Reflectie · 29 juni 2026

← Vorige

Je bent niet anoniem

Het vertrouwen dat je niet hebt gekozen

Simpel gezegd: met je e-mail kan iedereen in een paar seconden achterhalen waar je een account hebt, en soms ook je gezicht en je naam. Dit is geen fout: het is hoe het internet normaal gesproken werkt. De vraag is niet of ze je kunnen zien —dat kunnen ze—, maar op wie je gedwongen bent te vertrouwen. En er is maar één plek zonder iemand ertussenin: direct praten, van het ene apparaat naar het andere.

Eén e-mailadres is genoeg. Niet per se dat van jou: dat van wie dan ook. Het wordt ingevoerd in een handvol gratis hulpmiddelen —legaal, openbaar, beschikbaar voor iedereen die wil zoeken— en in een paar seconden verschijnt er een lijst: bij welke diensten dat e-mailadres is geregistreerd, soms een profielfoto, soms een voor- en achternaam waarvan de eigenaar dacht dat hij die aan niemand had gegeven. Je hoeft niet technisch onderlegd te zijn. Er worden geen wachtwoorden gekraakt. Er wordt geen misdaad begaan. Al die informatie was er al —gepubliceerd, geregistreerd of gelekt— wachtend tot iemand de moeite nam om het samen te voegen.

Het is verleidelijk om dit als een fout te lezen: een breuk, een slordigheid, iets wat iemand zou moeten repareren. Dat is het niet. Het is de normale werking van het open web. Elke keer dat je je aanmeldt voor een dienst, een formulier invult, een recensie publiceert of verschijnt in het datalek van een ander, laat je een spoor achter. Geen van die sporen is op zichzelf ernstig. Het probleem —als het al een probleem is— ontstaat door ze samen te voegen, en ze samenvoegen is eenvoudig.

Hier verdedigen veel mensen zich met een redelijke zin: «ik heb niets te verbergen», of «ik pas op mijn accounts». De eerste verwart verstoppen met kiezen; daar komen we nog op terug. De tweede gaat eraan voorbij dat het grootste deel van dat spoor niet door jou is achtergelaten: het is achtergelaten door het handelsregister, de website die het datalek had, de kennis die een foto met jou heeft geüpld en je heeft getagd. Anonimiteit op het internet is bijna nooit een eigenschap die je bezit; het is op zijn best duisternis: het tijdelijke feit dat niemand nog de moeite heeft genomen om te kijken.

Tot nu toe hebben we het gehad over wat één persoon in een paar seconden handmatig kan doen. Verwijder nu de persoon. Wat de meesten van ons jarenlang heeft beschermd, was niet de anonimiteit, maar het gebrek aan interesse: om je te vinden, moet iemand de moeite nemen om te kijken, en niemand heeft de tijd om naar iedereen te kijken. Die laatste barrière —de moeite van het kijken— is precies wat een machine niet heeft. Een automatisch systeem kan diezelfde kruiscontrole niet tegen één doelwit uitvoeren, maar tegen een hele bevolking; niet één keer, maar meedogenloos; niet op basis van verdenking, maar standaard. Wat voorheen een onderzoeker uren per persoon kostte, gebeurt nu bij miljoenen tegelijk, zonder dat het iemand tijd of aandacht kost. We hoeven niet te veronderstellen wie dit zou willen doen —een bedrijf, een groep, een staat—; het is voldoende om te begrijpen dat men niet meer hoeft te kiezen naar wie men kijkt. Iedereen kan bekeken worden.

