filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

Il principio di accountability ai sensi del Regolamento UE 2016/679

16 Ottobre 2018
Antonella Di Cerbo

Il verbo "*to account*" ed il termine "*ability*" sono rispettivamente tradotti in italiano con le espressioni "dar conto" ed "essere in grado di". Il principio di accountability, infatti, impone agli enti una **gestione aziendale responsabile che tenga conto dei rischi connessi all'attività svolta e che sia idonea a garantire la piena conformità del trattamento dei dati personali ai principi sanciti dal Regolamento e dalla legislazione nazionale**.

È evidente che il principio guida della nuova disciplina del trattamento dei dati personali abbia un significato distinto e più ampio rispetto al termine, di comune radice, "responsabilità" con cui è, impropriamente, tradotto nel nuovo regolamento europeo. La traduzione nostrana tradisce l'approccio voluto dal legislatore europeo tralasciando la fondamentale dicotomia responsabilizzazione/responsabilità che, invece, rappresenta una delle più importanti novità della riforma. Infatti, **mentre con la Direttiva 95/46 l'accento era posto sugli adempimenti formali e sulle conseguenze che si sarebbero potute verificare dopo la violazione, ora l'enfasi è rivolta sulla concreta efficacia dei comportamenti proattivi assunti dal titolare per prevenire violazioni ed abusi**.

Il risultato è la responsabilizzazione del titolare del trattamento a cui viene affidato sia il compito di decidere autonomamente le modalità, le garanzie ed i limiti del trattamento dei dati personali in considerazione della realta? produttiva nella quale opera[1]**,** sia, invertendo l'onere della prova, dimostrare di aver diligentemente tutelato i dati personali che utilizza. A tal fine il legislatore europeo auspica che il titolare del trattamento tenga, sotto la sua responsabilità, un registro delle attività di trattamento svolte e che cooperi con l'autorità di controllo mettendo, su richiesta, detti registri a sua disposizione per consentirle di esaminare, in maniera obiettiva ed in ogni momento, il percorso seguito (v. Considerando 82).

Un approccio completamente diverso rispetto alla Direttiva 95/46 (articolo 33 del codice) che dettava misure minime di sicurezza uguali per tutti, indipendentemente dalla categoria, dalla modalità e dalla quantità dei dati trattati.

Oggi, per adottare le misure di sicurezza adeguate in base al tipo di trattamento svolto, il titolare dovrà effettuare un'analisi del rischio, vale a dire valutare tutti i possibili rischi che possono verificarsi in ordine ai dati trattati (articolo 24 del Regolamento).

In ogni caso, il Regolamento chiarisce che gli sforzi richiesti devono sempre essere accuratamente calibrati con la realta? economica dell'azienda interessata, pertanto non essere onerosi al punto da lederne l'economia.

Le principali novità in termini di adempimenti e di valutazioni rimesse direttamente al titolare del trattamento

L'approccio responsabilizzante funge da criterio guida all'interno di tutta la nuova disciplina europea. Di

seguito sono indicati alcuni dei casi in cui le previsioni normative rette dal criterio de quo hanno comportato maggiori oneri ed una più ampia autonomia per il titolare del trattamento:
- la designazione da parte del titolare del trattamento di un **responsabile della protezione dati** (ovvero DPO se si utilizza l'acronimo inglese), finalizzata a facilitare l'attuazione del Regolamento. Si pensi, infatti, che tra i compiti dell'RPD rientra la "sensibilizzazione e la formazione del personale e la sorveglianza sullo svolgimento della valutazione d'impatto di cui all'articolo 35";
- **il processo di valutazione relativo al rischio** cui può dar luogo il trattamento in ordine alle libertà ed i diritti degli interessati, rimesso esclusivamente al titolare del trattamento che, tra l'altro, può decidere se dare inizio al trattamento o consultare il garante per ottenere indicazioni circa le misure correttive da adottare;
- la disciplina dettata dall'articolo 6 del Regolamento ai fini della **liceità del trattamento**, ove è stabilito che spetta al titolare, e non all'Autorità garante, il bilanciamento tra il legittimo interesse del titolare o del terzo e le libertà dell'interessato;
- **il processo di valutazione dei dati raccolti da fonti diverse dall'interessato** compiuto dal titolare e finalizzato a verificare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato tale da giustificarne l'esonero, come previsto dell'articolo 14 paragrafo 5 lettera b;
- la disciplina dei **diritti dell'interessato**, ove è previsto che, qualora esercitati, sia il titolare a valutare se le richieste siano manifestamente infondate o eccessive;
- o, ancora, con riferimento alle ipotesi di **data breach**, è il titolare del trattamento a dover valutare se, essendo probabile che dalla violazione derivino rischi per i diritti e le libertà degli interessi, è necessario notificare l'avvenuta violazione al Garante. Pertanto, la comunicazione al Garante non avviene di default ed obbligatoriamente, ma è rimessa ad una valutazione del titolare che, in ogni caso, non è esonerato dall'obbligo di documentare le violazioni subite ed i provvedimenti adottati per far fronte alle stesse.

Considerazioni finali:
Alla luce delle osservazioni e delle riflessioni appena esposte, è emerso che, nell'ottica del nuovo Regolamento, sono numerose le valutazioni e gli adempimenti rimessi al titolare del trattamento, ciononostante preme sottolineare che, anche a fronte di tali cambiamenti, l'Autorità di controllo mantiene inalterato il suo ruolo, primario e centrale, di controllo, fungendo, anzi, da guida "nel difficile passaggio alla responsabilizzazione".

[1] Considerando 74 "il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche".

TAG: *accountability, DPO, GDPR, privacy, Diritto dell'Unione Europea, Diritto delle nuove tecnologie e delle comunicazioni*
