No eres anónimo

La confianza que no elegiste

Para entendernos: con tu correo, cualquiera averigua en segundos dónde tienes cuenta, y a veces tu cara y tu nombre. No es un fallo: es internet funcionando como siempre. La pregunta no es si pueden verte —pueden—, sino a quién te ves obligado a confiar. Y solo hay un sitio sin nadie en medio: hablar directo, de un aparato a otro.

Basta un correo electrónico. No el tuyo necesariamente: cualquiera. Se escribe en un puñado de herramientas gratuitas —legales, públicas, al alcance de quien quiera buscarlas— y en cuestión de segundos aparece una lista: en qué servicios está registrado ese correo, a veces una foto de perfil, a veces un nombre y un apellido que su dueño creía no haber dado a nadie. No hace falta ser técnico. No se rompe ninguna contraseña. No se comete ningún delito. Toda esa información estaba ya ahí —publicada, registrada o filtrada— esperando a que alguien se molestara en juntarla.

Es tentador leer esto como un fallo: una brecha, un descuido, algo que alguien debería arreglar. No lo es. Es el funcionamiento normal de la web abierta. Cada vez que te das de alta en un servicio, rellenas un formulario, publicas una reseña o apareces en la filtración de otro, dejas una huella. Ninguna de esas huellas es grave por sí sola. El problema —si es que es un problema— nace de juntarlas, y juntarlas es sencillo.

Aquí mucha gente se defiende con una frase razonable: «yo no tengo nada que esconder», o «yo cuido mis cuentas». La primera confunde esconderse con elegir; volveremos a ello. La segunda pasa por alto que la mayor parte de ese rastro no lo dejaste tú: lo dejó el registro mercantil, la web que sufrió la filtración, el conocido que subió una foto contigo y te etiquetó. El anonimato en internet casi nunca es una propiedad que poseas; es, como mucho, oscuridad: el hecho provisional de que nadie se ha molestado todavía en mirar.

Hasta aquí hemos hablado de lo que una sola persona puede hacer en unos segundos, a mano. Ahora quita a la persona. Lo que durante años nos ha protegido a casi todos no fue el anonimato, sino el desinterés: para encontrarte, alguien tiene que molestarse en mirar, y nadie tiene tiempo de mirar a todo el mundo. Esa última barrera —el esfuerzo de mirar— es justo la que una máquina no tiene. Un sistema automático puede hacer ese mismo cruce no contra un objetivo, sino contra una población entera; no una vez, sino sin descanso; no por sospecha, sino por defecto. Lo que antes le llevaba horas a un investigador por cada persona pasa a hacerse sobre millones a la vez, sin que a nadie le cueste tiempo ni atención. No hace falta suponer quién querría hacerlo —una empresa, un grupo, un Estado—; basta con entender que ya no hay que elegir a quién mirar. Se puede mirar a todos.

Por eso «¿pueden encontrarme?» es la pregunta equivocada. La respuesta es sí, y lo será cada vez más. La pregunta útil es otra: ¿a quién, y cuánto, me veo obligado a confiar para vivir conectado? Porque eso es lo que de verdad haces cada día, casi siempre sin pensarlo. Confías en que el servicio donde te registras guardará bien tus datos. Confías en que tu operadora no escuchará tus llamadas. Confías en que la aplicación de mensajería que usan todos —pongamos WhatsApp— hace lo que dice hacer. Confías en el servidor que hay en medio, en la empresa que lo administra, en el país donde está, en la herramienta gratuita que alguien colgó en la red. Cada uno de esos eslabones es una decisión de confianza. La diferencia es que casi ninguna la tomaste conscientemente: venían incluidas. A esos eslabones que se cuelan entre tú y la otra persona los llaman, en jerga, intermediarios de confianza; el nombre importa menos que la idea de que están ahí, y de que son muchos.

Hay una manera honesta de comprobar todo esto: hacerlo contigo mismo. Y no necesitas que te demos nada. Abre tu navegador, escribe tres o cuatro palabras —algo como «qué sabe internet de mi correo»— y la propia web te pondrá delante las herramientas. Esa facilidad es, por sí sola, media respuesta: si tú das con ellas en diez segundos, cualquiera puede dar con lo que dicen de ti.

No te ofrecemos una lista nuestra, y es deliberado. Si te la diéramos, tendrías que confiar en nosotros: en que elegimos bien, en que esas páginas seguirán siendo de fiar dentro de cinco años, en que detrás de ninguna hay —hoy o mañana— alguien con malas intenciones. No podemos prometer eso de páginas que no controlamos, y preferimos no hacer una promesa que no podemos cumplir. Es, exactamente, de lo que trata este artículo. Pero buscarlo tú tiene un precio: el buscador no distingue lo legítimo de la trampa. Montar una página que imita a una herramienta real, te pide el correo y se lo queda es trivial. Así que, antes de escribir nada en ningún sitio, conviene saber leer una dirección.

