I rischi del cloud computing

Le società che utilizzano o intendono utilizzare servizi di cloud computing, ovvero che affidano i propri sistemi di hardware e software ad altre società operanti in remoto, devono fare attenzione ai potenziali rischi di contenzioso, avvertono gli esperti.

Il cloud computing permette infatti di ridurre i costi, ma le imprese che ne fanno uso devono dotarsi di sistemi di risk management adeguati, onde evitare che violazioni della privacy e illeciti informatici sfocino in cause legali. È quanto emerso alla Communications, Media and Technology Conference, tenutasi il mese scorso a Londra sotto l'egida di Marsh.

Il cloud computing è un servizio di outsourcing che permette alle aziende di esternalizzare banche dati e software su server gestiti da società terze accessibili tramite internet. Il cloud computing permette così di risparmiare, ma la mancanza di certezze in merito a dove le informazioni vengano archiviate, può comportare delle conseguenze legali.

Spesso le società che offrono questi servizi informatici in outsourcing operano su server localizzati in vari Paesi. Qualora si verificassero degli illeciti, bisognerebbe fare riferimento alla normativa del Paese in cui si trova fisicamente il server in cui sono immagazzinati i dati. Ma le normative che regolano la privacy differiscono molto da Paese a Paese.

Ad esempio, negli Stati Uniti manca ancora una normativa unitaria in materia di privacy, nota Milton Whitfield, partner dello studio legale Haynes & Boone di Washington. Anche il tipo di informazioni affidato a queste società terze deve essere vagliato attentamente. Per dati sensibili, come quelli relativi alla salute, è opportuno usare sistemi di criptaggio.

Il panorama europeo non differisce molto da quello americano, dove ogni singolo Paese dell'Unione ha una propria normativa sulla privacy.

Di recente sono state apportate delle modifiche alla direttiva sulla privacy e le comunicazioni elettroniche, ha precisato Nick Pantlin, dello studio legale Herbert Smith di Londra. Dal 25 maggio scorso, diversamente da quanto richiesto dalla normativa precedente, le società che raccolgono e archiviano informazioni e dati personali, sono tenute a informare tempestivamente le autorità, come il garante della privacy, di eventuali violazioni. Se la violazione può comportare conseguenze negative, il soggetto interessato deve esserne informato.

È importante allora, continua Pantlin, che una società consideri l'impatto che eventuali violazioni possono avere rispetto ai terzi coinvolti e considerare che le ammende comminate possono provenire da più fonti. Ad esempio, lo scorso agosto Zurich Insurance Services ha ricevuto una multa di oltre 2 mln £ (2,3 mln €) dal Financial Services Authority per non aver garantito la sicurezza delle informazioni personali di cui disponeva.

Un operatore di cloud computing sta per lanciare un servizio che garantisce che le informazioni provenienti da società e individui dell'Unione Europea rimangano archiviate in server localizzati all'interno dell'Unione stessa. In questo modo eventuali violazioni sarebbero soggette unicamente alla legislazione europea.

Dal punto di vista strettamente assicurativo, è però difficile stabilire in quale giurisdizione verrà implementata una eventuale denuncia, ha aggiunto Paul Skinner, technology & class underwriter presso Chubb Group of Insurance di Londra.

Fonte: Business Insurance