Analisi · 26 maggio 2026

← Precedente·Successivo →

Privacy reale vs apparente: le domande che conviene porsi

Sintesi operativa del ciclo 2: le domande che distinguono un servizio con privacy architetturale da uno con privacy dichiarativa. Un questionario per il professionista europeo prima di adottare qualsiasi strumento digitale per dati sensibili.

Per intenderci: Due servizi con la stessa informativa legale possono comportarsi in modo molto diverso. Uno protegge per design tecnico. L'altro protegge per promessa contrattuale. La differenza non si legge nell'informativa — si scopre formulando le domande concrete. La qualità delle risposte dice tanto del prodotto quanto il loro stesso contenuto.

La differenza tra privacy architetturale e privacy dichiarativa

Nel corso dei sette articoli precedenti di questo ciclo abbiamo attraversato livelli diversi della stessa questione. Il diritto dei trasferimenti internazionali con Schrems II. L'idea matematica dell'hash crittografico che sigilla ogni Cuaderno. La scelta architetturale del kill switch e la cattura istituzionale che quasi sempre l'accompagna. Il meccanismo della cifratura end-to-end e la domanda operativa su dove risiedono le chiavi. L'allineamento degli incentivi secondo il modello di business. L'identità crittografica autosovrana. Il self-hosting come strategia proporzionata. Ogni articolo si è occupato di un angolo. Questo, l'ultimo del ciclo, li riunisce in un questionario.

La distinzione che conviene ricordare è semplice: ci sono servizi la cui privacy è *architetturale* e ci sono servizi la cui privacy è *dichiarativa*. La prima è incastonata nel design tecnico: certe violazioni dell'impegno di privacy sono tecnicamente difficili o impossibili perché l'architettura non le consente. La seconda è depositata nel testo dell'informativa legale: certe violazioni sarebbero contrattualmente sanzionabili se si verificano, ma tecnicamente nulla le impedisce. Entrambi i modelli possono rispettare il GDPR; ma uno protegge per costruzione e l'altro protegge per promessa, e la differenza è operativamente enorme.

Le domande che seguono sono progettate per distinguere un caso dall'altro. Non sono domande tecniche avanzate. Sono le domande a cui qualsiasi fornitore onesto può rispondere nella sua documentazione pubblica. La qualità e la precisione della risposta dicono tanto del prodotto quanto la risposta stessa. Le domande si raggruppano in sei livelli; conviene porle tutte prima di adottare il servizio per dati sensibili, non solo quelle che il primo istinto identifica.

Livello 1: architettura

Conviene fissare un termine prima di proseguire. Per *operatore* intendiamo l'azienda che fornisce il servizio: l'entità che controlla i server e il software, non una persona specifica. Chiarito questo, la domanda architettonica di fondo è: che cosa fa l'operatore con il contenuto tra mittente e destinatario? Le risposte possibili sono tre e conviene saperle distinguere, perché tutte e tre vengono talvolta pubblicizzate con un vocabolario simile.

- La prima: il contenuto passa per un server dell'operatore in chiaro, dove l'operatore può leggerlo anche se promette di non farlo.

- La seconda: il contenuto passa per un server dell'operatore cifrato, dove l'operatore non può leggerlo se le chiavi risiedono esclusivamente sui dispositivi degli utenti.
- La terza: il contenuto non passa per alcun server dell'operatore, perché non esiste alcun server dell'operatore in quel flusso concreto.

La differenza tra queste tre non è di grado: è di tipo.

La domanda complementare —già formulata nel Cuaderno sulla cifratura— è: chi possiede le chiavi crittografiche che permettono di leggere il contenuto? Se le possiede l'utente e solo l'utente, la cifratura è reale. Se le possiede inoltre l'operatore in qualsiasi forma —anche sotto il nome di «recupero dell'account» o «sincronizzazione tra dispositivi»—, la cifratura è nominale. La domanda non ammette risposta intermedia onesta.

