DESIGN DIGITALE A PROVA DI GDPR

COSA CI INSEGNA LA SANZIONE DI 50 MILIONI A GOOGLE?

Progettare interfacce digitali accattivanti è complicato e l'avvento del GDPR lo ha reso una vera e propria sfida. Nemmeno i grandi colossi del mercato digitale sembrano ancora aver trovato la strategia giusta per creare un design trasparente e immediato.

Eppure, guadagnare la fiducia dei propri utenti sarà il vero punto di forza di chiunque vincerà questa sfida.

Come riuscirci?

In questo clima di incertezza alcune recenti pubblicazioni dell'Autorità Garante francese (CNIL) iniziano a tracciare la strada, a partire dalla sanzione nei confronti di Google.

LA SANZIONE A GOOGLE LCC

Il 21 gennaio Il Comitato ristretto della Commission Nationale de l'Informatique et des Libertés si è pronunciata condannando Google LCC ad una **sanzione di 50 milioni di euro per aver progettato alcune delle sue interfacce digitali in modo non trasparente.**

La CNIL, muovendosi a seguito del reclamo di due organizzazioni no profit che hanno ricevuto a loro volta numerose lamentele da parte degli utenti, ha deciso di sanzionare il colosso californiano essenzialmente per violazione del principio di trasparenza (art. 5, par. 1, lett. a del GDPR) e per la conseguente carenza di una base giuridica su cui possa fondarsi il trattamento dei dati personali.

In altre parole, la CNIL insiste sul fatto che **se non c'è chiarezza, trasparenza e facile accesso alle informazioni, il consenso, anche se formalmente prestato, non si sostanzia**.

Gli utenti Google che hanno intenzione di creare un account si trovano davanti ad un design delle interfacce digitali confusionario, che non permette di comprendere effettivamente come e perché i dati personali da loro rilasciati verranno trattati. Nonostante le informazioni siano presenti all'interno del sito, la CNIL ci offre un'importante lezione sul vero senso della nuova normativa privacy: ciò che conta non è l'aspetto formale delle azioni compiute dal titolare del trattamento dei dati, ma **la sostanza delle sue scelte e quello che effettivamente viene percepito dal vero protagonista della normativa: l'utente**.

Se dovessimo riassumere con una frase la delibera della CNIL, si potrebbe senza dubbio scegliere questa: "Gli obblighi di trasparenza e d'informazione sono essenziali poiché condizionano l'esercizio dei diritti degli interessati e permettono loro di mantenere il controllo sui dati personali". [*tradotto dagli autori*]

É di estrema importanza che le persone abbiano il controllo dei dati personali che li riguardano (considerando 7 GDPR); un aspetto primordiale del principio di trasparenza, secondo la CNIL, è che **l'interessato deve essere in grado di determinare in anticipo la portata e le conseguenze del trattamento dei dati**, in modo tale da non essere preso alla sprovvista ad uno stadio ulteriore del trattamento o rispetto alle modalità con cui i dati sono trattati.

In questo gli obblighi di trasparenza e d'informazione sono essenziali, in quanto hanno la facoltà di influenzare l'esercizio dei diritti delle persone e il controllo sui propri dati. Per di più si sottolinea che gli articoli 6, 12 e 13 relativi proprio a tali obblighi **rientrano tra le disposizioni di cui la violazione è più severamente sanzionata ai sensi del paragrafo 5 dell'articolo 83 del GDPR.**

Alla luce dei riportati principi, quali sono gli errori che sono costati a Google 50 milioni di euro?

L'interessato, per poter accedere effettivamente alle informazioni necessarie al fine di comprendere il reale utilizzo dei propri dati personali, deve aprire una numerosa serie di pagine e collegamenti. Per esempio,

- l'utente che vuole conoscere la durata di conservazione dei dati deve effettuare quattro clic prima di conoscere la risposta,
- sono cinque le azioni necessarie all'utente per accedere alle informazioni sulla personalizzazione degli annunci
- sei quelle indispensabili per saperne di più sulla geolocalizzazione.

Una tale modalità di accesso genera inevitabilmente confusione e nonostante le informazioni siano presenti, queste risultano frammentate e, di conseguenza, del tutto inefficaci.

Un altro elemento su cui si è concentrata la CNIL è la preselezione delle caselle del consenso al trattamento dei dati. Era stato il Gruppo di Lavoro ex art. 29, con le Linee guida sul consenso ai sensi del regolamento (UE) 2016/679 adottate nel 2017, a dissipare ogni dubbio in merito: "l'uso di caselle di adesione preselezionate non è valido ai sensi del regolamento".

