Kamu tidak anonim

Kepercayaan yang tidak kamu pilih

Dalam bahasa sederhana: dengan emailmu, siapa pun dapat mengetahui dalam hitungan detik di mana kamu memiliki akun, dan terkadang wajah serta namamu. Ini bukanlah sebuah kesalahan: beginilah cara internet selalu bekerja. Pertanyaannya bukanlah apakah mereka bisa melihatmu — mereka bisa —, tetapi kepada siapa kamu terpaksa percaya. Dan hanya ada satu tempat tanpa siapa pun di tengahnya: berbicara langsung, dari satu perangkat ke perangkat lain.

Hanya butuh sebuah email. Tidak harus milikmu: milik siapa saja. Diketikkan di beberapa alat gratis — legal, publik, dapat diakses oleh siapa saja yang ingin mencarinya — dan dalam hitungan detik muncul sebuah daftar: di layanan apa email tersebut terdaftar, terkadang foto profil, terkadang nama dan nama keluarga yang pemiliknya pikir tidak pernah diberikan kepada siapa pun. Tidak perlu menjadi ahli teknis. Tidak ada kata sandi yang dibobol. Tidak ada kejahatan yang dilakukan. Semua informasi itu sudah ada di sana — diterbitkan, didaftarkan, atau bocor — menunggu seseorang untuk repot-repot mengumpulkannya.

Sangat menggoda untuk membaca ini sebagai sebuah kesalahan: celah, kecerobohan, sesuatu yang harus diperbaiki seseorang. Tapi bukan itu. Ini adalah fungsi normal dari web terbuka. Setiap kali kamu mendaftar untuk sebuah layanan, mengisi formulir, mempublikasikan ulasan, atau muncul dalam kebocoran data orang lain, kamu meninggalkan jejak. Tidak satu pun dari jejak itu yang parah dengan sendirinya. Masalahnya — jika itu memang masalah — lahir dari menggabungkannya, dan menggabungkannya itu mudah.

Di sini banyak orang membela diri dengan kalimat yang masuk akal: «aku tidak punya apa-apa untuk disembunyikan», atau «aku menjaga akunku». Yang pertama mengacaukan menyembunyikan dengan memilih; kita akan kembali ke hal itu. Yang kedua mengabaikan fakta bahwa sebagian besar jejak itu tidak ditinggalkan olehmu: itu ditinggalkan oleh pendaftaran komersial, situs web yang mengalami kebocoran, teman yang mengunggah fotomu dan menandaimu. Anonimitas di internet hampir tidak pernah menjadi milik yang kamu miliki; itu, paling banter, adalah kegelapan: fakta sementara bahwa belum ada yang repot-repot untuk melihat.

Sejauh ini kita telah berbicara tentang apa yang dapat dilakukan satu orang dalam hitungan detik, secara manual. Sekarang singkirkan orang tersebut. Apa yang telah melindungi sebagian besar dari kita selama bertahun-tahun bukanlah anonimitas, melainkan ketidaktertarikan: untuk menemukanmu, seseorang harus repot-repot melihat, dan tidak ada yang punya waktu untuk melihat semua orang. Penghalang terakhir itu — upaya untuk melihat — justru tidak dimiliki oleh mesin. Sistem otomatis dapat melakukan pencocokan yang sama, bukan terhadap satu target, tetapi terhadap seluruh populasi; bukan sekali, tetapi tanpa henti; bukan karena kecurigaan, tetapi secara default. Apa yang dulunya memakan waktu berjam-jam bagi seorang penyelidik untuk setiap orang, kini dilakukan pada jutaan orang secara bersamaan, tanpa menghabiskan waktu atau perhatian siapa pun. Tidak perlu menebak siapa yang ingin melakukannya — perusahaan, grup, negara —; cukup untuk memahami bahwa tidak perlu lagi memilih siapa yang akan dilihat. Semua orang dapat dilihat.

