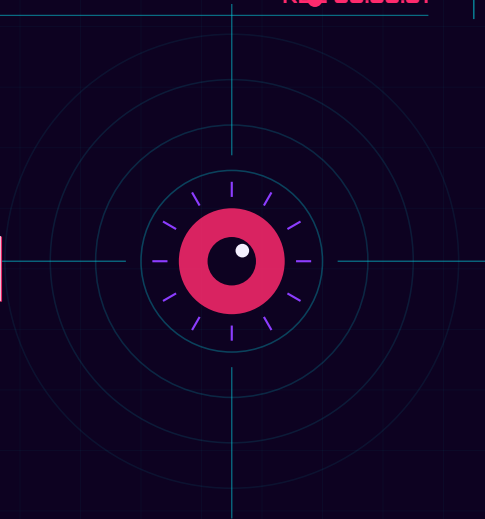


DATA CAPITALISM

e come difendersi

Roberto aka formica Marino



Di cosa parliamo

- 01 La datasfera
- 02 Le Big Tech che estraggono dati
- 03 Il surplus comportamentale
- 04 Capitalismo della sorveglianza
- 05 Espropria, monopolizza e vinci
- 06 Il business della realtà
- 07 La risposta del FLOSS
- 08 Strumenti e metodi di difesa
- 09 Conclusioni

Parleremo di un cattivo **modello economico**
che genera/richiede **cattiva tecnologia**.

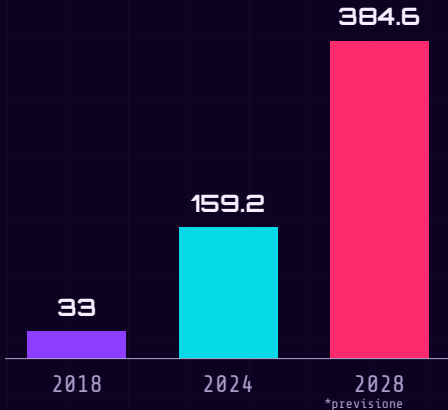
LA DATASFERA

Ossia la sterminata quantità di dati che
l'umanità crea, cattura e replica



Quanto è grande la datasfera?

zettabyte (ZB) creati per anno



- **1 ZB** = un miliardo di terabyte
- dal 2018 al 2024 la datasfera è quasi **quintuplicata**
- crescita prevista: **+24,4%** l'anno fino al 2028
- spinta da IoT, cloud e intelligenza artificiale

Fonte: IDC, *Data Age 2025* (2018); IDC, *Global DataSphere Forecast 2024-2028* (2024). Il dato 2028 è una previsione.

Data production pipeline

Dati che forniamo

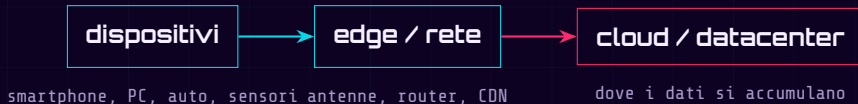
Post, foto, messaggi, ricerche, recensioni, moduli. Quello che **scegliamo** di condividere.

Dati (tracce) che lasciamo

Metadati, posizione, orari, clic, tempo di lettura, velocità di scrittura. Le **tracce** dell'uso.

Dati dedotti

Gusti, salute, orientamenti, stato d'animo, propensione a spendere. **Inferenze** sulla tua vita.



Fonte: IDC distingue tre luoghi della datasfera: endpoint, edge e core.

LE BIG TECH

Servizi gratuiti ovunque. Con quale scopo?



Chi estrae i dati, e quanto guadagna

ricavi pubblicitari 2024



† anno fiscale lug. 2023-giu. 2024, solo ricerca e news (Bing, MSN)

* stima: ~20 mld da Google per il default su Safari (2022)

+ 5-6 mld di pubblicità propria (stima degli analisti)

- per Meta la raccolta dati a fini pubblicitari vale circa il **98%** dei ricavi
- Alphabet, Amazon e Meta raccolgono il **44%** della spesa pubblicitaria *mondiale*
- **Apple** non estrae in prima persona: vende l'accesso ai suoi utenti
- Microsoft: poca pubblicità, ma **LinkedIn** e **Windows** sono miniere di dati
- il servizio è il **mezzo**: il fine è prevedere il comportamento

Fonte: bilanci 2024 di Alphabet, Meta, Amazon, Microsoft; WARC 2024; U.S. v. Google (D.D.C.); stime JP Morgan.

