No ets anònim

La confiança que no vas triar

Per entendre'ns: amb el teu correu, qualsevol esbrina en segons on tens un compte, i de vegades la teva cara i el teu nom. No és una fallada: és internet funcionant com sempre. La pregunta no és si et poden veure —poden—, sinó a qui et veus obligat a confiar. I només hi ha un lloc sense ningú al mig: parlar directe, d'un aparell a un altre.

N'hi ha prou amb un correu electrònic. No el teu necessàriament: qualsevol. S'escriu en un grapat d'eines gratuïtes —legals, públiques, a l'abast de qui vulgui buscar-les— i en qüestió de segons apareix una llista: en quins serveis està registrat aquest correu, a vegades una foto de perfil, a vegades un nom i un cognom que el seu amo creia no haver donat a ningú. No fa falta ser tècnic. No es trenca cap contrasenya. No es comet cap delicte. Tota aquesta informació ja hi era —publicada, registrada o filtrada— esperant que algú es molestés a ajuntar-la.

És temptador llegir això com una fallada: una bretxa, un descuit, alguna cosa que algú hauria d'arreglar. No ho és. És el funcionament normal de la web oberta. Cada vegada que et dones d'alta en un servei, omples un formulari, publiques una ressenya o apareixes a la filtració d'un altre, deixes una empremta. Cap d'aquestes empremtes és greu per si sola. El problema —si és que és un problema— neix d'ajuntar-les, i ajuntar-les és senzill.

Aquí molta gent es defensa amb una frase raonable: «jo no tinc res a amagar», o «jo cuido els meus comptes». La primera confon amagar-se amb triar; hi tornarem. La segona passa per alt que la major part d'aquest rastre no el vas deixar tu: el va deixar el registre mercantil, la web que va patir la filtració, el conegut que va pujar una foto amb tu i et va etiquetar. L'anonimat a internet gairebé mai és una propietat que posseeixis; és, a tot estirar, foscor: el fet provisional que ningú s'ha molestat encara a mirar.

Fins aquí hem parlat del que una sola persona pot fer en uns segons, a mà. Ara treu la persona. El que durant anys ens ha protegit a gairebé tots no va ser l'anonimat, sinó el desinterès: per a trobar-te, algú s'ha de molestar a mirar, i ningú té temps de mirar a tothom. Aquesta última barrera —l'esforç de mirar— és just la que una màquina no té. Un sistema automàtic pot fer aquest mateix encreuament no contra un objectiu, sinó contra una població sencera; no una vegada, sinó sense descans; no per sospita, sinó per defecte. El que abans li portava hores a un investigador per cada persona passa a fer-se sobre milions alhora, sense que a ningú li costi temps ni atenció. No fa falta suposar qui voldria fer-ho —una empresa, un grup, un Estat—; n'hi ha prou d'entendre que ja no cal triar a qui mirar. Es pot mirar a tothom.

Per això «em poden trobar?» és la pregunta equivocada. La resposta és sí, i ho serà cada vegada més. La pregunta útil és una altra: a qui, i quant, em veig obligat a confiar per a viure connectat? Perquè això és el que de veritat fas cada dia, gairebé sempre sense pensar-ho. Confies que el servei on et registres guardarà bé les teves dades. Confies que la teva operadora no escoltarà les teves trucades. Confies que l'aplicació de missatgeria que utilitzen tots —posem WhatsApp— fa el que diu fer. Confies en el servidor que hi ha al mig, en l'empresa que l'administra, en el país on és, en l'eina gratuïta que algú va penjar a la xarxa. Cadascuna d'aquestes baules és una decisió de confiança. La diferència és que gairebé cap la vas prendre conscientment: venien incloses. A aquestes baules que es colen entre tu i l'altra persona les anomenen, en argot, intermediaris de confiança; el nom importa menys que la idea que hi són, i que en són molts.

Hi ha una manera honesta de comprovar tot això: fer-ho amb tu mateix. I no necessites que et donem res. Obre el teu navegador, escriu tres o quatre paraules —alguna cosa com «què sap internet del meu correu»— i la mateixa web et posarà davant les eines. Aquesta facilitat és, per si sola, mitja resposta: si tu les trobes en deu segons, qualsevol pot trobar el que diuen de tu.

No t'oferim una llista nostra, i és deliberat. Si te la donéssim, hauries de confiar en nosaltres: en què hem triat bé, en què aquestes pàgines continuaran sent de fiar d'aquí a cinc anys, en què darrere de cap hi ha —avui o demà— algú amb males intencions. No podem prometre això de pàgines que no controlem, i preferim no fer una promesa que no pots complir. És, exactament, del que tracta aquest article. Però buscar-ho tu té un preu: el cercador no distingeix allò legítim de la trampa. Muntar una pàgina que imita una eina real, et demana el correu i se'l queda és trivial. Així que, abans d'escriure res enlloc, convé saber llegir una adreça.

