Du er ikke anonym

Den tillid, du ikke valgte

Kort og godt: med din e-mail kan enhver på få sekunder finde ud af, hvor du har en konto, og nogle gange dit ansigt og navn. Det er ikke en fejl: det er internettet, der fungerer, som det altid har gjort. Spørgsmålet er ikke, om de kan se dig — det kan de —, men hvem du er tvunget til at stole på. Og der er kun ét sted uden nogen i midten: at tale direkte, fra den ene enhed til den anden.

Det er nok med en e-mail. Ikke nødvendigvis din: hvilken som helst. Den skrives ind i en håndfuld gratis værktøjer — lovlige, offentlige, tilgængelige for enhver, der ønsker at lede efter dem — og på få sekunder vises en liste: hvilke tjenester e-mailen er registreret på, nogle gange et profilbillede, nogle gange et for- og efternavn, som ejeren troede, de ikke havde givet til nogen. Du behøver ikke at være teknisk anlagt. Ingen adgangskoder brydes. Der begås ingen kriminalitet. Al den information var der allerede — offentliggjort, registreret eller lækket — og ventede på, at nogen gad at samle den.

Det er fristende at læse dette som en fejl: et brud, en forglemmelse, noget nogen burde rette. Det er det ikke. Det er den normale funktion af det åbne web. Hver gang du tilmelder dig en tjeneste, udfylder en formular, udgiver en anmeldelse eller optræder i andres datalækage, efterlader du et spor. Ingen af disse spor er alvorlige i sig selv. Problemet — hvis det da er et problem — opstår, når man samler dem, og det er enkelt at samle dem.

Her forsvarer mange mennesker sig med en fornuftig sætning: »jeg har intet at skjule« eller »jeg passer på mine konti«. Den første forveksler det at skjule sig med at vælge; det vender vi tilbage til. Den anden overser, at det meste af det spor ikke blev efterladt af dig: det blev efterladt af erhvervsregisteret, den hjemmeside, der led af lækagen, bekendten, der uploadede et billede med dig og taggede dig. Anonymitet på internettet er næsten aldrig en egenskab, du besidder; det er højst ubemærkethed: den foreløbige kendsgerning, at ingen endnu har gidet at lede.

Indtil nu har vi talt om, hvad en enkelt person kan gøre på få sekunder, manuelt. Fjern nu personen. Det, der i årevis har beskyttet næsten os alle, var ikke anonymitet, men mangel på interesse: for at finde dig skal nogen gide at lede, og ingen har tid til at lede efter alle. Denne sidste barriere — indsatsen for at lede — er præcis, hvad en maskine ikke har. Et automatisk system kan foretage samme krydsning, ikke mod et mål, men mod en hel befolkning; ikke én gang, men uden pause; ikke på grund af mistanke, men som standard. Det, der før tog en forsker timer for hver person, gøres nu på millioner på samme tid, uden at det koster nogen tid eller opmærksomhed. Det er ikke nødvendigt at antage, hvem der vil gøre det — en virksomhed, en gruppe, en stat —; det er nok at forstå, at det ikke længere er nødvendigt at vælge, hvem man skal kigge på. Man kan kigge på alle.

Derfor er »kan de finde mig?« det forkerte spørgsmål. Svaret er ja, og det vil det i stigende grad være. Det nyttige spørgsmål er et andet: hvem, og hvor meget, er jeg tvunget til at stole på for at leve forbundet? For det er, hvad du i virkeligheden gør hver dag, næsten altid uden at tænke over det. Du stoler på, at den tjeneste, hvor du registrerer dig, opbevarer dine data godt. Du stoler på, at din teleudbyder ikke lytter til dine opkald. Du stoler på, at den besked-app, som alle bruger — lad os sige WhatsApp —, gør, hvad den siger, den gør. Du stoler på serveren i midten, på det firma, der administrerer den, på det land, hvor den er placeret, på det gratis værktøj, som nogen lagde ud på nettet. Hvert af disse led er en tillidsbeslutning. Forskellen er, at du næsten ikke tog

nogen af dem bevidst: de var inkluderet. Disse led, der sniger sig ind mellem dig og den anden person, kaldes i jargon for tillidsmellemmænd; navnet betyder mindre end ideen om, at de er der, og at de er mange.

Der er en ærlig måde at tjekke alt dette på: gør det med dig selv. Og du behøver ikke, at vi giver dig noget. Åbn din browser, skriv tre eller fire ord — noget i retning af »hvad ved internettet om min e-mail« — og nettet vil selv lægge værktøjerne foran dig. Denne lethed er i sig selv halvdelen af svaret: hvis du kan finde dem på ti sekunder, kan enhver finde, hvad de siger om dig.

Vi tilbyder dig ikke en liste fra os, og det er bevidst. Hvis vi gav dig den, ville du skulle stole på os: på at vi valgte rigtigt, på at de sider vil forblive pålidelige om fem år, på at der ikke bag nogen af dem er — i dag eller i morgen — nogen med dårlige hensigter. Vi kan ikke love det for sider, vi ikke kontrollerer, og vi foretrækker ikke at give et løfte, vi ikke kan holde. Det er præcis, hvad denne artikel handler om. Men der er en pris at betale for selv at lede: søgemaskinen skelner ikke mellem det legitime og en fælde. Det er trivielt at opsætte en side, der efterligner et rigtigt værktøj, beder om din e-mail og beholder den. Derfor er det klogt at vide, hvordan man læser en adresse, før man skriver noget som helst.