Luoghi e metodi di approvvigionamento

Luoghi

- sistemi operativi mobili e browser
- motori di ricerca, mappe, email
- social network e messaggistica
- assistenti vocali, smart TV, wearable

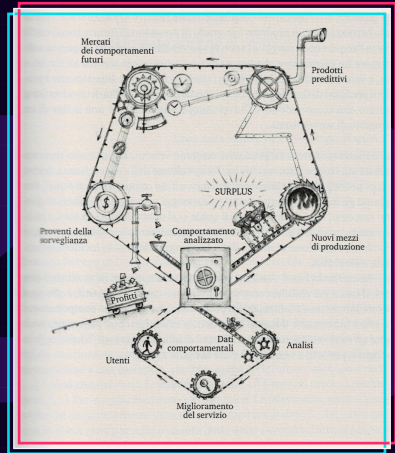
Metodi

- SDK di terze parti dentro le app
- Cookies, cookies, cookies...
- login unico "Accedi con..."
- data broker che rivendono profili

"Se è gratis, il prodotto sei tu" (ma non è ancora finita!)

SURPLUS COMPORTAMENTALE

In rete girano più dati di quelli che servono a far funzionare i servizi. Ed è proprio lì che sta il profitto.



Dal miglioramento del servizio alla previsione



- i dati in eccesso diventano **materia prima** per prevedere comportamenti futuri
- la previsione si vende a chi vuole **influenzare** quello che farai
- nasce in Google tra il 2001 e il 2002, con la pubblicità targettizzata sulle ricerche degli utenti

CAPITALISMO DELLA SORVEGLIANZA

Shoshana Zuboff, Department of Sociology,
Harvard



La definizione

“human experience as free raw material”

l'esperienza umana trattata come materia prima da accumulare

È un ordine economico

Che si appropria dell'esperienza umana per pratiche commerciali nascoste di estrazione, previsione e vendita.

È una logica di potere

Una forma di potere che punta a **conoscere e modellare** il comportamento umano per i fini di altri.

Zuboff ne dà una definizione in otto punti: non è una tecnologia, è una **ideologia** fondata sulla tecnologia.

Fonte: S. Zuboff, *The Age of Surveillance Capitalism*, 2019: definizione in apertura del volume (qui riassunta).

Capitalismo della sorveglianza: 8 definizioni

01

Un nuovo **ordine economico** che usa l'esperienza umana come materia prima gratuita, da estrarre in segreto per prevedere e vendere.

02

Una logica **parassitaria**: beni e servizi diventano un pretesto per modificare i comportamenti su scala globale.

03

Una **mutazione** del capitalismo che concentra ricchezza, conoscenza e potere come mai prima nella storia.

04

L'**infrastruttura** su cui poggia un'intera economia basata sulla sorveglianza.

05

Una minaccia per la **natura umana** paragonabile a quella che il capitalismo industriale ha rappresentato per l'ambiente.

06

L'origine di un nuovo **potere strumentalizzante** che domina la società e mette alla prova la democrazia.

07

Un progetto che vuole imporre un ordine collettivo fondato sulla **certezza totale** di cosa faremo.

08

Un esproprio di **diritti umani** fondamentali: un colpo di stato dall'alto contro la sovranità delle persone.

Fonte: S. Zuboff, *Il capitalismo della sorveglianza*, Luiss UP, 2019, "Definizione" (testo riformulato).

ESPROPRIA, MONOPOLIZZA E VINCI

Tre mosse che si ripetono da vent'anni:
prendere i dati senza chiedere, chiudere le
alternative, diventare inevitabili.



Tre mosse, in parole semplici

1. ESPROPRIA

Prendi prima, chiedi dopo.

Raccogli dati che nessuno ti ha dato, finché sembra normale.

Esempio: Street View fotografa la tua casa senza chiedere.

2. MONOPOLIZZA

Controlla tutte le strade ai dati

Occupa telefono, browser e ricerca. Compra i concorrenti.

Esempio: cerchi su Google, in Chrome, su Android.

3. VINCI

Diventa inevitabile.

Più dati, servizio migliore, più utenti: e uscirne costa troppo.

Esempio: lasci WhatsApp e perdi i gruppi.

Fonte: S. Zuboff, *Il capitalismo della sorveglianza*, Luiss University Press, 2019, cap. 5.

Espropria: il ciclo in 4 fasi

01

INCURSIONE

Si entra in uno spazio non protetto, senza chiedere.

2007: le auto fotografano strade e volti umani in tutto il mondo.

02

ABITUDINE

Il servizio è utile e la gente si abitua.

Street View diventa parte di Maps: lo usiamo tutti.

03

ADATTAMENTO

Arrivano proteste e multe: piccole concessioni.

2010: si scopre che le auto raccoglievano anche dati dalle reti Wi-Fi. Scuse, volti e targhe sfocati, accordi.

04

REINDIRIZZAMENTO

Stesso obiettivo, strada diversa.

La mappatura continua: foto degli utenti, recensioni, dati di posizione dagli smartphone.

La multa arriva anni dopo ed è piccola rispetto ai profitti: il dato ormai è stato preso.

