Analisi · 25 maggio 2026

← Precedente·Successivo →

Self-hosting come pratica professionale

Un server non è altro che un computer. La domanda non è se averne uno, ma dove vivono i dati dei tuoi clienti, chi li sostiene e chi si assume la responsabilità quando qualcosa non va.

Per intenderci: I tuoi dati vivono sempre nel computer di qualcuno: in quello di un gigante a cui affidi tutto, in uno noleggiato che gestisci tu, o nel tuo proprio. Più controllo vuoi, più responsabilità ti assumi. Delegare a un grande terzo rassicura, ma non esonera: l'informazione è tua —e dei tuoi clienti—, e il responsabile sei tu.

La domanda tra il cloud e la cantina

Conviene iniziare demistificando una parola che spaventa senza motivo: server. Un server non è una macchina misteriosa in una sala refrigerada. È, semplicemente, il computer di un'altra persona —o il tuo— che conserva informazioni e le consegna a chi le richiede. Per decenni abbiamo conservato i dati dei nostri clienti in una cartella, in uno schedario, sulla scrivania dell'ufficio, e nessuno perdeva il sonno per questo. L'informazione non faceva paura perché era su carta; non deve farne nemmeno perché è su un disco.

Il «cloud» non è nemmeno etereo. È il computer di un'azienda, quasi sempre lontano e quasi sempre di qualcun altro. L'ho imparato involontariamente il giorno in cui, fiducioso che i miei file fossero al sicuro su Google Drive, ho scoperto che la cartella del mio computer non conteneva i miei documenti, ma scorciatoie a documenti che vivevano altrove. Se quell'altro posto decidesse di chiudere, cambiare prezzo o disdire il servizio, la mia tranquillità se ne andrebbe con lui. Non possedevo le mie cose; avevo il permesso di accedervi.

Da qui nasce la domanda di questo Quaderno, più semplice da enunciare che da rispondere: dove dovrebbero vivere i dati dei tuoi clienti? E i tuoi? Il dibattito pubblico la pone come se ci fossero solo due risposte contrapposte — la nuvola delle grandi piattaforme oppure farselo da soli —, quasi una questione di schieramento. Ma non sono due strade: sono tre, e nessuna è un atto di fede. Lette con calma, hanno più sfumature e chiedono più di quanto sembri.

Questo ti riguarda, qualunque cosa tu venda

È facile pensare che la riservatezza sia una questione da avvocati, medici o giornalisti, e che gli altri non abbiano nulla da nascondere. È un errore, e di quelli costosi. Quasi ogni attività conserva dati dei propri clienti soggetti alla legge, e molti conservano, senza saperlo, informazioni molto più sensibili di quanto sembri.

Un negozio di divani annota il nome, l'indirizzo e il telefono di chi compra; se c'è un finanziamento, anche i suoi dati economici. Un'impresa di ristrutturazioni o di arredamento conserva foto dell'interno delle case dei suoi clienti e le planimetrie complete delle loro abitazioni. Un'impresa di pulizie gestisce le planimetrie degli uffici che pulisce, spesso segnate con colori e numeri che indicano quale dipendente entra dove, a che ora e con quale chiave. Niente di tutto ciò sembra gran cosa finché non ci si chiede a chi altro avrebbe valore: quelle planimetrie delle pulizie sono, viste con altri occhi, la mappa perfetta per chi voglia entrare a rubare.

Il fatto che un'attività sia piccola, o que venda divani invece di difendere cause legali, non rende i suoi dati privi di valore né fa sì che la legge smetta di applicarsi ad essa. Fa solo sì che il suo proprietario tenda a pensarci

meno. E pensare poco a qualcosa che è di tua responsabilità è esattamente il punto in cui iniziano i problemi.

Dove vivono i tuoi dati?

A quella domanda ci sono, in sostanza, tre risposte. E conviene ricordare che «i dati» non sono solo il dossier di un cliente o il blocco di fatture e preventivi: lo sono anche le tue conversazioni con lui — via WhatsApp, tramite un servizio di chat professionale, tramite Solo2. Le tre risposte che seguono non sono gradi di purezza né una scala dai buoni ai cattivi: sono tre modi di ripartire la stessa cosa, il controllo e la responsabilità.

