Non sei anonimo

La fiducia che non hai scelto

In parole povere: con la tua email, chiunque può scoprire in pochi secondi dove hai un account, e a volte il tuo viso e il tuo nome. Non è un errore: è internet che funziona come sempre. La domanda non è se possono vederti —possono—, ma a chi sei costretto ad affidarti. E c'è un solo posto senza nessuno in mezzo: parlare direttamente, da un dispositivo all'altro.

Basta un indirizzo email. Non necessariamente il tuo: uno qualsiasi. Si inserisce in una manciata di strumenti gratuiti —legali, pubblici, a disposizione di chiunque voglia cercarli— e in pochi secondi appare una lista: in quali servizi è registrata quell'email, a volte una foto profilo, a volte un nome e cognome che il proprietario credeva di non aver dato a nessuno. Non serve essere dei tecnici. Non si viola nessuna password. Non si commette alcun reato. Tutte quelle informazioni erano già lì —pubblicate, registrate o trapelate— in attesa che qualcuno si prendesse la briga di metterle insieme.

È allettante interpretare tutto questo come un difetto: una falla, una disattenzione, qualcosa che qualcuno dovrebbe sistemare. Non lo è. È il normale funzionamento del web aperto. Ogni volta che ti iscrivi a un servizio, compili un modulo, pubblichi una recensione o appari nella fuga di dati di qualcun altro, lasci una traccia. Nessuna di queste tracce è grave di per sé. Il problema —se di problema si tratta— nasce dall'unirle, ed unirle è semplice.

A questo punto molte persone si difendono con una frase ragionevole: «io non ho nulla da nascondere», o «io sto attento ai miei account». La prima confonde il nascondersi con lo scegliere; ci torneremo. La seconda ignora che la maggior parte di quelle tracce non le hai lasciate tu: le ha lasciate il registro delle imprese, il sito che ha subìto la violazione, il conoscente che ha caricato una foto con te e ti ha taggato. L'anonimato su internet non è quasi mai una proprietà che possiedi; è, al massimo, oscurità: il fatto provvisorio che nessuno si sia ancora preso la briga di guardare.

Finora abbiamo parlato di ciò che una singola persona può fare in pochi secondi, a mano. Ora togliamo la persona. Ciò che per anni ha protetto quasi tutti noi non è stato l'anonimato, ma il disinteresse: per trovarti, qualcuno deve prendersi la briga di cercare, e nessuno ha il tempo di controllare tutti. Quest'ultima barriera —lo sforzo di cercare— è esattamente ciò che manca a una macchina. Un sistema automatico può fare quello stesso incrocio di dati non contro un singolo bersaglio, ma contro un'intera popolazione; non una volta sola, ma senza sosta; non per sospetto, ma di default. Ciò che prima richiedeva ore a un investigatore per ogni singola persona, ora viene fatto su milioni contemporaneamente, senza che costi tempo o attenzione a nessuno. Non c'è bisogno di ipotizzare chi vorrebbe farlo —un'azienda, un gruppo, uno Stato—; basta capire che non bisogna più scegliere chi guardare. Si possono guardare tutti.

Per questo «possono trovarmi?» è la domanda sbagliata. La risposta è sì, e lo sarà sempre di più. La domanda utile è un'altra: a chi, e quanto, sono costretto ad affidarmi per vivere connesso? Perché questo è ciò che fai realmente ogni giorno, quasi sempre senza pensarci. Confidi che il servizio in cui ti registri custodirà bene i tuoi dati. Confidi che il tuo operatore non ascolterà le tue chiamate. Confidi che l'applicazione di messaggistica che usano tutti —diciamo WhatsApp— faccia ciò che dice di fare. Confidi nel server che sta nel mezzo, nell'azienda che lo gestisce, nel paese in cui si trova, nello strumento gratuito che qualcuno ha messo in rete. Ognuno di quegli anelli è una decisione di fiducia. La differenza è che quasi nessuna di queste l'hai presa consapevolmente:

erano incluse nel pacchetto. Quegli anelli che si inseriscono tra te e l'altra persona vengono chiamati, in gergo, intermediari di fiducia; il nome importa meno dell'idea che siano lì, e che siano tanti.

C'è un modo onesto per verificare tutto questo: farlo su te stesso. E non hai bisogno che ti diamo nulla. Apri il tuo browser, scrivi tre o quattro parole —qualcosa come «cosa sa internet della mia email»— e il web stesso ti metterà davanti gli strumenti. Quella facilità è, da sola, mezza risposta: se tu li trovi in dieci secondi, chiunque può trovare ciò che dicono di te.

Non ti offriamo una nostra lista, ed è intenzionale. Se te la dessimo, dovresti fidarti di noi: del fatto che abbiamo scelto bene, che quelle pagine saranno ancora affidabili tra cinque anni, che dietro a nessuna di esse c'è —oggi o domani— qualcuno con cattive intenzioni. Non possiamo prometterlo per pagine che non controlliamo, e preferiamo non fare una promessa che non possiamo mantenere. È, esattamente, di ciò di cui tratta questo articolo. Ma cercarlo da te ha un prezzo: il motore di ricerca non distingue ciò che è legittimo dall'inganno. Creare una pagina che imita uno strumento reale, ti chiede l'email e se la tiene è banale. Quindi, prima di scrivere qualcosa ovunque, è bene saper leggere un indirizzo.

