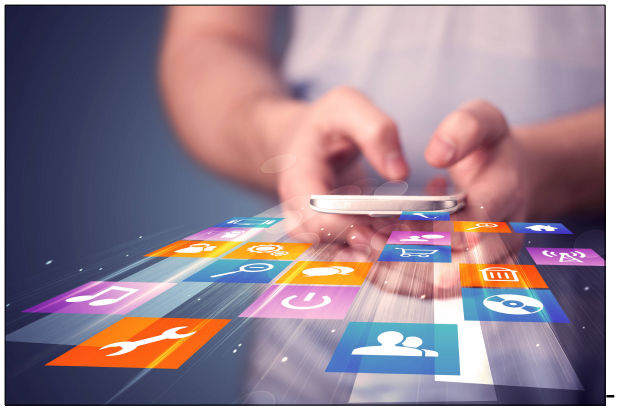
Smartphone: spegni il microfono, accendi la privacy - I suggerimenti del Garante

I sensori degli smartphone - e in particolare i microfoni - possono rimanere attivi anche quando non stiamo utilizzando il nostro dispositivo. In questo modo potrebbero essere utilizzati per raccogliere informazioni utilizzabili per diverse finalità anche da terzi: ad esempio per attività di marketing.

Quello delle app che, tra le autorizzazioni di accesso richieste al momento dell'installazione, inseriscono anche l'utilizzo del microfono, è un fenomeno diffuso. Spesso, come utenti, concediamo questi permessi senza pensarci troppo e senza informarci sufficientemente sull'uso che verrà fatto dei nostri dati.

Il Garante ha avviato un'indagine sulle app più scaricate per verificare se acquisiscono dati attraverso il microfono dei nostri smartphone anche quando non lo utilizziamo.

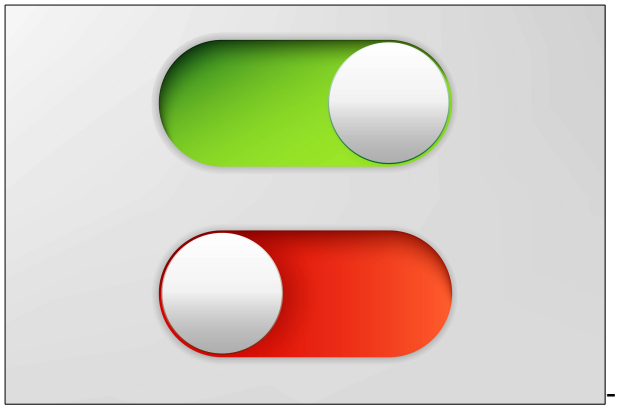
Poichè la prima linea di difesa della nostra privacy è sempre la consapevolezza, se vogliamo provare ad evitare di essere esposti ad eventuali ascolti indiscreti, possiamo adottare alcune semplici ma importanti accortezze.



- Innanzitutto, possiamo valutare di **limitare il numero di app sul nostro smartphone**, magari decidendo di installare solo quelle che consideriamo davvero utili e/o indispensabili per le nostre necessità quotidiane. Più app installiamo, infatti, maggiore sarà la quantità di dati che verranno raccolti, trattati e potenzialmente diffusi. E non tutte le app garantiscono gli stessi standard di sicurezza e protezione della privacy.

- Una app può richiedere l'**autorizzazione ad accedere a vari sensori e funzionalità** (fotocamera, microfono, geolocalizzazione, ecc.) **e ai nostri dati** (archivio immagini, rubrica, calendario, ecc.). Prima di accettare, chiediamoci sempre se tale accesso è davvero utile e indispensabile per l'utilizzo che faremo della app, oppure se è meglio evitare.

- Se decidiamo di concedere l'accesso da parte di una app ai sensori e funzionalità del nostro smartphone (fotocamera, microfono, geolocalizzazione, ecc.) e ai dati che contiene (archivio immagini, rubrica, calendario, ecc.), **leggiamo sempre PRIMA con attenzione l'informativa sul trattamento dei dati personali**, per capire, ad esempio, quali e quanti dati potranno essere raccolti, come potranno essere utilizzati, per quali fini, da chi.



- Anche quando abbiamo già concesso alle app l'autorizzazione per l'accesso ai sensori, alle funzionalità e ai dati del nostro smartphone, possiamo comunque decidere di **disattivare il permesso di utilizzo**, magari lasciando attive le autorizzazioni solo per quelle applicazioni per cui possono essere indispensabili o quasi (ad esempio, il microfono per la messaggistica, se si vogliono inviare anche messaggi vocali).

COME POSSO DISATTIVARE LE AUTORIZZAZIONI DI ACCESSO AL MICROFONO DA PARTE DELLE APP INSTALLATE SUL MIO SMARTPHONE?

DISATTIVARE L'USO DEI MICROFONI DA PARTE DELLE APP INSTALLATE SU SMARTPHONE CON SISTEMA OPERATIVO iOS

• Cliccare il pulsante "IMPOSTAZIONI"

• Cliccare il pulsante "PRIVACY"

• Cliccare "MICROFONO"

• Scegliere le app per cui l'uso del microfono non è essenziale e disattivarlo

DISATTIVARE L'USO DEI MICROFONI DA PARTE DELLE APP SUGLI SMARTPHONE CON SISTEMA OPERATIVO ANDROID

• Cliccare il pulsante "IMPOSTAZIONI"

• Cliccare il pulsante "PRIVACY"

• Cliccare "GESTISCI AUTORIZZAZIONI"

• Cliccare "MICROFONO"

• Nella lista delle app, scegliere quelle per cui l'uso del microfono non è ritenuto essenziale e disattivare il consenso all'utilizzo.

Per ulteriori informazioni o per segnalazioni al Garante: **urp@gpdp.it**

Per approfondimenti su app e protezione dei dati, vedi anche : www.gpdp.it/temi/app

Per approfondimenti su smartphone e protezione dei dati, vedi anche:
www.gpdp.it/temi/smartphone/fatti-smart