STUDIO GHIDINI, GIRINO & ASSOCIATI

I FERRI DEL MESTIERE

Con il cloud meglio stare coi piedi per terra

Nel mondo telematico non si parla d'altro. Anche il Garante della privacy ha preso partito: da strumento di condivisione, Internet «diviene la porta d'accesso alle risorse elaborative di un provider di servizi» dichiara nell'ultima relazione. Stiamo alludendo al cloud computing, che consente di alloggiare presso un provider specializzato i dati che normalmente riposerebbero nei sistemi aziendali. Social network a parte, le applicazioni professionali «in cloud» possono essere sorprendenti. Consentono di ridurre l'hardware proprietario e i relativi costi di gestione (manutenzione, sicurezza, privacy) e permettono anche alla piccola-media impresa di godere della migliore e più potente tecnologia che solo un provider specializzato può garantire. All'impresa non resta che pagare il servizio, ai costi tecnologici e di manutenzione provvede il provider. Prospettiva allettante, ma non priva di rischi. Le nuvole sono eteree, mentre i dati e le informazioni che verrebbero consegnati al provider possono essere riservati, costituenti know-how aziendale ovvero dati di terzi, soggetti alla disciplina della privacy. Il provider poi può servirsi di partner commerciali, al che il raggio di diffusione dei dati può allargarsi. Al solito si ritiene che affidarsi a un provider sicuro possa bastare. Il che è molto ma non è tutto. È il contratto ad avere importanza fondamentale.

Questi i punti cui fare molta attenzione. 1) Il luogo in cui il provider ha la sede e quello di conservazione dei dati indicati in contratto. Le garanzie di cui al decreto 70/2003 sui «servizi della società dell'informazione» e le norme Ue sulla sicurezza dei trattamenti (per intenderci le norme di salvataggio e ripristino dei dati) recepite nel codice della privacy valgono solo per i provider stabiliti in uno Stato europeo, ovvero che in tale Stato eseguano il trattamento. Provider basati altrove sfuggono a queste regole. 2) Disciplina della privacy. Il trasferimento al provider dei dati personali di terzi, implica l'onere per l'impresa, ovvero per il provider, di informare i soggetti interessati da tale comunicazione e dei relativi trattamenti, a seconda che il provider operi come titolare o responsabile del trattamento. Non ci si può permettere l'approssimazione, perché l'impresa sarebbe comunque destinataria degli strali dei clienti danneggiati. 3) I presidi, le garanzie e le manleve offerte dal provider in ordine a possibili default del sistema che determino l'indisponibilità temporanea o la perdita dei medesimi. Se è vero che il trattamento dei dati personali di terzi integra «attività pericolosa» ai sensi dell'art. 15 del codice privacy e dell'art. 2050 cc. e che, al verificarsi di un danno, il titolare del trattamento, per andare esente da responsabilità, è tenuto a dimostrare di aver adottato tutte le misure idonee per evitarlo, è anche vero che i segreti aziendali non integrano necessariamente «dati personali», che la suddetta disciplina non esaurisce dunque i contenuti affidati al provider e che, viceversa, la previsione di un'esplicita manleva o una penale assicura una più robusta tutela . 4) La conformità agli standard del linguaggio utilizzato per caricare e gestire i dati. L'imprenditore insoddisfatto del servizio, e che abbia avuto l'accortezza di inserire in contratto il diritto di recesso, avrebbe molte difficoltà a trasferire i contenuti ad altro provider se i dati fossero registrati in formato non leggibile dal secondo. L'abitudine di firmare moduli a occhi chiusi deve cessare. In gioco c'è qualcosa di molto prezioso e irrimediabilmente danneggiabile: un patrimonio di conoscenza. Il computer resti tra le nuvole, le imprese tengano i piedi per terra (e nei contratti).

Franco Estrangeros