

Sicuri di essere sicuri?

Letizia Maria Ferraris: by design e by default, una tutela in più per nostri dati in movimento

Quando le attività di raccolta dei dati personali da parte di un ente o di un fornitore avvengono tramite l'utilizzo di applicazioni, la normativa sulla protezione e la sicurezza delle persone fisiche (GDPR) richiede che questi strumenti siano realizzati e pensati (progettati) con una serie di cautele a favore dell'**Interessato** da parte di chi svolge un trattamento.

Questo approccio prende il nome di **privacy by design** e ha lo scopo di garantire l'esistenza di un corretto livello di protezione delle informazioni ricevute fin dalla fase di progettazione (*design*) di qualunque sistema, servizio, prodotto o processo e di applicare la medesima cura durante il loro ciclo di vita. Il principio è volto cioè a garantire un corretto livello di protezione dei dati in tutte le attività trattamentali effettuate all'interno di un'organizzazione.

La **privacy by design** si applica peraltro anche agli ambiti non informatici, ogni qualvolta titolare o responsabile debba ideare una procedura, un processo o una serie di attività che comporti un processo informativo.

Per la corretta realizzazione di queste procedure diventa quindi rilevante valutare e predisporre "misure tecniche e organizzative" idonee a fornire ogni idonea garanzia per la tutela dell'interessato, applicando gli altri principi fondamentali in materia di protezione di dati, quali trasparenza, limitazione delle finalità e minimizzazione.

È però vero che il concetto di **privacy by design**, a noi pervenuto con l'entrata in vigore del GDPR, era già applicato in ambiti extra europei, quando negli anni '90 per la prima volta la Commissaria per l'informazione e la privacy dell'Ontario, Ann Cavoukian, ne pose le basi con sette principi:

1. **approccio proattivo e preventivo** nei confronti di eventuali violazioni dei diritti sottesi al trattamento;
2. **privacy come impostazione di default** ovvero inserita come 'predefinita' in qualsiasi prodotto o servizio;
3. **privacy incorporata nel progetto**, ovvero attenzione alla minimizzazione dei propri dati personali fin dalla fase di progettazione;
4. **massima funzionalità** per assolvere allo stesso tempo privacy e sicurezza;
5. **protezione e sicurezza** durante tutto il ciclo-vita del prodotto offerto;
6. **visibilità e trasparenza** dell'intero processo di trattamento;
7. **centralità dell'utente**, la persona e i suoi diritti messi sempre al primo posto.

Presidi che oggi si possono declinare in quattro **fondamentali**

1. **Minimizzare:** raccogliere e trattare la minima quantità di dati possibile;
2. **Nascondere:** limitare l'esposizione dei dati per garantire la tutela degli obiettivi di riservatezza;
3. **Distaccare:** mantenere contesti autonomi di trattamento che rendano difficile correlare gruppi di informazioni codificabili o codificati, che dovrebbero essere disgiunti per evitare una profilazione completa del soggetto;

4. **Astrarre:** limitare il dettaglio dei dati utilizzando parole generiche o gruppi di valori.

Principio di pari rilevanza e complementare è la c.d. **privacy by default**. Esso richiede di definire – prima di iniziare il trattamento – quali dati siano effettivamente (e, cioè) strettamente necessari per la finalità specifica per cui sono stati acquisiti, ai fini di proteggere la riservatezza dei dati personali: un evidente rafforzamento del concetto di minimizzazione dei dati raccolti.

La **privacy by default** è particolarmente legata al tema della “trasparenza”, poiché solo conoscendo le caratteristiche del trattamento, l’Interessato sarà in grado di decidere, liberamente e con la consapevolezza delle possibili conseguenze, se andare oltre la configurazione iniziale, selezionando quelle opzioni dell’applicazione, del prodotto o del servizio che incidono significativamente sulla sua *privacy*.

Sono caratteristiche per proprie della modalità **by default**

- il **Consenso sempre esplicito**, necessario per qualsiasi utilizzo di dati oltre le funzionalità di base
- la **Facilità di gestione delle impostazioni di tutela**, sempre accessibili e comprensibili per gli utenti
- la **Protezione dei dati sempre attiva**, automaticamente, senza l’intervento dell’utente;
- la **Riduzione al minimo dei tempi di conservazione dei dati**, che non devono superare il tempo strettamente necessario per il trattamento.

Privacy by design e by default sono due aspetti complementari per la salvaguardia dei nostri dati e per Titolare e Responsabile sussiste l’obbligo di legge per attuare tali principi.

Certo è che nella veste di interessati e cittadini, ogni qualvolta aderiamo a un contratto *on line* (o scritto) o prestiamo il nostro consenso (*on line* o scritto) fornendo informazioni a terzi, compilando specifici moduli, form elettronici o tramite App, non potremo esimerci dal riflettere (sempre) su cosa stiamo inviando o sottoscrivendo, domandandoci se non stiamo fornendo più elementi di quelli che effettivamente servirebbero. La prima difesa dei nostri dati personali siamo sempre noi!

© 2024 CIVICO20NEWS – riproduzione riservata

Data di pubblicazione: 25/09/2024

Salvato in PDF in data: 23/10/2026

Link all'articolo: <https://civico20-news.it/la-tutela-dei-dati-personali/sicuri-di-essere-sicuri-3/25/09/2024/>