Análise · 16 de maio de 2026

← Anterior·Seguinte →

Quando não há ninguém no meio

Cifrar o que passa por um servidor protege o conteúdo. Não ter um servidor no meio elimina a pergunta. Não são o mesmo.

Duas pessoas, uma conversa

Quando duas pessoas falam face a face numa sala, ninguém tem de prometer que não ouviu nada. Não ouviu porque não estava lá. Quando duas pessoas passam um papel de uma mão para a outra, ninguém no meio tem de jurar que não o leu. Não há ninguém no meio.

A maior parte das coisas na vida quotidiana funciona assim. Não assinamos acordos de confidencialidade com o ar que transmite a nossa voz, nem com o papel que seguramos. A privacidade da conversa não descansa sobre a promessa de um intermediário, porque não há intermediário. Essa é uma das formas mais fortes que existe de ser privado: não porque algo ou alguém se comporte bem, mas porque não há algo ou alguém.

Quando a conversa se translada para um canal digital, isto muda por defeito. O modelo habitual é o seguinte: duas pessoas ligam-se a um servidor, o servidor recebe a mensagem, cifra-a ou guarda-a cifrada, e entrega-a ao destinatário. O servidor está no meio. O servidor pode ser honesto. Pode ser auditado. Pode operar numa jurisdição favorável e sob uma política de privacidade estrita. Tudo isso pode ser verdade. Mas o servidor está no meio.

A diferença entre cifrar e não recolher (segunda parte)

Num artigo anterior desta mesma série, sustentamos que cifrar o conteúdo e não recolher metadados não são o mesmo. Há um passo mais além que convém formular com clareza: cifrar o que passa por um servidor e não ter servidor também não são o mesmo.

O primeiro modelo — servidor no meio, conteúdo cifrado — protege o conteúdo do operador do servidor, do seu pessoal de manutenção, de um atacante externo que comprometa o sistema. E isso é importante. Mas não elimina o servidor. O servidor continua lá. Continua a processar metadados. Continua a ser um ponto que pode receber um requerimento judicial, una intervenção legal, uma pressão política, ou uma brecha de segurança. Continua a ser um ponto que requer depositar confiança em alguém.

O segundo modelo — não haver servidor entre as duas extremidades — não protege melhor o conteúdo cifrado: se a criptografia for sólida, o conteúdo vai protegido em ambos os casos. O que muda não é o conteúdo. O que muda é que a pergunta *«o que acontece com o servidor?»* deixa de ter objeto, porque não existe servidor sobre o qual perguntar.

Confiança, ausência, e a diferença entre ambas

A confiança pode estar bem depositada. Empresas honestas existem. Auditores rigorosos existem. Legislações favoráveis ao utilizador existem. Serviços sérios que cumprem escrupulosamente com tudo o anterior existem. A

confiança, quando se concede a um operador que a merece, não é um mau acordo.

Mas a confiança, por sólida que seja, continua a ser confiança. É uma solução social, não uma solução técnica. Uma empresa pode mudar de mãos. Uma jurisdição pode mudar de governo. Uma ordem judicial pode chegar amanhã. Uma vulnerabilidade nova pode descobrir-se no próximo mês. Nada disto acontece por má fé. Acontece porque o operador existe, e tudo o que existe está sujeito às contingências do mundo.

A ausência de um operador não está sujeita a essas mesmas contingências. Uma ordem judicial não pode pedir dados a um servidor que não existe. Um atacante não pode comprometer um servidor que não existe. Uma mudança na política de uma empresa não pode afetar dados que essa empresa nunca teve. A frase chave é simples: os dados que não existem não se podem perder.

Sobre o argumento legítimo do lado do servidor

Quem oferece um serviço de mensageiria profissional com servidor no meio costuma formular três argumentos perfeitamente válidos. Primeiro, que o servidor é necessário para garantir a entrega quando o destinatário está desligado. Segundo, que a cifragem do conteúdo é robusta e, portanto, o operador não pode lê-lo. Terceiro, que o serviço cumpre a legislação europeia e que os datos estão protegidos pela lei.