Delegare tutto a un fornitore. È la cosa più comune, e per la maggior parte è l'unica che conosce. Metto tutto in Google Workspace o in Microsoft 365 e lo affido interamente al fornitore. Pago il mio canone e smetto di pensarci. La forma più estrema di questo sono i servizi in cui non arrivi nemmeno ad avere i tuoi dati: certi programmi di fatturazione nella nuvola, per esempio, ti conservano le fatture e i preventivi — e funzionano molto bene —, ma l'informazione vive nel loro sistema, non nel tuo. Finché paghi, accedi; il giorno in cui te ne vai, scopri che portarti via il tuo stesso storico è difficile o impossibile. Tenere i tuoi dati mezzo in ostaggio è, per più di un fornitore, proprio ciò che ti impedisce di passare alla concorrenza. In cambio della comodità cedo il controllo e — senza dirlo ad alta voce — la sensazione che la responsabilità non sia più mia. Qui sta una sfumatura che quasi mai si fa: delegare non è sinonimo di americano. Posso delegare tutto altrettanto comodamente a un fornitore europeo — Infomaniak, per esempio — e risolvere in un colpo solo buona parte dei dubbi sui trasferimenti internazionali che abbiamo visto in «Schrems II», senza autogestire nulla. Non sono gli Stati Uniti contro il resto dell'universo: all'interno della pura delega ci sono già decisioni che contano.

Noleggiare e gestire il proprio server. Ho la stessa cosa che mi darebbe Microsoft o Google, ma lo configuro da solo. Noleggio un server presso un fornitore europeo —Hetzner, OVH, Scaleway—, installo software libero (Nextcloud per i file, ad esempio) e amministro io stesso il risultato. Guadagno un controllo reale: so cosa gira, dove e perché. Ma la macchina si trova ancora nel data center di un terzo e, soprattutto, cambia chi ne sopporta le conseguenze. Delegando, se qualcosa non va, hai qualcuno da incolpare. Gestendolo tu stesso, è molto probabile che la colpa sia tua.

Averlo sul proprio computer. Questa è l'opzione che quasi nessuno racconta, ed è il cuore di questo Quaderno. Non serve un server enorme acceso ventiquattr'ore su ventiquattro all'interno di un macro data center per ospitare i tuoi dati. Il computer del tuo ufficio è già un server: serve te. Lo lasci acceso in ufficio e ti connetti a lui dal portatile a casa di un cliente, o dal cellulare quando sei a casa. Lo chiamiamo «il computer dell'ufficio», non «il server», ma fa esattamente la stessa cosa delle due opzioni precedenti. Il controllo è massimo e così pure la vicinanza: i tuoi dati sono dove sei tu. La contropartita, detta senza abbellimenti, è che anche la responsabilità è massima. Se va via la luce non c'è un tecnico di guardia a Norimberga: tocca a te riattaccare l'interruttore. E perché quel computer sia accessibile dall'esterno serve qualcosa che getti un ponte tra il tuo portatile e lui. Non è magia, e conviene saperlo prima di scegliere questa strada.

E non è nemmeno necessario riutilizzare il computer dell'ufficio: esiste un dispositivo pensato proprio per questo, il NAS (li producono Synology, QNAP e altri). Come quasi tutto ciò che abbiamo visto in questi Cuadernos, al suo interno non c'è alcuna magia: è un computer specializzato, lo stesso tipo di macchina che noleggeresti in un centro dati, solo che è pensato per conservare i dati e servirli sulla rete, senza monitor né tastiera di mezzo. Collegaci uno schermo e una tastiera e hai un computer qualsiasi; installa il software adeguato sul tuo PC e hai un NAS. La differenza è che il NAS arriva già pronto all'uso. Lo compri, lo colleghi a casa o in ufficio, ed è tuo. Non paghi un canone mensile; lo paghi una volta e ti appartiene, come qualsiasi altro strumento della tua attività. Lo accendi, lo spegni, lo porti altrove se vuoi. E poiché è tuo, nulla ti impedisce di averne due —uno a casa, uno in ufficio— o tre, aggiungendone uno in un luogo sicuro, sincronizzati tra loro: la tua ridondanza, senza dipendere da un terzo che la mantenga. L'autoospitamento, in fin dei conti, non è una cosa sola: è una combinazione di macchine, di proprietà, di posizioni e di software.

