■ Data breach: profili di responsabilità in azienda secondo recente giurisprudenza

DATA BREACH... CHI È RESPONSABILE?*

• DI **LUCA DI SEVO** CONSULENTE DEL LAVORO IN BOLLATE (MI) •

La gestione dei dati personali e le relative responsabilità in caso di violazioni sono temi di crescente rilevanza per professionisti e aziende. L'Autore esegue un'analisi che permette di osservare uno spaccato significativo della situazione attuale, evidenziando nuovi orientamenti giurisprudenziali degni di nota.
È stato registrato un incremento delle violazioni dei dati personali (*data breach*) nel 2023: ben 2.037 casi notificati al Garante della Privacy, con un aumento del 50,8% rispetto all'anno precedente. È interessante notare come la maggior parte di questi casi, il 63%, abbia coinvolto soggetti privati, mentre il restante 37% ha riguardato enti pubblici. Questo *trend* evidenzia una vulnerabilità diffusa nei sistemi di protezione dei dati.
Un cambiamento significativo è stato introdotto dalla Corte di Giustizia UE con la sentenza del 4 maggio 2023. La Corte ha stabilito che non è necessario il superamento di una soglia minima di gravità per ottenere il risarcimento, ribaltando così l'orientamento precedente della giurisprudenza italiana. Questa decisione amplia notevolmente le possibilità di tutela per i soggetti i cui dati sono stati violati.
Un aspetto cruciale è costituito dalla responsabilità per errore umano. Il Titolare del trattamento risponde anche per gli errori dei propri dipendenti, come previsto dall'art. 2049 del codice civile. L'Autore riporta ad esempio il caso verificatosi in un Comune che ha erroneamente pubblicato dati personali di una dipendente nell'Albo pretorio, sottolineando come anche una semplice distrazione possa avere conseguenze rilevanti.

A livello pratico, emergono obblighi precisi in caso di violazione: il Titolare deve notificare il *data breach* al Garante entro 72 ore dalla scoperta, qualora ravvisi un possibile rischio per i diritti e le libertà delle persone. Nei casi in cui il rischio viene considerato più elevato, il Titolare deve informare anche i soggetti interessati. In caso di mancato rispetto degli obblighi previsti, le sanzioni di natura amministrativa possono arrivare fino a 10 milioni di euro o al 2% del fatturato annuo; a questo vanno aggiunte le possibili responsabilità penali per dichiarazioni false al Garante o inosservanza dei provvedimenti.

L'Autore dedica attenzione anche alle misure preventive che si possono mettere in campo, sottolineando l'importanza di due principi utilizzati nel settore: questi principi prendono il nome di *"privacy by design"* e *"by default"*; a questi due principi, si aggiunge il concetto di ➤

* Sintesi dell'articolo pubblicato su *D&PL, n. 47-48, 2024*, pag. 2790 dal titolo *Responsabilità di professionisti e aziende nella gestione dei dati personali in caso di data breach.*

accountability.
La prevenzione del rischio passa per l'adozione di alcuni strumenti fondamentali: il registro dei trattamenti, la valutazione d'impatto *privacy* (DPIA) e l'adozione di adeguate misure di sicurezza.

Dall'analisi proposta emergono alcuni spunti interessanti: l'esistenza di un *data breach* non implica automaticamente l'inadeguatezza delle misure di sicurezza adottate. In questi casi però, il Titolare del trattamento ha l'onere di dimostrare sia l'adeguatezza delle misure implementate sia la non imputabilità dell'evento dannoso.

Emerge chiaramente come sia fondamentale un approccio preventivo basato sul rischio e come la responsabilizzazione del Titolare rappresenti un principio cardine della normativa.

Infine, va notato come il panorama della protezione dei dati personali sia in continua evoluzione, richiedendo un approccio sempre più strutturato e professionale. La crescente complessità delle minacce e il quadro normativo in evoluzione impongono a professionisti e aziende di mantenere alta l'attenzione e di investire adeguatamente in misure di protezione e procedure di gestione delle violazioni.