Livello 2: modello di business

La domanda sul modello di business conta tanto quanto la domanda architetturale, e per la stessa ragione sostanziale: gli incentivi producono, nel corso del tempo, prodotti sistematicamente diversi anche con propositi dichiarati identici. Come guadagna denaro oggi l'operatore? Una sola fonte, due, una miscela? Se il finanziamento include pubblicità o monetizzazione dei dati, quali dati si monetizzano e su quale base giuridica del GDPR lo si fa? La finalità dichiarata nell'informativa legale copre i dati di terzi che il professionista intende affidare al servizio?

E la domanda di secondo ordine, non sempre formulata: qual è la situazione finanziaria dell'operatore in un orizzonte di tre o cinque anni? Un'azienda in fase di capitale di rischio opera sotto pressioni diverse da un'azienda in redditività stabile. Il cambio di modello di finanziamento è, ripetutamente, il momento in cui il contratto implicito con gli utenti viene riscritto senza negoziazione.

Livello 3: giurisdizione

Per il professionista europeo, la domanda della giurisdizione non è retorica. In quale giurisdizione è costituito l'operatore? In quale paese si trovano fisicamente i server che elaborano i dati? La risposta alle due domande precedenti è la stessa o diversa, e se differisce, quale legislazione si applica? Una regione europea operata da un'azienda statunitense non è, ai fini di Schrems II, una risposta europea: l'azienda è soggetta a FISA 702 indipendentemente da dove si trovino i server.

La domanda complementare operativa è: se arrivasse domani un ordine di intelligence valido nella giurisdizione dell'operatore che chiede la consegna dei miei dati o di quelli dei miei clienti, cosa accadrebbe? Se la risposta onesta inizia con «l'azienda sarebbe obbligata a consegnarli», il servizio non protegge contro tale ordine per quanto la pubblicità suggerisca il contrario. Se la risposta onesta inizia con «l'azienda non potrebbe consegnarli perché non li detiene in chiaro», il servizio protegge sì; e la differenza dipende quasi interamente dai primi due livelli, non dalla qualità dell'informativa sulla privacy.

Livello 4: operatore e kill switch

Quale capacità tecnica mantiene l'operatore per sospendere, bloccare, eliminare o degradare il servizio a distanza? La domanda non è paranoica: è operativa. Le piattaforme digitali hanno esercitato tale capacità ripetutamente negli ultimi anni, talvolta di propria iniziativa, talvolta su ordine di governi, talvolta dopo cambi di proprietà o di politica. Se la capacità esiste, conviene sapere sotto quali ipotesi contrattualmente dichiarate viene esercitata, e riservare un margine per le ipotesi non dichiarate che la pratica degli ultimi anni ha mostrato altrettanto rilevanti: ordine giudiziario inatteso, sanzione internazionale, cambio di governance aziendale, acquisizione da parte di un'entità con un'altra politica.

La domanda gemella è quella del piano di continuità: se l'operatore esercitasse la capacità contro il professionista —per qualsiasi ragione, giusta o meno—, quanto tempo di attività resterebbe disponibile, quale procedura di esportazione dei dati esiste, e verso quale fornitore alternativo si potrebbe migrare? Se la risposta inizia con «non dovrebbe accadere», non è una risposta operativa; è una promessa.

Livello 5: identità e accesso

Chi controlla le credenziali di accesso al servizio? Se l'operatore può reimpostare l'accesso dell'utente senza la partecipazione dell'utente —procedura tipicamente chiamata «recupero dell'account»—, l'operatore è, tecnicamente, il custode dell'account e può anche cederlo a chi lo richieda mediante la procedura adeguata. Se l'operatore non può reimpostare l'accesso perché l'identità risiede crittograficamente sul dispositivo dell'utente, l'operatore non può nemmeno cederla, neppure sotto ordine. Entrambe le modalità sono legittime a seconda del contesto; ma, ancora una volta, sono diverse, e conviene sapere quale si sta adottando.

