

Non ti stanno ascoltando. Ti stanno prevedendo!

L'idea del microfono-spia è intuitiva e teatrale. Il problema è che la realtà, per chi fa pubblicità e profilazione, è più semplice, più economica e spesso più invasiva.

Autore: Dario Buscaglia • Lettura: 10 min • Data: 02/02/2026

Succede così: parli di modellini di aeroplani, apri un social, e ti compare una pubblicità di modellini. Il cervello fa due più due e arriva alla spiegazione più cinematografica: “ci stanno ascoltando”.

È una spiegazione potente perché è semplice, perché dà un colpevole chiaro (il microfono) e perché assomiglia a un thriller. Ma proprio per questo è anche una trappola mentale: scambia una coincidenza plausibile per una prova.



Figura — Repertorio: due amici al bar, smartphone sul tavolo.

La pubblicità “che sembra leggerti nel pensiero” non nasce nel vuoto. I sistemi pubblicitari moderni vivono di segnali piccoli e numerosi: cosa hai cercato, quanto

tempo ti sei fermato su un contenuto, quali siti hanno un pixel pubblicitario, quali app condividono identificatori, dove ti trovi, che dispositivo usi, con chi ti muovi, a che ora. Non serve la frase detta a voce: spesso basta tutto il resto.

C'è anche un effetto psicologico banale ma forte: quando un tema entra nella tua giornata (ne parli, lo vedi, lo cerchi), inizi a notarlo ovunque. Se in più l'annuncio arriva davvero, lo ricordi molto più di tutte le volte in cui non è arrivato.

Perché “ascoltarci” non conviene (tecnicamente ed economicamente)

Immagina una piattaforma che attiva il microfono a tua insaputa, registra conversazioni, le manda ai server, le trascrive, capisce contesto e intenzione, e poi collega tutto a un profilo pubblicitario. Non è impossibile in assoluto, ma è una strategia pessima se l'obiettivo è vendere annunci.

Il motivo non è morale: è industriale. Su molti telefoni esistono indicatori visibili quando microfono o fotocamera sono in uso, e permessi specifici da concedere alle app. Se un'app “ascoltasse” in modo continuo o frequente, aumenterebbero i segnali osservabili: consumo anomalo di batteria, traffico dati, indicatori di utilizzo. È il tipo di comportamento che genera segnalazioni, analisi, cause legali e una crisi di reputazione.

I dati audio sono pesanti e costosi. Anche un audio “decente” produce decine o centinaia di megabyte ogni ora, prima ancora di parlare di invio, archiviazione e analisi. Moltiplica per milioni di utenti e capisci perché, dal punto di vista economico, è un'idea fragile e sproporzionata.

Il parlato è un dato sporco: rumore, ambiguità, ironia, contesti incompleti. La pubblicità non ha bisogno di capire perfettamente cosa dici: le basta una probabilità di interesse. E quella probabilità spesso la ottiene meglio dai comportamenti reali (clic, visite, acquisti, app installate, spostamenti).

Questo non significa che lo smartphone non possa essere compromesso. Malware e spyware esistono, e in alcuni casi possono intercettare microfono e comunicazioni. Ma quello è un altro film: criminalità o sorveglianza mirata, non un modello di business pubblicitario che deve funzionare in massa.

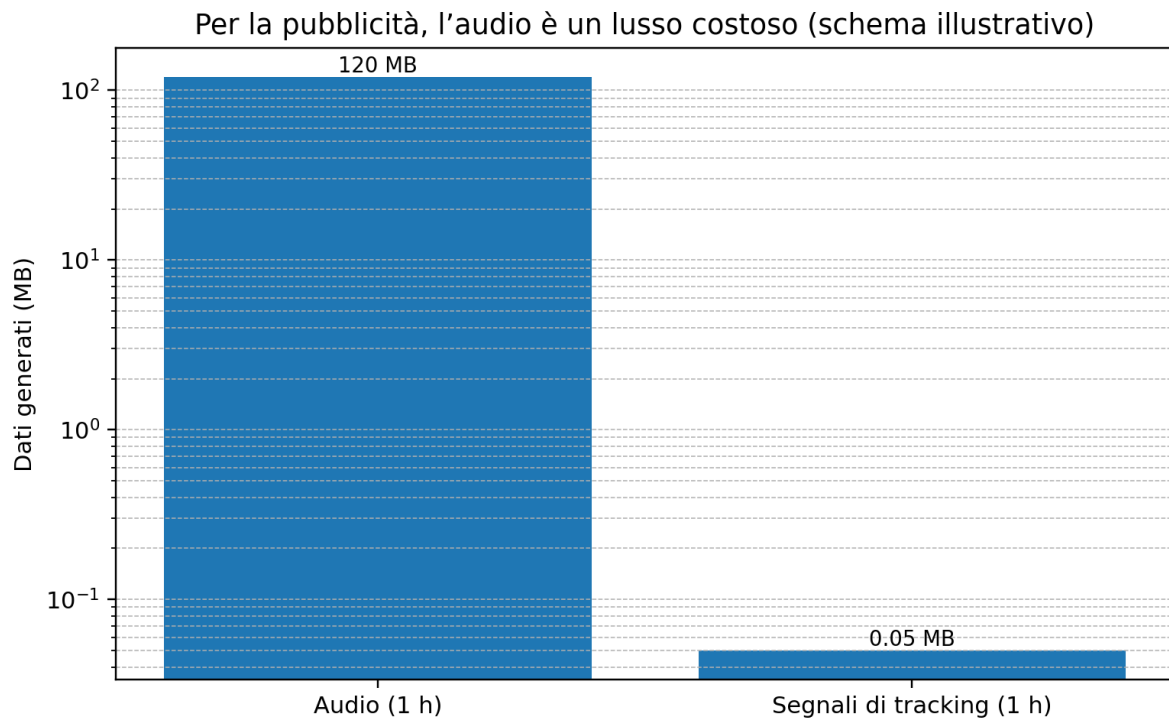


Figura 1 — Ordine di grandezza: audio vs segnali di tracking (scala logaritmica).

