Privacy Italia: PA e aziende indietro nell'adeguamento alle nuove norme. E la politica non aiuta

GDPR, ITALIA IN RITARDO

Da domani in vigore la legge Ue sulla privacy

TESTI DI ROBERTO CARCANO

«Il Regolamento europeo riconosce la portabilità dei dati personali. Ovvero, se una società che possiede i miei dati li usa in modo insoddisfacente, posso riprendermeli e portarli altrove; e quella società ha l'obbligo di cancellare completamente ogni dato relativo alla mia persona. Questo requisito riconosce di fatto il principio della proprietà del dato personale». È questo uno degli aspetti più rilevanti del General Data Protection Regulation secondo **Raffaele Barberio**, presidente di Privacy Italia, società che si pone come obiettivo lo sviluppo di una maggiore sensibilità nei confronti dei temi della privacy e la costruzione di una più diffusa consapevolezza della tutela dei dati personali in istituzioni, imprese e cittadini. Il tema è caldo, tanto più alla luce dei recenti scandali internazionali, ma in Italia forse non c'è ancora la necessaria attenzione. «Il Gdpr entra in vigore domani ma il livello di adeguamento delle Pubbliche Amministrazioni e delle aziende italiane è molto basso», spiega Barberio. «Si è sottovalutata la scadenza e solo negli ultimi mesi tutti si sono mossi disordinatamente, cercando di adeguarsi, magari con l'acquisto di un software gestionale, o affidandosi a consulenti spesso non all'altezza. Ma non è questa la soluzione». Il Regolamento, infatti, non ha soglie di requisiti da soddisfare. «La norma, in sostanza, dice: tu conosci i dati che tratti e tu, e solo tu, sai quali sono le soluzioni migliori: adottale e giustifica le tue scelte in caso di ispezioni», continua il presidente di Privacy Italia. «Ma la cosa più importante è che non ci si adegua con la logica del «mettere a posto le carte». L'adeguamento è un punto di vantaggio di un'impresa, che sarà riconosciuto anche dai clienti; i quali, se non saranno soddisfatti, potranno ricorrere alla portabilità dei propri dati. Ormai sta cambiando la sensibilità dell'opinione pubblica sull'importanza dei dati personali e le aziende dovranno tenerne conto». Di sicuro, la messa in sicurezza dei dati sarà uno degli aspetti cruciali per il futuro. La cronaca di questi mesi ha registrato casi anche emblematici di furti che hanno coinvolto in alcuni casi milioni di cittadini in molti Paesi nel mondo. Con il nuovo regolamento tali violazioni di sicurezza non potranno più essere nascoste. «In caso di Data breach, ovvero quando un sistema di cybersicurezza viene violato, l'impresa o la pubblica amministrazione vittima della violazione avrà l'obbligo di informare il Garante della protezione dei dati personali entro 72 ore dall'accaduto», chiarisce Barberio. «Contestualmente, si avrà l'obbligo di informare tutti i clienti i cui dati sono stati violati. È un cambio di passo molto significativo». Un altro aspetto estremamente rilevante, secondo il presidente di Privacy Italia, è che su un tema così delicato l'Europa parla per la prima volta con una sola voce. Ciascun Paese ha l'obbligo di adeguamento al regolamento europeo delle normative nazionali sulla privacy precedentemente adottate, e sotto questo profilo l'Italia è in palese ritardo. «È anche vero che in questo ritardo non siamo soli. Altre nazioni sono nelle nostre stesse condizioni. Ma noi scontiamo un maggiore distacco dei nostri politici nei confronti di tutte le problematiche legate al valore dei dati, al loro sfruttamento commerciale indebito, al modo in cui il loro uso scorretto può danneggiare la dignità della persona o intaccare le libertà individuali. Tutte cose che peseranno sempre di più in futuro. La nostra classe politica dovrà fare un salto di qualità, perché i dati sono alla base del modello di crescita dell'economia digitale, e il loro uso deviato può danneggiare la gestione delle nostre risorse finanziarie e minare la nostra sovranità nazionale». (riproduzione riservata)