Nota — leggere un indirizzo prima di fidarsene. Una pagina falsa può copiare fino all'ultimo pixel di una vera; ciò che quasi mai può falsificare è il suo indirizzo. Prima di scrivere qualcosa su un sito, leggi la barra degli indirizzi, non la pagina. Il nome che comanda è quello attaccato a sinistra dell'ultima parte (`.com`, `.org`, `.it`): in `banca-sicura.sito-strano.top`, il vero proprietario non è la tua banca, è `sito-strano.top`. Diffida di lettere scambiate (uno `0` al posto di una `o`), di parole in più, di trattini dove non te li aspetti e di desinenze insolite. Il lucchetto e l'`https` indicano solo che la connessione è cifrata —non che il proprietario sia onesto—: anche un truffatore ha il lucchetto. E i primi risultati contrassegnati come «annuncio» sono lì perché qualcuno ha pagato, non perché siano affidabili. Ognuna di queste verifiche è, in fondo, la stessa domanda: quanto mi fido di questo indirizzo, e perché?

Arrivati a questo punto, conviene descrivere il contrario di tutto ciò: un canale senza intermediari. Due persone, sole in cima a una montagna, che parlano. Non c'è un postino, né un centralino, né un server, né un'azienda, né un paese di mezzo. Eppure, nota bene: nemmeno lì scompare la fiducia. Se racconti un segreto all'altra persona, ti stai fidando di lei. Quella fiducia non si può togliere —e non serve farlo—, perché è l'unica che hai scelto veramente: sai di chi ti fidi, e perché.

Ciò che non c'è sulla montagna è tutto il resto. Nessuno in mezzo. E questo, non un altro, è l'unico modello che può essere riprodotto in modo onesto nel digitale: un canale diretto da un dispositivo all'altro, senza niente e nessuno lungo il percorso. Non elimina la fiducia —sarebbe mentire—; elimina gli intermediari. Ti lascia da solo con l'unica fiducia inevitabile, quella che hai scelto tu. È, per inciso, l'architettura su cui costruiamo queste pagine; ma l'argomento si regge da solo, a prescindere da chi lo costruisca.

Quindi no, non sei anonimo, e probabilmente non tornerai mai ad esserlo. Ma quella non è mai stata la battaglia importante. Non si può vivere —né navigare— senza fidarsi di nessuno; chi ci prova non è più libero, è solo più solo. La maturità non è la diffidenza, che è un'altra forma di ingenuità. È essere esigenti: sapere a chi concedi la tua fiducia, quanta, in cambio di cosa e —soprattutto— sapere quando la stai concedendo a qualcuno senza averlo deciso.

Quasi nulla nella vita è bianco o nero; quasi tutto vive nel grigio in mezzo, e imparare a muoversi in quel grigio è buona parte di ciò che significa avere criterio. L'unica eccezione è ciò che è fatto bene di fabbrica: ciò che, per design, non ti chiede di fidarti di nessuno tranne che della persona con cui hai già deciso di parlare. Il resto — tutto il resto— è questione di quanto, e di chi.

Nota editoriale: quando questi Cuadernos menzionano aziende o prodotti, non è per accusare. Chi li costruisce fa un lavoro che milioni di persone usano e apprezzano. Ciò che segnaliamo è strutturale — il modello, non il marchio. I marchi appaiono come esempio perché sono quelli che il lettore riconosce.

Fonti e letture aggiuntive

- OSINT (open-source intelligence) — raccogliere informazioni da dati già pubblici; non è intrusione né spionaggio.
- Reglamento (UE) 2016/679 (RGPD) — sul trattamento dei dati personali, inclusa l'aggregazione di dati che singolarmente erano pubblici.
- Registri pubblici (imprese, tribunali, proprietà) — fonte legittima e abbondante di informazioni personali in quasi tutta Europa.
- In questa stessa raccolta: i quaderni sulla crittografia end-to-end e «Ciò che una firma non può sistemare» sviluppano, da un'altra prospettiva, la stessa idea.

← PrecedenteCiò che una firma non può risolvere

Letture recenti

- Riflessione · 27 maggio 2026 Ciò che una firma non può risolvere
- Analisi · 26 maggio 2026 Privacy reale vs apparente: le domande da porsi
- 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 f8a7fb25aea48b4908bbad8535e12c2dd8139d85dd1ee0b5c123142f17154d27

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

Questo sito non utilizza cookie. Tutto ciò che il tuo browser carica è scritto o supervisionato da noi e ospitato sui nostri server europei: il contatore di visite anonimo (Umami, autoospitato) e il minimo JavaScript necessario per il selettore di lingua e la tua preferenza di tema chiaro/scuro, che viene salvata sul tuo dispositivo. Senza risorse di terze parti, senza tracker, senza profilazione, senza condivisione di dati. Se vuoi seguirci: RSS.