Cosa accade ai dati del professionista se il professionista perde l'accesso? Esistono meccanismi di recupero —di account, di file, di sessione— che dipendono dall'operatore? Tali meccanismi sono compatibili con la deontologia professionale del settore se l'operatore viene coartato a usarli?

Livello 6: futuro

Quest'ultimo livello tende a essere trascurato perché richiede proiezione. Cosa accadrebbe se il servizio venisse acquisito da un'altra azienda? Quasi tutte le acquisizioni comportano una revisione dei termini di servizio nei mesi successivi. Cosa accadrebbe se cambiassero i requisiti regolamentari? Il diritto europeo ha incrementato gli obblighi di rimozione e blocco dal 2022, non li ha ridotti. Cosa accadrebbe se l'operatore scomparisse? Una parte significativa dei servizi cloud non ha un piano di uscita documentato per lo scenario di chiusura dell'operatore; il professionista scopre il problema quando non c'è più tempo per prepararlo.

C'è una formulazione che conviene ricordare per questo livello: le architetture che dipendono meno dall'operatore sono più resilienti ai cambiamenti dell'operatore. Il self-hosting in qualsiasi delle sue modalità, l'identità crittografica autosovrana, le comunicazioni senza server intermedio, tutte queste riducono la superficie di rischio futura mediante il procedimento di ridurre la superficie di dipendenza presente. Non la eliminano; la riducono.

La differenza tra struttura e promessa

Se dovessimo distillare il ciclo in una sola frase, sarebbe questa: le risposte strutturali si mantengono anche se l'operatore, l'amministrazione o la legislazione cambiano; le risposte per promessa si mantengono finché chi promette può e vuole mantenerle. Entrambe possono essere corrette nel momento in cui si adottano. Solo una delle due si sostiene indipendentemente dal passare del tempo e dal cambiamento delle circostanze.

Questo non significa che ogni professionista debba esigere risposte strutturali da tutti i servizi che adotta. La proporzionalità resta legittima: un foglio di calcolo per la contabilità interna non necessita della stessa risposta della cartella clinica di un paziente. Significa, sì, che la professionalità consiste nel sapere che tipo di risposta si è accettato in ogni caso, e nell'aver deciso consapevolmente che quel tipo di risposta è proporzionato al dato concreto.

Il questionario, ordinato

Dodici domande concrete che sintetizzano il ciclo, ordinate affinché la risposta a ciascuna informi la successiva:

1. Il contenuto passa per un server dell'operatore? Se passa: in chiaro, cifrato con chiavi dell'operatore, o cifrato con chiavi esclusive dell'utente?

2. Se si invoca la cifratura end-to-end, dove risiedono le chiavi crittografiche? L'operatore conosce o conserva una parte di esse in qualsiasi forma, compreso il «recupero»?
3. Quali metadati genera e conserva il servizio? Per quanto tempo? A chi sono visibili?
4. Come si finanzia l'operatore? Se il finanziamento include pubblicità o monetizzazione dei dati, la finalità dichiarata copre i dati di terzi affidati dal professionista?
5. Qual è la situazione finanziaria dell'operatore in un orizzonte di tre o cinque anni? Vi sono fattori che suggeriscono un cambio imminente di modello (quotazione in borsa in sospeso, round di finanziamento in esaurimento, acquisizione probabile)?
6. In quale giurisdizione è costituito l'operatore? In quale paese si trovano fisicamente i server? Se differiscono, quale legislazione nazionale si applica al trattamento?
7. Cosa accadrebbe se un ordine di intelligence valido nella giurisdizione dell'operatore chiedesse la consegna dei miei dati? L'azienda potrebbe ottemperarvi tecnicamente?
8. Quale capacità tecnica mantiene l'operatore per sospendere, bloccare o eliminare il servizio? Sotto quali ipotesi contrattuali? Sotto quali ipotesi non contrattuali storicamente documentate?
9. Quale piano di uscita esiste se l'operatore esercitasse tale capacità contro di me, giustamente o ingiustamente? Esiste una procedura documentata di esportazione dei dati verso un fornitore alternativo?
10. Chi controlla le credenziali di accesso? L'operatore può reimpostarle senza la mia partecipazione? Questo mi protegge o mi espone?
11. Esiste un'alternativa europea, autoospitata o senza server intermedio per questa funzione concreta? Qual è il suo costo reale, confrontato con il rischio valutato?
12. Se la decisione di oggi fosse esaminata tra cinque anni da un ispettore, un revisore o un cliente colpito da una violazione, la scelta attuale sarebbe difendibile con gli argomenti disponibili oggi, o richiederebbe di scusarsi per non aver posto domande ragionevoli?