UNA SEMPRE PIÙ DIFFUSA CONSAPEVOLEZZA SULLA TUTELA DEI DATI PERSONALI

Gli strumenti digitali, ormai, assistono quotidianamente le nostre azioni, proponendosi di svolgere per noi gli aspetti più meccanici delle attività di ogni giorno per concederci di incanalare tempo e risorse verso i compiti più complessi e più importanti. Eppure, in una società che tende sempre più verso la connessione globale tra persone, oggetti e servizi, in una complessa rete di comunicazioni, le caratteristiche e le funzioni degli strumenti digitali (sempre più veloci, personalizzabili, "smart") possono avere un impatto particolarmente profondo.

In buona sostanza, in qualità di utenti, la nostra stessa capacità di compiere scelte consapevoli è inevitabilmente condizionata dal modo in cui la tecnologia che utilizziamo viene progettata e presentata.

E il caso della sanzione a Google risulta esemplare della diffusione di una **maggiore consapevolezza della necessità che ogni utente sia messo nelle reali condizioni di poter esercitare un libero controllo sulle proprie informazioni**.

Le condizioni che determinano la libertà di scelta, tuttavia, non sono sempre nette o facilmente definibili, e analizzando la relazione tra comportamento umano e tecnologia, si evince come i concetti di trasparenza e libero controllo rivelino invece una serie di aspetti particolarmente complessi.

È proprio questo il tema centrale di una recente pubblicazione del CNIL intitolata "La forma delle scelte", che entra nel merito delle componenti che giocano un ruolo nell'interazione tra psicologia e tecnologia digitale.

I diversi modi in cui questi aspetti si influenzano vicendevolmente si esprime in particolare attraverso l'interfaccia degli strumenti digitali. A questo proposito, l'articolo 25 del GDPR sottolinea l'importanza di permettere una partecipazione attiva degli interessati nella protezione della loro privacy. Ovviamente, anche prima dell'avvento del digitale o delle regolamentazioni sui trattamenti di dati, il settore del commercio ha sviluppato e utilizzato strategie volte a influenzare i comportamenti di acquisto. Va tuttavia messo in evidenza che l'impatto di una progettazione ingannevole o artificiosa applicata alle interfacce dei servizi digitali (in virtù della loro velocità, della loro personalizzazione, della loro capillarità), può essere molto più pervasivo di quanto il mercato ci abbia abituati fino ad oggi. Anche per questo motivo, il GDPR prevede che i titolari del trattamento adottino politiche e attuino misure di protezione fin dalla progettazione e per impostazione predefinita, quali ridurre al minimo i trattamenti, pseudonimizzare i dati personali ogniqualvolta sia possibile, offrire un'effettiva trasparenza che garantisca il diritto degli interessati di controllare il trattamento dei propri dati.

LA TRASPARENZA COME SCELTA STRATEGICA

La decisione della CNIL nei confronti di Google ci impone una riflessione sulla natura bivalente della tecnologia, la quale, se per certi versi può dar vita a scenari insidiosi per gli utenti, d'altra parte può rafforzare la percezione di affidabilità di un'azienda, a condizione che proprio quegli elementi di insidia siano evitati per valorizzare la trasparenza.

L'opacità e la confusione delle informazioni possono essere determinate da un'architettura dei siti internet e degli applicativi in cui le informazioni sui dati personali sono difficilmente accessibili, o addirittura ingannevoli, e comunque non in grado di offrire una corretta percezione della natura e del volume dei dati raccolti dal titolare.

Ne *La forma delle scelte* vengono indicate una serie di "cattive prassi" che ogni designer dovrebbe evitare, per far sì che il suo servizio possa considerarsi trasparente e, di conseguenza, che il trattamento dei dati personali possa ritenersi lecito.

Non sarà difficile per il lettore riconoscere, nella tabella riportata sotto, anche alcuni esempi affini a quanto già descritto sulla sanzione rivolta a Google.

PRATICHE DA EVITARE NELLA PROGETTAZIONE DELL'INTERFACCIA DI UN SERVIZIO DIGITALE

FINALITÀ DELLA PRATICA	ESEMPI
Spingere l'individuo ad accettare la condivisione di una maggior quantità di dati rispetto al necessario	• Richiedere informazioni aggiuntive durante fasi in cui gli utenti sono sotto pressione o desiderano concludere il processo senza analizzare tutte le informazioni; • Fingere che la raccolta di un determinato dato sia necessaria per il servizio desiderato, mentre sarà utilizzata per altro; • Richiedere alcuni dati aggiuntivi e non necessari con la falsa promessa che saranno mantenuti invisibili e sotto il controllo dell'utente; • Vincolare l'accesso a un servizio al conferimento di un dato (come l'email per accedere a un articolo) senza specificare che il dato in questione sarà utilizzato per altri scopi (come l'invio di newsletter); • Utilizzare l'argomento del "miglioramento dell'esperienza" per spingere l'utente a condividere dati non necessari; • Preselezionare le opzioni di condivisione delle informazioni.

