Analisi · 16 maggio 2026

← Precedente·Successivo →

Crittografare non significa essere privati: ciò che i metadati dicono di te

Il contenuto crittografato e i metadati visibili sono due cose distinte. Quando un servizio parla di "crittografia end-to-end", racconta solo metà della storia.

Il lucchetto che non protegge tutto

Gran parte dei servizi di messaggistica attuali pubblicizzano la crittografia end-to-end. Ed è vero: il contenuto dei messaggi viaggia crittografato, in modo tale che nessuno lungo il percorso — nemmeno il fornitore del servizio — possa leggere il testo mentre è in transito. In questo senso, l'affermazione è esatta.

Il problema è che il contenuto è solo una parte della storia. Anche se nessuno può leggere ciò che dici, il servizio conosce altre cose con altissima precisione: con chi parli, a che ora, con quale frequenza, da quale posizione approssimativa, su quale dispositivo, quanti messaggi invii e quanti ne ricevi, quale numero di file condividi. Tutto questo si chiama metadati. E i metadati raccontano, in molti casi, quasi quanto il messaggio stesso.

Ciò che i metadati rivelano

Non serve leggere un messaggio per sapere molte cose. Se una persona chiama o scrive a un oncologo ogni martedì alle nove del mattino per sei mesi, non è necessario ascoltare la conversazione per intuire cosa stia succedendo. Se due persone si scambiano cento messaggi al giorno e improvvisamente smettono di farlo, non serve leggerne nessuno per capire cosa sia accaduto. Se un consulente fiscale riceve venti messaggi consecutivi dallo stesso cliente la sera prima di una chiusura trimestrale, il pattern parla da sé.

I metadati rivelano pattern di comportamento: chi si relaziona con chi, quali orari ha ogni persona, quando è sveglia, quando dorme, quando viaggia, quali clienti sono più attivi, quali relazioni professionali sono più intense. Un server che raccoglie metadati può costruire un profilo dettagliato della vita personale e professionale di qualsiasi utente senza aver mai letto una sola parola di ciò che scrive.

C'è un esempio storico che illustra questo con durezza. L'ex direttore della NSA, Michael Hayden, lo formulò senza mezzi termini nel 2014: *"We kill people based on metadata"*. L'affermazione si riferiva a operazioni militari statunitensi contro obiettivi identificati unicamente dai loro pattern di comunicazione. Nemmeno un messaggio letto. Solo il grafo dei contatti e gli orari.

Il fatto che un servizio raccolga metadati non implica che li userà contro i propri utenti. Implica che ne ha la capacità e che un terzo con accesso a quei dati — per ordine del tribunale, per violazione della sicurezza o per vendita a terzi se le condizioni del servizio lo consentono — ha anch'egli tale capacità.

L'accesso alla rubrica

Un altro vettore che passa quasi inosservato: la lista dei contatti. Gran parte dei servizi di messaggistica richiedono l'accesso alla rubrica del telefono al momento della registrazione. Caricano tutti i numeri sul proprio server per mostrare chi altro usa il servizio. Da quel momento in poi, l'azienda ha una mappa completa delle relazioni dell'utente, anche se quest'ultimo non ha mai scritto un solo messaggio a nessuno.

Per un professionista con segreto professionale — avvocato, medico, psicologo, consulente — quella mappa contiene clienti. Se la rubrica è stata caricata su un server di terzi, i nomi dei clienti si trovano in un'infrastruttura la cui giurisdizione e le cui politiche non sono controllate dal professionista. Il segreto professionale non si rompe il giorno in cui qualcuno trapela una conversazione: si è rotto molto prima, al momento di accettare il caricamento.

La differenza tra crittografare e non raccogliere

Crittografare significa proteggere il contenuto. Essere privati significa non raccogliere ciò che non serve. Sono cose diverse e la differenza è operativamente critica. Un servizio può crittografare tutti i messaggi alla perfezione e, allo stesso tempo, sapere quasi tutto sui suoi utenti attraverso i metadati. Le due cose sono perfettamente compatibili. Infatti, è il modello di business dominante nel settore.

La domanda corretta per valutare la reale privacy di un servizio non è *"crittografa il contenuto?"*. A questa domanda è stata data risposta anni fa. La domanda corretta è: *"quali metadati genera e dove vengono archiviati?"*. E, soprattutto: *"quali metadati non ha bisogno di generare?"*.

Un'architettura che riduce al minimo i metadati per progettazione — non per promessa, non per politica interna — è strutturalmente più privata di un'architettura che li raccoglie e li crittografa. Perché i dati che non esistono non possono essere trapelati, né venduti, né consegnati a un ordine del tribunale, né persi in una violazione.

Per il lettore professionale

Se la tua attività professionale comporta segreto, riservatezza o semplicemente rispetto per le informazioni di terzi, conviene porsi le domande in questo ordine:

1. L'applicazione che uso per comunicare crittografa il contenuto? (Probabilmente sì.)
2. Crittografa i metadati? (Probabilmente no.)
3. Genera metadati di cui *non ha bisogno* per funzionare? (Quasi certamente sì.)
4. Dove sono archiviati questi metadati e sotto quale giurisdizione? (Probabilmente al di fuori dello Spazio Economico Europeo.)
5. Il mio cliente o paziente sa che i suoi dati sono lì?

L'ultima domanda è quella scomoda. Perché la risposta onesta, nella maggior parte dei casi, è no.

Questo articolo è il primo di una serie sul reale funzionamento degli strumenti di comunicazione professionale. Le prossime uscite riguarderanno la conformità al GDPR nella messaggistica e il concetto di segreto professionale nell'era digitale.

Fonti e letture aggiuntive

- Hayden, M. — Dichiarazione alla Johns Hopkins University, 2014 ("We kill people based on metadata"). Trascrizioni pubbliche disponibili.
- GDPR (Regolamento UE 2016/679), artt. 4 e 5 — definizione di dati personali e principi del trattamento (i metadati sono dati personali).
- EDPS e EDPB — pareri sul trattamento dei dati relativi al traffico e dei metadati nelle comunicazioni elettroniche (Direttiva ePrivacy).

← PrecedenteUna breve storia del sigillo di ceralaccaSuccessivo →Il segreto professionale nell'era digitale

Letture recenti

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Porta questo articolo dove ne hai bisogno.

↓ Markdown ↓ Testo semplice ↓ PDF

Il file viene scaricato sul tuo dispositivo. Da lì puoi salvarlo, importarlo in Solo2 o condividerlo come preferisci. Cuadernos non decide la destinazione per te.

Sigillo di cera · SHA-256 f030d0a5ccb7a59dc34e30ba7a803418ca48e841eb2b44d343cec58bdaee414a

Cuadernos Lacre · Una pubblicazione di Menzuri Gestión S.L. ·
scritta da R.Eugenio · a cura del team di Solo2.