Le domande non si aspettano risposte perfette. Si aspettano risposte oneste, che l'operatore onesto sa dare e l'operatore meno onesto evita di formulare con precisione. La differenza operativa tra le due classi di operatore, lo diciamo senza drammi, si percepisce di solito leggendo lentamente le risposte che offrono volontariamente, prima ancora di dover chiedere di più.

Con questo articolo chiudiamo il secondo ciclo di Cuadernos Lacre. Abbiamo iniziato con il debito editoriale ereditato da Schrems II e terminiamo con un questionario operativo. Lungo il percorso abbiamo attraversato concetti —hash, cifratura, identità— e analisi applicate —kill switch, modello di business, self-hosting—. L'intenzione editoriale dichiarata della pubblicazione non era sopraffare il lettore con l'elenco esaustivo dei problemi, ma consegnargli strumenti affinché, di fronte a qualsiasi nuovo servizio, distingua che tipo di risposta sta accettando. Questa distinzione —tra architettura e promessa— è lo strumento. Il resto, ogni professionista lo metterà al servizio dei dati che ritiene, nella propria pratica, degni della domanda.

Fonti e letture aggiuntive

- Questa pubblicazione, ciclo 2 (maggio 2026) — *Schrems II, cinque anni dopo*, *Cos'è realmente SHA-256*, *Kill switch e cattura istituzionale*, *Crittografia end-to-end, spiegata davvero*, *Il modello di business come segnale di fiducia*, *Le 24 parole: cos'è un'identità crittografica*, *Self-hosting come pratica professionale*. I sette articoli su cui poggia questo questionario.
- Regolamento (UE) 2016/679 — Regolamento generale sulla protezione dei dati. Quadro giuridico di riferimento per tutte le domande che il questionario pone, in particolare gli articoli 5, 6, 25, 28, 32, 33 e il capo V.
- Comitato europeo per la protezione dei dati — linee guida e pareri operativi su Schrems II, trasferimenti internazionali, valutazioni d'impatto e responsabilità proattiva (pubblicazioni 2020-2024).
- Agenzia spagnola per la protezione dei dati — sanzioni pubblicate 2022-2024 a carico di titolari del trattamento per strumenti di trasferimento inadeguati o per valutazioni d'impatto formali prive di contenuto sostanziale.
- noyb.eu — Centro europeo per i diritti digitali, diretto da Maximilian Schrems. Repository pubblico di reclami, ricorsi e analisi sul rispetto reale, non apparente, delle norme europee di protezione dei dati.

← PrecedenteSelf-hosting come pratica professionaleSuccessivo →Ciò che una firma non può risolvere

Letture recenti

- Riflessione · 29 giugno 2026 Non sei anonimo
- Riflessione · 27 maggio 2026 Ciò che una firma non può risolvere
- Analisi · 25 maggio 2026 Self-hosting come pratica professionale

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 b00a0a85b18bb43a696b6a737c986e766a05fcca8046440c94ad43e5914e674c

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