

Perché autodifesa digitale?

Non ho niente da nascondere!

«Non ho niente da nascondere.»

È probabilmente una delle frasi più utili mai regalate gratuitamente a governi, aziende tecnologiche, inserzionisti, datori di lavoro e a chiunque altro abbia interesse a sapere qualcosa di noi. A prima vista sembra persino ragionevole. Se non sto facendo niente di illegale, perché dovrebbe preoccuparmi che qualcuno raccolga informazioni su di me?

Perché privacy e segretezza non sono la stessa cosa.

Quando chiudiamo la porta del bagno non stiamo necessariamente commettendo un reato. Quando mettiamo una lettera in una busta non significa che dentro ci siano i piani per far saltare una banca. Quando abbassiamo le tapparelle non stiamo confessando attività sovversive. Semplicemente, pensiamo che non tutto ciò che facciamo debba riguardare chiunque altro.

Eric Hughes, nel Cypherpunk's Manifesto del 1993, definiva la privacy come la possibilità di scegliere cosa rivelare di noi, a chi e quando. L'autodifesa digitale parte esattamente da qui. Non dal desiderio di sparire, ma dal desiderio di poter scegliere.

La nostra vita è diventata un gigantesco foglio Excel

Oggi lasciamo tracce praticamente in continuazione. Il telefono conosce i nostri spostamenti. Il browser conosce le nostre ricerche. Le piattaforme sanno cosa leggiamo, cosa guardiamo, quanto tempo rimaniamo davanti a qualcosa e con chi interagiamo. Una carta di pagamento racconta dove compriamo. Un'app di trasporto racconta dove andiamo. Un social network permette di ricostruire una parte consistente delle nostre amicizie, abitudini e interessi.

E non serve nemmeno leggere quello che scriviamo.

Esistono i metadati: informazioni su una comunicazione senza necessariamente conoscerne il contenuto. Chi ha parlato con chi, quando, per quanto tempo, da dove. EFF li paragona alle informazioni scritte all'esterno di una busta. Magari la lettera è chiusa, ma si vedono mittente e destinatario. E se si raccolgono abbastanza buste, si può capire parecchio anche senza aprirne una.

Se una persona telefona a un oncologo, poi alla propria famiglia e subito dopo alla compagnia assicurativa, non serve necessariamente ascoltare le conversazioni per intuire che potrebbe essere successo qualcosa.

Quindi sì, magari nessuno legge i nostri messaggi. Sa soltanto chi siamo, dove eravamo, chi abbiamo contattato e quando.

Che sollievo.

«Ma a Google non interessa quello che faccio io»

Probabilmente no. Dubito che qualcuno nella sede di Google aspetti con impazienza di sapere quale ristorante abbiamo cercato sabato sera. Il punto è proprio questo: non serve che una persona ci osservi. La raccolta è automatica, industriale e di massa.

Giap/Wu Ming ha parlato efficacemente di fracking delle nostre vite: un'estrazione continua di dati dalle attività quotidiane. Molti dei servizi che definiamo «gratuiti» non sono gratuiti nel senso comune della parola. Semplicemente, il pagamento avviene in un'altra forma: con i nostri dati, con la nostra attenzione, con informazioni sui nostri comportamenti, con la possibilità di prevedere cosa potremmo comprare, leggere, guardare o fare.

La questione della privacy non riguarda quindi soltanto qualche azienda particolarmente impicciona. Riguarda un modello economico. Le informazioni sulle persone hanno valore. E, come succede abbastanza spesso nel capitalismo, ciò che ha valore tende misteriosamente a concentrarsi nelle mani di pochi.

Il problema non è chi ci guarda. È chi può guardarci.

La seconda versione del «non ho niente da nascondere» è: «Va bene, raccolgono i dati. Ma tanto non ne faranno niente di male.»

Che presuppone una fiducia piuttosto notevole.

Significa costruire infrastrutture capaci di raccogliere, conservare, incrociare e analizzare informazioni su milioni di persone e poi confidare che chi le controlla rimanga per sempre democratico, ragionevole, competente e animato dalle migliori intenzioni. Governi compresi. Per sempre.

