanismi di supervisione della sicurezza. L'obiettivo è quello di favorire un utilizzo responsabile delle nuove tecnologie, garantendo che innovazione tecnologica e sicurezza delle reti vadano di pari passo.

Per le imprese che sviluppano o impiegano soluzioni di intelligenza artificiale, tale disposizione comporta la necessità di integrare la compliance lungo tutto il ciclo di vita dei sistemi tecnologici. In particolare, assume crescente rilievo l'adozione di adeguati meccanismi di data governance, la trasparenza degli algoritmi e la costante valutazione dei rischi, in coerenza con il progressivo consolidamento della disciplina cinese in ambito digitale.

Inasprimento del sistema sanzionatorio

Un ulteriore profilo centrale della riforma è rappresentato dall'inasprimento del sistema sanzionatorio. Il nuovo articolo 61 riorganizza e aggiorna il quadro delle responsabilità in precedenza disciplinato dagli articoli 59 e 60, introducendo un meccanismo graduato in base alla gravità delle violazioni e agli effetti che ne derivano.

In particolare, per le violazioni di minore entità è prevista un'ammenda compresa tra 10.000 e 50.000 RMB. Qualora l'operatore non provveda a correggere la violazione o

qualora ne derivino danni, l'ammenda può aumentare fino a un massimo di 500.000 RMB, mentre per i soggetti direttamente responsabili è prevista una sanzione compresa tra 10.000 e 100.000 RMB.

Nel caso in cui la violazione produca conseguenze gravi, la sanzione pecuniaria può raggiungere i 2 milioni di RMB, unitamente all'irrogazione di sanzioni individuali nei confronti delle persone fisiche responsabili e all'adozione di misure amministrative quali la sospensione dell'attività o l'ordine di rettifica. Nelle ipotesi di maggiore gravità, l'importo può arrivare fino a 10 milioni di RMB, con possibile revoca dei certificati o delle licenze operative.

Attraverso tale articolazione, il legislatore mira a rafforzare la prevedibilità del sistema e a stabilire una correlazione più chiara tra la gravità della violazione e l'entità delle sanzioni applicabili.

Maggiore coordinamento con le altre normative sulla protezione dei dati

La modifica della legge rafforza anche il coordinamento con le altre normative cinesi in materia di dati e sicurezza digitale. Il nuovo comma introdotto nell'articolo 42 stabilisce che gli operatori di rete che trattano informazioni personali devono rispettare non solo le disposizioni della Legge sulla cybersicurezza, ma anche quelle contenute nel Codice Civile della Repubblica Popolare Cinese, nella Legge sulla protezione delle informazioni personali (PIPL) e negli altri regolamenti amministrativi applicabili.

Questa previsione chiarisce la necessità di adottare un approccio integrato alla gestione della compliance, assicurando che ogni attività di trattamento dei dati soddisfi simultaneamente i requisiti previsti dai diversi strumenti normativi.

Con lo stesso spirito di armonizzazione, alcune disposizioni relative alla tutela dei diritti sulle informazioni personali sono state accorpate e coordinate con il sistema sanzionatorio previsto dalla PIPL, con l'obiettivo di evitare sovrapposizioni normative e garantire una maggiore coerenza nell'applicazione della legge.

Responsabilità rafforzate per gli operatori di infrastrutture critiche

La riforma reca, altresì, disposizioni specifiche in materia di operatori di infrastrutture informatiche critiche. In particolare, si prevede che, qualora tali operatori facciano ricorso a prodotti o servizi di rete non sottoposti alla prescritta revisione di sicurezza ovvero che non abbiano superato la medesima, le autorità competenti possano disporre la cessazione del relativo utilizzo e irrogare sanzioni commisurate al valore dell'appalto.

Il collegamento diretto tra l'entità della sanzione e il valore economico dell'attività rappresenta un elemento significativo della riforma, poiché rafforza l'importanza della cybersicurezza nella gestione della supply chain.

Per le imprese che operano in settori sensibili o che potrebbero essere classificate come operatori di infrastrutture critiche, ciò implica la necessità di integrare la sicurezza informatica tra i criteri principali nella selezione dei fornitori di tecnologie e servizi di rete, inclusi i servizi cloud. La capacità dei fornitori di garantire adeguati standard di sicurezza e conformità normativa diventa quindi un fattore determinante nella gestione dei contratti e degli approvvigionamenti.

Considerazioni conclusive

Nel complesso, la revisione della Legge sulla cybersicurezza rappresenta un ulteriore passo nel processo di consolidamento del sistema cinese di governance digitale. Attraverso il rafforzamento della dimensione strategica della cybersicurezza, l'inclusione delle nuove tecnologie nel quadro normativo e l'inasprimento del regime di responsabilità, il legislatore mira a costruire un sistema regolatorio più coerente, efficace e adattabile agli sviluppi tecnologici.

Per le imprese straniere operanti in Cina, le modifiche rappresentano principalmente un chiarimento e un rafforzamento del quadro giuridico esistente, contribuendo a rendere le regole più prevedibili e strutturate. In un contesto caratterizzato da una crescente attenzione alla sicurezza delle reti e dei dati, diventa essenziale mantenere sistemi robusti di governance digitale, monitorare costantemente l'evoluzione normativa e garantire uno sviluppo sostenibile e conforme delle proprie attività nel mercato cinese.

***