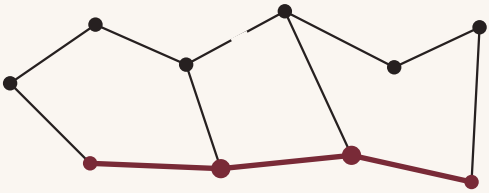
Luca Tomassini

QUANDO LA RETE SI FERMA

Sicurezza digitale, dipendenza e libertà di scegliere



Quando un servizio digitale si interrompe, scopriamo quanto dipendiamo da infrastrutture che non controlliamo. Una riflessione sulla sicurezza informatica, sulla sovranità tecnologica e sulla libertà di continuare a scegliere.

QUANDO LA RETE SI FERMA

Sicurezza digitale, dipendenza e libertà di scegliere

Luca Tomassini

QUADERNI DEL DOMANI / 12

© 2026 Luca Tomassini. Tutti i diritti riservati.

Nessuna parte di questa pubblicazione può essere riprodotta, copiata, modificata o diffusa senza autorizzazione scritta dell'autore, salvo quanto consentito dalla legge.

Edizione digitale gratuita pubblicata sul sito ufficiale:

www.lucatomassini.it

Quaderni del domani · N. 12 · Prima edizione, 2026

Il giorno in cui tutto si ferma

Ci siamo abituati a considerare la connessione una condizione naturale della nostra esistenza. Apriamo un documento e ci aspettiamo che sia disponibile. Inviamo un messaggio e diamo per scontato che raggiunga il destinatario. Entriamo in un ospedale, in una banca o in un ufficio pubblico senza domandarci quanti sistemi informatici debbano funzionare, nello stesso istante, perché un gesto ordinario possa compiersi.

Poi accade qualcosa. La posta elettronica smette di rispondere, i documenti non si aprono, le comunicazioni si interrompono. Non è necessario immaginare un attacco sofisticato. Può bastare un aggiornamento sbagliato, un errore di configurazione, un componente che smette di funzionare. Un problema apparentemente circoscritto attraversa infrastrutture condivise e si propaga fino a raggiungere persone che non hanno alcuna relazione con il luogo in cui si è verificato.

In quelle ore scopriamo una verità che conoscevamo già, ma che avevamo smesso di osservare: la nostra vita digitale dipende da una rete di decisioni tecniche, industriali e politiche prese spesso molto lontano da noi.

Non considero questi episodi una dimostrazione del fallimento della tecnologia. Al contrario, sono il segno di quanto profondamente essa sia entrata nella società. Il problema nasce quando la sua presenza diventa così pervasiva da renderci incapaci di immaginare che possa mancare.

La sicurezza comincia proprio qui. Non nel tentativo impossibile di impedire ogni guasto, ma nella consapevolezza che nessun sistema, per quanto avanzato, può essere considerato infallibile.

La fragilità della complessità

Ho trascorso molti anni nel mondo delle telecomunicazioni, quando la continuità del servizio era una responsabilità concreta, misurata ogni giorno. Una rete telefonica non poteva permettersi di funzionare soltanto nelle condizioni ideali. Doveva continuare a servire le persone anche quando un apparato si guastava, una tratta si interrompeva o una centrale incontrava un problema.

Quella cultura tecnica aveva un principio semplice: non basta che un sistema funzioni, bisogna comprendere come si comporterà quando qualcosa non funzionerà più. La ridondanza, la separazione dei percorsi, le procedure di emergenza non erano dettagli aggiunti alla fine del progetto. Facevano parte del progetto stesso.

Le infrastrutture digitali contemporanee sono immensamente più potenti e flessibili. La possibilità di distribuire risorse, concentrare capacità di calcolo e gestire servizi su scala mondiale ha reso accessibili strumenti che un tempo richiedevano investimenti enormi. È una conquista che non va sminuita.

Eppure ogni forma di efficienza porta con sé una domanda. Quando più servizi condividono gli stessi elementi, che cosa accade se uno di quegli elementi si ferma? L'integrazione riduce costi e complessità per chi utilizza la tecnologia, ma può aumentare la portata di un'interruzione.

È il paradosso dei sistemi complessi: diventano straordinariamente affidabili nella normalità e, proprio per questo, possono sorprenderci quando si presenta un evento inatteso. La sicurezza non consiste nel negare questa contraddizione. Consiste nel progettarla, nel misurarla e nel prepararsi a gestirla.

La domanda che dovremmo rivolgere a ogni infrastruttura essenziale non è soltanto quanto sia veloce o conveniente. È quanto sappia resistere, quanto rapidamente possa recuperare e quali funzioni riesca a garantire anche quando il resto si interrompe.