Daarom is «kunnen ze mij vinden?» de verkeerde vraag. Het antwoord is ja, en dat zal in toenemende mate zo zijn. De nuttige vraag is een andere: op wie, en in welke mate, ben ik gedwongen te vertrouwen om verbonden te leven? Want dat is wat je in werkelijkheid elke dag doet, bijna altijd zonder erbij na te denken. Je vertrouwt erop dat de dienst waar je je registreert je gegevens goed bewaart. Je vertrouwt erop dat je telecomprovider niet naar je gesprekken luistert. Je vertrouwt erop dat de berichtenapp die iedereen gebruikt —laten we zeggen WhatsApp— doet wat ze zegt te doen. Je vertrouwt de server in het midden, het bedrijf dat het beheert, het land waar het zich bevindt, het gratis hulpmiddel dat iemand op het netwerk heeft gezet. Elk van die schakels is een beslissing

van vertrouwen. Het verschil is dat je ze bijna nooit bewust hebt genomen: ze waren inbegrepen. De schakels die zich tussen jou en de andere persoon nestelen, worden in jargon vertrouwensintermediairs genoemd; de naam is minder belangrijk dan het idee dat ze er zijn, en dat er veel van zijn.

Er is een eerlijke manier om dit allemaal te controleren: doe het bij jezelf. En je hebt niets van ons nodig. Open je browser, typ drie of vier woorden in —iets als «wat weet het internet over mijn e-mail»— en het web zelf zal de tools voor je neus plaatsen. Dat gemak is op zichzelf al het halve antwoord: als jij ze in tien seconden vindt, kan iedereen vinden wat ze over jou zeggen.

We bieden je niet onze eigen lijst aan, en dat is opzettelijk. Als we je die wel zouden geven, zou je ons moeten vertrouwen: dat we goed gekozen hebben, dat die pagina's over vijf jaar nog steeds betrouwbaar zullen zijn, dat achter geen enkele daarvan —vandaag of morgen— iemand met slechte bedoelingen zit. Dat kunnen we niet beloven voor pagina's die we niet beheren, en we maken liever geen belofte die we niet na kunnen komen. Dat is precies waar dit artikel over gaat. Maar er zelf naar zoeken heeft een prijs: de zoekmachine onderscheidt het legitieme niet van de valstrik. Een pagina opzetten die een echt hulpmiddel imiteert, om je e-mail vraagt en deze behoudt, is triviaal. Voordat je ergens iets intypt, is het dus verstandig te weten hoe je een adres moet lezen.

Opmerking — lees een adres voordat je het vertrouwt. Een neppagina kan de echte pagina tot de laatste pixel kopiëren; wat bijna nooit vervalst kan worden, is het adres. Voordat je ergens iets typt, lees de adresbalk, niet de pagina. De naam die bepalend is, is degene die direct links van het laatste deel (`.com`, `.org`, `.nl`) staat: in `veilige-bank.rare-site.top` is je bank niet de echte eigenaar, dat is `rare-site.top`. Pas op voor gewijzigde letters (een `0` in plaats van een `o`), extra woorden, koppeltekens waar je ze niet verwacht en vreemde uitgangen. Het hangslot en de `https` betekenen alleen dat de verbinding versleuteld is —niet dat de eigenaar eerlijk is—: een oplichter heeft ook een hangslot. En de eerste resultaten die als «advertentie» zijn gemarkeerd, staan daar omdat iemand heeft betaald, niet omdat ze te vertrouwen zijn. Elk van deze controles is in de kern dezelfde vraag: hoeveel vertrouw ik dit adres, en waarom?

Nu we hier zijn, is het de moeite waard om het tegenovergestelde van dit alles te beschrijven: een kanaal zonder tussenpersonen. Twee mensen, alleen op de top van een berg, in gesprek. Er is geen postbode, geen telefooncentrale, geen server, geen bedrijf, geen land ertussenin. En toch, let op: het vertrouwen verdwijnt daar niet. Als je de andere persoon een geheim vertelt, vertrouw je hem of haar. Dat vertrouwen kan niet worden weggenomen —en dat hoeft ook niet—, want het is het enige dat je echt gekozen hebt: je weet wie je vertrouwt, en waarom.

