PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5395 di Martedì 23 maggio 2023

Dark Pattern: cosa sono e come evitarli

Il Garante della protezione dei dati personali ha pubblicato le linee guida sui modelli di progettazione ingannevoli che possono influenzare il comportamento di chi naviga online e ostacolare la protezione dei dati.

I Dark Pattern, o "modelli di progettazione ingannevoli", sono interfacce e percorsi di navigazione progettati per influenzare il nostro comportamento online, che possono anche ostacolare un'efficace protezione dei nostri dati personali.

Il Garante lancia una nuova pagina informativa per approfondire un fenomeno sempre più diffuso, ma ancora sconosciuto alla maggior parte degli utenti dei servizi digitali.

La pagina - che fa riferimento anche alle recenti Linee Guida dell'EDPB - è parte di un ampio progetto di informazione e sensibilizzazione sui temi della protezione dei dati, dell'educazione digitale e della sicurezza, per un uso consapevole di Internet e delle nuove tecnologie.

Modelli di progettazione ingannevoli (Dark Pattern)

Con la definizione di "modelli di progettazione ingannevoli" vengono indicate quelle interfacce e quei percorsi di navigazione progettati per influenzare l'utente affinché intraprenda azioni inconsapevoli o non desiderate - e potenzialmente dannose dal punto della privacy del singolo - ma favorevoli all'interesse della piattaforma o del gestore del servizio.

Detti anche **Dark Pattern**, i modelli di progettazione ingannevoli mirano dunque a influenzare il nostro comportamento e possono ostacolare la capacità di proteggere efficacemente i nostri dati personali.

Il 24 febbraio 2023, il Comitato europeo per la protezione dati (EDPB) ha pubblicato le linee guida su come riconoscere ed evitare questi sistemi. Il documento offre raccomandazioni pratiche a gestori dei social media, a designer e utenti su come comportarsi di fronte a queste interfacce che si pongono in violazione del Regolamento europeo in materia di protezione dati.

Le linee guida dell'EDPB individuano sei tipologie riguardo alle quali si può parlare di "modelli di progettazione ingannevoli":

? quando gli utenti si trovano di fronte a una enorme numero di richieste, informazioni, opzioni o possibilità finalizzate a spingerli a condividere più dati possibili e consentire involontariamente il trattamento dei dati personali contro le aspettative dell'interessato *(overloading)*

? quando le interfacce sono realizzate in modo tale che gli utenti dimentichino o non riflettano su aspetti legati alla protezione dei propri dati *(skipping)*

? quando le scelte degli utenti sono influenzate facendo appello alle loro emozioni o usando sollecitazioni visive *(stirring)*

? quando gli utenti sono ostacolati o bloccati nel processo di informazione sull'uso dei propri dati o nella gestione dei propri dati *(hindering)*

? quando gli utenti acconsentono al trattamento dei propri dati senza capire quali siano le finalità a causa di un'interfaccia incoerente o poco chiara *(flickle)*

? quando l'interfaccia è progettata in modo da nascondere le informazioni e gli strumenti di controllo della privacy agli utenti *(leftinthedark)*

Ricordiamo che interfacce e informazioni sottoposte agli utenti dovrebbero sempre riflettere fedelmente le conseguenze dell'azione intrapresa ed essere coerenti con il percorso di esperienza-utente.

L'approccio alla progettazione deve essere dunque quello di non mettere in discussione la decisione della persona per indurla a scegliere o mantenere un ambiente meno protettivo nei confronti dei propri dati. Il modello deve invece essere utilizzato per avvisare la persona che una scelta appena compiuta potrebbe comportare rischi per i propri dati e la privacy.

Le linee guida - Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them (pdf)

Fonte: Garante Privacy

www.puntosicuro.it