Il problema della sorveglianza non è soltanto ciò che viene fatto oggi con un'informazione. È ciò che potrà essere fatto domani con un'informazione raccolta oggi. Le leggi cambiano. I governi cambiano. I proprietari delle aziende cambiano. Le condizioni politiche cambiano. E quello che ieri non interessava a nessuno può improvvisamente diventare interessante.

Essere iscritti a un sindacato. Partecipare a una manifestazione. Frequentare un certo spazio politico. Visitare una clinica. Cercare informazioni su una malattia. Parlare con un giornalista. Cercare un altro lavoro senza dirlo al proprio datore.

Nulla di tutto questo richiede di essere un pericoloso terrorista internazionale. Richiede soltanto di avere una vita.

La sorveglianza non è soltanto leggere i messaggi

Quando si parla di sorveglianza si immagina spesso qualcuno davanti a uno schermo che legge conversazioni private. È una visione quasi rassicurante, perché sembra costosa, lenta e difficile.

La realtà è molto più semplice.

Il controllo può passare dai social network, dai sistemi di pagamento, dai servizi cloud, dai negozi di applicazioni, dai domini internet, dagli account, dalle banche e da decine di altri intermediari. Non serve necessariamente sequestrare un computer. A volte basta bloccare un account, chiudere un servizio, tagliare una forma di pagamento, rendere irraggiungibile un'infrastruttura.

La recente vicenda di Autistici/Inventati, collettivo che per venticinque anni aveva fornito strumenti digitali indipendenti e rispettosi della privacy, lo ha mostrato con particolare chiarezza. A/I aveva sempre considerato la privacy, il software libero e l'autogestione delle infrastrutture come strumenti politici, non come accessori tecnici. La sua chiusura nel 2026 ha ricordato quanto possa essere fragile l'autonomia digitale quando dipende comunque da soggetti esterni.

Il punto, però, va molto oltre il singolo caso. Il potere non consiste soltanto nel poter leggere un messaggio. Consiste anche nel poter decidere se quel messaggio potrà essere inviato.

Sorvegliare significa anche modificare i comportamenti

Riseup, altro progetto nato per fornire infrastrutture ai movimenti sociali, insiste da anni su un punto fondamentale: la sorveglianza non serve soltanto a raccogliere informazioni. Serve anche a modificare i comportamenti.

Se penso che il mio datore di lavoro possa leggere qualcosa, magari evito di scriverla. Se penso che partecipare a una manifestazione possa farmi finire in qualche archivio, magari rimango a casa. Se penso che alcune ricerche possano essere interpretate male, magari non le faccio.

È quello che viene chiamato effetto dissuasivo. La sorveglianza funziona anche quando nessuno interviene direttamente. Non serve vietarti qualcosa. A un certo punto cominci a vietartela da solo.

Molto efficiente. E anche relativamente economico.

«Io però non sono un attivista»

Ottimo. L'autodifesa digitale continua a riguardarti.

Potresti semplicemente non desiderare che un'azienda costruisca un profilo dettagliato delle tue abitudini. Potresti non voler rendere pubblica la tua posizione.

Potresti non volere che un futuro datore di lavoro sappia determinate cose. Potresti avere problemi familiari, debiti, una relazione privata, una ricerca imbarazzante fatta alle tre del mattino o semplicemente la discutibile abitudine di voler fare gli affari tuoi.

Poi ci sono truffatori, stalker, ex partner, ladri d'identità e aziende che non hanno alcun diritto automatico a conoscere la nostra vita solo perché possiedono i mezzi tecnici per raccoglierla.

L'autodifesa digitale non nasce quindi dalla convinzione che qualcuno ci stia osservando personalmente ventiquattr'ore su ventiquattro. Nasce dalla constatazione molto meno spettacolare che utilizziamo ogni giorno sistemi progettati per raccogliere informazioni.

La privacy non è individuale

Questo è probabilmente il limite più grosso del «non ho niente da nascondere».

I nostri dati non riguardano soltanto noi. La rubrica contiene altre persone. Le fotografie contengono altre persone. Le conversazioni hanno almeno due partecipanti. La nostra posizione permette di capire chi incontriamo.