La comodità di dipendere

La trasformazione digitale ci ha insegnato ad apprezzare la semplicità. Un unico ambiente per lavorare, comunicare, conservare documenti e accedere alle informazioni. Un solo contratto, un solo interlocutore, un'esperienza uniforme. Per un'impresa, soprattutto quando deve crescere rapidamente, questa scelta può essere perfettamente razionale.

Il rischio non si manifesta nel momento in cui si adotta una piattaforma. Si manifesta più tardi, quando ci si accorge che abbandonarla è diventato difficile, costoso o addirittura impraticabile. I documenti sono in un formato, le identità digitali in un altro sistema, le procedure aziendali dipendono da funzioni proprietarie e le competenze delle persone si sono adattate a un unico ambiente.

La dipendenza tecnologica raramente nasce da una decisione dichiarata. È il risultato di tante scelte ragionevoli, compiute una dopo l'altra. Nessuna sembra decisiva. Insieme, però, possono ridurre progressivamente la libertà di scegliere.

Non penso che la risposta sia rifiutare le grandi piattaforme o immaginare un ritorno a tecnologie meno evolute. Sarebbe un errore. La dimensione globale dei servizi digitali ha prodotto benefici reali e ha permesso anche alle imprese più piccole di accedere a capacità prima riservate a pochi.

Ma la convenienza di oggi non può essere l'unico criterio con cui decidiamo l'autonomia di domani. Il costo di una tecnologia dovrebbe comprendere anche il prezzo necessario per sostituirla, trasferire i dati, riprendere il controllo dei processi e continuare a lavorare se il fornitore non è disponibile.

Una scelta è davvero libera quando esiste la possibilità concreta di cambiarla.

La sicurezza non è soltanto difesa

Quando parliamo di cybersecurity, il pensiero corre agli attacchi informatici, al furto di dati, alle frodi, ai sistemi violati. Sono minacce reali, che richiedono competenze, investimenti e un aggiornamento continuo. Ma ridurre la sicurezza digitale alla capacità di respingere un aggressore significa osservare soltanto una parte del problema.

Un'infrastruttura può diventare indisponibile senza che nessuno l'abbia attaccata. Può essere perfettamente protetta contro l'accesso non autorizzato e, nello stesso tempo, dipendere da un unico servizio esterno. Può conservare i dati in modo sicuro, ma non essere in grado di utilizzarli quando ne ha più bisogno.

La sicurezza ha quindi almeno tre dimensioni inseparabili: proteggere ciò che possediamo, assicurare la continuità delle funzioni essenziali e mantenere la capacità di decidere. La riservatezza dei dati è importante. Lo è anche la loro disponibilità. E lo è la possibilità di sapere chi, in ultima istanza, può interrompere un servizio.

Penso agli ospedali, alle reti energetiche, ai trasporti, alle amministrazioni pubbliche. In questi luoghi la tecnologia non è un semplice strumento di produttività. È diventata parte dell'organizzazione di diritti e bisogni fondamentali. Un'interruzione non rappresenta soltanto un disservizio: può compromettere attività dalle quali dipendono persone reali.

Per questo la resilienza dovrebbe entrare nella cultura di chi governa le organizzazioni, non rimanere confinata nei reparti informatici. Il consiglio di amministrazione che discute un investimento digitale dovrebbe interrogarsi anche sulle conseguenze della sua indisponibilità. La responsabilità non può essere delegata interamente a chi gestisce i server.

La vera maturità digitale si riconosce quando la continuità del servizio diventa una responsabilità condivisa.

La sovranità che conta

Negli ultimi anni abbiamo cominciato a parlare sempre più spesso di sovranità digitale. È un'espressione che rischia di diventare uno slogan se non le attribuiamo un significato concreto. Per me non significa costruire confini intorno a Internet, né pretendere che ogni componente tecnologico sia prodotto nello stesso Paese.

Significa conservare una capacità effettiva di scelta. Sapere dove risiedono i dati e chi può accedervi, certamente. Ma anche conoscere le dipendenze che permettono ai servizi di funzionare, comprendere quali norme si applicano ai fornitori e disporre di alternative praticabili.

Un servizio può essere ospitato in un centro dati nazionale e continuare a dipendere, per il suo funzionamento, da tecnologie, licenze o infrastrutture controllate altrove. La localizzazione dei dati è una condizione importante in molti contesti, ma non coincide automaticamente con l'autonomia operativa.