Fonte: S. Zuboff, cit., cap. 5. Indagine Street View/Wi-Fi: dal 2010 in diversi Paesi; accordo con 38 Stati USA nel 2013.

Monopolizza: comprare chi raccoglie dati

Google / Alphabet

YouTube (2006): cosa guardi

Nest (2014): cosa succede in casa

Fitbit (2021): il tuo corpo

Facebook / Meta

Instagram (2012): foto e interessi

WhatsApp (2014): con chi parli

Oculus (2014): come ti muovi in VR

Amazon

Ring (2018): chi passa davanti alla tua porta

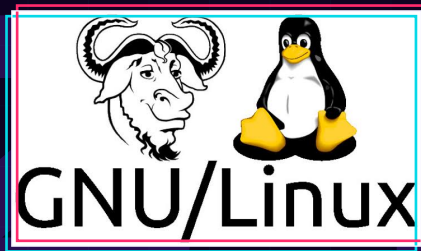
iRobot (2022): la mappa di casa tua

Meglio comprare che competere

idea espressa da Mark Zuckerberg in una email interna del 2008, citata dalla FTC

LA RISPOSTA DEL MOVIMENTO FLOSS

Il software libero non è solo codice gratis:
propone un altro rapporto tra persone,
codice e dati.



Cosa oppone il FLOSS

Trasparenza

Codice leggibile e verificabile: si può scoprire cosa raccoglie un programma, e toglierlo.

Decentralizzazione

Protocolli aperti e federati (email, Matrix, Fediverso): nessun singolo punto di raccolta.

Comunità

Valore prodotto e condiviso tra pari, non estratto da utenti ignari.

Le 4 libertà

Usare, studiare, modificare, ridistribuire: il controllo torna a chi usa.

Autogestione

Self-hosting, server di comunità, dati sul proprio hardware.

Ma attenzione

Anche le Big Tech usano FLOSS: Android, cloud, IA. Il codice libero è necessario, non sufficiente.

L'etica hacker: tre etiche in una

Pekka Himanen (2001) rilegge la cultura hacker come alternativa all'etica del capitalismo, in tre parti.

IL LAVORO

Si lavora per **passione** e curiosità, non solo per dovere.

Il codice di Linux nasce come "solo un hobby".

IL DENARO

Il valore sta nel **condividere**, non nell'accumulare.

Il riconoscimento arriva da ciò che dai alla comunità.

LA RETE: NET-ICA

Come ci si comporta in rete:

libertà di espressione,
privacy,
accesso per tutti,
responsabilità verso gli altri.

Dati pubblici: usali. Dati privati: proteggili.

uno dei principi dell'etica hacker del Chaos Computer Club

Fonte: P. Himanen, *L'etica hacker*, Feltrinelli, 2001; S. Levy, *Hackers*, 1984; CCC, *Hackerethik*.

Net-ica contro sorveglianza

Due modi opposti di guardare alla rete e alle persone che la abitano.

CAPITALISMO DELLA SORVEGLIANZA

estrazione nascosta

la tua vita privata è merce

utenti passivi da prevedere

piattaforme chiuse e monopoli

il fine è il profitto



NET-ICA HACKER

trasparenza: il codice si legge

la privacy è un diritto

persone attive che creano

protocolli aperti e decentrati

il fine è il valore per tutti

Il FLOSS è la **net-ica messa in pratica**: non solo codice libero, ma un patto tra chi crea la tecnologia e chi la usa.

STRUMENTI E METODI DI DIFESA

Nessuna bacchetta magica: se non è sufficiente il solo codice libero dobbiamo puntare sulle pratiche collettive



Prima di tutto: da cosa ti difendi?

Un modello di minaccia sono tre domande:

- 1 **Cosa** voglio proteggere?
abitudini, posizione, contatti...
- 2 **Da chi?**
pubblicitari, data broker...
- 3 **Quanto** sono disposto a cambiare?
Al bando la pigrizia...

TIPS

Contro il capitalismo della sorveglianza l'obiettivo non è nascondersi: è **non alimentare** la raccolta di surplus.

Non esiste la privacy perfetta.
Esiste la privacy **migliore di ieri**.

Il browser: la porta principale

IL PROBLEMA

Quasi ogni sito carica **tracker**: piccoli pezzi di codice di altre aziende che ti riconoscono da un sito all'altro e ricostruiscono dove vai.

TIPS

Usare un browser libero e **bloccare** i tracker prima che si carichino.

> Firefox

browser libero: imposta la protezione antitracciamento su "Rigorosa"

> uBlock Origin

estensione che blocca pubblicità e tracker: la prima cosa da installare

> LibreWolf

Firefox già configurato per la privacy

> Tor Browser

quando serve anonimato vero: nasconde anche il tuo indirizzo IP, ma rende tutto più lento

La ricerca: quello che chiedi dice chi sei

IL PROBLEMA

Durante le tue ricerche lasci tracce su di te. Collegate al tuo account, diventano un profilo. Pane per i data broker.

