Il nuovo Regolamento generale europeo in materia di dati personali

Sintesi didattica delle novità introdotte dal Regolamento europeo 2016/679

di Giulia Migliore

L'evoluzione della tutela dei dati personali nella normativa europea

La **Direttiva comunitaria 95/46/CE**, definita anche "Direttiva madre", è il testo di riferimento che a livello europeo ha fissato i principi generali della normativa in materia di dati personali. Si tratta di un testo nato in un'epoca antecedente alla diffusione di internet e delle nuove tecnologie, che hanno poi cambiato anche il modo di condividere e raccogliere i dati. In Italia tale direttiva è stata recepita tramite la legge n. 675/1996: *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*.
Le **Direttive 2002/58/CE e 2009/136/UE** hanno introdotto nuovi principi: oltre al trattamento dei dati personali, è stato affrontato il tema della tutela della vita privata nel settore delle comunicazioni elettroniche. Si è iniziato a disciplinare l'uso di internet e il relativo trattamento dei dati personali, effettuato online e con l'uso dei cookies.
Dal 2012 ha avuto inizio una nuova fase, con la decisione della Commissione europea di avviare la definizione di regole destinate ad accompagnare l'evoluzione tecnologica e sociale delle generazioni future. Tale decisione ha portato all'approvazione del **Regolamento europeo 2016/679** in materia di protezione dei dati personali che, insieme alla **Direttiva 2016/680**, è parte integrante del cosiddetto *Pacchetto europeo di protezione dati*. Il 24 maggio 2016 è entrato in vigore il Regolamento, applicabile in tutti i Paesi UE a partire dal 25 maggio 2018.
Il **Regolamento generale sulla protezione dei dati personali** è un testo normativo unico, che trova applicazione diretta in tutti gli Stati dell'Unione europea, senza necessità di leggi di recepimento nazionali. Con il Regolamento vengono introdotti nuovi diritti e regole più stringenti per la gestione e il trattamento dei dati, si attribuiscono maggiori responsabilità al titolare del trattamento, si prevedono sanzioni rilevanti e commisurate al fatturato aziendale.
I Paesi dell'Unione europea hanno quindi avuto due anni di tempo per recepire i principi del Regolamento e adeguare le proprie politiche in materia di dati personali.

L'ambito territoriale di applicazione del Regolamento

La normativa si applica a tutti i soggetti, dentro e fuori l'Unione, che trattano i dati di dipendenti, clienti, utenti e fornitori all'interno dell'UE. Viene introdotto il principio dell'applicazione del diritto dell'Unione anche ai trattamenti di dati personali svolti fuori dall'Unione stessa, ma che riguardano l'offerta di beni e servizi a cittadini UE e/o il monitoraggio dei loro comportamenti.
Il luogo in cui ha sede il titolare del trattamento guida l'applicazione della normativa. Ne deriva che social network, piattaforme web e motori di ricerca, anche se gestiti da società con sede fuori dall'Unione, dovranno sottostare alla normativa europea qualora si riferiscano a titolari del trattamento con sede nell'UE.

Il principio dell'accountability

Il Regolamento introduce il principio della **responsabilizzazione** (*accountability*) e rendicontazione ad opera del titolare del trattamento. Egli dovrà effettuare e opportunatamente documentare un'analisi dei rischi e dovrà valutare le modalità di gestione più adatte a prevenirli.
Le aziende dovranno dotarsi di un sistema documentale di gestione della privacy, istituendo il **Registro del trattamento dei dati**, al fine di rendere tracciabili e documentabili tutte le operazioni di trattamento. Tale registro potrà avere anche forma elettronica e dovrà essere reso consultabile al Garante su sua eventuale richiesta.

