Vous n'êtes pas anonyme

La confiance que vous n'avez pas choisie

En clair : avec votre e-mail, n'importe qui peut découvrir en quelques secondes où vous avez un compte, et parfois votre visage et votre nom. Ce n'est pas une faille : c'est internet qui fonctionne comme à son habitude. La question n'est pas de savoir s'ils peuvent vous voir — ils le peuvent —, mais à qui vous êtes obligé de faire confiance. Et il n'y a qu'un seul endroit sans personne au milieu : parler en direct, d'un appareil à l'autre.

Un e-mail suffit. Pas nécessairement le vôtre : n'importe lequel. Il est saisi dans une poignée d'outils gratuits — légaux, publics, à la portée de quiconque veut chercher — et en quelques secondes une liste apparaît : sur quels services cet e-mail est enregistré, parfois une photo de profil, parfois un nom et un prénom que son propriétaire pensait n'avoir donnés à personne. Pas besoin d'être un technicien. Aucun mot de passe n'est piraté. Aucun délit n'est commis. Toutes ces informations étaient déjà là — publiées, enregistrées ou divulguées — attendant que quelqu'un prenne la peine de les rassembler.

Il est tentant de voir cela comme une faille : une brèche, une imprudence, quelque chose que quelqu'un devrait réparer. Ce n'est pas le cas. C'est le fonctionnement normal du web ouvert. Chaque fois que vous vous inscrivez à un service, remplissez un formulaire, publiez un avis ou apparaissez dans la fuite de données de quelqu'un d'autre, vous laissez une trace. Aucune de ces traces n'est grave en soi. Le problème — s'il y a un problème — vient de leur rassemblement, et les rassembler est simple.

Ici, beaucoup se défendent avec une phrase raisonnable : « je n'ai rien à cacher », ou « je fais attention à mes comptes ». La première confond se cacher avec choisir ; nous y reviendrons. La seconde ignore que la majeure partie de cette trace n'a pas été laissée par vous : c'est le registre du commerce, le site web qui a subi la fuite, la connaissance qui a téléchargé une photo avec vous et vous a identifié. L'anonymat sur internet n'est presque jamais une propriété que vous possédez ; c'est tout au plus de l'obscurité : le fait provisoire que personne n'a encore pris la peine de regarder.

Jusqu'ici, nous avons parlé de ce qu'une seule personne peut faire à la main en quelques secondes. Maintenant, enlevez la personne. Ce qui nous a protégés presque tous pendant des années n'était pas l'anonymat, mais le manque d'intérêt : pour vous trouver, quelqu'un doit prendre la peine de chercher, et personne n'a le temps de chercher tout le monde. Cette dernière barrière — l'effort de chercher — est précisément celle qu'une machine n'a pas. Un système automatique peut faire ce même croisement non pas contre une cible, mais contre une population entière ; non pas une fois, mais sans relâche ; non pas par suspicion, mais par défaut. Ce qui prenait auparavant des heures à un enquêteur pour chaque personne se fait désormais sur des millions en même temps, sans que cela coûte de temps ni d'attention à personne. Il n'est pas nécessaire de supposer qui voudrait le faire — une entreprise, un groupe, un État — ; il suffit de comprendre qu'il n'est plus nécessaire de choisir qui regarder. On peut regarder tout le monde.

C'est pourquoi « peuvent-ils me trouver ? » est la mauvaise question. La réponse est oui, et ce sera de plus en plus le cas. La question utile est autre : à qui, et dans quelle mesure, suis-je obligé de faire confiance pour vivre connecté ? Car c'est ce que vous faites vraiment chaque jour, presque toujours sans y penser. Vous avez confiance que le service où vous vous inscrivez gardera bien vos données. Vous avez confiance que votre opérateur n'écoutera pas vos appels. Vous avez confiance que l'application de messagerie que tout le monde utilise — disons WhatsApp — fait ce qu'elle dit faire. Vous avez confiance dans le serveur au milieu, dans l'entreprise qui

l'administre, dans le pays où il se trouve, dans l'outil gratuit que quelqu'un a mis sur le réseau. Chacun de ces maillons est une décision de confiance. La différence, c'est que vous n'en avez pris presque aucune consciemment : elles étaient incluses. Ces maillons qui s'infiltrent entre vous et l'autre personne sont appelés, dans le jargon, des intermédiaires de confiance ; le nom importe moins que l'idée qu'ils sont là, et qu'ils sont nombreux.

Il y a une manière honnête de vérifier tout cela : le faire vous-même. Et vous n'avez pas besoin que nous vous donnions quoi que ce soit. Ouvrez votre navigateur, écrivez trois ou quatre mots — quelque chose comme « que sait internet de mon adresse e-mail » — et le web lui-même vous mettra les outils sous les yeux. Cette facilité est, à elle seule, la moitié de la réponse : si vous les trouvez en dix secondes, n'importe qui peut trouver ce qu'ils disent de vous.

Nous ne vous proposons pas de liste de notre part, et c'est délibéré. Si nous vous la donnions, vous devriez nous faire confiance : que nous avons bien choisi, que ces sites seront toujours fiables dans cinq ans, que derrière aucun d'eux ne se cache — aujourd'hui ou demain — quelqu'un avec de mauvaises intentions. Nous ne pouvons pas promettre cela pour des pages que nous ne contrôlons pas, et nous préférons ne pas faire une promesse que nous ne pouvons pas tenir. C'est exactement le sujet de cet article. Mais chercher vous-même a un prix : le moteur de recherche ne distingue pas le légitime du piège. Monter une page qui imite un outil réel, vous demande votre e-mail et le conserve est trivial. Donc, avant d'écrire quoi que ce soit où que ce soit, il convient de savoir lire une adresse.

