INFORMATICA RIBELLE

Infarinatura computeristica compagna

CUR Trento

cur@hackinpovo.it

INDICE

Ultimo aggiornamento opuscolo:
20/11/2025

A day in your life (Google lo sa)

Introduzione presa dalla fanzine "Perché è necessario e urgente liberarsi di Google – e come cominciare a farlo" di Wu Ming.
https://www.wumingfoundation.com/giap/2020/03/degoogling/

Ti svegli dopo un sonno di sei ore. Hai dormito male, sonno leggero e agitato. Google lo sa: lo ha rilevato dall'accelerometro e dal microfono nel tuo smartphone.
Dall'analisi della rete a cui sei connessa sa pure che non eri a casa tua, ma in un appartamento dall'altra parte della città e, dal registro dei tuoi spostamenti, sa pure che da circa un mese ti ci rechi almeno un paio di volte a settimana.

Google sa chi vive in quella casa, perché il GPS del suo smartphone indica giornalmente la sua presenza lì. Conosce bene quella persona, come conosce te. Sa che non fa parte della tua cerchia di amici ristretti, perché il suo numero non è nelle loro rubriche e molto raramente si trova negli stessi posti che loro frequentano. Sa che vi siete registrati a vicenda in rubrica qualche mese fa, ma solo negli ultimi tre avete iniziato a chiamarvi spesso.

Ieri sera avete visto un film sul Chromecast. Ovviamente Google sa qual era il film e poiché i dati GPS indicavano che eravate entrambi in casa e non vi siete mossi, deduce che probabilmente eravate in salotto.
Sa pure che all'altra persona il film non doveva interessare molto, perché mentre lo stavate guardando non faceva che giocare con un videogame sul suo smartphone Android.

Grazie al DNS Google sa che, appena alzata, come ogni mattina, hai controllato le news sul solito sito. Android e Chrome glielo confermano.

Dall'archivio delle tue abitudini di lettura degli ultimi anni, Google sa che le notizie relative alle occupazioni abitative sono di tuo interesse, ma che leggi in dettaglio solo quelle che parlano di sgomberi. Dall'analisi dei testi delle tue email sa che ne parli anche con amici e conoscenti e che manifesti crescente preoccupazione per le dichiarazioni di un certo assessore. Dall'analisi dei movimenti del tuo dito sullo schermo sa quali titoli di notizie hanno attirato la tua attenzione anche se poi non li hai letti, e ritiene che se in questi titoli fossero state presenti determinate parole la probabilità che tu li aprissi sarebbe stata maggiore.

Alle otto hai percorso un certo tragitto in città. Google lo sa, sempre grazie al GPS e per via del distacco dal wi-fi dell'appartamento. Dall'analisi di percorso e velocità Google deduce che lo spostamento sia avvenuto in bicicletta. Sa che poi sei entrata in un certo bar, probabilmente a fare colazione, dato che ti sei trattenuta mezz'ora, e che lì ti sei connessa al Wifi sbagliando il captcha tre volte, deducendone che forse sei ancora un po' addormentata, poiché di solito li becchi al primo colpo.

Google rileva che poi ti sei agganciata alla rete della biblioteca e hai cercato un certo oggetto che ritiene ti debba interessare molto, poiché la ricerca ti ha portato a girar diversi siti, finendo per trovarlo su quello di un certo negozio online dove l'hai acquistato fornendo la tua solita carta di credito. Ritiene statisticamente probabile che possa trattarsi di un regalo per una delle tue migliori amiche, quella che compirà gli anni tra un paio di settimane e che a sua volta acquista spesso oggetti dallo stile simile.

Poi scrivi un testo su un'app che hai scaricato dal Play Store e anche se non è un'app di Google, l'azienda ha accesso alla tastiera di Android e quindi è comunque in grado di comprendere cosa hai digitato, incluse le parti cancellate. Il testo contiene passaggi in

inglese e dalla velocità con cui le hai digitate capisce che è una lingua che pensi di padroneggiare bene, anche se in realtà nota che ripeti sempre gli stessi errori di grammatica.

A quel punto ricevi una chiamata da una persona che nella tua rubrica è registrata come «Mamma», e parlate per cinque minuti. Google rileva una certa ansia nella tua voce e ciò gli conferma quel che aveva già presunto: c'è tensione tra te e tua madre.
Lo aveva dedotto da diversi fattori, tra cui il gran numero di volte che non rispondi alle sue chiamate anche se sei a casa, e dal fatto che durante le feste sei lontana da lei e non la chiami.

Più tardi ti scatti un selfie con alcuni amici e dai metadati della foto Google può sapere dove e quando è stata scattata. Analizzando l'immagine può identificare le persone ritratte così come il tipo d'abbigliamento, dal quale può dedurre gusti e marche, dato utile per confermare cose che già sa sul tuo e loro livello economico.

Arriva la sera e fai una corsa nel parco ascoltando musica e indossando un braccialetto elettronico che registra le tue attività come il tipo di andatura, il battito cardiaco ecc. Non ci hai mai fatto caso, ma sia l'app per la musica in streaming sia quella del braccialetto avvisavano da qualche parte che i dati sarebbero stati condivisi con «terze parti», ossia partner commerciali. Ciò che non potevi sapere è che tra questi vi è pure Google, che quindi conosce anche i tuoi dati fisiologici, le tue abitudini sportive, oltre ovviamente ai tuoi gusti musicali.

Google sa anche che sei una persona romantica e riflessiva, perché traspare da ciò che cerchi online nei momenti liberi; sa che fai letture impegnate, e che hai un debole per i panda.

Non possiamo affermare con certezza quali rilevazioni Google faccia costantemente, quali una tantum a scopo "sperimentale" e quali invece siano rilevazioni che tecnicamente potrebbe fare ma in

realtà non esegue. Non possiamo dirlo, perché quel che accade nei server di Google lo può sapere solo Google, e perché i suoi strumenti sono spesso chiusi e non permettono una verifica trasparente.