Qui emerge una questione che supera la tecnica. Le reti globali hanno reso il mondo più interconnesso, ma alcuni passaggi sono controllati da un numero limitato di soggetti. Questa concentrazione può trasformarsi in potere economico e, in determinate circostanze, anche in potere politico.

Non è necessario immaginare intenzioni ostili per riconoscere il problema. Basta osservare che un'organizzazione incapace di sostituire un servizio essenziale ha un margine di negoziazione molto ridotto. La sua libertà non dipende soltanto dalle condizioni contrattuali, ma dalla possibilità di fare una scelta diversa.

L'Europa dovrebbe affrontare questo tema senza chiudersi in una logica difensiva. La sovranità non si costruisce soltanto con le norme. Richiede competenze, investimenti, imprese capaci di competere, infrastrutture affidabili e una domanda pubblica che sappia premiare anche l'interoperabilità e la continuità.

Essere sovrani, nel mondo digitale, non significa fare tutto da soli. Significa non essere costretti a dipendere da una sola possibilità.

L'intelligenza artificiale e il nuovo punto di dipendenza

Con l'intelligenza artificiale questa riflessione diventa ancora più importante. Per molti anni abbiamo affidato alle piattaforme digitali la conservazione e la trasmissione delle informazioni. Oggi cominciamo ad affidare loro anche una parte della loro interpretazione.

Un sistema di intelligenza artificiale può assistere un professionista, sintetizzare documenti, suggerire soluzioni, supportare una decisione. In numerosi settori questi strumenti rappresentano un progresso straordinario. Ma se diventano indispensabili a un processo, la loro indisponibilità può interrompere non soltanto un flusso di dati, bensì una capacità operativa.

Esiste poi un rischio più sottile. Quando l'accesso alle conoscenze e agli strumenti di analisi passa attraverso pochi modelli, le scelte tecnologiche possono influenzare anche il modo in cui le organizzazioni formulano problemi e valutano risposte. La dipendenza non riguarda più soltanto le infrastrutture. Può riguardare le competenze.

Non credo che questo debba portarci a diffidare dell'intelligenza artificiale. Credo, al contrario, che dovremmo imparare a utilizzarla con maggiore consapevolezza. Un'organizzazione solida non rinuncia al giudizio umano perché dispone di uno strumento più veloce. Lo rafforza, sapendo che la tecnologia può assistere le decisioni ma non assumersi la responsabilità delle loro conseguenze.

La sfida è costruire sistemi capaci di collaborare con le persone senza renderle progressivamente incapaci di operare in loro assenza. È una questione di formazione, di progettazione e, soprattutto, di cultura.

La libertà tecnologica non consiste nel fare a meno degli strumenti più avanzati. Consiste nel non perdere, utilizzandoli, la capacità di comprendere e decidere.

Il valore di una via d'uscita

Ogni volta che un grande servizio digitale si interrompe, per qualche ora riscopriamo il valore di strumenti che consideravamo superati. Una telefonata, una copia locale, una procedura manuale, un canale alternativo. Poi i sistemi tornano a funzionare e tutto riprende come prima. Il rischio è dimenticare la lezione insieme al disservizio.

Non propongo di tornare indietro. Ho dedicato la mia vita professionale all'innovazione e continuo a considerarla una delle più grandi possibilità di crescita per la società. Ma proprio per questo penso che il progresso debba essere accompagnato da una responsabilità più grande della semplice adozione di nuove tecnologie.

La sicurezza richiede investimenti che spesso non producono risultati visibili. Un sistema di riserva non impressiona quando tutto funziona. Una procedura di emergenza sembra superflua finché non arriva il momento di utilizzarla. La possibilità di cambiare fornitore può apparire costosa fino al giorno in cui diventa indispensabile.

Eppure sono proprio queste scelte a distinguere un'organizzazione efficiente da un'organizzazione realmente preparata. La prima sa funzionare bene nelle condizioni previste. La seconda conserva la capacità di agire anche quando quelle condizioni vengono meno.

Dovremmo imparare a considerare la resilienza non come un costo imposto dalla paura, ma come un investimento nella libertà. Non elimina gli errori, non impedisce ogni attacco e non garantisce che tutto andrà sempre bene. Riduce, però, la possibilità che un evento esterno decida al nostro posto.

La tecnologia ci ha insegnato a connettere ogni cosa. Ora deve insegnarci anche a non dipendere da una sola cosa.

Il progresso non si misura soltanto da quanto velocemente riusciamo ad andare avanti. Si misura anche dalla capacità di non fermarci quando la strada che avevamo scelto, improvvisamente, non è più disponibile.