Não és anónimo

A confiança que não escolheste

Para sermos claros: com o teu e-mail, qualquer pessoa descobre em segundos onde tens conta, e às vezes o teu rosto e o teu nome. Não é uma falha: é a internet a funcionar como sempre. A pergunta não é se te podem ver — podem —, mas a quem te vês obrigado a confiar. E só há um lugar sem ninguém pelo meio: falar direto, de um aparelho para o outro.

Basta um correio eletrónico. Não necessariamente o teu: o de qualquer pessoa. Escreve-se num punhado de ferramentas gratuitas — legais, públicas, ao alcance de quem as queira procurar — e numa questão de segundos aparece uma lista: em que serviços esse e-mail está registado, às vezes uma foto de perfil, às vezes um nome e um apelido que o seu dono julgava não ter dado a ninguém. Não é preciso ser técnico. Não se quebra nenhuma palavra-passe. Não se comete nenhum crime. Toda essa informação já lá estava — publicada, registada ou divulgada — à espera que alguém se desse ao trabalho de a juntar.

É tentador ler isto como uma falha: uma brecha, um descuido, algo que alguém deveria corrigir. Não é. É o funcionamento normal da web aberta. Cada vez que te registas num serviço, preenches um formulário, publicas uma avaliação ou apareces na fuga de dados de outro, deixas um rasto. Nenhum desses rastos é grave por si só. O problema — se é que é um problema — nasce de os juntar, e juntá-los é simples.

Aqui muitas pessoas defendem-se com uma frase razoável: «eu não tenho nada a esconder», ou «eu cuido das minhas contas». A primeira confunde esconder-se com escolher; voltaremos a isso. A segunda ignora que a maior parte desse rasto não foste tu quem o deixou: deixou-o o registo comercial, o site que sofreu a fuga de dados, o conhecido que publicou uma foto contigo e te identificou. O anonimato na internet quase nunca é uma propriedade que possuas; é, quando muito, obscuridade: o facto provisório de que ninguém se deu ainda ao trabalho de procurar.

Até aqui falámos do que uma única pessoa pode fazer em poucos segundos, à mão. Agora retira a pessoa. O que durante anos nos protegeu a quase todos não foi o anonimato, mas o desinteresse: para te encontrar, alguém tem de se dar ao trabalho de procurar, e ninguém tem tempo de procurar toda a gente. Essa última barreira — o esforço de procurar — é exatamente aquela que uma máquina não tem. Um sistema automático pode fazer esse mesmo cruzamento não contra um alvo, mas contra uma população inteira; não uma vez, mas sem descanso; não por suspeita, mas por defeito. O que antes levava horas a um investigador por cada pessoa passa a ser feito sobre milhões em simultâneo, sem que a ninguém custe tempo nem atenção. Não é preciso supor quem quereria fazê-lo — uma empresa, um grupo, um Estado —; basta entender que já não é preciso escolher quem procurar. Pode procurar-se toda a gente.

Por isso «podem encontrar-me?» é a pergunta errada. A resposta é sim, e sê-lo-á cada vez mais. A pergunta útil é outra: a quem, e quanto, me vejo obrigado a confiar para viver conectado? Porque isso é o que realmente fazes todos os dias, quase sempre sem pensar. Confias que o serviço onde te registas guardará bem os teus dados. Confias que a tua operadora não ouvirá as tuas chamadas. Confias que a aplicação de mensagens que todos usam — digamos o WhatsApp — faz o que diz fazer. Confias no servidor que está no meio, na empresa que o administra, no país onde se encontra, na ferramenta gratuita que alguém publicou na rede. Cada um desses elos é uma decisão de confiança. A diferença é que quase nenhuma tomaste de forma consciente: já vinham incluídas. A

esses elos que se intrometem entre ti e a outra pessoa chamam, na gíria, intermediários de confiança; o nome importa menos que a ideia de que estão aí, e de que são muitos.

Há uma forma honesta de comprovar tudo isto: fá-lo contigo mesmo. E não precisas que te demos nada. Abre o teu navegador, escreve três ou quatro palavras — algo como «o que sabe a internet do meu e-mail» — e a própria web colocar-te-á as ferramentas à frente. Essa facilidade é, por si só, meia resposta: se tu dás com elas em dez segundos, qualquer um pode dar com o que dizem de ti.

Não te oferecemos uma lista nossa, e é deliberado. Se a déssemos, terias de confiar em nós: de que escolhemos bem, de que essas páginas continuarão a ser de confiança daqui a cinco anos, de que por trás de nenhuma delas há — hoje ou amanhã — alguém com más intenções. Não podemos prometer isso de páginas que não controlamos, e preferimos não fazer uma promessa que não podemos cumprir. É, exatamente, do que trata este artigo. Mas seres tu a procurar tem um preço: o motor de busca não distingue o legítimo da armadilha. Montar uma página que imita uma ferramenta real, te pede o e-mail e fica com ele é trivial. Por isso, antes de escreveres algo em algum lado, convém saber ler um endereço.