Nota — llegir una adreça abans de confiar-hi. Una pàgina falsa pot copiar fins a l'últim píxel d'una de veritat; el que gairebé mai pot falsificar és la seva adreça. Abans d'escriure res en un lloc, llegeix la barra d'adreces, no la pàgina. El nom que mana és el que està enganxat a l'esquerra de l'última part (`.com`, `.org`, `.cat`): a `banc-segur.lloc-rar.top`, l'amo real no és el teu banc, és `lloc-rar.top`. Desconfia de lletres canviades (un `0` per una `o`), de paraules de més, de guions on no els esperes i d'acabaments estranys. El cadenat i el `https` només diuen que la connexió va xifrada —no que l'amo sigui honrat—: un estafador també té cadenat. I els primers resultats marcats com a «anunci» hi són perquè algú ha pagat, no perquè siguin de fiar. Cadascuna d'aquestes comprovacions és, en el fons, la mateixa pregunta: quant confio en aquesta adreça, i per què?

Arribats aquí, convé descriure el contrari de tot això: un canal sense intermediaris. Dues persones, soles dalt d'una muntanya, parlant. No hi ha carter, ni centraleta, ni servidor, ni empresa, ni país pel mig. I, malgrat tot, fixa't: tampoc allà desapareix la confiança. Si li expliques un secret a l'altra persona, hi estàs confiant. Aquesta confiança no es pot treure —ni falta que fa—, perquè és l'única que vas triar de veritat: saps en qui confies, i per què.

El que no hi ha a la muntanya és tota la resta. Ningú al mig. I aquest, no un altre, és l'únic model que pot reproduir-se de manera honesta en el món digital: un canal directe d'un dispositiu a un altre, sense res ni ningú pel camí. No elimina la confiança —això seria mentir—; elimina els intermediaris. Et deixa a soles amb l'única confiança inevitable, la que sí que vas escollir. És, dit de passada, l'arquitectura des de la qual escrivim aquestes pàgines; però l'argument se sosté sol, el construeixi qui el construeixi.

De manera que no, no ets anònim, i segurament no tornis a ser-ho. Però aquesta mai va ser la batalla que importava. No es pot viure —ni navegar— sense confiar en ningú; qui ho intenta no és més lliure, només està més sol. La maduresa no és la desconfiança, que és una altra forma d'ingenuïtat. És ser exigent: saber a qui concedeixes la teva confiança, quanta, a canvi de què i —sobretot— saber quan l'hi estàs concedint a algú sense haver-ho decidit.

Gairebé res a la vida és blanc o negre; gairebé tot viu en el gris del mig, i aprendre a moure's per aquest gris és bona part del que significa tenir criteri. L'única excepció és el que ve ben fet de fàbrica: allò que, per disseny, no et demana confiar en ningú més que en la persona amb la qual ja vas decidir parlar. La resta —tota la resta— és qüestió de quant, i de a qui.

Nota editorial: quan aquests Cuadernos nomenen empreses o productes, no és per acusar. Els qui els construeixen fan treballs que milions de persones usen i aprecien. El que assenyalem és estructural — el model, no la marca. Les marques apareixen com a exemple perquè són les que el lector reconeix.

Fonts i lectura addicional

- OSINT (intel·ligència de fonts obertes) — reunir informació a partir de dades ja públiques; no és intrusió ni espionatge.
- Reglamento (UE) 2016/679 (RGPD) — sobre el tractament de dades personals, inclosa l'agregació de dades que individualment eren públiques.

- Registres públics (mercantils, judicials, de la propietat) — font legítima i abundant d'informació personal a gairebé tota Europa.
- En aquesta mateixa col·lecció: els quaderns sobre el xifratge d'extrem a extrem i «El que una signatura no pot arreglar» desenvolupen, des d'un altre angle, la mateixa idea.

← AnteriorEl que una signatura no pot arreglar

Lectures recents

- Reflexió · 27 de maig del 2026 El que una signatura no pot arreglar
- Anàlisi · 26 de maig del 2026 Privadesa real vs aparent: les preguntes que convé fer-se
- Anàlisi · 25 de maig del 2026 Self-hosting com a pràctica professional

Emporta't aquest article on el necessitis.

↓ Markdown ↓ Text pla ↓ PDF

L'arxiu es descarrega al teu dispositiu. Des d'allà pots guardar-lo, importar-lo a Solo2, o compartir-lo on vulguis. Cuadernos no decideix el destí per tu.

Segell de lacre · SHA-256 d9bd525903e892f50cf1bc130db6cbac5002e8dcb228f2a513a6fb1ba72e961e

Cuadernos Lacre · Una publicació de Menzuri Gestión S.L. ·
escrita per R.Eugenio · editada per l'equip de Solo2.