Qui è inevitabile nominare ciò che facciamo, e lo facciamo senza travestimenti: in Solo2 quel ponte lo tende l'applicazione stessa. Il computer del tuo ufficio resta accessibile solo ai tuoi dispositivi fidati, e sempre sotto cifratura, e i tuoi altri apparecchi si riconnettono a esso da soli. Quando un cliente parla con te, è il tuo computer

— non quello di un terzo — a parlare con il cliente. Non risolviamo l'interruzione di corrente; risolviamo il ponte. E non siamo gli unici: per quasi ogni esigenza esistono oggi programmi — liberi o proprietari — che permettono proprio questo, avere i dati sul tuo dispositivo e raggiungerli da fuori. Il nostro è un esempio; l'importante è l'idea, non il marchio.

La ridondanza non è un superpotere

Qui sorge l'obiezione immediata, ed è ragionevole: se ho tutto sul computer del mio ufficio, cosa succede se si rompe? La domanda è buona. La risposta è che la rete di sicurezza che immaginiamo nei grandi fornitori è più modesta —e più imitabile— di quanto sembri.

Quando lascio i miei dati nel data center di una multinazionale, confido che abbia copie in diversi posti. E probabilmente le ha: in una seconda sede, forse in una terza. Ma quella ridondanza non è infinita e, soprattutto, non è mia: resta un disco rigido di cui non sono il proprietario, gestito da qualcuno in cui ripongo una fede che non verifico quasi mai.

Quella stessa rete posso tesserla io, e con un vantaggio decisivo. Il mio servizio quotidiano vive sul computer dell'ufficio. Da lì conservo una copia crittografata sul computer di un'azienda amica —un collega, un altro ufficio di fiducia— e un'altra copia crittografata, se voglio, presso quello stesso fornitore europeo di cui parlavamo. La differenza è tutto: quello che lascio fuori non è il mio servizio né i miei dati in chiaro, ma una copia crittografata che solo io posso aprire. Il fornitore esterno conserva uno scrigno chiuso di cui non ha la chiave. Non gli affido le mie informazioni: gli affido alcuni byte che, senza di me, non significano nulla.

Era al sicuro finché non ha smesso di esserlo

Permettetemi una storia personale, perché illustra questo meglio di qualunque argomento. Per più di dieci anni sono stato un cliente devoto di CrashPlan, un servizio di backup tecnicamente straordinario. Eseguivo il backup nel loro cloud di tutti i miei computer e di quelli della mia famiglia —quelli dell'azienda e quelli di casa, tutto—, con versioni che potevo recuperare alla frequenza che volevo, viaggiando a ritroso nel tempo fino a un file specifico di mesi prima. Dopo la prima copia trasmetteva solo le differenze, crittografate e compresse, in modo da mantenere aggiornato un enorme backup con pochissimo sforzo. Mi ha salvato molte volte, da un documento sciocco a un intero disco. Il prezzo è salito negli anni e non mi importava: pagavo felice.

Quello que non sapevo è che CrashPlan aveva commesso un errore di calcolo: aveva promesso per contratto archiviazione illimitata, in spazio e tempo. E lo spazio moltiplicato per il tempo —anni di cronologia, versioni ogni pochi minuti— cresce fino a diventare insostenibile. Un giorno ci hanno comunicato che il servizio terminava. Lo hanno fatto con eleganza e con un preavviso generoso, quasi un anno, e ci hanno dato i mezzi per scaricare i nostri dati. Ma dove si va con più di dieci anni di copie versionate di tutti i propri dischi? Lì scopri che non hai né come scaricare tutto né dove metterlo, e che, pur potendo, il nuovo magazzino costerebbe una fortuna.

Ho salvato quattro cose indispensabili. Il resto se n'è andato quando hanno spento l'interruttore. Io ero tranquillo, le mie informazioni erano al sicuro... finché non lo furono più. E non per un tradimento: CrashPlan si è comportato in modo impeccabile — al contrario di Evernote, che anni dopo si è comportato in modo vergognoso —; semplicemente, il mio angelo custode nella nuvola ha deciso, con tutto il diritto, di smettere di esserlo. Il risultato, per me, fu identico: ciò che credevo al sicuro è scomparso.