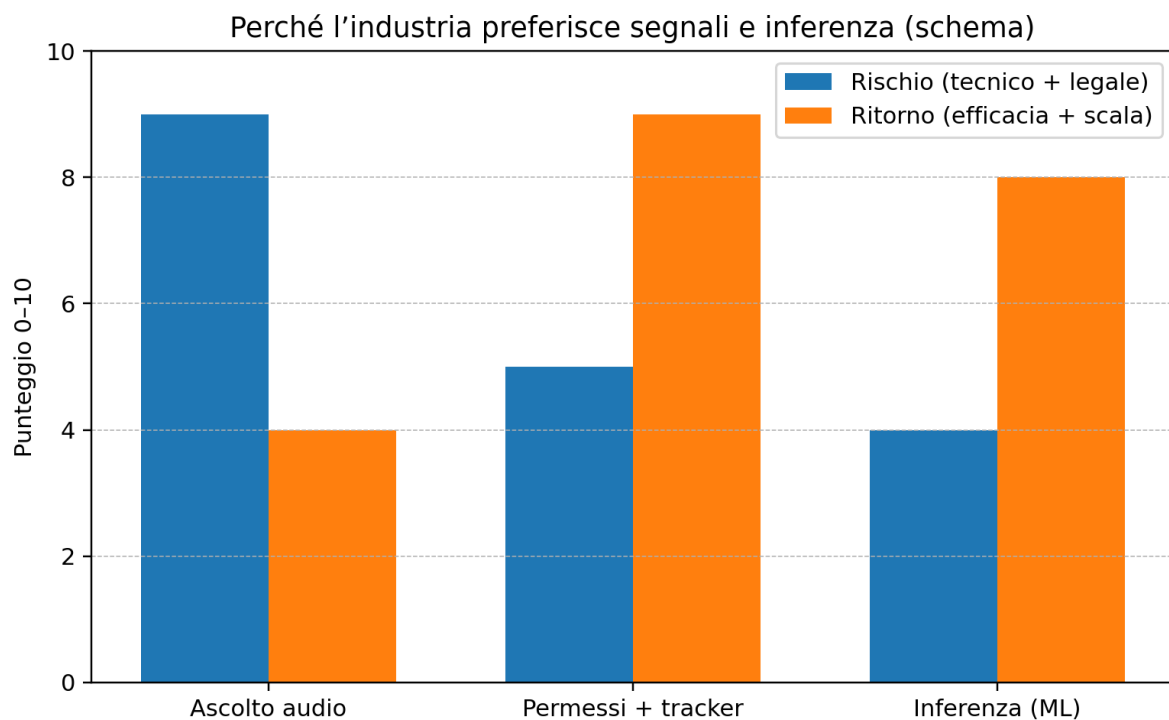


Figura 2 — Schema: rischio vs ritorno per diverse strategie (punteggi illustrativi).

La cosa più inquietante non è l'ascolto: è l'inferenza

La parte meno cinematografica e più inquietante è questa: molte aziende non hanno bisogno di ascoltare perché, in pratica, ti "indovinano". Non indovinano con magia: indovinano con statistica.

Se tante persone che comprano modellini di aeroplani fanno anche altre cose (seguono certe pagine, visitano certi siti, passano in certi negozi, usano certe app), allora il sistema impara correlazioni. Non serve sapere che hai detto “modellini” a voce: basta che tu assomigli abbastanza a chi li compra.

Il punto delicato è che questi indizi spesso viaggiano in un ecosistema di intermediari: SDK pubblicitari nelle app, pixel, identificatori, e aste in tempo reale (real-time bidding). Quando apri una pagina o un’app, può partire una richiesta che più soggetti ricevono per fare un’offerta in millisecondi.

Se l’audio-spia fa paura perché “entra” in casa, l’ecosistema della profilazione fa paura perché è distribuito: non è un solo orecchio, è un mercato. E quando i segnali includono posizione o contesti sensibili, il rischio non è solo “mi mostrano annunci”, ma “qualcuno può ricostruire abitudini e routine”.

La conclusione non è paranoia: è lucidità. Se vuoi proteggerti, spesso ha più senso guardare a permessi, localizzazione, tracker, consensi pubblicitari e configurazioni del dispositivo, piuttosto che immaginare un microfono sempre acceso come spiegazione universale.

Fonti (selezione)

Apple — Indicatori arancione/verde per microfono e fotocamera (iOS)

<https://support.apple.com/en-jo/108331>

FTC — Azione contro Mobilewalla e dati sensibili (location/RTB)

<https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-mobilewalla-collecting-selling-sensitive-location-data>

FTC Tech Blog — Real-time bidding nel caso Mobilewalla

<https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/12/unpacking-real-time-bidding-through-ftcs-case-mobilewalla>

IAB Tech Lab — OpenRTB (standard)

<https://iabtechlab.com/standards/openrtb/>

IAB Tech Lab — OpenRTB 2.6 (PDF)

https://iabtechlab.com/wp-content/uploads/2022/04/OpenRTB-2-6_FINAL.pdf

EFF — Commercial surveillance e RTB (contesto)

<https://www.eff.org/deeplinks/2024/09/ftc-report-confirms-commercial-surveillance-out-control>

Reuters — Data broker e dati sensibili (contesto)

<https://www.reuters.com/technology/cybersecurity/ftc-settles-with-data-brokers-that-sold-political-pregnancy-info-2024-12-03/>