La privacy come processo aziendale

Viene esplicitato il principio secondo cui **la privacy costituisce un vero e proprio processo aziendale** (*privacy by design*). La valutazione di ogni processo aziendale dovrà tener conto, già in fase di progettazione, dell'impatto e degli eventuali rischi connessi alla privacy; tali valutazioni dovranno tener conto anche delle dotazioni informatiche di supporto utilizzate. Ciò si traduce in primo luogo nella garanzia che vengano trattati solo i dati personali strettamente necessari per ogni finalità.
Le aziende dovranno fare una scrupolosa analisi preventiva di tutti i trattamenti dei dati personali che intendono svolgere, valutare attentamente i possibili rischi connessi e gli eventuali abusi nell'utilizzo di tali dati. Il titolare del trattamento dovrà prevedere meccanismi di protezione dei dati (riservatezza, integrità, esattezza, sicurezza fisica e rimozione) per tutto il ciclo di vita degli stessi, dalla fase di progettazione delle attività, alla raccolta e archiviazione, fino alla cancellazione.

La valutazione degli impatti

Il Regolamento impone di effettuare una **valutazione degli impatti ai fini della privacy** nei casi in cui il trattamento di dati previsto in un processo aziendale presenti rischi specifici per i diritti e le libertà degli interessati.
Ogni qualvolta si rendesse necessario attivare una valutazione degli impatti occorrerà:

- analizzare i rischi e valutare i relativi gap da colmare;
- pianificare un *action plan* per colmare in modo opportuno i gap;
- monitorare periodicamente gli interventi effettuati o da effettuare per ridurre i rischi.

Il Data Protection Officer

Il Regolamento introduce la nuova figura professionale del *Data Protection Officer* (DPO), ossia il **responsabile per la protezione dei dati personali**, cioè il manager del trattamento dei dati. Egli deve conoscere molto bene l'organizzazione in cui opera, disporre di competenze trasversali e ampie in ambito organizzativo, giuridico e informatico, essere coinvolto in tutte le valutazioni e le decisioni strategiche che abbiano un impatto sulla gestione dei dati.
Tale ruolo dovrà essere presente in tutti gli organismi pubblici e in tutte le imprese che trattano i dati di un numero rilevante di soggetti e/o trattano dati che per loro natura siano soggetti a particolari rischi. Il DPO dovrà operare con assoluta indipendenza, autorevolezza e competenza ed essere un interlocutore referente per il Garante. Tra i compiti del DPO rientra, infine, la sensibilizzazione e formazione del personale.
La figura del DPO completa e arricchisce il quadro delle responsabilità che vede persistere i ruoli del titolare del trattamento e del responsabile.
Il **titolare** (persona fisica o giuridica) agisce come *data controller*: è la figura responsabile giuridicamente dell'osservanza e conformità agli obblighi previsti dalla normativa ed è colui che determina finalità, modalità e mezzi del trattamento dei dati personali.
Il **responsabile** (persona fisica o giuridica), cosiddetto *data processor*, viene nominato per trattare i dati per conto del titolare, con il quale mette in atto le misure tecniche e organizzative idonee ad assicurare un livello di sicurezza adeguato ai rischi ipotizzati.

Rispetto al d.lgs. n. 196/2003, sembra invece venir meno il riferimento all'**incaricato del trattamento**, ma rimane valida la facoltà del titolare e/o del responsabile di nominare terzi (persone fisiche o giuridiche) autorizzati al trattamento sotto la diretta responsabilità di chi li ha nominati.

L'informativa all'interessato del trattamento

Cambia il modo in cui deve essere redatta l'informativa all'interessato del trattamento dei dati.
Le informazioni dovranno essere fornite "possibilmente" (non obbligatoriamente) **per iscritto** o con altri mezzi (eventualmente in formato elettronico); potranno essere fornite anche oralmente, ma dovrà essere comprovata l'identità dell'interessato.
L'informativa andrà espressa con un **linguaggio** chiaro e semplice (soprattutto se rivolta a minori), essere concisa, trasparente, intellegibile e facilmente accessibile. L'informativa potrà anche essere rappresentata attraverso icone facilmente riconoscibili ed esplicative. È fondamentale che sia precisato il periodo di conservazione dei dati o almeno i criteri utilizzati per determinare tale periodo.
Qualora i dati non siano raccolti presso l'interessato, ne va indicata l'origine.