Quali che siano le rilevazioni effettivamente fatte, sappiamo che Google ci osserva attraverso innumerevoli canali, e registra le nostre attività. La mole dati a cui Google ha accesso gli permette di ricostruire la vita delle persone in modi che nemmeno un social network potente e pervasivo come Facebook può sognare.

“Eh vabbè, che mi interessa della privacy?! Io non ho niente da nascondere...”

Scomodando Westin e l’etica, la **privacy** viene definita come il **controllo sull’accesso alle proprie informazioni personali.** Questo permette alle persone di avere e mantenere separate diverse parti della propria vita (vita privata, lavorativa, sentimentale, **...**) online e non.

La privacy è una questione di potere e bisogna prendersene cura.

Una contro-argomentazione comune ai movimenti pro-privacy è l'idea che non si ha bisogno di privacy se non si ha "nulla da nascondere". Questo è un pericoloso malinteso, perché di fatto crea la categoria delle persone buone e trasparenti e quella delle persone cattive, invischiate nella mafia o organizzatrici di attacchi terroristici.
La privacy non è solo di giornalisti, criminali e di persone facilmente attenzionabili.
La privacy è l’unico modo per tutelare la propria sfera di espressione individuale: Anche se, in quanto genere umano, siamo socialmente pron3 a condividere delle nostre informazioni personali (sia nella vita privata che su internet), chiunque ha il bisogno di ritornare in un posto tranquillo in cui potersi privare degli sguardi giudicanti della gente. Quel posto, proprio per le sue proprietà, è terreno fertile per creatività, esplorazione, dissenso.
Quando ci troviamo in una condizione nella quale **c’è la possibilità di essere osservati, il nostro range di comportamenti si restringe considerevolmente.** Questo, tendenzialmente, in un modo conforme alle regole e alle aspettative sociali della parte del mondo che viviamo. Una società che può essere sorvegliata, è una società che

inevitabilmente segue delle logiche di conformità, obbedienza e sottomissione.
Qualsiasi organizzazione (da quelle statali a quelle indipendenti) che vuole avere un esito di questo tipo sarà facilmente attratta da sistemi di sorveglianza di massa.
Come nel caso della lotta contro le carceri, anche in questo contesto possiamo affermare che la vera metrica dello stato di una società non si trova in come tratta chi vi si conforma, ma in come gestisce chi le si oppone, dissente e ostacola l'esercizio del potere.
Cito Rosa Luxemberg: "*Chi non si muove non può rendersi conto delle proprie catene*".

In ultimo, non dovremmo confondere la privacy con la segretezza. Sappiamo tutt3 cosa succede nel bagno di casa tua, ma chiudi comunque la porta. Questo perché vuoi la privacy, non la segretezza. In più, pensate a tutte quelle cose che diremmo allu nostru psicologu, ad una ama, al dottoru, all'avvocatu, che mai vorremmo le altre persone venissero a sapere. Ci sono sempre alcuni fatti su di noi - come informazioni sulla salute personale o sulla propria vita sessuale - che non vorremmo che il mondo intero sapesse, e va bene così. Il bisogno di privacy è legittimo, ed è questo che ci rende umani. La privacy riguarda il rafforzamento dei diritti sulle tue informazioni, non il nascondere segreti.

Piccoli step e buone pratiche per iniziare a riprendere in mano la propria privacy e non contribuire alla macchina della sorveglianza:

- **Cambiamo il nostro browser (su pc e smartphone) e motore di ricerca**: Brave browser è un browser libero (vedi paragrafo su

FOSS) con a cuore la privacy. Se volete comparare Brave con il vostro attuale browser, visitate questa pagina: https://brave.com/compare/
Come motore di ricerca consiglio duckduckgo <3

- Prestare **attenzione ai permessi che le app ti chiedono** prima di concederle. Bastano due secondi per chiedersi attivamente se si pensa servano a qualcosa o se è solo per avere ancora più accesso ai tuoi profumatissimi dati: *"Perché mai la mia nuova app per prendere le note mi sta chiedendo l'accesso ai contatti e alla posizione?!"*
- Usare delle **password forti e differenti** per ogni servizio. Per agevolare questo processo, consiglio dei gestori delle password come Bitwarden.
- Prestiamo attenzione agli **aggiornamenti**. Questi sono lo strumento che ci viene fornito per evitare che lu cattivonu sfruttino delle falle nei programmi che usiamo per fare i loro interessi.
- Usiamo dei servizi di **messaggistica cha abbiano crittografia end-to-end** abilitata di default e che non raccolgano dati non strettamente necessari.
- Quando possibile, potremmo **disinstallare** dai nostri dispositivi tutte quelle app le cui funzioni sono fruibili anche attraverso il browser. Quest'ultimo infatti ha molte meno capacità di raccolta e analisi dei nostri comportamenti.
- **Rifiutiamo le pubblicità mirate**. Quando ti viene chiesto il consenso per queste, pensa sempre al fatto che la vera domanda che ti sta venendo posta è "possiamo spiare in modo invasivo i tuoi comportamenti così da alimentare i nostri profitti e quelli delle aziende a noi vicine?"

- **Rifiutiamo i cookies**. La maggior parte dei siti che visitiamo permettono a siti terzi *(cookies di terze parti)* di installare cookies sui nostri dispositivi al fine di tracciare il nostro utilizzo di servizi digitali per profilarci e fornirci pubblicità mirate.
- **Cerchiamo app e programmi alternativi**: Per fortuna, esistono alternative validissime ai programmi/app che usiamo tutti i giorni. Ogni volta che scarichiamo un'app, chiediamoci e cerchiamo se ne esiste una (quasi) equivalente che però ha realtmente a cuore noi utenti e la nostra privacy.

Big tech merdacce

Il business model delle big tech attuali è precisamente il **capitalismo della sorveglianza.** Questo termine è stato coniato da **Shoshana Zuboff**, una professoressa della Harward Business School.

