Anàlisi · 16 de maig de 2026

← Anterior·Següent →

Xifrar no és ser privat: el que les metadades expliquen sobre tu

El contingut xifrat i les metadades visibles són dues coses distintes. Quan un servei diu "xifratge d'extrem a extrem", explica només mitja història.

El cadenat que no ho protegeix tot

Bona part dels serveis de missatgeria actuals anuncien xifratge d'extrem a extrem. I és cert: el contingut dels missatges viatja xifrat, de tal manera que ningú en el camí —ni tan sols el proveïdor del servei— pot llegir el text mentre està en trànsit. Fins aquí, l'afirmació és exacta.

El problema és que el contingut és només una part de la història. Encara que ningú pugui llegir el que dius, el servei sí que sap altres coses amb altíssima precisió: amb qui parles, a quina hora, amb quina freqüència, des de quina ubicació aproximada, en quin dispositiu, quants missatges envies i quants en reps, quin nombre d'arxius comparteixes. A tot això se'n diu metadades. I les metadades expliquen, en molts casos, gairebé tant com el missatge en si.

El que les metadades revelen

No cal llegir un missatge per saber moltes coses. Si una persona truca o escriu a un oncòleg cada dimarts a les nou del matí durant sis mesos, no és necessari escoltar la conversa per intuir què està passant. Si dues persones s'intercanvien cent missatges al dia i de cop deixen de fer-ho, no cal llegir-ne cap per entendre què ha passat. Si un assessor fiscal rep vint missatges seguits del mateix client la nit abans d'un tancament trimestral, el patró parla sol.

Les metadades revelen patrons de comportament: qui es relaciona amb qui, quins horaris té cada persona, quan està desperta, quan dorm, quan viatja, quins clients són més actius, quines relacions professionals són més intenses. Un servidor que recull metadades pot construir un perfil detallat de la vida personal i professional de qualsevol usuari sense haver llegit mai ni una sola paraula del que escriu.

Hi ha un exemple històric que il·lustra això amb duresa. L'antic director de la NSA, Michael Hayden, ho va formular sense matisos el 2014: *"We kill people based on metadata"*. L'afirmació es referia a operacions militars estatunidenques contra objectius identificats únicament pels seus patrons de comunicació. Ni un sol missatge llegit. Només el graf de contactes i els horaris.

Que un servei reculli metadades no implica que hagi d'usar-les contra els seus usuaris. Implica que té la capacitat de fer-ho, i que un tercer amb accés a aquestes dades —per ordre judicial, per bretxa de seguretat, o per venda a tercers si les condicions de servei ho permeten— també la té.

L'accés a l'agenda

Un altre vector que passa gairebé desapercebut: la llista de contactes. Bona part dels serveis de missatgeria demanen accés a l'agenda del telèfon en registrar-se. Pugen tots els números al seu servidor per mostrar qui més usa el servei. A partir d'aquell moment, l'empresa té un mapa complet de les relacions de l'usuari, encara que aquest no hagi escrit mai cap missatge a ningú.

Per a un professional amb secret professional —advocat, metge, psicòleg, assessor— aquest mapa conté clients. Si l'agenda s'ha pujat a un servidor de tercers, els noms dels clients estan en una infraestructura la jurisdicció i polítiques de la qual el professional no controla. El secret professional no es trenca el dia que algú filtra una conversa: es va trencar molt abans, en el moment d'acceptar la pujada.

La diferència entre xifrar i no recollir

Xifrar és protegir el contingut. Ser privat és no recollir el que no es necessita. Són coses distintes, i la diferència és operativament crítica. Un servei pot xifrar tots els missatges a la perfecció i, alhora, saber gairebé tot sobre els seus usuaris a través de les metadades. Les dues coses són perfectament compatibles. De fet, és el model de negoci dominant en el sector.

La pregunta correcta per avaluar la privadesa real d'un servei no és *"¿xifra el contingut?"*. Aquesta pregunta es dóna per resposta fa anys. La pregunta correcta és: *"¿quines metadades genera i on s'emmagatzemen?"*. I, sobretot: *"¿quines metadades no necessita generar?"*.

Una arquitectura que minimitza les metadades per disseny —no per promesa, no per política interna— és estructuralment més privada que una arquitectura que les recull i les xifra. Perquè les dades que no existeixen no es poden filtrar, ni vendre, ni lliurar a una ordre judicial, ni perdre en una bretxa.

Per al lector professional

Si la teva activitat professional implica secret, confidencialitat, o simplement respecte a la informació de tercers, convé plantejar-se les preguntes en aquest ordre:

1. ¿L'aplicació que uso per comunicar-me xifra el contingut? (Probablement sí.)
2. ¿Xifra les metadades? (Probablement no.)
3. ¿Genera metadades que *no necessita* per funcionar? (Gairebé segur que sí.)
4. ¿On estan emmagatzemades aquestes metadades i sota quina jurisdicció? (Probablement fora de l'Espai Econòmic Europeu.)
5. ¿El meu client o pacient sap que les seves dades són allà?

L'última pregunta és la incòmoda. Perquè la resposta honesta, en la majoria dels casos, és que no.

Aquest article és el primer d'una sèrie sobre el funcionament real de les eines de comunicació professional. Properes entregues abordaran el compliment RGPD en missatgeria i el concepte de secret professional en l'era digital.

Fonts i lectura addicional

- Hayden, M. — Declaració a Johns Hopkins University, 2014 ("We kill people based on metadata"). Transcripcions públiques disponibles.
- RGPD (Reglament UE 2016/679), arts. 4 i 5 — definició de dades personals i principis de tractament (les metadades sí que són dades personals).
- EDPS i EDPB — opinions sobre tractament de dades de trànsit i metadades en comunicacions electròniques (Directiva ePrivacy).

← AnteriorUna breu història del lacreSegüent →El secret professional en l'era digital

Lectures recents

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Emporta't aquest article on el necessitis.

↓ Markdown ↓ Text pla ↓ PDF

L'arxiu es descarrega al teu dispositiu. Des d'allà pots guardar-lo, importar-lo a Solo2, o compartir-lo on vulguis. Cuadernos no decideix el destí per tu.

Segell de lacre · SHA-256 3a1b0af5944ab40747798523b6a4b34b6642a1448b412e75c9a785ca7bd28967

Cuadernos Lacre · Una publicació de Menzuri Gestión S.L. ·
escrita per R.Eugenio · editada per l'equip de Solo2.