Note — lire une adresse avant de lui faire confiance. Une fausse page peut copier jusqu'au dernier pixel d'une vraie ; ce qu'elle ne peut presque jamais falsifier, c'est son adresse. Avant d'écrire quoi que ce soit sur un site, lisez la barre d'adresse, pas la page. Le nom qui compte est celui qui est collé à gauche de la dernière partie (`.com`, `.org`, `.fr`) : dans `banque-securisee.site-bizarre.top`, le vrai propriétaire n'est pas votre banque, c'est `site-bizarre.top`. Méfiez-vous des lettres changées (un `0` pour un `o`), des mots en trop, des tirets là où vous ne les attendez pas et des terminaisons étranges. Le cadenas et le `https` disent seulement que la connexion est chiffrée — pas que le propriétaire est honnête — : un escroc a aussi un cadenas. Et les premiers résultats marqués comme « annonce » sont là parce que quelqu'un a payé, pas parce qu'ils sont fiables. Chacune de ces vérifications est, au fond, la même question : à quel point ai-je confiance en cette adresse, et pourquoi ?

Arrivé ici, il convient de décrire le contraire de tout cela : un canal sans intermédiaires. Deux personnes, seules au sommet d'une montagne, en train de parler. Il n'y a pas de facteur, ni de standard, ni de serveur, ni d'entreprise, ni de pays au milieu. Et pourtant, remarquez : là non plus la confiance ne disparaît pas. Si vous racontez un secret à l'autre personne, vous lui faites confiance. Cette confiance ne peut pas être enlevée — et ce n'est pas nécessaire —, car c'est la seule que vous avez vraiment choisie : vous savez à qui vous faites confiance, et pourquoi.

Ce qu'il n'y a pas sur la montagne, c'est tout le reste. Personne au milieu. Et c'est là, et pas ailleurs, le seul modèle qui peut être reproduit de manière honnête dans le numérique : un canal direct d'un appareil à l'autre, sans rien ni personne en chemin. Il n'élimine pas la confiance — ce serait mentir — ; il élimine les intermédiaires. Il vous laisse seul avec la seule confiance inévitable, celle que vous avez choisie. C'est d'ailleurs l'architecture depuis laquelle nous écrivons ces pages ; mais l'argument tient tout seul, peu importe qui le construit.

Donc non, vous n'êtes pas anonyme, et vous ne le serez probablement plus jamais. Mais ce n'a jamais été la bataille qui importait. On ne peut pas vivre — ni naviguer — sans faire confiance à personne ; celui qui essaie n'est pas plus libre, il est juste plus seul. La maturité ce n'est pas la méfiance, qui est une autre forme de naïveté. C'est être exigeant : savoir à qui vous accordez votre confiance, combien, en échange de quoi et — surtout — savoir quand vous l'accordez à quelqu'un sans l'avoir décidé.

Presque rien dans la vie n'est tout blanc ou tout noir ; presque tout vit dans le gris du milieu, et apprendre à se mouvoir dans ce gris est une grande part de ce que signifie avoir du discernement. La seule exception est ce qui vient bien fait d'usine : ce qui, par conception, ne vous demande de faire confiance à personne d'autre qu'à la personne avec qui vous avez déjà décidé de parler. Le reste — tout le reste — est une question de combien, et à qui.

Note éditoriale : quand ces Cuadernos nomment des entreprises ou des produits, ce n'est pas pour accuser. Ceux qui les construisent font un travail que des millions de personnes utilisent et apprécient. Ce que nous soulignons est structurel — le modèle, pas la marque. Les marques apparaissent comme exemples car ce sont celles que le lecteur reconnaît.

Sources et lectures complémentaires

- OSINT (renseignement d'origine sources ouvertes) — rassembler des informations à partir de données déjà publiques ; ce n'est ni de l'intrusion ni de l'espionnage.
- Reglamento (UE) 2016/679 (RGPD) — sur le traitement des données personnelles, y compris l'agrégation de données qui étaient individuellement publiques.
- Registres publics (commerce, justice, propriété) — source légitime et abondante d'informations personnelles dans presque toute l'Europe.
- Dans cette même collection : les carnets sur le chiffrement de bout en bout et « Ce qu'une signature ne peut pas réparer » développent, sous un autre angle, la même idée.

← PrécédentCe qu'une signature ne peut pas réparer

Lectures recentes

- Réflexion · 27 mai 2026 Ce qu'une signature ne peut pas réparer
- Analyse · 26 mai 2026 Confidentialité réelle vs apparente : les questions à se poser
- Analyse · 25 mai 2026 Self-hosting comme pratique professionnelle

Emportez cet article où vous en avez besoin.

↓ Markdown ↓ Texte brut ↓ PDF

Le fichier est téléchargé sur votre appareil. À partir de là, vous pouvez l'enregistrer, l'importer dans Solo2 ou le partager comme vous le souhaitez. Cuadernos ne décide pas de la destination pour vous.

Cachet de cire · SHA-256 fc0a8a060e9693c67288bcbf3e98a14591d41f86828751308b178564667deb8e

Cuadernos Lacre · Une publication de Menzuri Gestión S.L. ·
écrite par R.Eugenio · éditée par l'équipe de Solo2.