Per iniziare un'analisi sul capitalismo della sorveglianza, è necessario partire da un modello estremamente semplificato del capitalismo industriale.
Prendiamo come esempio una fabbrica di auto. La fabbrica stessa e i suoi strumenti sono mezzi di produzione che vengono usati dall3 lavorator3 per costruire dei prodotti. Generalmente, le persone che giocano al gioco del capitalismo sono incentivate ad efficentare tutto il processo attraverso forza lavoro più esperta o macchinari più funzionali per aumentare il proprio profitto. Profitto che poi verrà in parte reinvestito nell'efficentamento dell'azienda. Tutto questo al fine di rimanere vivi nel mercato.

Parlando di innovazione nel gioco del capitalismo - secondo Shoshana Zuboff - Google sarebbe la Ford del capitalismo della sorveglianza. Questo, però, non da subito!
All'inizio Google, come molte altre big tech, aveva in mente un business model che aveva come clientela gli utenti e raccoglieva dati che spesso l'utente forniva direttamente (ricerche, post, commenti, ecc.) al fine di migliorare il/i proprio/i programma/i (*anche detto software*). Questo processo [*accumulazione di dati → analisi dei dati → miglioramento del software*] invogliava nuovi e vecchi utenti ad usare il software stesso. Possiamo mettere questo processo sotto alla categoria del **capitalismo dell'informazione.** In questo sistema l'utente, anche detto prosumer (producer + consumer) produce volontariamente dei contenuti e consuma informazioni.

Il vero punto di svolta è stato quando Google e tutte le altre big tech hanno scoperto la potenzialità di altre categorie di dati degli utenti che, fino a quel momento storico, erano completamente ignorate. Questi dati vengono chiamati digital breadcrumbs (briciole digitali) o "**exhaust data**" (dati di scarico) che in realtà sono tutt'altro che "di scarico". Dentro a questa definizione cadono tutti quei dati che ci "lasciamo dietro" durante le nostre navigazioni: contenuti che postiamo online, cronologia di ricerche e siti visitati, cookies e dati per il tracciamento, metadati rigurdanti le nostre interazioni con il mondo digitale, uso di applicazioni specifiche, coordinate GPS, IP che ci vengono assegnati, metodi di pagamento, ritmo di digitazione, pattern di utilizzo, **...** Potete immaginare che la lista sia ancora lunga.

Questi dati sono una vera e propria risorsa quando si tratta di capire il carattere, pattern psicologici, interessi e stati emotivi degli utenti.

Questo però è solo parte di quello che è possibile ricavare da queste informazioni: il vero oro che le big tech hanno scoperto è la **possibilità di leggere in questi dati il nostro futuro.** Sono letteralmente una sfera di cristallo e troppo spesso non ce ne rendiamo conto.
In questa situazione non è difficile pensare a come il business delle pubblicità sia cambiato radicalmente. Le previsioni accennate poco fa sono infatti diventate il punto di partenza per un nuovo tipo di pubblicità basato sul **"mercato dei comportamenti futuri"**, come definito da Zuboff.
Questo è stato il vero punto di svolta che ha trasformato il capitalismo dell'infromazione in **capitalismo della sorveglianza.**

Avrete sentito nominjare la frase: "Se il servizio è gratis è perché il prodotto sei tu!".
Bene, secondo Zuboff questa affermazione è sbagliata perché, in realtà, noi siamo le risorse e il vero prodotto sono predizioni su di noi.

	Capitalismo dell'informazione	**Capitalismo della sorveglianza**
Cliente	Utenti	Creator3 di pubblicità
Prodotto	Il programma (aka *software*)	Predizioni su di te
E i tuoi dati?	Per migliorare il software	Per migliorare le predizioni su di te

Chiaramente, questo non poteva che produrre una raccolta di informazioni massiccia che Zuboff chiama **"Extraction imperative".** Questa è stata facilitata da ingenti cambiamenti nelle interfacce

delle app che siamo abituat3 ad usare per fare in modo di estrapolare più informazioni possibili su di noi.
Pensate agli algoritmi che vogliono tenerci incollati al telefono il più possibile, o alla trasformazione (su Facebook) dal semplice "like" ai post alla reazione tramite emoji.

Tutto questo fa già abbastanza paura così. Tuttavia, c'è un ultimo modo in cui si possono rendere le previsioni ancora più accurate: manipolare il comportamento degli utenti in modo che questo rispetti le predizioni fatte su di loro.
Instagram potrebbe farti uscire dei post riguardo alla tua recente rottura (perché è chiaro che lo sa) per farti intristire e successivamente proporti le pubblicità perfette per sfruttare la tua vulnerabilità; Google Maps potrebbe variare leggermente la strada consigliata per farti passare vicino al ristorante di cui sa che hai dei coupon...

Ora un paio di domande:
Come ti fa sentire sapere queste informazioni?
Secondo te, cosa si può predire di te in base ai tuoi dati online?

Casi studio:
- *Snowden (2013)*
- Cambridge Analitica (2018)

APP DI MESSAGGISTICA A CONFRONTO

End to End encryption (E2EE)

La comunicazione avviene in maniera cifrata tra l3 interlocutor3: questo vuol dire che nè le persone che non fanno parte di quella conversazione, nè le aziende che offrono il servizio possono leggere quello che avviene in quella conversazione.
Se prendiamo una conversazione tra due persone, è come se si creasse un tunnel diretto tra queste due persone a cui NESSUN ALTRX può avere accesso.

SIGNAL

- Signal ha creato un suo protocollo per la End to End Encryption, e lo ha fatto BENE!
- Signal si salva pochissime informazioni su di noi: numero di telefono *(che, sebbene sia necessario per la registrazione, è poi oscurabile a qualsiasi utente e rimpiazzabile da uno username)* e data dell'ultimo accesso.

Questo è attualmente la **punta di diamante delle app di messaggistica privacy-centered** di uso comune.
Passiamo a Signal! Facciamo passare le nostre nonne, l3 nostr3 spaccin3, e chiunque abbiamo a cuore a Signal!