EFF usa un'espressione molto efficace: la privacy è uno sport di squadra. Anche una persona estremamente prudente può essere identificata da amici che pubblicano fotografie, condividono posizioni o rendono pubbliche le proprie relazioni.

Magari tu non hai niente da nascondere. La persona che ti scrive potrebbe averlo. E soprattutto non sta a te decidere per lei.

Questo è anche uno dei motivi per cui la crittografia funziona meglio quando diventa normale. Se soltanto giornalisti, dissidenti, sindacalisti e attivisti usano comunicazioni cifrate, il semplice fatto di cifrare qualcosa può diventare un'informazione. Se invece la crittografia viene usata normalmente da tutti, diventa soltanto il modo abituale di comunicare.

La sicurezza di una persona aumenta quando aumenta quella delle persone con cui comunica. Riseup insiste proprio su questo: privacy e sicurezza non possono essere risolte soltanto attraverso scelte individuali. Servono strumenti migliori, ma servono anche pratiche collettive.

Autodifesa, non paranoia

Autistici/Inventati parlava di autodifesa digitale. Il termine è importante.

Non «sicurezza informatica» intesa come acquisto compulsivo di antivirus, VPN e servizi premium. Autodifesa.

Vuol dire comprendere almeno un minimo gli strumenti che utilizziamo e ridurre la quantità di fiducia che siamo costretti a concedere. Preferire, quando possibile,

strumenti che raccolgono pochi dati. Usare comunicazioni cifrate. Tenere aggiornati i dispositivi. Usare password diverse e robuste. Evitare di concentrare posta, documenti, fotografie, contatti, calendario, posizione e identità digitale nelle mani della stessa azienda. Preferire software libero quando rappresenta un'alternativa valida.

Il movimento del software libero insiste da decenni su un principio semplice: se un programma controlla una parte importante della nostra vita, dovremmo almeno avere la possibilità di sapere cosa fa e di modificarlo. Questo non rende automaticamente il software libero sicuro o rispettoso della privacy. Ma rende un po' meno inevitabile una formula che ormai conosciamo bene:

«Fidati.»

Il Progetto Winston Smith, che in Italia ha lavorato per anni su privacy, anonimato e critica della sorveglianza, usava uno slogan magnificamente poco rassicurante:

«La paranoia è una virtù.»

Naturalmente non significa trasferirsi in una baita senza elettricità e avvolgere il telefono nella carta stagnola. Significa fare una domanda prima di consegnare un'informazione:

serve davvero?

È una forma abbastanza modesta di paranoia. Più o meno come controllare di aver chiuso la porta di casa.

Curiosamente nessuno, vedendoci girare la chiave, domanda: «Perché? Hai qualcosa da nascondere?»

Quindi abbiamo qualcosa da nascondere?

Probabilmente sì. Come tutti.

Conversazioni private. Problemi familiari. Informazioni economiche. Relazioni. Malattie. Paure. Errori. Dubbi. Ricerche assurde. Opinioni dette a una persona ma non a un'altra.

Non perché siano necessariamente illegali.

Perché sono nostre.

Ma forse la domanda è sbagliata fin dall'inizio. Perché dovremmo essere noi a spiegare perché vogliamo conservare una parte della nostra vita privata? Forse dovrebbe essere chi vuole osservare, registrare, archiviare, classificare e analizzare la nostra vita a spiegare perché ne ha bisogno.

L'autodifesa digitale non consiste nel diventare invisibili. Non significa credere di poter scomparire completamente dalla rete. E non consiste nemmeno nell'acquistare l'ennesimo servizio che promette «privacy assoluta» a 9,99 euro al mese.

Consiste nel sottrarre, dove possibile, informazioni e quindi potere a chi ne possiede già moltissimo: Stati, piattaforme, aziende, data broker, intermediari tecnologici.

La questione, alla fine, è abbastanza semplice.

Una società nella quale tutti sono trasparenti davanti a pochi non è una società più trasparente.

È semplicemente una società nella quale i pochi vedono tutti e gli altri vedono molto poco.

E se davvero non abbiamo niente da nascondere, tanto meglio.

Possiamo comunque chiudere la porta.