Oleh karena itu «bisakah mereka menemukan saya?» adalah pertanyaan yang salah. Jawabannya ya, dan akan semakin sering. Pertanyaan yang berguna adalah yang lain: kepada siapa, dan seberapa besar, aku terpaksa percaya untuk hidup terhubung? Karena itulah yang benar-benar kamu lakukan setiap hari, hampir selalu tanpa memikirkannya. Kamu percaya bahwa layanan tempatmu mendaftar akan menjaga datamu dengan baik. Kamu percaya bahwa operatormu tidak akan menyadap panggilanmu. Kamu percaya bahwa aplikasi pesan yang

digunakan semua orang — katakanlah WhatsApp — melakukan apa yang dikatakannya. Kamu percaya pada server yang ada di tengah, pada perusahaan yang mengelolanya, pada negara tempat server itu berada, pada alat gratis yang ditaruh seseorang di jaringan. Setiap tautan itu adalah keputusan kepercayaan. Perbedaannya adalah hampir tidak ada yang kamu buat secara sadar: mereka sudah termasuk di dalamnya. Tautan-tautan yang menyelinap antara kamu dan orang lain ini disebut, dalam jargon, perantara tepercaya; namanya kurang penting daripada gagasan bahwa mereka ada di sana, dan ada banyak dari mereka.

Ada cara jujur untuk memeriksa semua ini: lakukan sendiri. Dan kamu tidak butuh kami memberikan apa pun. Buka browsermu, ketik tiga atau empat kata — sesuatu seperti «apa yang internet ketahui tentang emailku» — dan web itu sendiri akan menaruh alat-alat itu di depanmu. Kemudahan itu, dengan sendirinya, adalah setengah dari jawaban: jika kamu menemukannya dalam sepuluh detik, siapa pun dapat menemukan apa yang mereka katakan tentangmu.

Kami tidak menawari daftar milik kami sendiri, dan itu disengaja. Jika kami memberikannya, kamu harus percaya pada kami: bahwa kami memilih dengan baik, bahwa halaman-halaman itu akan tetap dapat dipercaya dalam lima tahun ke depan, bahwa di balik semua itu — hari ini atau esok — tidak ada orang dengan niat buruk. Kami tidak dapat menjanjikan itu dari halaman yang tidak kami kendalikan, dan kami lebih suka tidak membuat janji yang tidak dapat kami penuhi. Tepatnya, itulah yang dibahas dalam artikel ini. Namun mencarinya sendiri ada harganya: mesin pencari tidak membedakan mana yang sah dan mana jebakan. Membuat halaman yang meniru alat nyata, meminta emailmu dan menyimpannya adalah hal yang sepele. Jadi, sebelum menulis apa pun di mana pun, kamu perlu tahu cara membaca alamat URL.

Catatan — baca alamat sebelum memercayainya. Halaman palsu dapat menyalin hingga piksel terakhir dari halaman asli; apa yang hampir tidak pernah bisa dipalsukan adalah alamatnya. Sebelum menulis apa pun di sebuah situs, bacalah bilah alamat, bukan halamannya. Nama penguasa adalah nama yang menempel di sebelah kiri bagian terakhir (`.com`, `.org`, `.id`): di `bank-aman.situs-aneh.top`, pemilik aslinya bukanlah bankmu, melainkan `situs-aneh.top`. Waspadai huruf yang diubah (`0` untuk `o`), kata tambahan, tanda hubung di tempat yang tidak kamu harapkan, dan akhiran yang aneh. Gembok dan `https` hanya mengatakan bahwa koneksinya dienkripsi — bukan bahwa pemiliknya jujur —: penipu juga punya gembok. Dan hasil pertama yang ditandai sebagai «iklan» ada di sana karena seseorang telah membayar, bukan karena dapat dipercaya. Setiap pemeriksaan itu, pada dasarnya, adalah pertanyaan yang sama: seberapa besar aku percaya pada alamat ini, dan mengapa?

Sampai di sini, ada baiknya mendeskripsikan kebalikan dari semua ini: sebuah saluran tanpa perantara. Dua orang, sendirian di puncak gunung, saling berbicara. Tidak ada tukang pos, tidak ada panel kontrol, tidak ada server, tidak ada perusahaan, tidak ada negara di antaranya. Dan, tetap saja, perhatikan: bahkan di sana kepercayaan tidak hilang. Jika kamu menceritakan sebuah rahasia kepada orang lain, kamu memercayainya. Kepercayaan itu tidak dapat dihilangkan — dan tidak perlu — karena itu adalah satu-satunya yang benar-benar kamu pilih: kamu tahu kepada siapa kamu percaya, dan mengapa.

