Analisi · 16 maggio 2026

← Precedente·Successivo →

# Quando non c'è nessuno in mezzo

Cifrare ciò che passa per un server protegge il contenuto. Non avere un server in mezzo elimina la domanda. Non sono la stessa cosa.

## Due persone, una conversazione

Quando due persone parlano faccia a faccia in una stanza, nessuno deve promettere di non aver sentito nulla. Non ha sentito perché non c'era. Quando due persone si passano un foglio di carta da una mano all'altra, nessuno in mezzo deve giurare di non averlo letto. Non c'è nessuno in mezzo.

La maggior parte delle cose nella vita quotidiana funziona così. Non firmiamo accordi di riservatezza con l'aria che trasmette la nostra voce, né con la carta che teniamo in mano. La privacy della conversazione non si basa sulla promessa di un intermediario, perché non c'è nessun intermediario. Questo è uno dei modi più forti che esistano per essere privati: non perché qualcosa o qualcuno si comporti bene, ma perché non c'è qualcosa o qualcuno.

Quando la conversazione si sposta su un canale digitale, questo cambia di default. Il modello consueto è il seguente: due persone si connettono a un server, il server riceve il messaggio, lo cifra o lo salva cifrato, e lo consegna al destinatario. Il server è in mezzo. Il server può essere onesto. Può essere verificato. Può operare in una giurisdizione favorevole e con una rigorosa politica sulla privacy. Tutto questo può essere vero. Ma il server è in mezzo.

## La differenza tra cifrare e non raccogliere (seconda parte)

In un precedente articolo di questa stessa serie sosteniamo che cifrare il contenuto e non raccogliere metadati non sono la stessa cosa. C'è un passo ulteriore che va formulato con chiarezza: cifrare ciò che passa per un server e non avere alcun server non sono ugualmente la stessa cosa.

Il primo modello — server in mezzo, contenuto cifrato — protegge il contenuto dall'operatore del server, dal suo personale di manutenzione, da un aggressore esterno che comprometta il sistema. E questo è importante. Ma non elimina il server. Il server è ancora lì. Continua a elaborare metadati. Continua a essere un punto che può ricevere un'ingiunzione del tribunale, un intervento legale, pressioni politiche o una violazione della sicurezza. Continua a essere un punto che richiede di riporre fiducia in qualcuno.

Il secondo modello — nessun server tra i due estremi — non protegge meglio il contenuto cifrato: se la crittografia è solida, il contenuto è protetto in entrambi i casi. Ciò che cambia non è il contenuto. Ciò che cambia è che la domanda *«che fine fa il server?»* perde di senso, perché non esiste un server su cui farsi domande.

## Fiducia, assenza, e la differenza tra le due

La fiducia può essere ben riposta. Le aziende oneste esistono. Gli auditor rigorosi esistono. Le leggi favorevoli agli utenti esistono. I servizi seri che rispettano scrupolosamente tutto ciò esistono. La fiducia, quando viene

concessa a un operatore che la merita, non è un cattivo accordo.

Ma la fiducia, per quanto solida possa essere, rimane fiducia. È una soluzione sociale, non una soluzione tecnica. Un'azienda può cambiare proprietario. Una giurisdizione può cambiare governo. Un ordine del tribunale può arrivare domani. Una nuova vulnerabilità potrebbe essere scoperta il mese prossimo. Nulla di tutto ciò accade in malafede. Accade perché l'operatore esiste e tutto ciò che esiste è soggetto agli imprevisti del mondo.

L'assenza di un operatore non è soggetta agli stessi imprevisti. Un'ingiunzione del tribunale non può richiedere dati a un server che non esiste. Un aggressore non può compromettere un server che non esiste. Un cambiamento nella politica di un'azienda non può influire su dati che l'azienda non ha mai posseduto. La frase chiave è semplice: i dati che non esistono non possono andare perduti.

## Sul legittimo argomento lato server

Chiunque offra un servizio di messaggistica professionale con un server in mezzo formula di solito tre argomenti perfettamente validi. Primo, che il server è necessario per garantire la consegna quando il destinatario è offline. Secondo, che la crittografia del contenuto è forte e quindi l'operatore non può leggerlo. Terzo, che il servizio rispetta la legislazione europea e che i dati sono protetti dalla legge.

Tutti e tre gli argomenti sono veri. Nessuno cambia la natura della questione. È vero che un server consente di archiviare i messaggi per la consegna differita; è anche vero che la consegna differita può essere risolta in altro modo, attraverso protocolli di comunicazione diretta tra dispositivi, affinati da decenni e oggi operativi. È vero che la crittografia dei contenuti in transito è solida nei servizi seri. Ed è vero che la legislazione europea protegge gli utenti più di molti altri luoghi.