FINALITÀ DELLA PRATICA	ESEMPI
Influenzare il consenso	• Scrivere una domanda in modo che una lettura rapida possa produrre l'opposto di ciò che ci si aspetta di ottenere, ad esempio tramite l'uso di doppie negazioni; • Chiedere il consenso in un momento in cui l'utente si trova evidentemente in uno stato di debolezza, fretta o impazienza; • Distrarre l'utente attirando la sua attenzione sulla conferma al consenso e nascondendo o rendendo difficilmente fruibili le altre informazioni utili; • Modificare la formulazione delle opzioni per rendere difficile all'utente adottare una routine; • Utilizzare un codice grafico compreso universalmente in un senso contrario creando confusione (come per esempio inserire all'interno di una pagina non sicura l'immagine di un lucchetto).
Limitare le azioni volte alla protezione dei dati personali	• Vincolare l'accesso a un servizio alla creazione di un account anche quando non è assolutamente necessario per l'utilizzo del servizio; • Rendere semplice accettare tutte le condizioni di trattamento e rendere invece complesso il percorso di chi vuole rifiutare alcuni termini e personalizzare il trattamento dei dati, mettendolo di fronte ad un'infinità di "per saperne di più" e di barre di contaminazione; • Inserire spesso incitazioni di condivisione di dati personali durante la navigazione sul sito; • Rendere le informazioni più dettagliate talmente complicate da spingere l'utente ad abbandonare la lettura e la comprensione.
Dirottare l'utente	• Fare in modo che un parametro o una scelta effettuata da un individuo produca un risultato diverso da quello desiderato, come per esempio dare un valore d'accettazione a un pulsante su cui è disegnata una croce; • Utilizzare, su un servizio terzo, lo stesso stile e lo stesso design del sito sul quale l'interessato stava navigando, per fare credere a quest'ultimo che ci sia una continuità nella navigazione (ad esempio, un sito di noleggio auto che si aggiunge al processo di acquisto di un biglietto aereo); • Inserire pubblicità all'interno di altri contenuti o elementi, in modo tale da spingere l'interessato a cliccarci sopra senza sapere che si tratta effettivamente di una pubblicità.

Il documento della CNIL sul design delle interfacce digitali risulta quindi uno strumento particolarmente utile per comprendere quali possano essere le pratiche che, seppur in certi casi ancora molto diffuse, violano il Regolamento 2016/679.

Al tempo stesso, però, questa analisi può aiutare a studiare strategie che siano in grado di attuare concretamente il principio di trasparenza, tramutando l'insidiosità del mondo digitale in un valore aggiunto per la propria compliance e, quindi, per la propria credibilità nei confronti dell'utente finale. La tecnologia, infatti, può essere sfruttata a proprio vantaggio prendendo ciò che è funzionale al proprio obiettivo: essere chiari rispetto al trattamento di dati che si ha intenzione di effettuare.

Tutto ciò per due motivi essenziali: **rispettare la normativa privacy e di conseguenza non incorrere in considerevoli sanzioni ma, soprattutto, rendere trasparenza e affidabilità un punto di forza per il proprio business**.

Proprio in virtù della crescente consapevolezza sull'importanza della tutela dei dati personali, risulterà sempre più importante saper generare un clima di fiducia che consenta lo sviluppo dell'economia digitale in tutto il mercato interno (Considerando 7 del GDPR).

È qui che il lavoro di chi progetta il design delle interfacce digitali deve intervenire per produrre l'indispensabile affidabilità agli occhi degli utenti.

Questi ultimi, ormai disincantati da una realtà che ha portato alla luce vicende sconcertanti come quella di Cambridge Analytica, valutano sempre più spesso, aiutati da sempre maggiori conoscenze, i servizi che gli vengono offerti proprio in base alle richieste di condivisione dei dati e al modo con cui il trattamento viene giustificato.

Tale realtà è da prendere in considerazione se si vuole creare un servizio non solo che rispetti la normativa privacy, evitando di conseguenza di incorrere in ingenti sanzioni, **ma che sia anche attraente per la sua trasparenza e la sua chiarezza**, valori ormai imprescindibili in una società sempre più consapevole.

Fonti:

CNIL "La forma delle scelte"

CNIL "Deliberation de la formation restreinte N. SAN 2019-001 du 21 janvier 2019