Via libera al pacchetto dall'Europarlamento. Ci saranno due anni per organizzarsi

Regole privacy in stile europeo

Diritto all'oblio e data protection officer in imprese e p.a.

DI ANTONIO CICCIA MESSINA

Diritto all'oblio e alla portabilità di dati da un social network. E ancora diritto ad essere informati in caso di violazione dei dati personali. Queste alcune delle novità del Regolamento europeo sulla privacy, approvato ieri dal Parlamento Ue, che, tempo due anni manderà in soffitta il codice della privacy italiano e le leggi sulla riservatezza degli stati Ue. Sulla privacy, dunque, si riparte a tinte europee e con una legislazione uniforme in tutto il vecchio continente. Nel pacchetto privacy c'è anche una direttiva sui trasferimenti di dati a fini giudiziari e di polizia. Si applica ai trasferimenti di dati attraverso le frontiere all'interno dell'Unione europea e stabilisce, per la prima volta, norme minime per il trattamento dei dati a fini di polizia all'interno di ogni Stato membro. Il regolamento, che aggiorna la direttiva risalente al 1995, riguarda anche la disciplina dell'organizzazione degli adempimenti per le imprese e per le pubbliche amministrazioni. Scompariranno adempimenti formali, come la notificazione dei trattamenti al Garante. Ma saranno da curare adempimenti di tutela sostanziale, come la valutazione dell'impatto dei trattamenti sulla protezione dei dati e la eventuale verifica delle prescrizioni da adottare presso le autorità di controllo. E il tutto si realizzerà sotto l'occhio del responsabile della protezione dei dati: figura da nominare obbligatoriamente nelle p.a. e nelle imprese, se impegnate nel trattamento dei dati delle persone su larga scala. Riformulato l'apparato sanzionatorio, calcolato in misura percentuale sul fatturato delle aziende (così da diventare veramente efficace verso colossi planetari).

Portabilità dei dati. All'interessato viene riconosciuto il diritto di ottenere la restituzione dei propri dati personali trasmessi ad un'azienda o a un servizio online e trasmetterli ad altri (social network, fornitori di servizi internet, fornitori di streaming online ecc.).

Sportello unico. L'interessato può rivolgersi al Garante del proprio paese per segnalare eventuali violazioni, qualunque sia il luogo in cui il trattamento è effettuato.

Oblio. Il regolamento codifica il diritto dell'interessato di chiedere ai motori di ricerca di deindicizzare una pagina web o chiedere ad un sito web di cancellare informazioni.

Profilazione. Il regolamento sancisce il diritto a non subire profilazioni (trattamenti automatizzati) a propria insaputa.

Consenso. Il regolamento pretende che il consenso dell'interessato sia effettivo e inequivocabile. Può essere formulato, ad esempio, mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Questo può avvenire anche mediante selezione di un'apposita casella in un sito web, ma non è consenso il silenzio, l'inattività o la preselezione di caselle.

Valutazione d'impatto. In casi specifici, come il ricorso a tecnologie a rischio per i diritti delle persona, il trattamento deve essere testato con una valutazione d'impatto privacy ed eventualmente con consultazione preventiva del garante.

Privacy by design e by default. Il regolamento impone di progettare sistemi e applicativi, di regola tarati sul principio dell'uso minimo e indispensabili dei dati personali. Si devono adottare d esempio sistemi di pseudonomizzazione oppure misure e sistemi che abbiano come impostazione predefinita solo l'uso dei soli dati necessari per una certa finalità.

Sicurezza. Scomparsi adempimenti burocratici, viene esaltato un approccio basato sull'analisi dei rischi e sull'adeguatezza delle misure di tutela. Utile l'adesione a sistemi di certificazione e codici di condotta.

Violazione dati. Si estende a tutti la regola della notifica di violazione dei dati personali al garante e all'interessato (a quest'ultimo in caso di rischio elevato per i suoi diritti).

Data protection officer. È una nuova figura di riferimento per imprese e p.a., per utenti e clienti ed è l'interfaccia per le autorità garanti. Nel settore privato dovrà essere nominato in caso di trattamenti di dati su larga scala o di monitoraggio sistematico degli interessati su larga scala.

Codici etici e certificazioni. Codici di autoregolamentazione e ricorso alle certificazioni dei trattamenti e sono incoraggiati. Si tratta di «bollini blu», di cui si terrà conto nelle verifiche, ispezioni e anche nella determinazione delle sanzioni.

Direttiva dati giudiziari. Le nuove norme mirano a proteggere gli individui, vittime, criminali o testimoni, stabilendo diritti chiari e limitazioni al trasferimento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, compresa la protezione delle persone e la prevenzione di minacce alla sicurezza pubblica. Allo stesso tempo, il testo mira a facilitare la cooperazione giudici-polizia.

Prossime tappe. Ora tocca al Consiglio Ue prendere atto formalmente dell'approvazione del pacchetto da parte del Parlamento. Seguirà la pubblicazione in *Gazzetta ufficiale dell'Unione europea*, prevedibilmente entro fine giugno. Il Regolamento entrerà in vigore 20 giorni dopo la pubblicazione e, dopo due anni, le sue disposizioni saranno direttamente applicabili in tutta l'Ue. Gli Stati membri avranno due anni per recepire le disposizioni.

Reazioni. Secondo **Antonello Soro**, presidente Garante privacy, regolamento e direttiva «si pongono anche come una sfida sia per le Autorità garanti sia per imprese, soggetti pubblici, liberi professionisti chiamati ad un ruolo di grande rilievo e responsabilità».

Le novità in arrivo

Portabilità dei dati	Diritto al trasferimento dati da un titolare a un altro (ad esempio, tra social netwok)
Oblio	Diritto a deindicizzare pagina web o informazioni in rete
Profilazioni	Stop a trattamenti automatizzati inconsapevoli
Consenso	Espresso e inequivoco (non va bene la preselezione di caselle)
Valutazione di impatto e sicurezza	Analisi dei rischi derivanti dal trattamento
Privacy by design	Progettare trattamenti conformi al regolamenti
Privacy by default	Impostazioni predefinite sul trattamento minimo di dati
Violazione dati	Diritto di venire a conoscenza della violazione (hackering) dei propri dati personali
Responsabile protezione dati	Nomina obbligatoria per p.a. e imprese che trattano dati su larga scala
Codici etici e certificazioni	Incentivata l'adesione che porta benefici in caso di valutazione della legittimità dei trattamenti (anche in sede ispettiva e sanzionatoria)

IO ONLINE Il regolamento sul sito www.italiaoggi.it/documenti