WHATSAPP

Attualmente Whatsapp funziona usando il protocollo di End to End Encryption sviluppato da Signal. La prima cosa che possiamo pensare è: "Beh, allora top! Ci si può fidare". **No.**

E' vero che viene usato lo stesso algoritmo, però questo non vuol dire che tutte le informazioni vengono cifrate. Infatti Whatsapp (Meta) raccoglie un sacco di info su di noi e sulle nostre conversazioni. C'è da dire che alcune delle seguenti informazioni vengono raccolte da Meta solo se usiamo alcuni dei servizi offerti da Whatsapp.

Questo intanto è il raccolto della vendemmia di Meta (in cui noi siamo le viti):

- Account info (numero di telefono, nome account, stato, e altre – cito dalla loro privacy policy - "basic info")
- I messaggi che non arrivano allx destinatarix vengono salvati per 30 giorni (i messaggi salvati sono nella loro forma cifrata e quindi non leggibile da Meta)
- I media che condividiamo vengono salvati, sempre nella loro forma criptata, per del tempo (non specificato)
- Se usiamo la feature di "contact upload", forniamo a Whatsapp tutti i nostri contatti con una cadenza fissa. Però tranquill3, se qualche nostro contatto non ha whatsapp, sono così gentili da gestire le loro informazioni in modo che quei contatti non possano essere identificati da Whatsapp.
- Se usiamo la feature per i pagamenti, gli facciamo collezionare dei dati:
  - metodo di pagamento
  - dettagli per la consegna
  - quanto abbiamo speso
- Se usiamo qualsiasi feature legata alla posizione:
  - quando stiamo usando la posizione
  - le posizioni precise

Qui invece delle informazioni che vengono collezionate in ogni caso:

- Attività sui loro servizi
  - come usiamo il servizio;

    - le nostre impostazioni;
    - come interagiamo con gli altri (anche se non direttamente le persone che chiamiamo o messaggiamo)
    - quando, per quanto e la frequenza in cui usiamo l'app;
    - quando ci siamo iscritt3;
    - le features che usiamo;
    - il nome, le immagini e la descrizione dei nostri gruppi;
    - la nostra foto profilo;
    - quando siamo online;
    - l'ultima volta in cui abbiamo usato l'app;
    - l'ultima volta che abbiamo aggiornato il nostro stato.
- Informazioni sui dispositivi con cui ci connettiamo e installiamo l'app:
    - modello dei dispositivi
    - il sistema operativo dei dispositivi
    - il livello della batteria
    - potenza del segnale di rete
    - la versione dell'app
    - informazioni riguardanti il browser che usiamo
    - numero di telefono
    - nome dell'operatore a cui siamo iscritt3
    - identificativi per capire quali altri servizi Meta usiamo su quei dispositivi con account della stessa persona
- Anche quando decidiamo di non usare nulla riguardo alla posizione:
    - Stime sulla nostra posizione date dal nostro numero di telefono
- Cookies (soprattutto quando usiamo Whatsapp web)

Whatsapp riceve informazioni su di noi anche tramite altri utenti (allo stesso modo, noi forniamo info sulle altre persone).

Anche quando usiamo altri servizi (anche non di Meta) e ci colleghiamo attraverso uno dei loro servizi (Whatsapp, Facebook, ...), Meta riceve tutti i dati del caso.
Tutti questi dati non stanno solo dentro Whatsapp, ma vengono usati da tutte le aziende di Meta per profilarci e per fare profitto.

TELEGRAM

Telegram NON è un'app di messaggistica a cui frega veramente qualcosa di privacy e crittografia!
La End to End encryption non è abilitata di default e per i gruppi non esiste proprio la possibilità di attivarla.

QUESTO VUOL DIRE CHE TUTTE LE CHAT NON ESPLICITAMENTE SEGRETE E LE CHAT DI TUTTI I GRUPPI SONO VISIBILI SUI SERVER DI TELEGRAM!!!!
A questo punto la giusta reazione comprende sdegno, nausea, incredulità e un pizzico di tristezza.

Secondo Matthew Green (esperto in crittografia) – anche se abilitiamo la End to End encryption per le chat uno a uno - il metodo di crittografia di telegram è considerato "unusual" e molte delle scelte fatte farebbero sorgere numerose domande da parte di esperti di crittografia.

Scappiamo da Telegram a gambe levate e lasciamo che siano solo i gruppi di fasci a continuare ad usare questo serviziaccio!

BRIAR*

Se vi è capitato di partecipare a grosse mobilitazioni o di trovarvi in luoghi estremamente affollati, avrete notato che la connessione ad internet tende a vacillare, se non ad essere completamente assente.

Uno strumento per poter far fronte a disastri ambientali, situazioni di piazza colme di persone o governi che intenzionalmente decidono di limitare l'accesso alla rete è Briar.
Per chattare, è richiesto un consenso esplicito da parte le persone che parteciperanno alla chat. Fatto questo, i messaggi potranno essere scambiati anche attraverso il **Bluetooth**!
Il suo punto di forza sta proprio nel fatto che, **più gente c'è, più questa applicazione funziona meglio**: usando l'app, ogni persona si fa portavoce anche dei messaggi che si scambiano le persone a lei vicine!

Ma allora le altre persone a me vicine potranno leggere i miei messaggi!?
NO! I messaggi dell3 altre persone – come i tuoi – non saranno leggibile dai telefoni delle persone attraverso cui passeranno!