Wat er niet op de berg is, is al het andere. Niemand ertussenin. En dat model, geen enkel ander, is het enige dat op een eerlijke manier in de digitale wereld kan worden gereproduceerd: een direct kanaal van het ene apparaat naar het andere, zonder iets of iemand onderweg. Het neemt het vertrouwen niet weg —dat zou een leugen zijn —; het verwijdert de tussenpersonen. Het laat je alleen met het enige onvermijdelijke vertrouwen, dat jijzelf gekozen hebt. Dat is overigens de architectuur van waaruit we deze pagina's schrijven; maar het argument staat op zichzelf, ongeacht wie het bouwt.

Dus nee, je bent niet anoniem, en waarschijnlijk zul je dat ook nooit meer worden. Maar dat was nooit de strijd die ertoe deed. Men kan niet leven —of internetten— zonder op iemand te vertrouwen; degenen die dat proberen, zijn niet vrijer, ze zijn gewoon eenzamer. Volwassenheid is geen wantrouwen, wat slechts een andere vorm van naïviteit is. Het is veeleisend zijn: weten aan wie je je vertrouwen geeft, hoeveel, in ruil waarvoor en —bovenal— weten wanneer je het aan iemand geeft zonder de beslissing te hebben genomen.

Bijna niets in het leven is zwart of wit; bijna alles leeft in het grijze gebied daartussenin, en leren navigeren in dat grijze gebied is een groot deel van wat het betekent om een goed oordeelsvermogen te hebben. De enige uitzondering is wat goed gemaakt uit de fabriek komt: dat wat, door zijn ontwerp, niet van je vraagt om iemand anders te vertrouwen dan de persoon waarmee je al had besloten te praten. De rest —al het andere— is slechts een kwestie van hoeveel, en in wie.

Noot van de redactie: wanneer deze Cuadernos bedrijven of producten noemen, is dat niet om te beschuldigen. Degenen die ze bouwen, leveren werk dat miljoenen mensen gebruiken en waarderen. Wat we aanstippen is

structureel — het model, niet het merk. Merken verschijnen als voorbeeld omdat dit de merken zijn die de lezer herkent.

Bronnen und verdere lectuur

- OSINT (open-source intelligence) — informatie verzamelen uit reeds openbare data; het is geen inbraak of spionage.
- Reglamento (UE) 2016/679 (RGPD) — over de verwerking van persoonsgegevens, inclusief het samenvoegen van gegevens die afzonderlijk openbaar waren.
- Openbare registers (handels-, gerechtelijke en eigendomsregisters) — legale en overvloedige bron van persoonlijke informatie in bijna heel Europa.
- In deze zelfde collectie: de notitieboekjes over end-to-end encryptie en «Wat een handtekening niet kan oplossen» die hetzelfde idee vanuit een andere invalshoek ontwikkelen.

← VorigeWat een handtekening niet kan oplossen

Recente artikelen

- Reflectie · 27 mei 2026 Wat een handtekening niet kan oplossen
- Analyse · 26 mei 2026 Echte vs. schijnbare privacy: de vragen die men zich moet stellen
- Analyse · 25 mei 2026 Self-hosting als professionele praktijk

Neem dit artikel mee naar waar u het nodig heeft.

↓ Markdown ↓ Platte tekst ↓ PDF

Het bestand wordt gedownload naar uw apparaat. Van daaruit kunt u het opslaan, importeren in Solo2 of delen waar u maar wilt. Cuadernos beslist niet voor u over de bestemming.

Lakzegel · SHA-256 1a206b450199ae7dc46357470ac8e3cfb4383e994c6c4573f7175e988ebfa3b2

Cuadernos Lacre · Een uitgave van Menzuri Gestión S.L. ·
geschreven door R.Eugenio · geredigeerd door het team van Solo2.

Deze website gebruikt geen cookies. Alles wat uw browser laadt, is door ons geschreven of onder ons toezicht en wordt gehost op onze Europese servers: de anonieme bezoeksteller (Umami, zelf gehost) en het minimale JavaScript dat nodig is voor de taalkeuze en uw voorkeur voor een licht/donker thema, die op uw eigen apparaat wordt opgeslagen. Geen bronnen van derden, geen trackers, geen profilering, geen delen van gegevens. Als u ons wilt volgen: RSS.