Nota — leer una dirección antes de confiar en ella. Una página falsa puede copiar hasta el último píxel de una de verdad; lo que casi nunca puede falsificar es su dirección. Antes de escribir nada en un sitio, lee la barra de direcciones, no la página. El nombre que manda es el que está pegado a la izquierda de la última parte (`.com`, `.org`, `.es`): en `banco-seguro.sitio-raro.top`, el dueño real no es tu banco, es `sitio-raro.top`. Desconfía de letras cambiadas (un `0` por una `o`), de palabras de más, de guiones donde no los esperas y de terminaciones extrañas. El candado y el `https` solo dicen que la conexión va cifrada —no que el dueño sea honrado—: un estafador también tiene candado. Y los primeros resultados marcados como «anuncio» están ahí porque alguien ha pagado, no porque sean de fiar. Cada una de esas comprobaciones es, en el fondo, la misma pregunta: ¿cuánto confío en esta dirección, y por qué?

Llegados aquí, conviene describir lo contrario de todo esto: un canal sin intermediarios. Dos personas, solas en lo alto de una montaña, hablando. No hay cartero, ni centralita, ni servidor, ni empresa, ni país de por medio. Y, sin embargo, fíjate: tampoco ahí desaparece la confianza. Si le cuentas un secreto a la otra persona, estás confiando en ella. Esa confianza no se puede quitar —ni falta que hace—, porque es la única que elegiste de verdad: sabes en quién confías, y por qué.

Lo que no hay en la montaña es todo lo demás. Nadie en medio. Y ese, no otro, es el único modelo que puede reproducirse de forma honesta en lo digital: un canal directo de un dispositivo a otro, sin nada ni nadie por el camino. No elimina la confianza —eso sería mentir—; elimina los intermediarios. Te deja a solas con la única confianza inevitable, la que sí escogiste. Es, dicho sea de paso, la arquitectura desde la que escribimos estas páginas; pero el argumento se sostiene solo, lo construya quien lo construya.

De modo que no, no eres anónimo, y seguramente no vuelvas a serlo. Pero esa nunca fue la batalla que importaba. No se puede vivir —ni navegar— sin confiar en nadie; quien lo intenta no es más libre, solo está más solo. La madurez no es la desconfianza, que es otra forma de ingenuidad. Es ser exigente: saber a quién concedes tu confianza, cuánta, a cambio de qué y —sobre todo— saber cuándo se la estás concediendo a alguien sin haberlo decidido.

Casi nada en la vida es blanco o negro; casi todo vive en el gris de en medio, y aprender a moverse por ese gris es buena parte de lo que significa tener criterio. La única excepción es lo que viene bien hecho de fábrica: aquello que, por diseño, no te pide confiar en nadie más que en la persona con la que ya decidiste hablar. Lo demás —todo lo demás— es cuestión de cuánto, y de a quién.

Nota editorial: cuando este Cuaderno nombra empresas o productos, no es para acusar. Quienes los construyen hacen trabajos que millones de personas usan y aprecian. Lo que señalamos es estructural — el modelo, no la marca. Las marcas aparecen como ejemplo porque son las que el lector reconoce.

Fuentes y lectura adicional

- OSINT (inteligencia de fuentes abiertas) — reunir información a partir de datos ya públicos; no es intrusión ni espionaje.

- Reglamento (UE) 2016/679 (RGPD) — sobre el tratamiento de datos personales, incluida la agregación de datos que individualmente eran públicos.
- Registros públicos (mercantiles, judiciales, de la propiedad) — fuente legítima y abundante de información personal en casi toda Europa.
- En esta misma colección: los cuadernos sobre el cifrado de extremo a extremo y «Lo que una firma no puede arreglar» desarrollan, desde otro ángulo, la misma idea.

← AnteriorLo que una firma no puede arreglar

Lecturas recientes

- Reflexión · 27 de mayo de 2026 Lo que una firma no puede arreglar
- Análisis · 26 de mayo de 2026 Privacidad real vs aparente: las preguntas que conviene hacerse
- Análisis · 25 de mayo de 2026 Self-hosting como práctica profesional

Llévate este artículo donde lo necesites.

↓ Markdown ↓ Texto plano ↓ PDF

El archivo se descarga a tu dispositivo. Desde ahí puedes guardarlo, importarlo a Solo2, o compartirlo donde quieras. Cuadernos no decide el destino por ti.

Sello de lacre · SHA-256 75686c067536722ce8c7152daac096c4b25dd8f3926c40653cd27e5c6e302bff

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