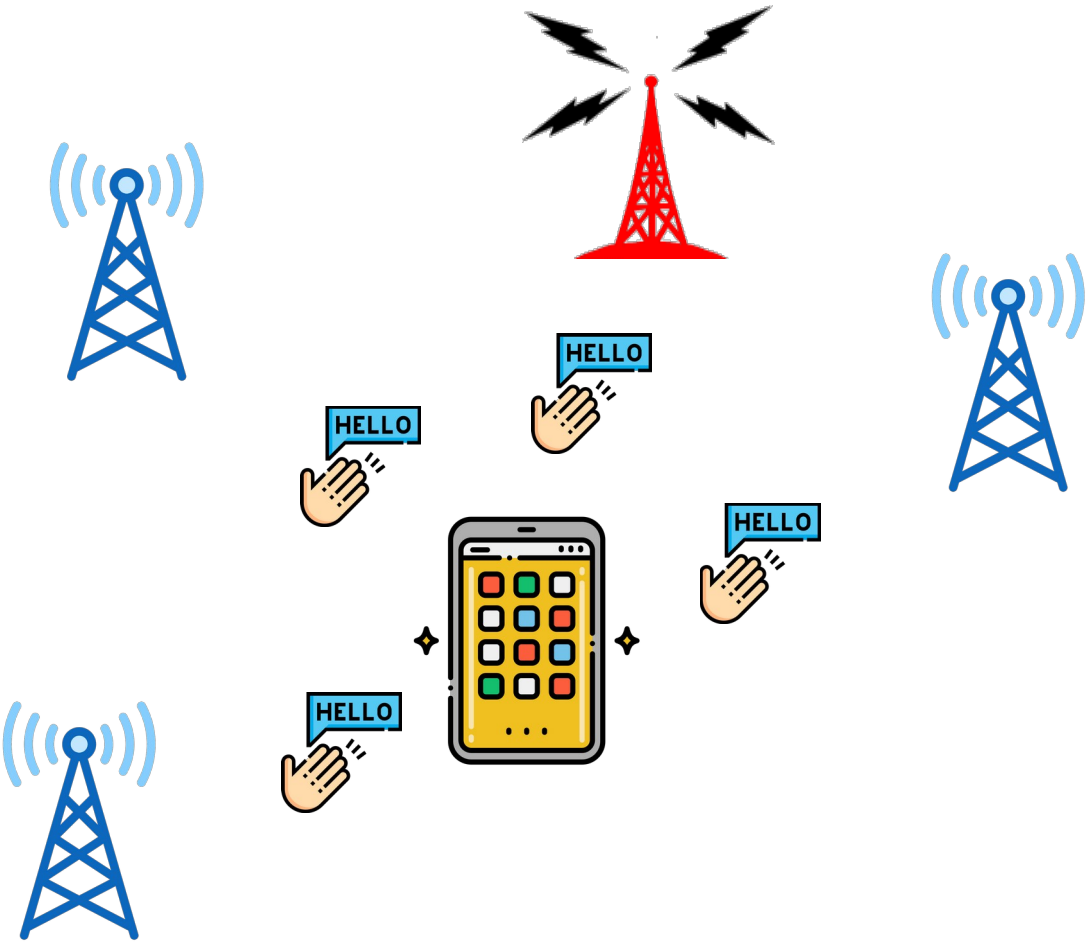
Nota sulla **privacy** di Briar:
L'applicazione non salva e non comunica nessuna nostra info personale :)

*Purtroppo **Briar non è disponibile per dispositivi iOS** e non lo sarà a meno di cambiamenti tecnici in merito alla gestione della batteria da parte degli iPhone.
Don't blame Briar, blame Apple!

BREVE NOTA SUI MOMENTI DI PIAZZA

Nel fare un'analisi su come comportarsi in momenti di piazza, bisogna fare delle valutazioni attente in base alla figura che si ricopre e sul livello di repressione generale dello stato in cui si vive. Il cellulare può facilmente trasformarsi da strumento di tutela (perché ci permette di stare in contatto con l3 compagn3) a strumento di sorveglianza da parte dello stato nei nostri confronti.

Immaginate il telefono come un oggetto estremamente estroverso che, per connettersi alla rete e per effettuare le chiamate, inizia a salutare e a dire il proprio nome a tutte le torri cellulari vicine che possono offrirgli la connettività.



Lo stato italiano lo sa e ha la possibilità di sfruttare questa dinamica a suo vantaggio attraverso l'installazione di torrette telefoniche malevole (IMSI-catchers).
Queste torrette telefoniche malevole (molto portatili, date le ridotte dimensioni) si fingono a tutti gli effetti delle reali celle telefoniche e vengono principalmente usate per geolocalizzare gli smartphones che si connettono ad esse.

Per evitare tutto questo, nei momenti di piazza come in qualsiasi altro momento nel quale non si vuole dare la possibilità di essere tracciat3, è bene lasciare lo smartphone a casa (acceso e magari con qualche download attivo).

Esistono altri dispositivi che possono essere usati per comunicare in maniera privata evitando di usare internet e di connettersi alle torrette telefoniche. Questo viene fatto usado le onde radio (completamente indipendenti da internet e dalla rete cellulare!). *Questo tema purtroppo non verrà esplorato in questa 'zine per non divagare :)*

Giusto un ultimo breve inciso per sfatare un mito: **non basta avere un secondo telefono da usare in piazza per essere anonimi!**
Elenco di una breve e non esaustiva lista di cose che non rendono il tuo secondo telefono anonimo: tenerlo acceso e connesso vicino al primo; interscambiare schede SIM con il primo telefono; avere una seconda SIM, ma comprata fornendo il tuo documento di identità; avere i tuoi soliti account sul secondo telefono; ...

