IL FORO MALATESTIANO

IN VIGORE IL NUOVO REGOLAMENTO PRIVACY UE. COME CAMBIA LO SCENARIO RELATIVO AL TRATTAMENTO DEI DATI

Gloria Paci

Dopo un iter durato oltre quattro anni, il 24 maggio 2016 è ufficialmente entrato in vigore il Regolamento 2016/679/UE (nel seguito anche "Regolamento") sulla protezione dei dati personali che dispiegherà la propria completa efficacia a partire dal prossimo 25 maggio 2018 quando dovrà essere garantito il perfetto allineamento fra la normativa nazionale in materia di protezione dati e le disposizioni del Regolamento.

Resta quindi un anno per prepararsi a questa importante scadenza. Un periodo di tempo che andrà utilizzato al meglio considerando i significativi cambiamenti che la norma ha introdotto.

Delle nuove regole, a cui i Titolari del trattamento dati dovranno quindi adeguarsi tassativamente entro il 25 maggio 2018 per non rischiare multe fino a 20 milioni di euro o al 4% del fatturato annuo globale, è giusto parlarne ma con la consapevolezza che in questo periodo transitorio, per la gestione degli adempimenti da adottare potranno intervenire chiarimenti e precisazioni in particolare dal Garante per la protezione dei dati italiano (che prenderà il nome di Autorità di controllo) che avrà l'arduo compito di sensibilizzare i titolari del trattamento ad attivarsi per rispondere ai nuovi precetti normativi.
Oltre alle Autorità di controllo dei singoli Paesi, il Regolamento attribuisce alla Commissione europea il potere di adottare atti delegati e di esecuzione, al fine di rendere operativa la disciplina, ma affida ai legislatori nazionali la facoltà di introdurre, a seconda delle situazioni, norme nazionali ad hoc. Questa ampia discrezionalità lasciata ai Garanti per la protezione dei dati dei singoli Paesi sta suscitando numerose perplessità fra gli addetti ai lavori che temono il venir meno di uno degli scopi principali del Regolamento: veder applicata un'unica normativa per imprese e pubbliche

amministrazioni appartenenti all'Unione europea. Solo il tempo potrà chiarire se tale scelta sia utile o solo il frutto di decisioni imposte a livello comunitario da Paesi più autorevoli.
Una cosa è comunque certa: nell'era del tutto digitale, dell'Internet of Things, dei Big Data e delle città intelligenti, il Regolamento riconoscerà più diritti e maggiori garanzie ai cittadini mentre imprese nonché tutti i soggetti coinvolti saranno obbligati a rivedere l'attuale impostazione di gestione degli adempimenti relativi al trattamento dei dati personali.
Il nuovo dettato normativo punta infatti più alla sostanza che alla forma, imponendo nuove modalità di esecuzione degli atti. A titolo esemplificativo, l'attuale obbligo di informare il soggetto interessato al trattamento dati (articolo 13 del D.Lgs n. 196/03) non viene abrogato ma solo rivisto: l'utente dovrà essere informato ma in modo trasparente e conciso avvalendosi di un linguaggio chiaro e di semplice comprensione. Addio quindi a documenti ridondanti e di difficile comprensione.
Ribaditi, anzi, ampliati anche i diritti degli interessati. Primo fra tutti quello della "***portabilità dei dati***", che garantirà a ciascun individuo il diritto di riprendersi i dati trasmessi ad un'azienda o ad un servizio online e trasmetterli ad altri (social network, fornitori di servizi Internet, fornitori di streaming online, ecc.). E ancora. In alcuni casi, sarà legittimo chiedere ai motori di ricerca di deindicizzare una pagina web se minaccia la privacy o chiedere ad un sito di cancellare informazioni che riguardano la sfera personale (diritto all'oblio). Introdotti anche nuovi principi: "***accountability***", per cui il titolare dovrà dimostrare l'adozione di politiche privacy e misure adeguate in conformità al Regolamento. Il principio della "***privacy by design***" (dal quale discende l'attuazione di adeguate misure tecniche e organizzative sia all'atto della progettazione che dell'esecuzione del trattamento) fino a quello della "***privacy by default***" (che alla stregua del principio di necessità di cui all'attuale articolo 3 del D.Lgs n. 196/03, stabilisce che i dati vengano trattati solamente per le finalità previste e per il periodo strettamente necessario a tali fini).
Il Regolamento porta con se anche la nascita di nuove figure professionali. Primi fra tutti il responsabile della protezione dei dati (Data protection officer), un esperto nominato dal titolare del trattamento o dal responsabile del trattamento, che dovrà possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, nonché adempiere alle proprie funzioni in piena indipendenza ed in assenza di conflitti di interesse operando alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio. Numerosi i compiti in capo a tale figura: sarà suo onere informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati. E ancora. Verificare l'attuazione e l'applicazione del Regolamento, delle altre disposizioni dell'Unione o degli

Stati membri relative alla protezione dei dati, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi. Infine fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti. Il DPO dovrà altresì fungere da punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti.
Il *Data Protection Officer* (Responsabile per la protezione dei dati) dovrà essere designato obbligatoriamente da parte delle amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie; da tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il controllo regolare e sistematico degli interessati; infine da tutti i soggetti la cui attività principale consiste nel trattamento, su larga S
di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici. Sebbene siano stati individuati i titolari che dovranno designare un Dpo, il Garante si è affrettato a precisare che ogni titolare del trattamento o un responsabile del trattamento possono comunque designare un Responsabile della protezione dei dati anche in casi diversi da quelli sopra indicati.

E per chi ha tirato un sospiro di sollievo per l'abolizione del Dpss, brutte notizie. Con l'introduzione del Regolamento viene chiesto ai Titolari la messa in atto di misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato, in relazione ai rischi che il trattamento comporta. L'adeguatezza di tali misure deve derivare dai risultati di un'adeguata analisi dei rischi.

I quattro aspetti che la nuova normativa prevede sono l'origine del rischio (ossia le possibili minacce), la natura, la particolarità e la gravità (i possibili danni che può arrecare) dello stesso.
Esteso anche l'obbligo di notificare le violazioni (i *data breach*): in caso di violazione ai sistemi informatici **è obbligatorio per il Titolare del trattamento notificare l'evento all'Autorità Garante entro 72 ore** dal momento in cui ne è venuto a conoscenza. Non meno importante che la comunicazione deve essere inoltrata anche all'Interessato quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.