Du är inte anonym

Förtroendet du inte valde

På ren svenska: med din e-postadress kan vem som helst på några sekunder ta reda på var du har konton, och ibland ditt ansikte och ditt namn. Det är inget fel: det är så internet fungerar. Frågan är inte om de kan se dig – det kan de – utan vem du tvingas lita på. Och det finns bara en plats utan någon i mitten: att prata direkt, från en enhet till en annan.

En e-postadress räcker. Inte nödvändigtvis din: vems som helst. Den skrivs in i en handfull gratisverktyg – lagliga, offentliga, tillgängliga för alla som vill söka efter dem – och på några sekunder dyker en lista upp: vilka tjänster den e-postadressen är registrerad på, ibland en profilbild, ibland ett för- och efternamn som ägaren trodde sig inte ha gett till någon. Man behöver inte vara teknisk. Inga lösenord knäcks. Inget brott begås. All den informationen fanns redan där – publicerad, registrerad eller läckt – och väntade på att någon skulle bry sig om att samla in den.

Det är frestande att tolka detta som ett fel: en lucka, ett misstag, något som någon borde åtgärda. Det är det inte. Det är så den öppna webben normalt fungerar. Varje gång du registrerar dig för en tjänst, fyller i ett formulär, publicerar en recension eller dyker upp i någon annans läcka, lämnar du ett spår. Inget av dessa spår är allvarligt i sig självt. Problemet – om det nu är ett problem – uppstår när man sätter ihop dem, och att sätta ihop dem är enkelt.

Här försvarar sig många med en rimlig fras: ”jag har inget att dölja”, eller ”jag tar hand om mina konton”. Den första förväxlar att gömma sig med att välja; vi återkommer till det. Den andra förbiser att du inte lämnade det mesta av det spåret: företagsregistret, webbplatsen som drabbades av läckan, bekantskapen som laddade upp en bild med dig och taggade dig, gjorde det. Anonymitet på internet är nästan aldrig en egenskap du äger; det är som bäst otydlighet: det tillfälliga faktumet att ingen har brytt sig om att titta ännu.

Hittills har vi talat om vad en enda person kan göra på några sekunder, manuellt. Ta nu bort personen. Det som under åren har skyddat de flesta av oss var inte anonymitet, utan ointresse: för att hitta dig måste någon bry sig om att titta, och ingen har tid att titta på alla. Den sista barriären – ansträngningen att titta – är precis den som en maskin inte har. Ett automatiskt system kan göra samma sökning, inte mot ett enda mål, utan mot en hel befolkning; inte en gång, utan oavbrutet; inte på grund av misstanke, utan som standard. Det som tidigare tog timmar för en utredare per person görs nu på miljontals människor samtidigt, utan att det kostar någon tid eller uppmärksamhet. Vi behöver inte anta vem som skulle vilja göra det – ett företag, en grupp, en stat – det räcker med att förstå att man inte längre behöver välja vem man ska titta på. Man kan titta på alla.

Därför är ”kan de hitta mig?” fel fråga. Svaret är ja, och det kommer att bli det allt oftare. Den användbara frågan är en annan: vem, och hur mycket, tvingas jag lita på för att leva uppkopplad? För det är vad du egentligen gör varje dag, oftast utan att tänka på det. Du litar på att tjänsten där du registrerar dig kommer att lagra dina data väl. Du litar på att din operatör inte kommer att lyssna på dina samtal. Du litar på att meddelandeappen som alla använder – låt oss säga WhatsApp – gör vad den säger att den gör. Du litar på servern i mitten, på företaget som driver den, på landet där den finns, på det gratisverktyg som någon lade ut på nätet. Var och en av dessa länkar är ett beslut om förtroende. Skillnaden är att du knappt fattade något av dem medvetet: de ingick. Dessa länkar som smyger sig in mellan dig och den andra personen kallas i jargong för betrodda mellanhänder; namnet spelar mindre roll än tanken att de finns där, och att de är många.

Det finns ett ärligt sätt att kontrollera allt detta: gör det med dig själv. Och du behöver inte att vi ger dig något. Öppna din webbläsare, skriv tre eller fyra ord – något i stil med «vad vet internet om min e-post» – och webben själv kommer att lägga verktygen framför dig. Den enkelheten är i sig halva svaret: om du hittar dem på tio sekunder, kan vem som helst hitta vad de säger om dig.

Vi erbjuder dig ingen lista från oss, och det är avsiktligt. Om vi gav dig den skulle du behöva lita på oss: på att vi valde väl, på att de sidorna fortfarande kommer att vara pålitliga om fem år, på att bakom ingen av dem finns – idag eller imorgon – någon med dåliga avsikter. Vi kan inte lova det för sidor vi inte kontrollerar, och vi föredrar att inte ge ett löfte vi inte kan hålla. Det är exakt vad den här artikeln handlar om. Men att söka efter det själv har ett pris: sökmotorn skiljer inte mellan det legitima och fällan. Att sätta upp en sida som imiterar ett riktigt verktyg, ber om din e-post och behåller den är trivialt. Så innan du skriver något någonstans är det bra att veta hur man läser en adress.

