Non es anónimo

A confianza que non elixiches

Para entendernos: co teu correo, calquera averigua en segundos onde tes conta, e ás veces a túa cara e o teu nome. Non é un fallo: é internet funcionando como sempre. A pregunta non é se poden verte —poden—, senón a quen te ves obrigado a confiar. E só hai un sitio sen ninguén no medio: falar directo, dun aparello a outro.

Basta un correo electrónico. Non o teu necesariamente: calquera. Escríbese nun feixe de ferramentas gratuítas —legais, públicas, ao alcance de quen queira buscalas— e en cuestión de segundos aparece unha lista: en que servizos está rexistrado ese correo, ás veces unha foto de perfil, ás veces un nome e un apelido que o seu dono cría non dar a ninguén. Non fai falta ser técnico. Non se rompe ningunha contrasinal. Non se comete ningún delito. Toda esa información xa estaba aí —publicada, rexistrada ou filtrada— agardando a que alguén se molestase en xuntala.

É tentador ler isto como un fallo: unha fenda, un descoido, algo que alguén debería arranxar. Non o é. É o funcionamento normal da web aberta. Cada vez que te das de alta nun servizo, enches un formulario, publicas unha recensión ou apareces na filtración doutro, deixas unha pegada. Ningunha desas pegadas é grave por si soa. O problema —se é que é un problema— nace de xuntalas, e xuntalas é sinxelo.

Aquí moita xente deféndese cunha frase razoable: «eu non teño nada que agochar», ou «eu coido as miñas contas». A primeira confunde agocharse con elixir; volveremos a iso. A segunda pasa por alto que a maior parte dese rastro non o deixaches ti: deixouno o rexistro mercantil, a web que sufriu a filtración, o coñecido que subiu unha foto contigo e te etiquetou. O anonimato na internet case nunca é unha propiedade que posúas; é, como moito, escuridade: o feito provisional de que ninguén se molestou aínda en mirar.

Ata aquí falamos do que unha soa persoa pode facer nuns segundos, a man. Agora quita a persoa. O que durante anos nos protexeu a case todos non foi o anonimato, senón o desinterese: para atoparte, alguén ten que molestarse en mirar, e ninguén ten tempo de mirar a todo o mundo. Esa última barreira —o esforzo de mirar— é xusto a que unha máquina non ten. Un sistema automático pode facer ese mesmo cruce non contra un obxectivo, senón contra unha poboación enteira; non unha vez, senón sen descanso; non por sospeita, senón por defecto. O que antes lle levaba horas a un investigador por cada persoa pasa a facerse sobre millóns á vez, sen que a ninguén lle custe tempo nin atención. Non fai falta supoñer quen querería facelo —unha empresa, un grupo, un Estado—; abonda con entender que xa non hai que elixir a quen mirar. Pódese mirar a todos.

Por iso «poden atoparme?» é a pregunta equivocada. A resposta é si, e serao cada vez máis. A pregunta útil é outra: a quen, e canto, me vexo obrigado a confiar para vivir conectado? Porque iso é o que de verdade fas cada día, case sempre sen pensalo. Confías en que o servizo onde te rexistras gardará ben os teus datos. Confías en que a túa operadora non escoitará as túas chamadas. Confías en que a aplicación de mensaxería que usan todos —poñamos WhatsApp— fai o que di facer. Confías no servidor que hai no medio, na empresa que o administra, no país onde está, na ferramenta gratuíta que alguén colgou na rede. Cada un deses elos é unha decisión de confianza. A diferenza é que case ningunha a tomaches conscientemente: viñan incluídas. A eses elos que se coan entre ti e a outra persoa chámanos, en xerga, intermediarios de confianza; o nome importa menos que a idea de que están aí, e de que son moitos.

Hai un xeito honesto de comprobar todo isto: facelo contigo mesmo. E non necesitas que te deamos nada. Abre o teu navegador, escribe tres ou catro palabras —algo como «que sabe internet do meu correo»— e a propia web poñeráche diante as ferramentas. Esa facilidade é, por si soa, media resposta: se ti das con elas en dez segundos, calquera pode dar co que din de ti.

Non che ofrecemos unha lista nosa, e é deliberado. Se cho désemos, terías que confiar en nós: en que eliximos ben, en que esas páxinas seguirán sendo de fiar dentro de cinco anos, en que detrás de ningunha hai —hoxe ou mañá— alguén con malas intencións. Non podemos prometer iso de páxinas que non controlamos, e preferimos non facer unha promesa que non podemos cumprir. É, exactamente, do que trata este artigo. Pero buscalo ti ten un prezo: o buscador non distingue o lexítimo da trampa. Montar unha páxina que imita a unha ferramenta real, pídiche o correo e quédallo é trivial. Así que, antes de escribir nada en ningún sitio, convén saber ler un enderezo.

