Análise · 16 de maio de 2026

← Anterior·Seguinte →

Cifrar non é ser privado: o que os metadatos contan sobre ti

O contido cifrado e os metadatos visibles son dúas cousas distintas. Cando un servizo di "cifrado de extremo a extremo", conta só media historia.

O cadeado que non o protexe todo

Boa parte dos servizos de mensaxería actuais anuncian cifrado de extremo a extremo. E é certo: o contido das mensaxes viaxa cifrado, de tal xeito que ninguén no camiño —nin sequera o provedor do servizo— pode ler o texto mentres está en tránsito. Ata aí, a afirmación é exacta.

O problema é que o contido é só unha parte da historia. Aínda que ninguén poida ler o que dis, o servizo si sabe outras cousas con altísima precisión: con quen falas, a que hora, con que frecuencia, desde que localización aproximada, en que dispositivo, cantas mensaxes envías e cantas recibes, que número de arquivos compartes. A todo iso chámaselle metadatos. E os metadatos contan, en moitos casos, case tanto como a mensaxe en si.

O que os metadatos revelan

Non fai falta ler unha mensaxe para saber moitas cousas. Se unha persoa chama ou escribe a un oncólogo todos os martes ás nove da mañá durante seis meses, non é necesario escoitar a conversa para intuír que está pasando. Se dúas persoas se intercambian cen mensaxes ao día e de súpeto deixan de facelo, non fai falta ler ningunha para entender que ocorreu. Se un asesor fiscal recibe vinte mensaxes seguidas do mesmo cliente a noite antes dun peche trimestral, o patrón fala só.

Os metadatos revelan patróns de comportamento: quen se relaciona con quen, que horarios ten cada persoa, cando está esperta, cando dorme, cando viaxa, que clientes son máis activos, que relacións profesionais son máis intensas. Un servidor que recolle metadatos pode construír un perfil detallado da vida persoal e profesional de calquera usuario sen ter lido xamais unha soa palabra do que escribe.

Hai un exemplo histórico que ilustra isto con dureza. O antigo director da NSA, Michael Hayden, formulouno sen matices en 2014: *"We kill people based on metadata"*. A afirmación referíase a operacións militares estadounidenses contra obxectivos identificados unicamente polos seus patróns de comunicación. Nin unha soa mensaxe lida. Só o grafo de contactos e os horarios.

Que un servizo recolla metadatos non implica que vaia usalos contra os seus usuarios. Implica que ten a capacidade de facelo, e que un terceiro con acceso a eses datos —por orde xudicial, por brecha de seguridade, ou por venda a terceiros se as condicións de servizo o permiten— tamén a ten.

O acceso á axenda

Outro vector que pasa case desapercibido: a lista de contactos. Boa parte dos servizos de mensaxería piden acceso á axenda do teléfono ao rexistrarse. Suben todos os números ao seu servidor para mostrar quen máis usa o servizo. A partir dese momento, a empresa ten un mapa completo das relacións do usuario, aínda que este non escribise xamais unha soa mensaxe a ninguén.

Para un profesional con segredo profesional —avogado, médico, psicólogo, asesor— ese mapa contén clientes. Se a axenda subiu a un servidor de terceiros, os nomes dos clientes están nunha infraestrutura cuxa xurisdición e políticas o profesional non controla. O segredo profesional non se rompe o día que alguén filtra unha conversa: rompeuse moito antes, no momento de aceptar a subida.

A diferenza entre cifrar e non recoller

Cifrar é protexer o contido. Ser privado é non recoller o que non se necesita. Son cousas distintas, e a diferenza é operativamente crítica. Un servizo pode cifrar todas as mensaxes á perfección e, ao mesmo tempo, saber case todo sobre os seus usuarios a través dos metadatos. As dúas cousas son perfectamente compatibles. De feito, é o modelo de negocio dominante no sector.

A pregunta correcta para avaliar a privacidade real dun servizo non é *"¿cifra o contido?"*. Esa pregunta dáse por respondida hai anos. La pregunta correcta é: *"¿que metadatos xera e onde se almacenan?"*. E, sobre todo: *"¿que metadatos non necesita xerar?"*.

Unha arquitectura que minimiza os metadatos por deseño —non por promesa, non por política interna— é estructuralmente máis privada que unha arquitectura que os recolle e os cifra. Porque os datos que non existen non se poden filtrar, nin vender, ni entregar a unha orde xudicial, nin perder nunha brecha.

Para o lector profesional

Se a túa actividade profesional implica segredo, confidencialidade, ou simplemente respecto á información de terceiros, convén plantexarse as preguntas nesta orde:

1. ¿A aplicación que uso para comunicarme cifra o contido? (Probablemente si.)
2. ¿Cifra os metadatos? (Probablemente non.)
3. ¿Xera metadatos que *non necesita* para funcionar? (Case seguro que si.)
4. ¿Onde están almacenados eses metadatos e baixo que xurisdición? (Probablemente fóra do Espazo Económico Europeo.)
5. ¿O meu cliente ou paciente sabe que os seus datos están alí?

A última pregunta é a incómoda. Porque a resposta honesta, na maioría dos casos, é que non.

Este artigo é o primeiro dunha serie sobre o funcionamento real das ferramentas de comunicación profesional. Próximas entregas abordarán o cumprimento RGPD en mensaxería e o concepto de segredo profesional na era dixital.

Fontes e lectura adicional

- Hayden, M. — Declaración en Johns Hopkins University, 2014 ("We kill people based on metadata"). Transcricións públicas dispoñibles.
- RGPD (Regulamento UE 2016/679), arts. 4 e 5 — definición de datos persoais e principios de tratamento (os metadatos si son datos persoais).
- EDPS e EDPB — opinións sobre tratamento de datos de tráfico e metadatos en comunicacións electrónicas (Directiva ePrivacy).

← AnteriorUnha breve historia do selo de lacreSeguinte →O segredo profesional na era dixital

Lecturas recentes

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Leva este artigo onde o necesites.

↓ Markdown ↓ Texto plano ↓ PDF

O arquivo descárgase no teu dispositivo. Desde aí podes gardalo, importalo a Solo2, o compartilo onde queiras. Cuadernos no decide o destino por ti.

Selo de lacre · SHA-256 9a1003539a2e8b221269ef3d2d0af0c6fd8d70078ebec340cf27272b4fec7070

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