Análise · 16 de maio de 2026

← Anterior·Seguinte →

Cifrar não é ser privado: o que os metadados contam sobre si

O conteúdo cifrado e os metadados visíveis são duas coisas distintas. Quando um serviço diz "criptografia de ponta a ponta", conta apenas metade da história.

O cadeado que não protege tudo

Grande parte dos serviços de mensagens atuais anunciam criptografia de ponta a ponta. E é verdade: o conteúdo das mensagens viaja cifrado, de tal modo que ninguém no caminho — nem mesmo o fornecedor do serviço — pode ler o texto enquanto está em trânsito. Até aí, a afirmação é exata.

O problema é que o conteúdo é apenas uma parte da história. Embora ninguém possa ler o que diz, o serviço sabe outras coisas com altíssima precisão: com quem fala, a que horas, com que frequência, de que localização aproximada, em que dispositivo, quantas mensagens envia e quantas recebe, que número de ficheiros partilha. A tudo isso chama-se metadados. E os metadados contam, em muitos casos, quase tanto como a mensagem em si.

O que os metadados revelam

Não é preciso ler uma mensagem para saber muitas coisas. Se uma pessoa liga ou escreve a um oncologista todas as terças-feiras às nove da manhã durante seis meses, não é necessário ouvir a conversa para intuir o que se está a passar. Se duas pessoas trocam cem mensagens por dia e de repente deixam de o fazer, não é preciso ler nenhuma para entender o que aconteceu. Se um consultor fiscal recebe vinte mensagens seguidas do mesmo cliente na noite anterior a um encerramento trimestral, o padrão fala por si.

Os metadados revelam padrões de comportamento: quem se relaciona com quem, que horários tem cada pessoa, quando está acordada, quando dorme, quando viaja, que clientes são mais ativos, que relações profissionais são mais intensas. Um servidor que recolhe metadados pode construir um perfil detalhado da vida pessoal e profissional de qualquer utilizador sem nunca ter lido uma única palavra do que escreve.

Há um exemplo histórico que ilustra isto com dureza. O antigo diretor da NSA, Michael Hayden, formulou-o sem rodeios em 2014: *"We kill people based on metadata"*. A afirmação referia-se a operações militares norte-americanas contra alvos identificados unicamente pelos seus padrões de comunicação. Nem uma única mensagem lida. Apenas o grafo de contactos e os horários.

Que um serviço recolha metadados não implica que vá usá-los contra os seus utilizadores. Implica que tem a capacidade de o fazer, e que um terceiro com acesso a esses dados — por ordem judicial, por quebra de segurança, ou por venda a terceiros se as condições de serviço o permitirem — também a tem.

O acesso à agenda

Outro vetor que passa quase despercebido: a lista de contactos. Grande parte dos serviços de mensagens pedem acesso à agenda do telefone ao registar-se. Enviam todos os números para o seu servidor para mostrar quem mais usa o serviço. A partir desse momento, a empresa tem um mapa completo das relações do utilizador, embora este nunca tenha escrito uma única mensagem a ninguém.

Para um profissional com segredo profissional — advogado, médico, psicólogo, consultor — esse mapa contém clientes. Se a agenda foi enviada para um servidor de terceiros, os nomes dos clientes estão numa infraestrutura cuja jurisdição e políticas o profissional não controla. O segredo profissional não se quebra no dia em que alguém filtra uma conversa: quebrou-se muito antes, no momento de aceitar o envio.

A diferença entre cifrar e não recolher

Cifrar é proteger o conteúdo. Ser privado é não recolher o que não é necessário. São coisas distintas, e a diferença é operacionalmente crítica. Um serviço pode cifrar todas as mensagens com perfeição e, ao mesmo tempo, saber quase tudo sobre os seus utilizadores através dos metadados. As duas coisas são perfeitamente compatíveis. De facto, é o modelo de negócio dominante no setor.

A pergunta correta para avaliar a privacidade real de um serviço não é *"cifra o conteúdo?"*. Essa pergunta já foi respondida há anos. A pergunta correta é: *"que metadados gera e onde são armazenados?"*. E, sobretudo: *"que metadados não precisa de gerar?"*.

Uma arquitetura que minimiza os metadados por desenho — não por promessa, não por política interna — é estruturalmente mais privada do que uma arquitetura que os recolhe e os cifra. Porque os dados que não existem não podem ser filtrados, nem vendidos, nem entregues a uma ordem judicial, nem perdidos numa quebra.

Para o leitor profissional

Se a sua atividade profissional implica segredo, confidencialidade, ou simplesmente respeito pela informação de terceiros, convém colocar as questões por esta ordem:

1. A aplicação que utilizo para me comunicar cifra o conteúdo? (Provavelmente sim.)
2. Cifra os metadados? (Provavelmente não.)
3. Gera metadados de que *não precisa* para funcionar? (Quase de certeza que sim.)
4. Onde estão armazenados esses metadados e sob que jurisdição? (Provavelmente fora do Espaço Económico Europeu.)
5. O meu cliente ou paciente sabe que os seus dados estão lá?

A última pergunta é a desconfortável. Porque a resposta honesta, na maioria dos casos, é não.

Este artigo é o primeiro de uma série sobre o funcionamento real das ferramentas de comunicação profissional. Próximas edições abordarão o cumprimento do RGPD em mensagens e o conceito de segredo profissional na era digital.

Fontes e leitura adicional

- Hayden, M. — Declaração na Johns Hopkins University, 2014 ("We kill people based on metadata"). Transcrições públicas disponíveis.
- RGPD (Regulamento UE 2016/679), arts. 4 e 5 — definição de dados pessoais e princípios de tratamento (os metadados são dados pessoais).
- EDPS e EDPB — opiniões sobre tratamento de dados de tráfego e metadados em comunicações eletrónicas (Diretiva ePrivacy).

← AnteriorUma breve historia do selo de lacreSeguinte →O segredo profissional na era digital

Leituras recentes

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Leve este artigo para onde precisar.

↓ Markdown ↓ Texto simples ↓ PDF

O arquivo é descarregado no seu dispositivo. A partir daí, pode guardá-lo, importá-lo no Solo2 ou partilhá-lo onde quiser. Cuadernos não decide o destino por si.

Selo de lacre · SHA-256 26662ec521740773301ea9568f9693e82e9a8559eb981a2b4e955c8b8dce03f0

Cuadernos Lacre · Uma publicação da Menzuri Gestión S.L. ·
escrita por R.Eugenio · editada pela equipa do Solo2.