Il consenso dell'interessato

Il **consenso espresso** rimane un requisito necessario solo per le attività di profilazione, ossia quelle attività volte a raccogliere e analizzare i dati degli utenti di servizi con la finalità di studiarne il comportamento.
In generale si allarga la possibilità di raccogliere **consensi manifestati attraverso comportamenti positivi** da parte dell'interessato.
Il consenso mediante il quale l'interessato accetta che i propri dati personali siano oggetto di trattamento per **finalità commerciali**, dovrà consistere in una manifestazione di volontà libera, informata, specifica e inequivocabile. Non è fondamentale che il consenso sia documentato per iscritto, anche se questo rimane il modo migliore per tracciarlo e dimostrarlo.
Nel caso dei **minori**, il loro consenso diventa valido a partire dai 16 anni; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci. Al momento è in discussione all'interno di alcuni Paesi la possibilità di abbassare questa soglia a 13/14 anni.

La notifica delle violazione dei dati personali

Il nuovo Regolamento innalza il livello di sicurezza dei dati e la responsabilizzazione dei soggetti che detengono grandi quantità di dati. In quest'ottica, i titolari del trattamento sono responsabili della protezione dei dati che detengono e devono segnalare tempestivamente ogni eventuale violazione subita.
Sono **violazioni dei dati personali** (*personal data breaches*) la perdita, la distruzione, la modifica, la condivisione non autorizzata o l'accesso (accidentale o illecito) ai dati personali archiviati, trasmessi o comunque trattati.
A seguito di una violazione, sarà fondamentale fare una tempestiva **valutazione dei rischi** e attivarsi di conseguenza. I titolari dovranno informare l'Autorità Garante entro 72 ore dall'evento, ma solo nel caso in cui si ritenga che dalla violazione possano derivare rischi per gli interessati.
Nel caso in cui si valuti che il livello di rischio per gli interessati possa essere alto, sarà necessario informare anche loro della violazione.
L'obbligo generale di notificazione è sostituito quindi dall'obbligo di valutazione dell'impatto. Viene meno l'obbligo di notifica di specifici trattamenti all'Autorità Garante, in quanto tale adempimento è stato considerato poco efficace dal Legislatore.

I diritti degli interessati

Il Regolamento introduce due nuovi diritti per gli interessati al trattamento dei dati personali: il diritto all'oblio e il diritto alla portabilità del dato.
Attraverso il **diritto all'oblio**, il soggetto interessato può chiedere al titolare del trattamento la cancellazione dei dati personali che lo riguardano - e quindi bloccare l'eventuale diffusione di tali dati - nel caso in cui il consenso sia stato revocato, il trattamento non sia conforme al Regolamento, i dati non siano più necessari rispetto alle finalità. Il responsabile del trattamento dovrà adottare tutte le misure atte a informare eventuali terze parti con le quali siano stati condivisi i dati dell'interessato, comunicando la richiesta dell'interessato di bloccare e/o cancellare la riproduzione dei suoi dati.
Attraverso il **diritto alla portabilità del dato**, l'interessato può richiedere che i suoi dati (riferiti a un profilo utente) siano trasferiti da un sistema di trattamento elettronico a un altro e/o che siano scaricati in formato elettronico per poter essere riutilizzati.

Le sanzioni

In caso di violazioni al Regolamento, le aziende rischiano sanzioni amministrative pecuniarie molto rilevanti, che variano in relazione a diversi fattori, quali ad esempio le categorie di dati trattati, la natura e la gravità della violazione, il danno per gli interessati, il dolo nella violazione, le misure di sicurezza applicate dal titolare.
Nei casi più rilevanti, le sanzioni amministrative pecuniarie possono arrivare **fino a € 20.000.000**, o rappresentare **fino al 4%** del fatturato complessivo totale annuo (consolidato) per i gruppi societari. Tali sanzioni sono pensate per punire le condotte illecite commesse da multinazionali che trattano dati in diverse aree geografiche e che in passato sono riuscite a eludere i controlli rigorosi rispetto al trattamento dei dati, svolgendo tali attività all'interno di Paesi dove i controlli sono meno strutturati e rigidi.

Per approfondimenti si rimanda al sito ufficiale del Garante per la protezione dei dati personali: www.garanteprivacy.it