Os três argumentos são verdadeiros. Nenhum altera a natureza do assunto. É verdade que um servidor permite armazenar mensagens para entrega diferida; também é verdade que a entrega diferida pode ser resolvida de outra forma, através de protocolos de comunicação direta entre dispositivos refinados há décadas e operativos hoje. É verdade que a cifragem do conteúdo em trânsito é robusta nos serviços sérios. E é verdade que a legislação europeia protege os utilizadores mais do que a de muitos outros lugares.

A questão não é se os serviços com servidor no meio são legais, nem se são seguros, nem se protegem o conteúdo. Podem sê-lo, são legais, e costumam ser seguros. A questão é que ter um servidor no meio é uma escolha arquitetónica, não uma imposição técnica. E cada escolha tem consequências. Uma arquitetura com servidor no meio gera necessariamente um ator no qual é preciso confiar. Uma arquitetura sem servidor no meio não.

O que a lei diz, e o que a arquitetura faz

O RGPD não exige um modelo arquitetónico concreto. Exige resultados: minimização de dados, finalidade limitada, proteção desde o design e por defeito, capacidade de demonstrar o cumprimento. Um serviço com servidor no meio pode cumprir todos estes requisitos. Um serviço sem servidor no meio cumpre vários deles por construção, não por declaração. A minimização absoluta — não recolher nada que não seja estritamente necessário para entregar a mensagem — é trivial quando não existe um servidor que possa recolher algo.

Para os usos quotidianos não sensíveis, uma arquitetura com servidor é perfeitamente razoável, e a confiança num operador sério é um acordo válido. Para os outros usos — os que envolvem segredo profissional regulado, os que acarretam responsabilidade deontológica, os que tocam informação especialmente sensível — a ausência de um ponto de confiança não é um luxo, é uma vantagem estrutural.

Para o leitor profissional

As perguntas que convém fazer ante um serviço de comunicação profissional, já familiares de artigos anteriores nesta mesma série, completam-se com uma única pergunta arquitetónica mais:

1. Cifra o conteúdo em trânsito? (Provavelmente sim.)
2. Gera e armazena metadados sobre com quem falo e quando? (Provavelmente sim.)
3. Existe um servidor no caminho entre o meu dispositivo e o do destinatário?

4. Se existe: quem o opera, em que jurisdição, e o que teria de acontecer para que entregasse dados sobre mim?
5. Se não existe: as perguntas anteriores não têm objeto.

A diferença entre as duas categorias não é de grau, mas de tipo. Chegada a hora de explicá-lo a um cliente, a um paciente, ou a um colega, a formulação mais honesta é também a mais simples: numa há alguém no meio; na outra, não.

Este artigo fecha o ciclo inicial de Cuadernos Lacre. Depois de falar da cifragem, dos metadados e do segredo profissional, completamos o quadro arquitetónico: cifrar o conteúdo e não ter servidor no meio são coisas distintas. As duas podem ser legais; apenas uma elimina o ponto de confiança.

Fontes e leitura adicional

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Texto fundacional do princípio segundo o qual as garantias de um sistema devem ser implementadas nas extremidades, não no canal intermédio.
- Regulamento (UE) 2016/679, art. 25 — proteção de dados desde o design e por defeito.
- Regulamento (UE) 2016/679, art. 5.1.c — princípio de minimização de datos.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Capítulos sobre arquiteturas que minimizam a recolha por construção.

← AnteriorRGPD e mensagens profissionais: por que a maioria incumpre sem saberSeguinte →CUADERNOS_LIST_SCHREMS_TITLE

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 0c084a2865c30c03593b219008cbb33ad87c7b7a6feff4223162e7fb10448b3e

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