La questione non è se i servizi con un server in mezzo siano legali, né se siano sicuri, né se proteggano i contenuti. Possono esserlo, sono legali e di solito sono sicuri. Il punto è che avere un server in mezzo è una scelta architettonica, non un'imposizione tecnica. E ogni scelta ha delle conseguenze. Un'architettura con un server in mezzo genera necessariamente un attore di cui fidarsi. Un'architettura senza server in mezzo no.

## Cosa dice la legge e cosa fa l'architettura

Il GDPR non richiede un modello architettonico specifico. Richiede risultati: minimizzazione dei dati, limitazione delle finalità, protezione fin dalla progettazione e per impostazione predefinita, capacità di dimostrare la conformità. Un servizio con un server in mezzo può soddisfare tutti questi requisiti. Un servizio senza un server in mezzo ne soddisfa molti per costruzione, non per dichiarazione. La minimizzazione assoluta — non raccogliere nulla che non sia strettamente necessario per consegnare il messaggio — è banale quando non c'è alcun server in grado di raccogliere alcunché.

Per usi quotidiani non sensibili, un'architettura server è perfettamente ragionevole e la fiducia in un operatore serio è un accordo valido. Per gli altri usi — quelli che implicano il segreto professionale regolamentato, quelli che comportano responsabilità deontologiche, quelli che toccano informazioni particolarmente sensibili — l'assenza di un punto di fiducia non è un lusso, è un vantaggio strutturale.

## Per il lettore professionista

Le domande che dovrebbero essere poste di fronte a un servizio di comunicazione professionale, già note da articoli precedenti di questa stessa serie, sono completate da un'ulteriore domanda architettonica:

1. Cifra il contenuto in transito? (Probabilmente sì.)
2. Genera e memorizza metadati su con chi parlo e quando? (Probabilmente sì.)
3. C'è un server nel percorso tra il mio dispositivo e quello del destinatario?
4. Se esiste: chi lo gestisce, in quale giurisdizione e cosa dovrebbe succedere affinché consegni i miei dati?

5. Se non esiste: le domande precedenti non hanno senso.

La differenza tra le due categorie non è di grado, ma di tipo. Quando arriva il momento di spiegarlo a un cliente, a un paziente o a un collega, la formulazione più onesta è anche la più semplice: in una c'è qualcuno in mezzo; nell'altra, no.

---

*Questo articolo chiude il ciclo iniziale di Cuadernos Lacre. Dopo aver parlato di crittografia, metadati e segreto professionale, completiamo il quadro architettonico: cifrare i contenuti e non avere un server in mezzo sono cose diverse. Entrambe possono essere legali; solo una elimina il punto di fiducia.*

## Fonti e letture aggiuntive


- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Testo fondamentale del principio secondo cui le garanzie di un sistema devono essere implementate agli estremi, non nel canale intermedio.
- Regolamento (UE) 2016/679, art. 25 — protezione dei dati fin dalla progettazione e per impostazione predefinita.
- Regolamento (UE) 2016/679, art. 5.1.c — principio di minimizzazione dei dati.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Capitoli sulle architetture che riducono al minimo la raccolta by design.



← PrecedenteGDPR e messaggistica professionale: perché la maggioranza è inadempiente senza saperloSuccessivo →CUADERNOS_LIST_SCHREMS_TITLE


## Letture recenti


- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE


Porta questo articolo dove ne hai bisogno.

↓ Markdown ↓ Testo semplice ↓ PDF

Il file viene scaricato sul tuo dispositivo. Da lì puoi salvarlo, importarlo in Solo2 o condividerlo come preferisci. Cuadernos non decide la destinazione per te.


Sigillo di cera · SHA-256 6e51f2561ecc6db5e2d5dae04f37403d0d30d2adcb1bfafb7a3347fdbea1395b

Cuadernos Lacre · Una pubblicazione di Menzuri Gestión S.L. ·
scritta da R.Eugenio · a cura del team di Solo2.



Questo sito non utilizza cookie e non carica risorse di terze parti. Utilizza un contatore di visite anonimo auto-ospitato (Umami, sul nostro server europeo) e il minimo JavaScript necessario per la tua preferenza di tema chiaro/scuro. Nessun tracker, nessuna profilazione, nessuna condivisione di dati. Se vuoi seguirci: RSS.