Notera — läs en adress innan du litar på den. En falsk sida kan kopiera ner till sista pixeln av en riktig; vad den nästan aldrig kan förfalska är dess adress. Innan du skriver något på en sida, läs adressfältet, inte sidan. Namnet som bestämmer är det som sitter fast till vänster om den sista delen (`.com`, `.org`, `.se`): i `saker-bank.konstig-sajt.top` är den verkliga ägaren inte din bank, det är `konstig-sajt.top`. Misstro ändrade bokstäver (en `0` i stället för ett `o`), extra ord, bindestreck där du inte förväntar dig dem och märkliga ändelser. Hänglåset och `https` säger bara att anslutningen är krypterad – inte att ägaren är hederlig – en bedragare har också ett hänglås. Och de första resultaten markerade som ”annons” finns där för att någon har betalat, inte för att de är pålitliga. Var och en av dessa kontroller är i grunden samma fråga: hur mycket litar jag på den här adressen, och varför?

När vi har kommit hit är det värt att beskriva motsatsen till allt detta: en kanal utan mellanhänder. Två personer, ensamma på toppen av ett berg, som pratar. Det finns ingen brevbärare, ingen växel, ingen server, inget företag, inget land emellan. Och ändå, observera: inte heller där försvinner förtroendet. Om du berättar en hemlighet för den andra personen litar du på hen. Det förtroendet kan inte tas bort – och det behövs inte heller – för det är det enda du verkligen valde: du vet vem du litar på, och varför.

Vad som inte finns på berget är allt det andra. Ingen i mitten. Och det, inget annat, är den enda modellen som kan reproduceras ärligt digitalt: en direkt kanal från en enhet till en annan, utan något eller någon längs vägen. Det eliminerar inte förtroendet – det vore att ljuga – det eliminerar mellanhänderna. Det lämnar dig ensam med det enda oundvikliga förtroendet, det du faktiskt valde. Det är, för övrigt, den arkitektur som vi skriver dessa sidor från; men argumentet står för sig självt, vem som än bygger det.

Så nej, du är inte anonym, och du kommer förmodligen aldrig att bli det igen. Men det var aldrig den strid som spelade roll. Man kan inte leva – eller surfa – utan att lita på någon; den som försöker är inte friare, bara ensammare. Mognad är inte misstro, som är en annan form av naivitet. Det är att vara krävande: att veta till vem du ger ditt förtroende, hur mycket, i utbyte mot vad och – framför allt – att veta när du ger det till någon utan att ha bestämt det.

Nästan ingenting i livet är svart eller vitt; nästan allt lever i den gråzonen däremellan, och att lära sig att navigera i det gråa är en stor del av vad det innebär att ha omdöme. Det enda undantaget är det som är välbyggt från fabriken: det som, av design, inte ber dig att lita på någon annan än den person du redan bestämt dig för att prata med. Resten – allt annat – handlar om hur mycket, och till vem.

Redaktionell not: när dessa Cuadernos nämner företag eller produkter är det inte för att anklaga. De som bygger dem gör ett jobb som miljontals människor använder och uppskattar. Det vi pekar på är strukturellt — modellen, inte varumärket. Varumärken visas som exempel eftersom det är dessa läsaren känner igen.

Källor och vidare läsning

- OSINT (öppen källkodsinformation) – samla information från redan offentliga data; det är inte intrång eller spionage.

- Reglamento (UE) 2016/679 (RGPD) – om behandling av personuppgifter, inklusive sammanslagning av uppgifter som var offentliga enskilt.
- Offentliga register (företags-, domstols-, fastighetsregister) – en legitim och riklig källa till personlig information i nästan hela Europa.
- I samma samling: anteckningsböckerna om end-to-end-kryptering och ”Vad en signatur inte kan fixa” utvecklar, från en annan vinkel, samma idé.

← FöregåendeDet en signatur inte kan fixa

Senaste läsning

- Reflektion · 27 maj 2026 Det en signatur inte kan fixa
- Analys · 26 maj 2026 Verklig vs skenbar integritet: Frågorna man bör ställa sig
- Analys · 25 maj 2026 Self-hosting som yrkespraxis

Ta med dig den här artikeln dit du behöver den.

↓ Markdown ↓ Klartext ↓ PDF

Filen laddas ner till din enhet. Därifrån kan du spara den, importera den till Solo2 eller dela den var du vill. Cuadernos bestämmer inte destinationen åt dig.

Lacksigill · SHA-256 779ed6035bb26d9c66ea35fd62d0119f21987546adc9d3718a029505740d8767

Cuadernos Lacre · En utgåva från Menzuri Gestión S.L. ·
skriven av R.Eugenio · redigerad av teamet bakom Solo2.