Quello che questa storia insegna davvero ha più a che fare con la natura umana che con la tecnologia. Quando uno sente che qualcosa è sua responsabilità, agisce in modo preventivo: fa copie, si copre le spalle, diffida con buon criterio. Quando crede —erroneamente— che la responsabilità sia sostenuta da un terzo grande e solvibile, si rilassa e lascia fare. Quella tranquillità delegata non è prudenza: è, senza trucco, una forma di irresponsabilità.

Pagare non è la stessa cosa che adempiere

Quella tranquilla irresponsabilità somiglia molto a quella di due genitori che iscrivono il figlio alla scuola più costosa, gli pagano poi un master, e con ciò credono di aver adempiuto al proprio dovere. Non hanno adempiuto. Essere genitori significa preoccuparsi di cosa ha imparato oggi, di ciò che non capisce, dei suoi valori, della sua sicurezza in se stesso. Se a venticinque anni quel figlio non sa lavorare né comportarsi, la colpa non è della scuola che ha incassato: è di chi ha delegato e pagato credendo che bastasse. Pagare un terzo non esime dalla responsabilità. Non lo ha mai fatto.

Con i dati succede lo stesso, e la storia recente lo conferma. Cinquanta o cento anni fa un professionista custodiva le cose dei suoi clienti in cartelle, nel suo studio o a casa sua, e se ne sentiva responsabile. Raramente si perdeva qualcosa. Siamo passati al mondo digitale e, con una facilità sbalorditiva, carichiamo tutto su «la nuvola» — che non è altro che il computer di una multinazionale — e smettiamo di preoccuparcene. E spesso ci sono incidenti, e ci sono aziende che perdono tutto, e allora si dice: la colpa è stata di Google, la colpa è stata di Microsoft. No. L'informazione è tua, o dei tuoi clienti, ma il responsabile sei tu.

Ospitare i propri dati non è un capriccio tecnico: è recuperare quella serenità di decenni fa, quella di sapere dove si trova ogni cosa e perché. La protezione dei dati, nel frattempo, ha vissuto un brusco pendolo —dal non esserci alcuna norma, quando chiunque esibiva i dati di un cliente senza pensarci, a un'esigenza che ricade con durezza sproporzionata sul più piccolo, il lavoratore autonomo che dà il telefono di un cliente al fattorino. Non discuto il fine; osservo lo squilibrio. Ma lo squilibrio non ci esenta: il giorno in cui l'amministrazione avrà i mezzi per tracciare e sanzionare su scala, la dimensione smetterà di proteggere chiunque, e conviene non aspettare quel giorno con la casa in disordine. Avere il dato sotto il proprio controllo aiuta ad adempiere e aiuta a dimostrarlo. E, soprattutto, riporta le cose al loro posto: quando l'informazione è tua, la responsabilità è interamente tua — non c'è un terzo da incolpare, né un terzo il cui fallimento ti esponga—.

La responsabilità protegge anche

Sarebbe disonesto dipingere tutto questo senza ombre. Prendere il posto dell'intermediario significa farsi carico del suo onere: mantenere le copie aggiornate, applicare gli aggiornamenti e una responsabilità legale — quella del RGPD — che, in realtà, non ha mai del tutto smesso di essere tua (i riferimenti a piè di pagina dettagliano gli articoli). C'è lavoro, e c'è un giorno in cui qualcosa si rompe al momento sbagliato. Non lo nascondiamo.

Ma la paura che circonda quella parola, responsabilità, è mal calibrata. È molto più facile perdere i tuoi file in un servizio della nuvola che chiude, o le tue foto in Google Photos, che perdere quella cartella di documenti importanti che hai sul tuo computer: quella di cui sai dove si trova e di cui noteresti l'assenza non appena sparisse. Ciò che senti tuo, lo curi; ciò che credi al sicuro nelle mani di un altro, lo trascuri.

Pensa agli album di foto di una volta, quelli di carta sviluppata custoditi in un cassetto. Hai mai sentito qualcuno dire di aver «perso» il proprio album di famiglia? Si sente della casa che è bruciata con l'album dentro; perderlo così, no. E invece, gente che aveva tutte le sue foto in Google Photos o in Apple Foto e si è ritrovata senza niente: quella storia torna ogni pochi mesi, perché credevano che fosse al sicuro. Google Photos cura le tue foto, certo che sì; ma non le cura come dei genitori curano l'album dove ci sono i loro figli e i loro nipoti. Quella differenza non la aggiusta nessun centro dati: la responsabilità, quando è tua, non è solo un peso; è anche la migliore garanzia.

