Privacy 2.0: portabilità, diritto all'oblio, datarisk e certificazioni

Il tanto atteso Regolamento Privacy è stato pubblicato sulla *Gazzetta Ufficiale* Ue lo scorso 4 maggio. Altra rivoluzione organizzativa per imprese e amministrazioni? Le novità del Regolamento che hanno avuto maggior risalto mediatico sono l'introduzione del diritto alla portabilità dei dati (art. 20) e del diritto all'oblio (art. 17). Il primo consente all'interessato di ricevere, dal titolare in precedenza autorizzato al trattamento, i propri dati personali «in formato strutturato, di uso comune e leggibile da dispositivo automatico». Tale novità non persegue solo fini di protezione del singolo bensì anche obiettivi concorrenziali, poiché garantisce la migrazione dell'interessato da un fornitore a un altro: nel mirino gli operatori che offrono servizi in cloud o gestione di social network. Questi dovranno tecnicamente organizzarsi per consentire la facile e agile migrazione degli interessati permettendo loro di evitare la perdita del proprio data base.

Ben diversa, e più scottante, la portata della seconda novità. Diritto all'oblio significa diritto alla cancellazione dei dati di terzi che siano stati resi pubblici dal titolare del trattamento, obbligando quest'ultimo a fare quanto possibile per comunicare agli altri titolari (che abbiano creato collegamenti alla fonte, che abbiano fatto copia o riprodotto i dati) la richiesta di cancellazione. La norma formalizza quanto statuito dalla Corte di Giustizia escludendo, fra l'altro, la legittimità della richiesta di cancellazione, e dunque il diritto all'oblio, nei casi in cui la pubblicazione di tali dati risponda al «diritto alla libertà di espressione e di informazione». Il diritto all'oblio riguarda principalmente operatori come i gestori di social e le testate giornalistiche online, che saranno tenuti ad adottare misure ragionevoli per assicurare il risultato finale, pur non assumendosene l'obbligo: dovranno infatti fare il possibile per comunicare ai terzi che abbiano ripubblicato il dato la intervenuta richiesta di cancellazione dell'interessato, ma non risponderanno del relativo diniego eventualmente opposto dai terzi.

Novità, dunque, senz'altro rilevanti in ambito sociale ma che non comportano adeguamenti specifici e organizzativi generalizzati.

Ma la vera innovazione del Regolamento è un'altra: i nuovi presidi organizzativi imposti a carico di ciascun titolare e/o responsabile del trattamento e della possibilità di ottenere la certificazione quale possibile esimente di responsabilità. In sintesi: 1) adozione di un registro delle attività di trattamento, cioè un vademecum che tracci trattamenti eseguiti e misure di sicurezza adottate (art. 30); 2) obbligo di notifica all'Autorità di Controllo, entro 72 ore, dell'intervenuta violazione dei dati personali (es.: intrusione di terzi nei sistemi informatici, sottrazione di codici di accesso a sistemi di home banking: art. 33) e, in alcuni casi, dovere di tempestiva comunicazione agli interessati (art. 34); 3) obbligo di valutare preventivamente i rischi derivanti dal trattamento dei dati personali di terzi (art. 35) e consultazione preventiva dell'Autorità di Controllo circa le misure adottate dall'operatore per attenuarli (art. 36); 4) obbligo di nominare un responsabile della protezione dei dati, che diviene interfaccia esterna dell'operatore potendo gli interessati rivolgersi a quest'ultimo per l'esercizio dei propri diritti (art. 37). La certificazione, invece, potrà essere rilasciata da organismi costituiti ad hoc ai sensi dell'art. 43, ovvero, direttamente, dalle Autorità di Controllo.

La finalità sottesa a tale nuovo modello organizzativo è dunque quella di attuare sia un controllo interno certificato che garantisca un monitoraggio continuo del trattamento dei dati e dei sistemi di sicurezza sia la pronta reazione in caso di violazione dei sistemi.

Alle disposizioni ci si dovrà adeguare entro il 24 maggio 2018, ma occorrerà monitorare gli ulteriori provvedimenti esecutivi (Garante Privacy e legislatore italiano). E non c'è da scherzare: l'art. 83 eleva la sanzione massima a 10 milioni ovvero, se superiore, al 2% del fatturato mondiale totale annuo dell'esercizio precedente. Sottovalutare il problema, avvertito più come un impiccio burocratico che come una doverosa tutela, di solito costa caro. Stavolta particolarmente caro.

Franco Estrangeros