Verso l'impresa 4.0. Nuvole e Privacy nel nuovo Regolamento UE

di Alessandra Nisticò

Se si parla di impresa 4.0 è perché i vantaggi offerti dalle interconnessioni di rete hanno determinato aumento di efficienza e produttività.
Negli ultimi anni abbiamo assistito a diverse trasformazioni: il lavoro è diventato *agile*, la produzione *smart* e l'organizzazione flessibile e *mobile*.
Gli stessi clienti sembrano apprezzare le potenzialità della Rete, mentre sistemi come la block-chain possono rappresentare la soluzione per garantire complesse operazioni su lunghe distanze.
Tuttavia, se l'impresa si apre al mondo per sfruttarne le potenzialità, occorre tenere presente alcuni profili di sicurezza relativamente ai dati che possono essere sensibili per i titolari, ma anche relativamente a informazioni confidenziali che, in un mondo interconnesso, rischiano di essere divulgate.
In primo luogo, è importante considerare il tipo di dati e informazioni che vengono caricati in Rete (sensibili o meno, confidenziali o di pubblico dominio), in quanto la decisione di condividere è sempre in capo a colui che immette le informazioni e, in secondo luogo, occorre prestare attenzione al tipo di servizio utilizzato, valutando attentamente le condizioni di licenza, il servizio che si acquista, la collocazione geografica dei server, oltre alle misure di sicurezza minime offerte (dalla cifratura dei dati contro accessi indesiderati ai backup contro il rischio di perdite).
Tra i molteplici strumenti a servizio dell'impresa 4.0, un ruolo predominante sta svolgendo il cloud computing, che non solo consente di alleggerire l'infrastruttura di rete in azienda o di potenziare quella esistente, ma al contempo permette di lavorare in mobilità, determinando un incremento della produttività e andando incontro alle esigenze di flessibilità vita lavoro richieste dai lavoratori.
Il cloud, come noto, consente lo sfruttamento di risorse online, come l'archiviazione di dati, il loro accesso e la sincronizzazione dei contenuti tra vari dispositivi di accesso.
La scelta del servizio, naturalmente, si basa sulle concrete necessità aziendali, al giorno d'oggi è possibile scegliere tra cloud privati, pubblici e sistemi ibridi.
Gli elementi da tenere d'occhio sono la presenza o meno di investimenti pregressi in un'infrastruttura di rete, che potrebbero spingere su un cloud privato o un sistema ibrido, oppure la necessità di utilizzare un servizio flessibile senza sopportare i costi iniziali infrastrutturali (ad esempio per una start-up) che potrebbero portare a preferire soluzioni di cloud pubblico.
La scelta del servizio (e del fornitore) ha delle ricadute in ambito di compliance alla regolamentazione privacy, soprattutto alla luce del nuovo Regolamento sui Dati Personali dell'Unione Europea (2016/679) che diventerà obbligatorio il 28 maggio 2018.
La nuova normativa, infatti, modifica la definizione del Titolare del trattamento legittimando formalmente la possibilità della condivisione del ruolo del titolare tra l'utente e il fornitore del servizio (cloud nel nostro caso). Il titolare è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali."
Il regolamento prescrive, inoltre, in capo al titolare del trattamento il compimento di una serie di attività e l'adozione di particolari misure come il monitoraggio degli accessi ai dati, la gestione della sicurezza dei dati lungo tutto il loro ciclo di vita, la cifratura dei dati e la loro pseudonimizzazione.
La sicurezza dei dati è uno degli aspetti centrali del nuovo regolamento, in virtù della rilevanza e della sensibilità delle istituzioni dell'Unione Europea sul tema, ufficializzata con la pronuncia della Corte di Giustizia del 6 ottobre 2015 nella quale viene dichiarato contrario ai principi di correttezza e necessarietà del trattamento dei dati l'accordo tra UE e USA sul trattamento dei dati personali Safe Harbor.
Nella pronuncia si afferma che: "non è limitata allo stretto necessario una normativa che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta."
I principi di diritto enucleati dalla Corte di Giustizia, unitamente alle previsioni del nuovo regolamento UE, impone di tenere presente tra i criteri per la scelta del cloud provider anche la localizzazione dei server.
La nuova normativa, infatti, prevede che il Titolare del trattamento ha l'obbligo di provvedere, immediatamente o comunque entro 72 ore, a notificare la violazione all'Autorità garante competente ed agli interessati i cui dati sono stati violati, se ci sono rischi per i loro diritti e le loro libertà.
Particolare attenzione, pertanto, deve essere rivolta alle condizioni contrattuali del servizio acquistato, proprio in forza della minore forza negoziale che le piccole e medie imprese hanno nei confronti dei colossi dell'informatica, privilegiando i fornitori che offrono garanzia di collaborazione nell'adempimento degli obblighi derivanti dalla normativa privacy.
A livello operativo, nonostante il tempo trascorso e le trasformazioni legislative in atto, resta di attualità il decalogo che nel 2012 il Garante della Privacy aveva elaborato per aiutare le imprese nella scelta del servizio cloud, indipendentemente dal tipo di infrastruttura che si desidera realizzare. Il Garante suggeriva, infatti, di effettuare una verifica sull'affidabilità del fornitore, privilegiare i servizi che favoriscono la portabilità dei dati, assicurarsi la disponibilità dei dati in caso di necessità; Selezionare i dati da inserire nella nuvola, non perdere di vista i dati, informarsi su dove risiederanno concretamente i dati; Attenzione alle clausole contrattuali, verificare tempi e modalità di conservazione dei dati, esigere adeguate misure di sicurezza e formare adeguatamente il personale. ■

Alessandra Nisticò

Iscritta all'Albo degli Avvocati del Foro di Milano, dal 2013 è partner dello Studio Legale Faotto - Tricarico, oggi con sede in via Lamarmora n. 36 a Milano, fondato dagli Avvocati Luca Faotto e Melissa Tricarico; ne sono partner anche gli avvocati Pierluigi Ferri, Paola Rizzi e Desirée Arioli. L'avvocato Nisticò si occupa di diritto civile e, in particolare, di contrattualistica e consulenza alle aziende, prestando assistenza sia in ambito stragiudiziale che giudiziale. Ha partecipato, in qualità di relatore, a convegni e seminari sulle tematiche della Marcatura CE. Si interessa di temi legati al diritto dell'informatica, l'innovazione e le tecnologie.