Quattro domande prima di decidere

Se stai pensando di fare il passo, in qualunque sua forma, conviene rispondere prima a quattro domande con spassionata onestà:

1. Quale parte dei tuoi dati ti dispiacerebbe perdere, o non poter portare via? E attenzione a scartare il «routinario»: lo storico delle fatture sembra la cosa più prosaica del mondo finché non cambi programma e scopri che quelle fatture erano del fornitore, non tue — che, al massimo, puoi stamparle in PDF, senza più

poter cercare al loro interno. Non è solo una questione di sensibilità: è di a chi appartiene davvero ciò che hai bisogno di conservare.
2. Quale opzione è proporzionata alla tua reale capacità tecnica? Un computer proprio ben curato è alla portata di chiunque; amministrare un intero server, non tanto. Sii onesto su ciò che sai e ciò che non sai. E ricorda che tra montarti un server intero e delegare tutto c'è un terreno intermedio molto ragionevole: programmi — liberi o proprietari — che custodiscono i tuoi dati sul tuo stesso dispositivo e ti lasciano raggiungerli da fuori. Per molte persone è il miglior equilibrio.
3. Quale piano hai per il giorno peggiore? Una violazione, un disco che muore, un fornitore che chiude, il tecnico in malattia. Se il piano inizia con «non dovrebbe succedere», non è un piano.
4. Sapresti dimostrare di essere in regola se domani ti ispezionassero? Farlo bene e poter provare che lo fai bene non sono la stessa cosa. La legge chiede la seconda.

Non c'è una risposta universale. C'è una risposta proporzionata, assunta con onestà su ciò che si guadagna e ciò che si eredita. E, al di là della tecnica, una semplice certezza: i tuoi dati vivono nel computer di qualcuno. L'unica domanda che conta davvero è di chi vuoi che sia quel computer.

L'autohosting non è né virtù né vizio: è uno strumento con un'impronta concreta di capacità e responsabilità. La domanda non è mai stata se ospitare i propri dati, ma quali, come e con quale rete di supporto. Recuperare il controllo dei dati non significa tornare in cantina né diffidare di tutto: significa tornare a sentirsi responsabili di ciò che è nostro, come quando quei dati vivevano in una cartella sulla scrivania. Tale responsabilità, ben compresa, è il vero servizio che un professionista presta ai suoi clienti.

Fonti e letture aggiuntive

- Regolamento (UE) 2016/679 — articolo 28 (responsabile del trattamento), articolo 32 (sicurezza del trattamento), articolo 33 (notifica di una violazione), articolo 37 (designazione del Responsabile della Protezione dei Dati).
- Agenzia Spagnola per la Protezione dei Dati — *Guida pratica per l'analisi dei rischi nel trattamento dei dati personali* (revisione vigente). Quadro di riferimento per i titolari del trattamento che assumono proprie funzioni tecniche.
- Comitato Europeo per la Protezione dei Dati — *Guidelines 1/2024 on processing of personal data based on legitimate interests*. Applicabile anche all'esame di proporzionalità nelle decisioni su infrastrutture proprie.
- Commissione Europea — elenco pubblico dei fornitori di servizi di informazione stabiliti in giurisdizione europea. Punto di partenza amministrativo per identificare opzioni di hosting gestito europeo.
- Nextcloud GmbH (Germania) — *Nextcloud Enterprise architecture and compliance documentation*. Caso documentato di software libero con modalità autohosted e gestite da un fornitore europeo; utile come riferimento tecnico di un progetto sostenuto in giurisdizione europea dal 2016.

← PrecedenteLe 24 parole: cos'è un'identità crittograficaSuccessivo →Privacy reale vs apparente: le domande da porsi

Letture recenti

- Riflessione · 29 giugno 2026 Non sei anonimo
- Riflessione · 27 maggio 2026 Ciò che una firma non può risolvere
- Analisi · 26 maggio 2026 Privacy reale vs apparente: le domande da porsi

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 c1bfa81705ccad4a0ed5df540942d6cd1afb82bb89ca949cf6f2509ea19b9245

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