Professionisti e privacy: una formazione di qualità per stare al passo con l'innovazione normativa e tecnologica

Date : 12 febbraio 2016

Lo sviluppo esponenziale della *Internet and Communication Technology* (ICT) e la sua capillare diffusione tanto in ambito pubblico quanto in ambito privato rappresenta una vera e propria rivoluzione per l'individuo, sia nella sua dimensione di cittadino, che in quella di utente e consumatore. L'ICT determina flussi, interscambi e immagazzinamento di dati personali in una dimensione e con una intensità mai conosciute prima. Basti pensare, per esempio, alla mole di dati personali trattati dalle pubbliche amministrazioni ma anche a quelli trattati quotidianamente dalle imprese, metaforicamente ormai vere e proprie "nuvole" che trattano dati di milioni di utenti, più o meno consapevoli di quello che avviene alla propria identità digitale.

In tale contesto, anche le istituzioni europee prevedono un importante sviluppo del mercato unico digitale, sviluppo soprattutto tecnologico, anche con l'adozione diffusa di nuovi modelli come per esempio il *cloud computing*. Lo sviluppo tecnologico deve però coniugarsi con il rispetto dei diritti fondamentali, primo fra tutti il diritto alla riservatezza e il diritto alla protezione dei dati personali. Diritti che vanno garantiti sia individuando innovative forme di tutela (si pensi al concetto di *data protection by design and by default*), sia rendendo omogenei nel territorio dell'Unione europea obblighi e adempimenti in capo ai soggetti pubblici e privati, al fine di rendere effettivo il godimento di tali diritti.

In quest'ottica va letta la scelta di superare la forma giuridica della direttiva per andare verso un regolamento in materia di dati personali, la cui proposta, elaborata dalla Commissione europea, è , ad oggi, in fase di trilogo tra Parlamento europeo e Consiglio.

Numerose sono le innovazioni contenute nel regolamento ma tra di esse una spicca per importanza e particolare portata innovativa: l'istituzione del Responsabile per la protezione dei dati personali o *Data Protection Officer* (DPO).

Il DPO, nella bozza di regolamento, è un supervisore indipendente che sarà designato sia dalle pubbliche amministrazioni che in ambito privato. A seconda del contesto in cui dovrà operare il DPO si troverà ad affrontare questioni giuridiche e tecnico-informatiche più o meno complesse, dalla responsabilità in materia di gestione delle banche dati, alla gestione dei rischi connessi alle differenti tipologie di trattamento, alla gestione delle richieste degli interessati.

Si potrebbe provare a sintetizzare le mansioni del DPO nel modo che segue:

1. sorvegliare la corretta applicazione della normativa sulla protezione dei dati, incluse le misure e le procedure tecniche e organizzative;
2. sorvegliare la corretta applicazione della protezione dei dati sin dalla progettazione degli applicativi (*data protection by design*), garantendo per gli stessi delle impostazioni privacy predefinite (*data protection by default*) nonché la sicurezza dei dati;
3. effettuare ispezioni, consultazioni, attività di documentazione;
4. partecipare alla redazione dei *Data Protection Impact Analysis* (c.d. DPIA), laddove le caratteristiche dei trattamenti dei dati lo rendano indispensabile;
5. fungere da punto di contatto e collaborare con l'Autorità Garante per la protezione dei dati personali;
6. controllare che le violazioni dei dati personali siano documentate, notificate e comunicate (c.d. *Data Breach Notification Management*).

Tutti questi temi richiedono spesso alta specializzazione da parte delle imprese e delle istituzioni che trattano i dati personali, anche sensibili, degli individui. Il DPO, in altre parole, diverrà il referente unico della privacy di ciascuna organizzazione complessa, pubblica o privata che sia. Tale figura, che dovrà caratterizzarsi per indipendenza e competenza, è del tutto innovativa e si presenta come ben distinta da altre figure già note e recepite nell'ordinamento italiano, quali quelle del responsabile o dell'incaricato del trattamento.

Questa peculiare figura professionale è peraltro già prevista come obbligatoria da oltre dieci anni all'interno delle istituzioni dell'Unione Europea (Regolamento n. 45/2001) e, analogamente, molti sono i paesi europei che hanno introdotto già questa figura (Germania, Grecia, Ungheria, Slovacchia, Francia).

La previsione di tale ruolo è ormai prossima e certamente auspicabile, a prescindere, verrebbe da dire, persino dall'approvazione del citato regolamento. Diviene, dunque, cruciale chiedersi quale sia il percorso di formazione più appropriato per il DPO e quali siano i requisiti professionali per esso. L'esperienza maturata in questi anni in ambito europeo, soprattutto nelle istituzioni, è un importante punto di riferimento per comprendere la figura del DPO, così come molto potranno dire in merito i vari documenti contenenti le best practices europee sul DPO, nonché gli eventuali atti delegati che deriveranno dal nuovo regolamento.

Ciò che è certo è che al DPO sarà richiesta una "conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati" e la capacità di fronteggiare sfide sempre più difficili nel campo della protezione dati. È in questo frangente che una formazione di qualità offerta dal mondo universitario può fare la differenza, con un'offerta formativa che sia ampia e generale ma al contempo in grado di offrire approfondimenti di tipo specialistico nei vari settori della protezione dati.

Questa è la sfida che il Dipartimento di Giurisprudenza dell'Università di Roma Tre intende raccogliere, proponendo, a partire dal gennaio 2016, il Master universitario di II livello in "Responsabile per la protezione dei dati personali: *Data Protection Officer e Privacy Expert*". Il Master, che si fregia del patrocinio del Garante per la protezione dei dati personali, intende

assicurare una preparazione adeguata sia dal punto di vista del quadro teorico di riferimento, che delle conoscenze pratico-applicative necessarie a ricoprire la figura professionale di *Data protection officer*, così come di altre figure professionali delegate all'attuazione e implementazione della disciplina in materia di protezione dei dati personali.

L'offerta formativa – e in ciò consiste un importante elemento di novità rispetto alla comune offerta post lauream – si articola in due possibilità: l'iscrizione all'intero corso, che permette di conseguire il Diploma di Master universitario di II livello, e la frequenza di alcuni "Percorsi", realizzati per soddisfare specifiche esigenze professionali (*Privacy Supervisor* in ambito lavorativo, sanitario, bancario e assicurativo e nelle comunicazioni elettroniche; è previsto anche un modulo specifico sul rapporto tra privacy e trasparenza amministrativa).

Una sfida che l'Università di Roma Tre ha voluto cogliere, proiettandosi, come sempre, verso il futuro ma con la dovuta attenzione per la cultura dei diritti fondamentali.

Tutte le informazioni sono reperibili sul sito: http://www.masterprotezionedatipersonali. it/

Per informazioni scrivere a: masterprivacy@uniroma3.it

A cura di:
Carlo Colapietro, Professore ordinario di Istituzioni di diritto pubblico presso il Dipartimento di Giurisprudenza dell'Università degli Studi Roma Tre – Direttore del Master universitario di II livello in "Responsabile per la protezione dei dati personali: Data Protection Officer e Privacy Expert".
Fabio Di Resta, Avvocato – LL.M. – ISO 27001 ICT Security auditor – Presidente del Centro europeo per la privacy (EPCE) – Componente del Consiglio del Master universitario di II livello in "Responsabile per la protezione dei dati personali: Data Protection Officer e Privacy Expert".

Articolo pubblicato sulla rivista ICT Security – Ottobre 2015