LA LOTTA DI LIBERAZIONE DEL SOFTWARE

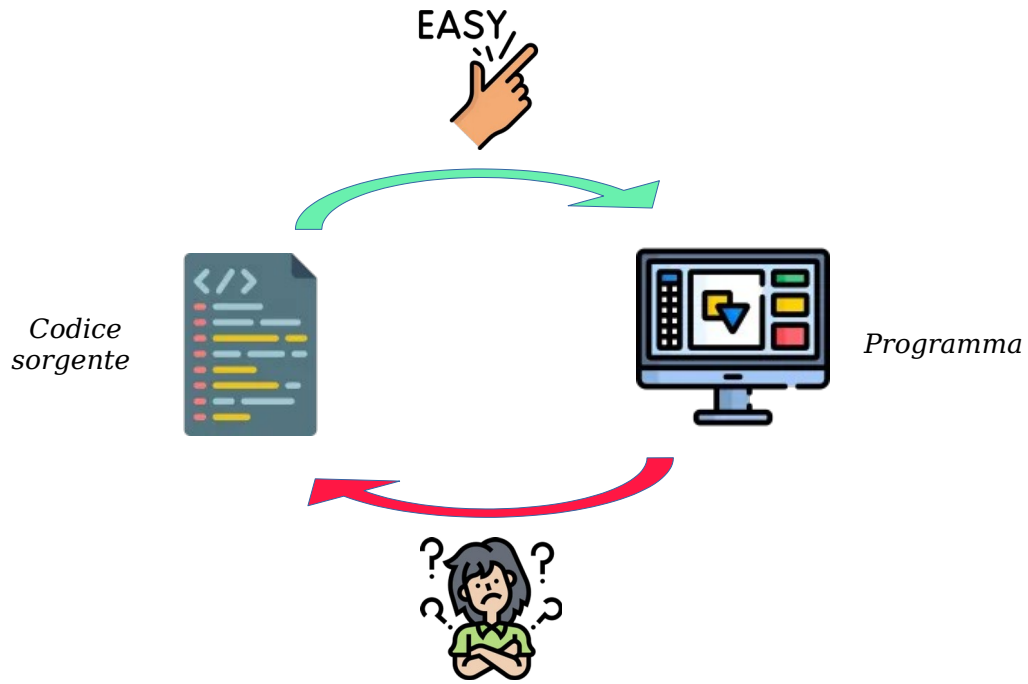
→ FOSS: Free Libre Open Source Software

(Free as in freedom, not as in gratis!)

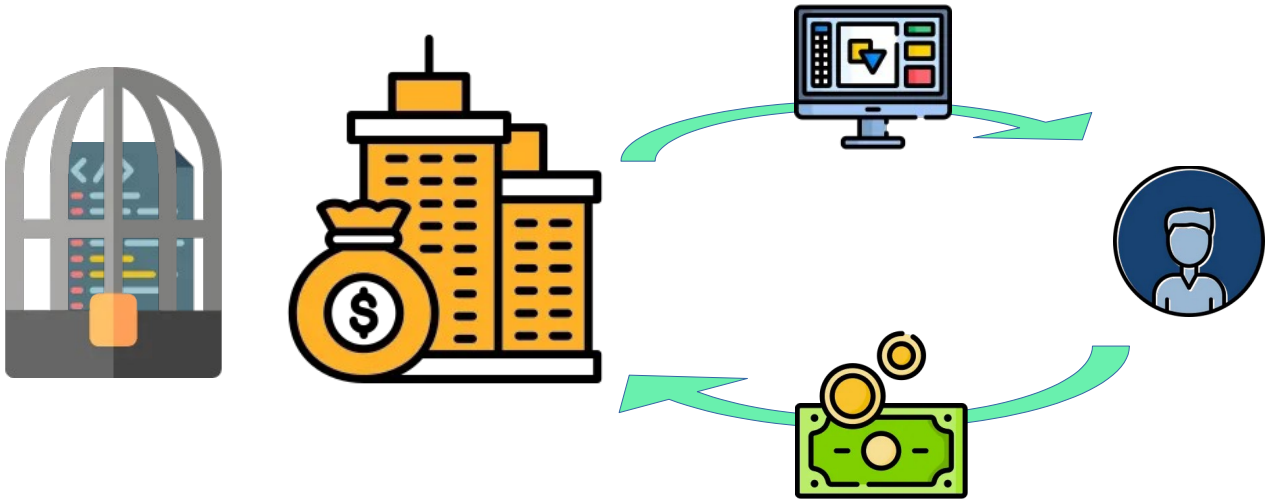
Partiamo dal principio: **Come nasce un programma? :)**

Un programma *(anche detto software)* - che questo sia fatto per telefono, pc, tablet, **...** - nasce dalla scrittura di codice. Non importa che linguaggio di programmazione si usi, il programma viene sempre partorito dal codice. Quest'ultimo è chiamato *codice sorgente* o, in inglese, *source code*.

Un passaggio fondamentale per capire tutti i punti seguenti è che dal codice sorgente è facile creare il programma, ma il viceversa è estremamente complicato: anche solo per provare a ricavare il codice sorgente a partire da un programma - senza nessuna certezza di successo - servono conoscenze estremamente specifiche ed avanzate.



La stragrande maggioranza delle aziende che vogliono fare profitto (e, a volte, anche che non vogliono fare profitto) con i propri programmi scrivono il codice sorgente, partoriscono e vendono il programma tenendosi gelosamente stretto il codice sorgente che sta alla base.
Questo perché vogliono essere le uniche persone a poterlo leggere e a metterci mano.
Il codice sorgente che segue questa logica è chiamato **codice proprietario.**



NON DEVE PER FORZA FUNZIONARE COSÌ !!!

*Imagine a world where every piece of software you use is locked behind corporate walls, restricting how you interact with technology. This was the reality of computing in the early 1980s, when proprietary software was rapidly becoming the industry norm. One man, Richard Stallman, saw this as a fundamental problem — one that needed a radical solution. The birth of the **GNU Project** wasn't just about software; it was about **freedom**, **collaboration**, and ensuring technology remained open for everyone.*

Il messia

(Richard Stallman)

Come accennato nel riquadro azzurro qui sopra, la prima persona ad aver pensato che il software potesse e dovesse essere libero è stata proprio **Richard Stallman** che, dopo aver fondato il GNU project e la Free Software Foundation, porta tutt'ora avanti un **movimento di resistenza attiva all'interno del mondo dell'informatica.**

Calma, calma, calma... per ora, in questa 'zine abbiamo citato solo il software proprietario. Cos'è tutta questa storia del software libero?!