Apa yang tidak ada di gunung adalah segalanya yang lain. Tidak ada siapa pun di tengah. Dan itu, bukan yang lain, adalah satu-satunya model yang dapat direproduksi dengan jujur di dunia digital: saluran langsung dari satu perangkat ke perangkat lain, tanpa apa pun atau siapa pun di jalurnya. Ini tidak menghilangkan kepercayaan — itu bohong —; itu menghilangkan perantara. Itu meninggalkanmu sendirian dengan satu-satunya kepercayaan yang tak terhindarkan, yang kamu pilih. Omong-omong, itu adalah arsitektur dari mana kami menulis halaman-halaman ini; tetapi argumen ini berdiri sendiri, tidak peduli siapa yang membangunnya.

Jadi tidak, kamu tidak anonim, dan mungkin tidak akan pernah anonim lagi. Tapi itu tidak pernah menjadi pertempuran yang penting. Seseorang tidak dapat hidup — atau berselancar — tanpa memercayai siapa pun; siapa pun yang mencobanya tidak lebih bebas, hanya lebih kesepian. Kedewasaan bukanlah ketidakpercayaan, yang merupakan bentuk lain dari kenaifan. Itu adalah menjadi penuntut: mengetahui kepada siapa kamu memberikan kepercayaanmu, berapa banyak, dengan imbalan apa dan — di atas segalanya — mengetahui kapan kamu memberikannya kepada seseorang tanpa memutuskan hal tersebut.

Hampir tidak ada dalam hidup ini yang hitam atau putih; hampir semuanya hidup dalam zona abu-abu di tengahnya, dan belajar bergerak di zona abu-abu itu adalah sebagian besar dari apa artinya memiliki kriteria. Satu-satunya pengecualian adalah apa yang sudah dibuat dengan baik dari pabriknya: apa yang, berdasarkan desain, tidak memintamu untuk memercayai siapa pun selain orang yang sudah kamu putuskan untuk diajak bicara. Sisanya — semuanya — adalah soal seberapa banyak, dan kepada siapa.

Catatan editor: ketika Cuadernos ini menyebutkan perusahaan atau produk, itu bukan untuk menuduh. Mereka yang membangunnya melakukan pekerjaan yang digunakan dan dihargai oleh jutaan orang. Apa yang kami tunjukkan adalah struktural — modelnya, bukan mereknya. Merek muncul sebagai contoh karena merekalah yang dikenali oleh pembaca.

Sumber dan bacaan lebih lanjut

- OSINT (kecerdasan sumber terbuka) — mengumpulkan informasi dari data yang sudah menjadi konsumsi publik; itu bukan intrusi atau spionase.
- Reglamento (UE) 2016/679 (RGPD) — tentang pemrosesan data pribadi, termasuk agregasi data yang secara individual bersifat publik.
- Catatan publik (komersial, peradilan, properti) — sumber informasi pribadi yang sah dan berlimpah di hampir seluruh Eropa.
- Dalam koleksi yang sama: buku catatan tentang enkripsi ujung ke ujung dan «Apa yang tidak bisa diperbaiki oleh tanda tangan» yang mengembangkan, dari sudut lain, ide yang sama.

← SebelumnyaApa yang tidak bisa diperbaiki oleh tanda tangan

Bacaan terbaru

- Refleksi · 27 Mei 2026 Apa yang tidak bisa diperbaiki oleh tanda tangan
- Analisis · 26 Mei 2026 Privasi nyata vs semu: pertanyaan yang perlu Anda ajukan
- Analisis · 25 Mei 2026 Self-hosting sebagai praktik profesional

Bawa artikel ini bersama Anda ke mana pun Anda membutuhkannya.

↓ Markdown ↓ Teks murni ↓ PDF

File akan diunduh ke perangkat Anda. Dari sana Anda dapat menyimpannya, mengimpornya ke Solo2, atau membagikannya di mana pun Anda mau. Cuadernos tidak memutuskan tujuan untuk Anda.

Segel lilin · SHA-256 7fdbd4a79804880cd83f3d393991987a262fd0a24c42fb0de9ae9fcc255849fa

Cuadernos Lacre · Publikasi dari Menzuri Gestión S.L. ·
ditulis oleh R.Eugenio · disunting oleh tim Solo2.