Du er ikke anonym

Tilliten du ikke valgte

Kort fortalt: med e-posten din kan hvem som helst finne ut på få sekunder hvor du har en konto, og noen ganger ansiktet ditt og navnet ditt. Det er ikke en feil: det er slik internett normalt fungerer. Spørsmålet er ikke om de kan se deg —det kan de—, men hvem du er tvunget til å stole på. Og det finnes bare ett sted uten noen i midten: å snakke direkte, fra en enhet til en annen.

En e-postadresse er nok. Ikke nødvendigvis din: hvem som helst sin. Den skrives inn i en håndfull gratis verktøy —lovlige, offentlige, tilgjengelige for alle som vil lete— og i løpet av få sekunder dukker det opp en liste: hvilke tjenester den e-posten er registrert i, noen ganger et profilbilde, noen ganger et fornavn og etternavn som eieren trodde at de ikke hadde gitt til noen. Du trenger ikke å være teknisk anlagt. Ingen passord knekkes. Ingen lovbrudd begås. All den informasjonen var allerede der —publisert, registrert eller lekket— og ventet bare på at noen skulle ta seg bryet med å sette den sammen.

Det er fristende å lese dette som en feil: et brudd, en forglemmelse, noe noen burde fikse. Det er det ikke. Det er den normale funksjonen til det åpne nettet. Hver gang du registrerer deg for en tjeneste, fyller ut et skjema, publiserer en anmeldelse eller dukker opp i en annens datalekkasje, legger du igjen et spor. Ingen av disse sporene er alvorlige i seg selv. Problemet —hvis det i det hele tatt er et problem— oppstår ved å sette dem sammen, og å sette dem sammen er enkelt.

Her forsvarer mange seg med en rimelig setning: «jeg har ingenting å skjule», eller «jeg passer på kontoene mine». Den første forveksler det å gjemme seg med det å velge; vi kommer tilbake til det. Den andre overser at mesteparten av det sporet ikke ble lagt igjen av deg: det ble lagt igjen av foretaksregisteret, nettstedet som led av datalekkasjen, bekjenten som lastet opp et bilde med deg og tagget deg. Anonymitet på internett er nesten aldri en egenskap du besitter; det er på det meste dunkelhet: det midlertidige faktum at ingen har tatt seg bryet med å se etter ennå.

Så langt har vi snakket om hva én person kan gjøre på noen få sekunder, manuelt. Fjern nå personen. Det som har beskyttet de fleste av oss i årevis var ikke anonymitet, men mangel på interesse: for å finne deg må noen ta seg bryet med å lete, og ingen har tid til å se på alle. Den siste barrieren —innsatsen med å lete— er akkurat den maskinen ikke har. Et automatisk system kan gjøre den samme kryssjekkingen, ikke mot ett mål, men mot en hel befolkning; ikke én gang, men nådeløst; ikke på grunn av mistanke, men som standard. Det som tidligere tok timer for en etterforsker per person, gjøres nå på millioner samtidig, uten å koste noen tid eller oppmerksomhet. Man trenger ikke å anta hvem som ønsker å gjøre det —et selskap, en gruppe, en stat—; det er nok å forstå at det ikke lenger er nødvendig å velge hvem man skal se på. Alle kan sees.

Derfor er «kan de finne meg?» feil spørsmål. Svaret er ja, og det vil det i økende grad være. Det nyttige spørsmålet er annerledes: hvem, og hvor mye, er jeg tvunget til å stole på for å leve tilkoblet? Fordi det er det du egentlig gjør hver dag, nesten alltid uten å tenke over det. Du stoler på at tjenesten der du registrerer deg, vil oppbevare dataene dine på en god måte. Du stoler på at teleoperatøren din ikke lytter til samtalene dine. Du stoler på at meldingsappen som alle bruker —la oss si WhatsApp— gjør det den sier den gjør. Du stoler på serveren i midten, på selskapet som driver den, på landet den befinner seg i, på det gratis verktøyet som noen la ut på nettet. Hvert av disse leddene er en beslutning om tillit. Forskjellen er at du nesten aldri tok dem bevisst: de

var inkludert. De leddene som sniker seg inn mellom deg og den andre personen, kalles i sjargong for tillitsmellommenn; navnet betyr mindre enn ideen om at de er der, og at de er mange.

Det finnes en ærlig måte å sjekke alt dette på: gjør det med deg selv. Og du trenger ikke at vi gir deg noe. Åpne nettleseren din, skriv tre eller fire ord —noe som «hva vet internett om min e-post»— og nettet vil selv legge verktøyene foran deg. Den enkelheten er i seg selv halve svaret: hvis du finner dem på ti sekunder, kan hvem som helst finne ut hva de sier om deg.

Vi tilbyr ikke vår egen liste, og det er bevisst. Hvis vi ga deg den, måtte du stole på oss: at vi valgte riktig, at disse sidene vil forbli pålitelige om fem år, at bak noen av dem ikke finnes —i dag eller i morgen— noen med dårlige hensikter. Vi kan ikke love det for sider vi ikke kontrollerer, og vi foretrekker å ikke gi et løfte vi ikke kan holde. Det er nøyaktig hva denne artikkelen handler om. Men å søke etter det selv har en pris: søkemotoren skiller ikke det legitime fra fellen. Å sette opp en side som imiterer et ekte verktøy, ber om e-posten din og beholder den, er trivielt. Så, før du skriver noe noen steder, bør du vite hvordan du leser en adresse.