Il "*software libero*" è software che **rispetta la libertà degli utenti e la comunità.** In breve, significa che gli utenti hanno la libertà di eseguire, copiare, distribuire, studiare, modificare e migliorare il software. Quindi è una questione di libertà, non di prezzo. Per capire il concetto, bisognerebbe pensare alla "libertà di parola" e non alla "birra gratis"; in inglese a volte usiamo libre, riciclando la parola che significa "libero" in francese e spagnolo, per disambiguare [NdT: il termine free in inglese significa sia gratuito che libero, in italiano il problema non esiste].

Potreste aver pagato per una copia di un programma libero, o potreste averne ottenuto copie gratuitamente. Ma a prescindere da come lo si è ottenuto, rimane sempre la libertà di copiare e modificare il software, o anche di venderne copie.

Noi difendiamo attivamente le libertà citate, perché tutti hanno diritto ad averle. Tramite queste libertà gli utenti (individualmente o nel loro complesso) controllano il programma e le sue funzioni. **Quando non sono gli utenti a controllare il programma, allora il programma** (che in quel caso chiamiamo "non libero" o "proprietario") **controlla gli utenti; e gli sviluppatori controllano il programma, che quindi diventa uno strumento di abuso.**

Magari non hai mai sentito parlare del software libero, ma potresti aver sentito nominare di sfuggita il famigerato "*open source*" (dove per "source" si intende il source code o, in italiano, codice sorgente - già accennato in precedenza)**.**

Il nome è autoesplicativo: I programmi *open source* sono programmi che rendono pubblico il proprio codice sorgente.

Ecco, una cosa che mi piacerebbe far passare è come i programmi open source siano profondamente diversi dal free software (= programmi liberi).

Cito dal sito di GNU:

The terms "free software" and "open source" stand for almost the same range of programs. However, they say deeply different things about those programs, based on different values. **The free software**

movement campaigns for freedom for the users of computing; it is a movement for freedom and justice. By contrast, the open source idea values mainly practical advantage and does not campaign for principles. This is why **we do not agree with open source, and do not use that term.**

Per riassumere, il **software libero** ha un **carico ideologico forte** dettato dalle sue 4 regole fondamentali atte ad inseguire l'idea di libertà:

0. Libertà di **eseguire** il programma per qualsiasi scopo.
1. Libertà di **studiare** il programma e modificarlo.
2. Libertà di **ridistribuire** copie del programma in modo da aiutare altre persone.
3. Libertà di **migliorare il programma e di distribuirne pubblicamente i miglioramenti**, in modo tale che tutta la comunità ne tragga beneficio.

Il software meramente "*open source*" non fa niente di tutto ciò. Quest'ultimo si limita a pubblicare il codice sorgente (dal quale nasce il programma) sperando che tante persone lo guardino e che contribuiscano a farlo diventare funzionante il prima possibile**……**

Detto ciò, spesso viene usato e si sente nominare il termine ombrello “FOSS”:

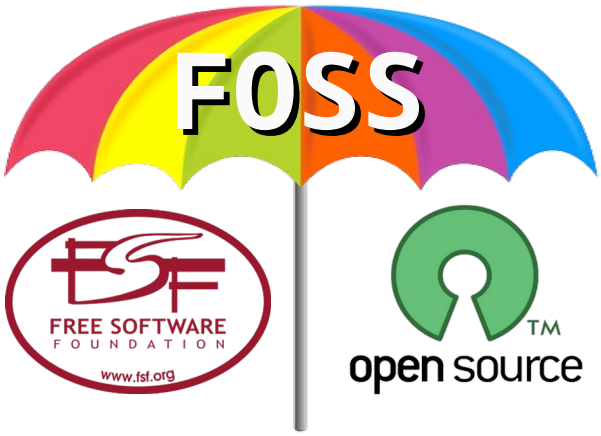
*** FOSS ***

Free &

Open

Source

Software



CI SPIANO?

Lo stato dell’arte nella nostra penisola

Ok, penso che tutt3 noi abbiamo visto i casi di cronaca del 2024/2025: compagn3 e non che sono state avvertite dalla stessa *Meta* di essere vittime di spionaggio. Spionaggio avvenuto attraverso dei programmi spia – in gergo, “*spyware*” - di origine israeliana (Paragon). Questi casi ci danno l’ennesimo motivo per alimentare il nostro fuoco nei confronti di israele, ma noi italiani non siamo da meno... purtroppo.

Il nostro motto alimenta-stereotipi potrebbe benissimo diventare:

Pizza, pasta e spyware

A riprova di ciò, il sito https://nascondino.github.io/ elenca le aziende italiane che producono spyware.

Per evitare che un giorno non sia più online, riporto qui di seguito le informazioni ad oggi (20/10/2025)

Nome	VAT number	Nome del prodotto	Potenzialità
Tykelab S.r.l.	11090591006	Ubiqo	SS7/SIGTRAN Network Surveillance, IP Network Surveillance, Deep Packet Inspection (DPI)
SIO S.p.A.	04154970968	SIOAGENT, INTEGRA, Xtreme, Spyrtacus	Spyware, Video/Audio Surveillance, GPS/location Trackers, Wiretapping
RESI Informatica S.p.A.	05633751002	GEMINI-NET	Wiretapping, IP Network Surveillance, Deep Packet Inspection (DPI), SS7/SIGTRAN Network Surveillance
RCS S.p.A.	07715580630	"Hermit" (*unofficial*)	Spyware, 0-day Exploits, IP Network Surveillance, Video/Audio Surveillance
Negg S.r.l.	02758100800	"Skygofree" (*unofficial*)	Spyware
MementoLabs S.r.l.	03924730967	unknown	IP Network Surveillance, Spyware, Rootkit, Remote Control System, IMSI Catchers
IPS S.p.A.	02021190596	GENESI Monitoring Center, MEDUSA Labs	Video/Audio Surveillance, GPS/location Trackers, Wiretapping, IP Network Surveillance, Deep Packet Inspection (DPI), OSINT Surveillance
Hacking Team S.r.l.	03924730967	DaVinci, Galileo	IP Network Surveillance, Spyware, Rootkit, Remote Control System
eSurv S.r.l.	03395880796	"Exodus" (*unofficial*)	Spyware, IP Network Surveillance, Video/Audio Surveillance

DataForense S.r.l.	07623991218	unknow	Spyware
Cy4Gate S.p.A.	13129151000	Epeius, Hydra, Gens.AI	Spyware, IP Network Surveillance, Online Disinformation
B.E.A. S.r.l.	07081770013	ENEA, TESEO, BE24	Video/Audio Surveillance, GPS/location Trackers, Wiretapping
ASIGINT S.r.l.i.	04467470615	Spyrtacus	Spyware
Area S.p.A.	03320220126	MCR Studio, MCR Captor, MCR Tracer-V3, MCR Tracer-V4	IP Network Surveillance, Video/Audio Surveillance, GPS/location Trackers, Wiretapping

Quanto costa agli sbirri (cioè al governo) sbloccarci il telefono?