Bemærk — læs en adresse, før du stoler på den. En falsk side kan kopiere en rigtig side ned til den mindste pixel; det, den næsten aldrig kan forfalske, er dens adresse. Før du skriver noget på en side, skal du læse adresselinjen, ikke siden. Det navn, der gælder, er det, der står til venstre for den sidste del (`.com`, `.org`, `.dk`): på `sikker-bank.maerkelig-side.top` er den reelle ejer ikke din bank, det er `maerkelig-side.top`. Vær mistænksom over for ændrede bogstaver (et `0` i stedet for et `o`), ekstra ord, bindestreger, hvor du ikke forventer dem, og mærkelige endelser. Hængelåsen og `https` siger kun, at forbindelsen er krypteret — ikke at ejeren er ærlig —: en svindler har også en hængelås. Og de første resultater markeret som »annonce« er der, fordi nogen har betalt, ikke fordi de er pålidelige. Hver af disse kontroller er i bund og grund det samme spørgsmål: hvor meget stoler jeg på denne adresse, og hvorfor?

Her er det passende at beskrive det modsatte af alt dette: en kanal uden mellemmænd. To mennesker, alene på toppen af et bjerg, der taler sammen. Der er ingen postbud, intet omstillingsbord, ingen server, intet firma, intet land i midten. Og alligevel, læg mærke til: tilliden forsvinder heller ikke der. Hvis du fortæller en hemmelighed til den anden person, stoler du på dem. Den tillid kan ikke fjernes — og der er heller ingen grund til det —, fordi det er den eneste, du virkelig har valgt: du ved, hvem du stoler på, og hvorfor.

Det, der ikke er på bjerget, er alt det andet. Ingen i midten. Og dette, og intet andet, er den eneste model, der ærligt kan reproduceres i den digitale verden: en direkte kanal fra en enhed til en anden, uden noget eller nogen på vejen. Det eliminerer ikke tillid — det ville være en løgn —; det eliminerer mellemmænd. Det efterlader dig alene med den eneste uundgåelige tillid, den du valgte. Det er for øvrigt den arkitektur, vi skriver disse sider ud fra; men argumentet holder af sig selv, uanset hvem der bygger det.

Så nej, du er ikke anonym, og det bliver du sandsynligvis aldrig igen. Men det var aldrig den kamp, der var vigtig. Man kan ikke leve — og heller ikke surfe — uden at stole på nogen; den, der forsøger, er ikke mere fri, bare mere ensom. Modenhed er ikke mistillid, hvilket blot er en anden form for naivitet. Det er at være krævende: at vide, hvem du giver din tillid, hvor meget, i bytte for hvad og — frem for alt — at vide, hvornår du giver den til nogen uden at have besluttet det.

Næsten intet i livet er sort eller hvidt; næsten alt lever i den grå zone i midten, og at lære at navigere i dette grå område er en stor del af, hvad det vil sige at have dømmekraft. Den eneste undtagelse er det, der kommer vellavet fra fabrikken: det, der ved sit design ikke beder dig stole på nogen anden end den person, du allerede har besluttet at tale med. Resten — alt det andet — er et spørgsmål om hvor meget, og til hvem.

Redaktionel note: Når disse Cuadernos nævner virksomheder eller produkter, er det ikke for at anklage. De, der bygger dem, udfører et stykke arbejde, som millioner bruger og værdsætter. Det, vi påpeger, er strukturelt — modellen, ikke brandet. Brands optræder som eksempler, fordi det er dem, læseren genkender.

Kilder og yderligere læsning

- OSINT (Open Source Intelligence) — at indsamle information fra allerede offentlige data; det er ikke indtrængen eller spionage.
- Reglamento (UE) 2016/679 (RGPD) — om behandling af personoplysninger, herunder sammenlægning af data, der individuelt var offentlige.
- Offentlige registre (erhvervs-, rets- og ejendomsregistre) — en legitim og rigelig kilde til personlige oplysninger i næsten hele Europa.
- I denne samme samling: hæfterne om end-to-end-kryptering og »Hvad en underskrift ikke kan fikse« udvikler samme idé fra en anden vinkel.

← ForrigeHvad en underskrift ikke kan løse

Seneste læsning

- Refleksion · 27. maj 2026 Hvad en underskrift ikke kan løse
- Analyse · 26. maj 2026 Reelt vs. tilsyneladende privatliv: De spørgsmål, man bør stille sig selv
- Analyse · 25. maj 2026 Self-hosting som professionel praksis

Tag denne artikel med dig, hvor du har brug for den.

↓ Markdown ↓ Almindelig tekst ↓ PDF

Filen downloades til din enhed. Derfra kan du gemme den, importere den til Solo2 eller dele den, hvor du vil. Cuadernos beslutter ikke destinationen for dig.

Laksegl · SHA-256 7e954af3add414d2cd2f96b9dd52cc3e6890456c64af24fa6b9c7d800c6647c8

Cuadernos Lacre · En udgivelse fra Menzuri Gestión S.L. ·
skrevet af R.Eugenio · redigeret af holdet bag Solo2.