

Regolamento Ue Misure per la privacy a presidio della 231

L'assetto organizzativo delle società conforme al regolamento europeo può prevenire i reati relativi alla sicurezza delle informazioni.

Riccardo Borsari

— a pagina 25

Misure per la privacy a presidio anche della 231

PROFESSIONISTI E AZIENDE

La tutela dei dati. L'assetto organizzativo conforme al regolamento europeo può prevenire i reati presupposto relativi alla sicurezza delle informazioni

Pagina a cura di

Riccardo Borsari

Il regolamento generale sulla protezione dei dati (regolamento Ue 2016/679), meglio noto con l'acronimo anglosassone "Gdpr", emanato nel 2016 dal Parlamento europeo e dal Consiglio Ue ed entrato in vigore nel maggio dello scorso anno, ha introdotto una nuova disciplina in materia di privacy e data protection direttamente applicabile all'interno degli Stati membri.

Il Gdpr ha sovvertito l'impianto precedente (direttiva 95/46/CE), fondato su un sistema di autorizzazione-notifica alle Autorità di controllo e di prescrizioni di dettaglio, attraverso l'allestimento di una normativa più funzionale alle esigenze dell'attuale sviluppo tecnologico, improntata sulla responsabilizzazione dei soggetti che trattano i dati.

Nel regolamento europeo, infatti, oltre a essere ribaditi i principi generali del trattamento dei dati personali in gran parte già risalenti alla direttiva 95/46/CE (liceità, correttezza e trasparenza del trattamento, minimizzazione, limitazione della conservazione, finalità del trattamento), si aggiunge il principio di "responsabilizzazione" o "accountability" (articolo 5), in forza del quale il titolare del trattamento è tenuto a porre in essere tutte le misure tecniche e organizzative

adeguate per garantire e dimostrare che il trattamento dei dati personali degli interessati è effettuato nel rispetto della normativa. È quindi il singolo titolare a dover individuare modalità concrete del trattamento conformi agli standard di tutela stabiliti dal Gdpr ed essere in grado di documentarlo (articolo 5, comma 2). Questi, salvo taluni casi specifici, non è più tenuto a interloquire preventivamente con il Garante, ma assume su di sé il rischio dei trattamenti effettuati.

Diventa dunque necessario predisporre un sistema di gestione della privacy che possa essere oggetto di prova da parte del titolare in caso di verifiche dell'Autorità.

Nella direzione dell'organizzazione preventiva del trattamento dei dati si colloca l'articolo 32 del Gdpr, che sancisce l'obbligo di predisposizione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza conforme al rischio connesso alla gestione dei dati. Questo assetto è finalizzato alla gestione dei rischi associati ai differenti trattamenti posti in essere, in particolar modo derivanti «dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati».

Varie sono le misure organizzative che il titolare del trattamento può mettere in campo, quali l'indicazione

del rischio connesso a ciascun trattamento; la predisposizione di un organigramma privacy, con attribuzione dei relativi compiti e responsabilità; la previsione di procedure peculiari relative a singole evenienze; procedure volte a garantire la sicurezza dei dati o la loro accessibilità; infine, controlli periodici sulla "tenuta" del modello organizzativo. A livello tecnico, invece, il Gdpr indica, in via meramente esemplificativa, la pseudonimizzazione e la cifratura dei dati.

L'onere organizzativo può essere assolto attraverso l'adesione ai codici di condotta elaborati da associazioni di categoria secondo quanto stabilito dall'articolo 40 del Gdpr, o avvalendosi delle procedure di certificazione previste dall'articolo 42 del regolamento. Una volta adottate le misure, il titolare dovrà darne atto nel registro dei trattamenti, istituito in base all'articolo 30 dello stesso testo.

Il Gdpr presenta evidenti affinità, quanto alla ratio, con la disciplina del-

la responsabilità da reato degli enti ex Dlgs 231/01, laddove entrambe le normative puntano sul dovere di auto-organizzazione rivolto alla prevenzione di condotte illecite o per così dire "patologiche", in senso lato. Nondimeno, va anzitutto osservato che, mentre le prescrizioni del Gdpr sono vincolanti per il titolare del trattamento, la disciplina del Dlgs 231/01 non impone (almeno per ora) l'adozione di un modello da parte dell'ente. Differenti sono poi le finalità cui tendono le due normative, poiché, mentre il Gdpr esige un assetto funzionale agli scopi del regolamento e, dunque, preventivo rispetto alla lesione dei diritti degli interessati, il modello del Dlgs 231/01 deve essere idoneo a prevenire la commissione di reati-presupposto tassativamente elencati.

Sul piano dei contenuti, c'è invece un importante profilo di interferenza tra i settori di rischio presidiati da Dlgs 231/01 e Gdpr, ossia quello connesso alla commissione di reati-presupposto che possono avere all'origine o portare alla violazione di dati personali. Rilevano, in particolare, i delitti informatici e di trattamento illecito di dati indicati nell'articolo 24 bis: accesso abusivo a sistema informatico o telematico; intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche; installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche; danneggiamento di informazioni, dati e programmi informatici; installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche; danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente o comunque di pubblica utilità; detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici; diffusione di apparecchiature, dispositivi o programmi diretti a danneggiare o interrompere un sistema informatico.

È quindi ben possibile che l'adozione di misure organizzative conformi al Gdpr apporti un contributo anche in termini di prevenzione di condotte direttamente o indirettamente prodromiche alla commissione dei reati di cui all'articolo 24 bis del decreto 231; e, viceversa, che l'adozione di un modello 231 idoneo a prevenire i reati di cui all'articolo 24 bis possa rivelarsi funzionale a prevenire la lesione dei diritti degli interessati nel trattamento dei dati personali.

© RIPRODUZIONE RISERVATA

**In parallelo
i «modelli»
possono
supportare
gli
interventi
in campo
per
preservare
i dati
sensibili**

I PUNTI CHIAVE

Gdpr e Dlgs 231/01

- **Accountability:** spetta al titolare del trattamento individuare modalità concrete del trattamento che siano conformi agli standard di tutela stabiliti dal Gdpr e a documentarlo
- Non vi è identità fra Mog e misure organizzative privacy. Vi sono però reati-presupposto che possono avere all'origine o portare alla violazione di dati personali: l'adozione di misure organizzative conformi al Gdpr può quindi contribuire alla prevenzione dei "reati 231", mentre l'adozione del Modello 231 può rivelarsi funzionale a prevenire la lesione dei diritti degli interessati
- Dpo e Odv possono coincidere, ma è necessario il rispetto dei rispettivi requisiti legali e il possesso delle imprescindibili competenze giuridiche e di settore
- L'Odv non è né titolare di trattamento, né responsabile di trattamento, bensì parte dell'organizzazione del titolare priva dei connotati di entrambe le figure