Merknad — les en adresse før du stoler på den. En falsk side kan kopiere den ekte ned til minste piksel; det som nesten aldri kan forfalskes, er adressen dens. Før du skriver noe på et nettsted, les adresselinjen, ikke siden. Navnet som gjelder er det som står helt til venstre for den siste delen (`.com`, `.org`, `.no`): i `trygg-bank.rar-side.top` er ikke den virkelige eieren banken din, det er `rar-side.top`. Vær på vakt mot endrede bokstaver (en `0` for en `o`), ekstra ord, bindestreker der du ikke forventer dem, og merkelige endelser. Hengelåsen og `https` betyr bare at tilkoblingen er kryptert —ikke at eieren er ærlig—: en svindler har også en hengelås. Og de første resultatene som er merket som «annonse» er der fordi noen har betalt for dem, ikke fordi de er til å stole på. Hver av disse sjekkene er dypest sett det samme spørsmålet: hvor mye stoler jeg på denne adressen, og hvorfor?

Når vi har kommet hit, er det verdt å beskrive det motsatte av alt dette: en kanal uten mellomledd. To personer, alene på toppen av et fjell, i samtale. Det er ingen postbud, ingen sentralbord, ingen server, intet selskap, og intet land i mellom. Og likevel, legg merke til: tilliten forsvinner ikke engang der. Hvis du forteller en hemmelighet til den andre personen, stoler du på dem. Den tilliten kan ikke fjernes —og det er det heller ikke behov for— for det er den eneste du virkelig valgte: du vet hvem du stoler på, og hvorfor.

Det som mangler på fjellet, er alt det andre. Ingen i midten. Og den modellen, ingen annen, er den eneste som kan reproduseres ærlig i det digitale rommet: en direkte kanal fra én enhet til en annen, uten noe eller noen på veien. Den fjerner ikke tilliten —det ville være løgn— den fjerner mellomleddene. Den lar deg være alene med den eneste uunngåelige tilliten, den du selv valgte. Det er forøvrig arkitekturen vi skriver disse sidene fra; men argumentet står på egne ben, uavhengig av hvem som bygger det.

Så nei, du er ikke anonym, og du blir det sannsynligvis aldri igjen. Men det var aldri den kampen som gjaldt. Man kan ikke leve —eller navigere— uten å stole på noen; de som prøver på det blir ikke friere, de blir bare mer ensomme. Modenhet er ikke mistillit, som bare er en annen form for naivitet. Det er å være kravstor: å vite hvem du gir tilliten din til, hvor mye, i bytte mot hva og —fremfor alt— å vite når du gir den til noen uten å ha tatt en beslutning om det.

Nesten ingenting i livet er svart eller hvitt; nesten alt lever i gråsonen i midten, og det å lære å navigere i den gråsonen er en stor del av det å ha dømmekraft. Det eneste unntaket er det som kommer vellaget fra fabrikken: det som, gjennom sin design, ikke ber deg om å stole på noen andre enn den personen du allerede har bestemt deg for å snakke med. Resten —alt det andre— er bare et spørsmål om hvor mye, og på hvem.

Redaksjonell note: når disse Cuadernos nevner selskaper eller produkter, er det ikke for å anklage. De som bygger dem, gjør en jobb som millioner av mennesker bruker og verdsetter. Det vi påpeker er strukturelt — modellen, ikke merkevaren. Merkevarene vises som eksempler fordi det er disse leseren kjenner til.

Kilder og videre lesing

- OSINT (Open Source Intelligence) — innhenting av informasjon fra data som allerede er offentlige; det er ikke innbrudd eller spionasje.

- Reglamento (UE) 2016/679 (RGPD) — om behandling av personopplysninger, inkludert sammenslåing av data som hver for seg var offentlige.
- Offentlige registre (foretaks-, retts-, og eiendomsregistre) — lovlig og rikelig kilde til personopplysninger i nesten hele Europa.
- I denne samme samlingen: notatbøkene om ende-til-ende-kryptering og «Det en signatur ikke kan fikse» utdyper den samme ideen fra en annen vinkel.

← ForrigeDet en signatur ikke kan fikse

Siste lesninger

- Refleksjon · 27. mai 2026 Det en signatur ikke kan fikse
- Analyse · 26. mai 2026 Reelt vs. tilsynelatende personvern: Spørsmålene man bør stille seg selv
- Analyse · 25. mai 2026 Self-hosting som profesjonell praksis

Ta med deg denne artikkelen dit du trenger den.

↓ Markdown ↓ Klartekst ↓ PDF

Filen lastes ned til enheten din. Derfra kan du lagre den, importere den til Solo2 eller dele den hvor du vil. Cuadernos bestemmer ikke destinasjonen for deg.

Lakksegl · SHA-256 e7268da030ba398526157611ca8fbf7223e4ff06f20e22f292b9dacc3f15ec08

Cuadernos Lacre · En utgivelse fra Menzuri Gestión S.L. ·
skrevet av R.Eugenio · redigert av teamet bak Solo2.