Poco.

Gli costa troppo poco: sono poche centinaia di euro a sblocco *(che non è nulla per lo stato italiano, soprattutto se si tratta di provare a fermare l'ondata dissidente).*

E a chi vanno quei soldi? Sarete stupit3 di sentire che, anche questa volta, stiamo finanziando il sistema israele :((((

Mi spiego meglio.

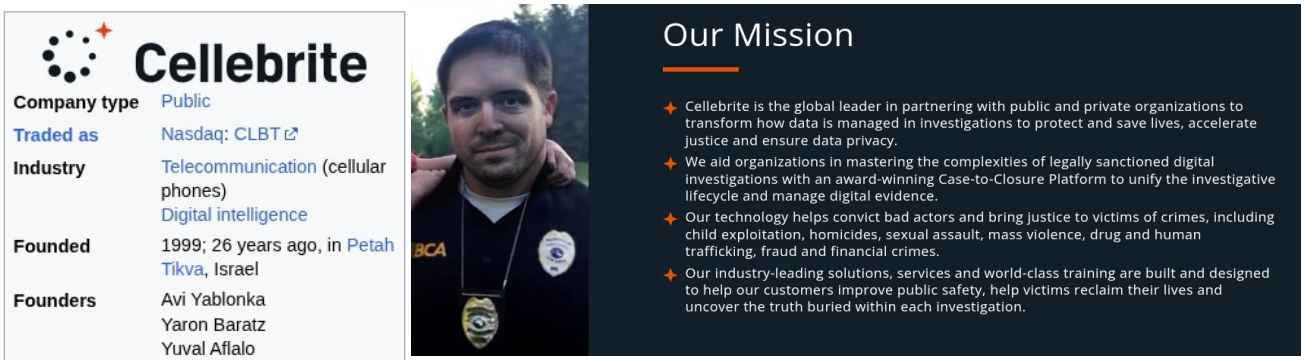
Siete ad una manifestazione e vi sequestrano il telefono?

Vi fanno un blitz a casa e vi sequestrano il telefono?

State comprando il gelato e vi sequestrano il telefono?

State sicur3 che, una volta tornati nelle loro fogne puzzone, lo sbloccheranno. Si, anche se avete messo la vostra password più sicura di sempre.

Per farlo, usano una tecnologia chiamata Cellebrite-Inseyets dell'omonima azienda (nata in Israele) Cellebrite.



La cosa più paurosa di tutte è che riescono a sbloccare la stragrande maggioranza di dispositivi, sia Android che Apple, anche molto recenti. E, soprattutto, Cellebrite si tiene gelosamente segreti i trucchetti che usa per sbloccare i telefoni cosicché chiunque voglia usare i suoi servizi sia costrettə a continuare a pagarli profumatamente.

Lo stato Italiano paga ben volentieri questo servizio ogni volta che finisce gli *x* sblocchi precedentemente acquistati. Ed è invogliato a farlo perché non vorrebbe mai farsi scappare la chance di installare dei software di spionaggio *(spyware)* sul telefono di unə militantə. Questo, infatti, quando vi viene requisito e successivamente sbloccato il telefono, succede **SEMPRE**: il vostro dispositivo non vi verrà mai restituito senza qualche piccola aggiunta da parte delle forze dell'ordine.

Spesso e volentieri la seguente misura di sicurezza viene comunque bypassata ma, se vi stanno sequestrando il telefono, fate di tutto per spegnerlo. Gli metterete almeno un po' i bastoni fra le ruote ;)

Cosa fare quando si ha paura di avere il telefono attenzionato?

Pensi di essere in questa situazione? Niente panico.
Per fortuna esistono dei collettivi italiani* che fanno il loro meglio per controllare lo stato del vostro telefono. Per farlo, hanno bisogno dell'equivalente di una scannerizzazione dalla testa ai piedi del vostro cellulare: in gergo tecnico, questa è chiamata "Bug report" per sistemi Android e "Sysdiagnose" per sistemi Apple.

In ogni caso, prima di analizzare la scannerizzazione del vostro dispositivo verrete mess3 davanti ad un triage (come al pronto soccorso) in modo che loro possano capire se siete davvero in una situazione che va analizzata o meno.

In ogni caso, esistono anche gruppi più grandi che si occupano di controspionaggio come Citizen Lab → le stesse persone di Toronto che hanno confermato le operazioni di spionaggio sui telefoni dell3 giornalist3 italian3.

* per più info in zona Trento, contattaci!
Fuori da Trento, contatta il tuo hacklab di quartiere

Pensi che la privacy sia solo per chi ha *qualcosa da nascondere*?

Guardi Google o Amazon come guarderesti un piatto di pasta al pomodoro? *(adoro la pasta al pomodoro)*

Pensi che Telegram sia davvero capace di essere una buona app di messaggistica e la consigli attivamente a tutte le persone care convintə di farle un favore?

Vuoi saperne di più sul software libero e sull'intera lotta di liberazione del software?

Non sai cosa fanno gli sbirri quando ci perquisiscono il telefono?

Questo opuscolo vuole essere un'infarinatura per chiunque (soprattutto chi non mastica l'informatica)!