Análisis · 16 de mayo de 2026

← Anterior·Siguiente →

Cifrar no es ser privado: lo que los metadatos cuentan sobre ti

El contenido cifrado y los metadatos visibles son dos cosas distintas. Cuando un servicio dice "cifrado de extremo a extremo", cuenta solo media historia.

El candado que no lo protege todo

Buena parte de los servicios de mensajería actuales anuncian cifrado de extremo a extremo. Y es cierto: el contenido de los mensajes viaja cifrado, de tal modo que nadie en el camino —ni siquiera el proveedor del servicio— puede leer el texto mientras está en tránsito. Hasta ahí, la afirmación es exacta.

El problema es que el contenido es solo una parte de la historia. Aunque nadie pueda leer lo que dices, el servicio sí sabe otras cosas con altísima precisión: con quién hablas, a qué hora, con qué frecuencia, desde qué ubicación aproximada, en qué dispositivo, cuántos mensajes envías y cuántos recibes, qué número de archivos compartes. A todo eso se le llama metadatos. Y los metadatos cuentan, en muchos casos, casi tanto como el mensaje en sí.

Lo que los metadatos revelan

No hace falta leer un mensaje para saber muchas cosas. Si una persona llama o escribe a un oncólogo todos los martes a las nueve de la mañana durante seis meses, no es necesario escuchar la conversación para intuir qué está pasando. Si dos personas se intercambian cien mensajes al día y de repente dejan de hacerlo, no hace falta leer ninguno para entender qué ha ocurrido. Si un asesor fiscal recibe veinte mensajes seguidos del mismo cliente la noche antes de un cierre trimestral, el patrón habla solo.

Los metadatos revelan patrones de comportamiento: quién se relaciona con quién, qué horarios tiene cada persona, cuándo está despierta, cuándo duerme, cuándo viaja, qué clientes son más activos, qué relaciones profesionales son más intensas. Un servidor que recoge metadatos puede construir un perfil detallado de la vida personal y profesional de cualquier usuario sin haber leído jamás una sola palabra de lo que escribe.

Hay un ejemplo histórico que ilustra esto con dureza. El antiguo director de la NSA, Michael Hayden, lo formuló sin matices en 2014: *"We kill people based on metadata"*. La afirmación se refería a operaciones militares estadounidenses contra objetivos identificados únicamente por sus patrones de comunicación. Ni un solo mensaje leído. Solo el grafo de contactos y los horarios.

Que un servicio recoja metadatos no implica que vaya a usarlos contra sus usuarios. Implica que tiene la capacidad de hacerlo, y que un tercero con acceso a esos datos —por orden judicial, por brecha de seguridad, o por venta a terceros si las condiciones de servicio lo permiten— también la tiene.

El acceso a la agenda

Otro vector que pasa casi desapercibido: la lista de contactos. Buena parte de los servicios de mensajería piden acceso a la agenda del teléfono al registrarse. Suben todos los números a su servidor para mostrar quién más usa el servicio. A partir de ese momento, la empresa tiene un mapa completo de las relaciones del usuario, aunque este no haya escrito jamás un solo mensaje a nadie.

Para un profesional con secreto profesional —abogado, médico, psicólogo, asesor— ese mapa contiene clientes. Si la agenda se ha subido a un servidor de terceros, los nombres de los clientes están en una infraestructura cuya jurisdicción y políticas el profesional no controla. El secreto profesional no se rompe el día que alguien filtra una conversación: se rompió mucho antes, en el momento de aceptar la subida.

La diferencia entre cifrar y no recoger

Cifrar es proteger el contenido. Ser privado es no recoger lo que no se necesita. Son cosas distintas, y la diferencia es operativamente crítica. Un servicio puede cifrar todos los mensajes a la perfección y, al mismo tiempo, saber casi todo sobre sus usuarios a través de los metadatos. Las dos cosas son perfectamente compatibles. De hecho, es el modelo de negocio dominante en el sector.

La pregunta correcta para evaluar la privacidad real de un servicio no es *"¿cifra el contenido?"*. Esa pregunta se da por respondida hace años. La pregunta correcta es: *"¿qué metadatos genera y dónde se almacenan?"*. Y, sobre todo: *"¿qué metadatos no necesita generar?"*.

Una arquitectura que minimiza los metadatos por diseño —no por promesa, no por política interna— es estructuralmente más privada que una arquitectura que los recoge y los cifra. Porque los datos que no existen no se pueden filtrar, ni vender, ni entregar a una orden judicial, ni perder en una brecha.

Para el lector profesional

Si tu actividad profesional implica secreto, confidencialidad, o simplemente respeto a la información de terceros, conviene plantearse las preguntas en este orden:

1. ¿La aplicación que uso para comunicarme cifra el contenido? (Probablemente sí.)
2. ¿Cifra los metadatos? (Probablemente no.)
3. ¿Genera metadatos que *no necesita* para funcionar? (Casi seguro que sí.)
4. ¿Dónde están almacenados esos metadatos y bajo qué jurisdicción? (Probablemente fuera del Espacio Económico Europeo.)
5. ¿Mi cliente o paciente sabe que sus datos están allí?

La última pregunta es la incómoda. Porque la respuesta honesta, en la mayoría de los casos, es que no.

Este artículo es el primero de una serie sobre el funcionamiento real de las herramientas de comunicación profesional. Próximas entregas abordarán el cumplimiento RGPD en mensajería y el concepto de secreto profesional en la era digital.

Fuentes y lectura adicional

- Hayden, M. — Declaración en Johns Hopkins University, 2014 ("We kill people based on metadata"). Transcripciones públicas disponibles.
- RGPD (Reglamento UE 2016/679), arts. 4 y 5 — definición de datos personales y principios de tratamiento (los metadatos sí son datos personales).
- EDPS y EDPB — opiniones sobre tratamiento de datos de tráfico y metadatos en comunicaciones electrónicas (Directiva ePrivacy).

← AnteriorUna breve historia del lacreSiguiente →El secreto profesional en la era digital

Lecturas recientes

- Análisis · 18 de mayo de 2026 Privacidad real vs aparente: las preguntas que conviene hacerse
- Análisis · 18 de mayo de 2026 Self-hosting como práctica profesional
- Concepto · 18 de mayo de 2026 Las 24 palabras: qué es una identidad criptográfica

Llévate este artículo donde lo necesites.

↓ Markdown ↓ Texto plano ↓ PDF

El archivo se descarga a tu dispositivo. Desde ahí puedes guardarlo, importarlo a Solo2, o compartirlo donde quieras. Cuadernos no decide el destino por ti.

Sello de lacre · SHA-256 0c3824292061bcbec788e5d2cea23cda0615f28449db96353c8dbb0d4418ac0e

Cuadernos Lacre · Una publicación de Menzuri Gestión S.L. ·
escrita por R.Eugenio · editada por el equipo de Solo2.