Raffaele Barberio, presidente di Privacy Italia

Professione Dpo: si apre un mercato da 45 mila posti di lavoro

Informa management e dipendenti sugli obblighi relativi alla normativa, vigila sulla sua corretta applicazione e funge da garante dei diritti del personale. È il Data Protection Officer, una nuova figura professionale dagli ampi poteri e dalle grandi responsabilità, introdotta proprio dal nuovo regolamento Gdpr. Una funzione che, appena istituita, ha già un numero di compiti che le sono attribuiti piuttosto numeroso e in un campo d'azione esteso a molte funzioni aziendali. «Sono tutti ruoli che il Responsabile della protezione dei dati deve svolgere con indipendenza e senza conflitti d'interesse», esordisce **Nicola Bernardi**, presidente di Federprivacy, la principale associazione italiana dei professionisti della privacy e della protezione dei dati. «Il Dpo deve informare e consigliare sia il management aziendale sia i dipendenti sugli obblighi prescritti dal Regolamento Ue 2016/679 e dalle normative nazionali in materia di protezione dei dati, verificare che la normativa stessa e le policy interne siano correttamente applicate, inclusi gli adempimenti, le attribuzioni delle responsabilità, la formazione del personale, e i relativi audit. Inoltre, funge da punto di contatto sia con il Garante per la Privacy sia con gli interessati, che possono rivolgersi a lui per l'esercizio dei loro diritti. Questo significa che deve essere facilmente rintracciabile e i suoi recapiti devono essere sia comunicati all'Authority sia resi noti nelle informative e nel sito dell'azienda o dell'ente che lo ha designato».

La nuova figura professionale è obbligatoria in tutte le amministrazioni e gli enti pubblici, eccetto le autorità giudiziarie, e in tutte le imprese che trattano dati sensibili relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici, o che svolgono attività in cui i trattamenti richiedono il controllo regolare e sistematico degli interessati. Per esempio, chi svolge attività di profilazione online per monitorare gusti e preferenze degli utenti ricade pienamente nell'obbligo. «Considerato che tali parametri non sono del tutto perentori, ma richiedono la valutazione di un esperto che si assuma la responsabilità di determinare se occorra o meno nominare un responsabile della protezione dei dati, in molti casi può essere opportuno decidere di dotarsi comunque di questa figura», consiglia Bernardi. «In caso contrario, infatti, si dovranno documentare per iscritto le ragioni per cui si è ritenuto di non farlo».

Ma quali sono le competenze del Dpo e quale iter formativo deve aver percorso? «Innanzitutto deve possedere una conoscenza specialistica della normativa e delle prassi di gestione dei dati personali, ma anche il know-how necessario per applicarla correttamente ed essere in grado di adempiere alle proprie funzioni», risponde il presidente di Federprivacy. «Anche se si tratta di un profilo principalmente giuridico, il Garante ha chiarito che non vi sono titoli di studio o certificazioni obbligatorie, per cui non esiste un'abilitazione. Tuttavia, istruzione, percorsi formativi, bagaglio d'esperienza pregressa e competenze certificate da enti indipendenti di terza parte sono tutti importanti tasselli che concorrono a determinare i criteri per determinare se il candidato possiede o meno quella conoscenza specialistica della normativa e delle prassi di gestione dei dati personali che è richiesta dal Regolamento Ue». Considerando i delicati compiti che gli sono assegnati, l'inquadramento previsto per il Dpo dovrebbe essere equivalente a un dirigente o a un funzionario. «A livello retributivo, questa indicazione è in linea con le statistiche di cui disponiamo in base alle quali nell'area Ue un Responsabile della protezione dei dati percepisce in media un compenso lordo di 80 mila euro annui», precisa Bernardi, «Naturalmente, questa retribuzione può servire da riferimento per grandi realtà, nelle quali chi svolge questo ruolo lo fa a tempo pieno. Attualmente in Italia si osservano bandi di aziende che offrono remunerazioni molto più basse e professionisti che si offrono a costi più contenuti, ma chi possiede effettivamente le competenze necessarie difficilmente accetterà di essere sottopagato». Nel mercato del lavoro, dunque, è lecito attendersi che le richieste di questa nuova figura professionale aumentino nei prossimi mesi. «Il fabbisogno nel nostro Paese è stimato in circa 45 mila professionisti, ma il numero di quelli che sono in grado di svolgere questo ruolo è di gran lunga inferiore. Anche se il regolamento è stato approvato ormai due anni e mezzo fa, la maggioranza di coloro che oggi si propongono per ricoprirlo ha iniziato ad approfondire la materia solo da pochi mesi». Secondo le statistiche di Federprivacy, infatti, quelli che hanno partecipato a percorsi formativi specialistici in materia di protezione dei dati, sono poco più di 2 mila. (riproduzione riservata)