Nota — ler un enderezo antes de confiar nel. Unha páxina falsa pode copiar ata o último píxel dunha de verdade; o que case nunca pode falsificar é o seu enderezo. Antes de escribir nada nun sitio, le a barra de enderezos, non a páxina. O nome que manda é o que está pegado á esquerda da última parte (`.com`, `.org`, `.gal`): en `banco-seguro.sitio-raro.top`, o dono real non é o teu banco, é `sitio-raro.top`. Desconfía de letras cambiadas (un `0` por un `o`), de palabras de máis, de guións onde non os agardas e de terminacións estrañas. O cadeado e o `https` só din que a conexión vai cifrada —non que o dono sexa honrado—: un estafador tamén ten cadeado. E os primeiros resultados marcados como «anuncio» están aí porque alguén pagou, non porque sexan de fiar. Cada unha desas comprobacións é, no fondo, a mesma pregunta: canto confío neste enderezo, e por que?

Chegados aquí, convén describir o contrario de todo isto: unha canle sen intermediarios. Dúas persoas, soas no alto dunha montaña, falando. Non hai carteiro, nin centraliña, nin servidor, nin empresa, nin país polo medio. E, non obstante, fíxate: tampouco aí desaparece a confianza. Se lle contas un segredo á outra persoa, estás confiando nela. Esa confianza non se pode quitar —nin falta que fai—, porque é a única que elixiches de verdade: sabes en quen confías, e por que.

O que non hai na montaña é todo o demais. Ninguén no medio. E ese, non outro, é o único modelo que pode reproducirse de forma honesta no dixital: unha canle directa dun dispositivo a outro, sen nada nin ninguén polo camiño. Non elimina a confianza —iso sería mentir—; elimina os intermediarios. Déixate a soas coa única confianza inevitable, a que si escolliches. É, dito sexa de paso, a arquitectura desde a que escribimos estas páxinas; pero o argumento sostense só, constrúa o quen o constrúa.

De xeito que non, non es anónimo, e seguramente non volvas selo. Pero esa nunca foi a batalla que importaba. Non se pode vivir —nin navegar— sen confiar en ninguén; quen o tenta non é máis libre, só está máis só. A madurez non é a desconfianza, que é outra forma de inxenuidade. É ser esixente: saber a quen concedes a túa confianza, canta, a cambio de que e —sobre todo— saber cando llo estás concedendo a alguén sen telo decidido.

Case nada na vida é branco ou negro; case todo vive no gris do medio, e aprender a moverse por ese gris é boa parte do que significa ter criterio. A única excepción é o que vén ben feito de fábrica: aquilo que, por deseño, non che pide confiar en ninguén máis ca na persoa coa que xa decidiches falar. O demais —todo o demais— é cuestión de canto, e a quen.

Nota editorial: cando estes Cuadernos nomean empresas ou produtos, non é para acusar. Quenes os constrúen fan traballos que millóns de persoas usan e aprecian. O que sinalamos é estrutural — o modelo, non a marca. As marcas aparecen como exemplo porque son as que o lector recoñece.

Fontes e lectura adicional

- OSINT (intelixencia de fontes abertas) — reunir información a partir de datos xa públicos; non é intrusión nin espionaxe.
- Reglamento (UE) 2016/679 (RGPD) — sobre o tratamento de datos persoais, incluída a agregación de datos que individualmente eran públicos.

- Rexistros públicos (mercantís, xudiciais, da propiedade) — fonte lexítima e abundante de información persoal en case toda Europa.
- Nesta mesma colección: os cadernos sobre o cifrado de extremo a extremo e «O que unha sinatura non pode arranxar» desenvolven, desde outro ángulo, a mesma idea.

← AnteriorO que unha firma non pode arranxar

Lecturas recentes

- Reflexión · 27 de maio de 2026 O que unha firma non pode arranxar
- Análise · 26 de maio de 2026 Privacidade real vs aparente: as preguntas que convén facerse
- Análise · 25 de maio de 2026 Self-hosting como práctica profesional

Leva este artigo onde o necesites.

↓ Markdown ↓ Texto plano ↓ PDF

O arquivo descárgase no teu dispositivo. Desde aí podes gardalo, importalo a Solo2, o compartilo onde queiras. Cuadernos no decide o destino por ti.

Selo de lacre · SHA-256 f4ce6a963c80c6a51ffb0cafd4e9b07e95f459f51d3a79c2e51d2bffc97f2e70

Cuadernos Lacre · Unha publicación de Menzuri Gestión S.L. ·
escrita por R.Eugenio · editada polo equipo de Solo2.