Nota — ler um endereço antes de confiar nele. Uma página falsa pode copiar até o último pixel de uma verdadeira; o que quase nunca consegue falsificar é o seu endereço. Antes de escrever algo num site, lê a barra de endereços, não a página. O nome que manda é o que está colado à esquerda da última parte (`.com`, `.org`, `.pt`): em `banco-seguro.site-estranho.top`, o dono real não é o teu banco, é `site-estranho.top`. Desconfia de letras trocadas (um `0` por um `o`), de palavras a mais, de hífenes onde não os esperas e de terminações estranhas. O cadeado e o `https` apenas dizem que a conexão vai cifrada — não que o dono é honesto —: um burlão também tem cadeado. E os primeiros resultados marcados como «anúncio» estão aí porque alguém pagou, não porque sejam de confiança. Cada uma dessas verificações é, no fundo, a mesma pergunta: quanto confio neste endereço, e porquê?

Chegados aqui, convém descrever o contrário de tudo isto: um canal sem intermediários. Duas pessoas, sozinhas no alto de uma montanha, a falar. Não há carteiro, nem central telefónica, nem servidor, nem empresa, nem país pelo meio. E, no entanto, repara: a confiança também não desaparece aí. Se contares um segredo à outra pessoa, estás a confiar nela. Essa confiança não se pode retirar — nem é preciso —, porque é a única que escolheste de verdade: sabes em quem confias, e porquê.

O que não há na montanha é tudo o resto. Ninguém no meio. E esse, não outro, é o único modelo que pode ser reproduzido de forma honesta no meio digital: um canal direto de um dispositivo para outro, sem nada nem ninguém pelo caminho. Não elimina a confiança — isso seria mentir —; elimina os intermediários. Deixa-te a sós com a única confiança inevitável, a que de facto escolheste. É, diga-se de passagem, a arquitetura a partir da qual escrevemos estas páginas; mas o argumento sustenta-se por si só, seja quem for que o construa.

De modo que não, não és anónimo, e provavelmente não voltarás a sê-lo. Mas essa nunca foi a batalha que importava. Não se pode viver — nem navegar — sem confiar em ninguém; quem o tenta não é mais livre, apenas está mais só. A maturidade não é a desconfiança, que é outra forma de ingenuidade. É ser exigente: saber a quem concedes a tua confiança, quanta, em troca de quê e — sobretudo — saber quando a estás a conceder a alguém sem o teres decidido.

Quase nada na vida é preto ou branco; quase tudo vive no cinzento intermédio, e aprender a mover-se por esse cinzento é boa parte do que significa ter critério. A única exceção é o que já vem bem feito de fábrica: aquilo que, por conceção, não te pede para confiar em ninguém além da pessoa com quem já decidiste falar. O resto — tudo o resto — é questão de quanto, e de a quem.

Nota editorial: quando estes Cuadernos nomeiam empresas ou produtos, não é para acusar. Aqueles que os constroem fazem trabalhos que milhões de pessoas usam e apreciam. O que assinalamos é estrutural — o modelo, não a marca. As marcas aparecem como exemplo porque são as que o leitor reconhece.

Fontes e leitura adicional

- OSINT (inteligência de fontes abertas) — reunir informação a partir de dados já públicos; não é intrusão nem espionagem.
- Reglamento (UE) 2016/679 (RGPD) — sobre o tratamento de dados pessoais, incluindo a agregação de dados que individualmente eram públicos.
- Registos públicos (comerciais, judiciais, prediais) — fonte legítima e abundante de informação pessoal em quase toda a Europa.
- Nesta mesma coleção: os cadernos sobre a cifragem ponta-a-ponta e «O que uma assinatura não pode resolver» desenvolvem, a partir de outro ângulo, a mesma ideia.

← AnteriorLo que una firma no puede arreglar

Leituras recentes

- Reflexão · 27 de maio de 2026 Lo que una firma no puede arreglar
- Análise · 26 de maio de 2026 Privacidade real vs aparente: as perguntas que convém fazer-se
- Análise · 25 de maio de 2026 Self-hosting como prática profissional

Leve este artigo para onde precisar.

↓ Markdown ↓ Texto simples ↓ PDF

O arquivo é descarregado no seu dispositivo. A partir daí, pode guardá-lo, importá-lo no Solo2 ou partilhá-lo onde quiser. Cuadernos não decide o destino por si.

Selo de lacre · SHA-256 43d84fd341b2c3f31e9a061ef934db5f012c15964c482844c9de7de2e5498329

Cuadernos Lacre · Uma publicação da Menzuri Gestión S.L. ·
escrita por R.Eugenio · editada pela equipa do Solo2.