TIPS

Cercare con motori che **non costruiscono un profilo**, e senza essere loggati.

> DuckDuckGo

non registra le ricerche e non le lega alla tua identità

> Startpage

mostra risultati di Google, ma senza passargli i tuoi dati

> SearXNG

metamotore libero: interroga più motori per te. Puoi usare un'istanza pubblica o installarlo sul tuo server

Comunicare: il surplus sta nelle tue discussioni

IL PROBLEMA

Anche se il messaggio è cifrato, restano i **metadati**: chi scrive a chi, quando, quanto spesso, da dove. Bastano per capire relazioni e abitudini.

TIPS

App libere, cifrate, che raccolgono **meno metadati possibile**.

> Signal

cifratura end-to-end, codice libero, conserva pochissimi dati

> Matrix / Element

chat federata: hai la libertà di scegliere il server che vuoi

> Mastodon, PeerTube

social e video del Fediverso: niente pubblicità profilata, tanti server indipendenti

Lo smartphone: il sensore che porti in tasca

Il tuo smartphone sa dove sei, chi chiami, come dormi. Si può intervenire per livelli, dal più facile al più impegnativo.

LIVELLO 1 facile

Rivedi i **permessi**: posizione, microfono, contatti solo a chi serve davvero.

Cancella le app che non usi: ognuna può contenere tracker.

LIVELLO 2 medio

Installa **F-Droid**: uno store con sole app libere, che segnala chiaramente quelle con tracker o pubblicità.

LIVELLO 3 avanzato

Cambia sistema: **LineageOS**, **/e/OS** o **GrapheneOS**, versioni di Android senza i servizi Google.

Il computer e la rete di casa

GNU/Linux sul computer

Nessun account obbligatorio,
nessuna controllo remoto
aziendale, aggiornamenti dal tuo
gestore di pacchetti.

Il sistema lavora per te, non per
chi l'ha venduto.

Pi-hole o AdGuard Home

Un piccolo server (anche un
Raspberry Pi) che fa da "rubrica"
della rete.

Quando un dispositivo cerca
tracker.esempio.com, risponde: *non
esiste*.

Il blocco DNS protegge anche ciò su cui non puoi installare nulla:
smart TV, assistenti vocali, lampadine, console.

File, password e mappe

Il cloud

Il cloud è il computer di qualcun altro.

Nextcloud ti dà file, calendario e contatti su un server tuo, o di qualcuno di cui ti fidi.

Le password

Una diversa per ogni sito, salvate in un password manager libero.

KeePassXC: tutto in locale.

Bitwarden: sincronizzato tra dispositivi.

Le mappe

Le mappe sanno dove vai, ogni giorno.

OpenStreetMap è la mappa libera fatta dalle persone; OsmAnd e Organic Maps la usano anche offline.

Metodi: le abitudini contano più degli strumenti

Minimizza

Ogni dato che non dai è un dato che non può essere venduto o usato per altri scopi.

Separa

Evita le centralizzazioni e tieni distinti i contesti, così nessuno li unisce in un solo profilo.

Es.: un'email per lavoro, una per gli amici, una per iscrizioni e negozi.

Cambia i default

Le impostazioni predefinite sono scelte per raccogliere.

Es.: sui banner premi "Rifiuta tutto", disattiva ad esempio la cronologia delle posizioni.

IL GDPR: diritti che hai già

In Europa la legge ci dà strumenti concreti. Basta una email all'azienda (meglio al suo DPO, il responsabile della protezione dei dati).

ART. 15 accesso

"Mandatemi tutti i dati che avete su di me."

ART. 20 portabilità

"Datemeli in un formato leggibile, li porto altrove."

ART. 17 cancellazione

"Cancellateli." Vale quando non c'è più un motivo per tenerli.

ART. 21 opposizione

"Non usateli per il marketing." Lì devono fermarsi.

L'azienda deve rispondere **entro un mese**. Se non lo fa, puoi fare reclamo al **Garante per la protezione dei dati personali**.

Fonte: Regolamento (UE) 2016/679, artt. 12, 15, 17, 20, 21, 77.

La privacy è un fatto collettivo

IL PROBLEMA

Quando un'app legge la nostra rubrica, consegna anche i numeri dei tuoi amici. Una foto di gruppo identifica chi non ha mai espresso il suo consenso.

Principio di località: chi ti sta vicino rivela cose anche su di te.

TIPS

Difendersi da soli funziona poco: **ci si difende insieme.**

- porta almeno un amico su una piattaforma libera, come Signal o Mastodon
- chiedi prima di pubblicare foto di altri
- sostieni i progetti liberi: segnala bug, traduci, dona
- frequenta una community, come il MeLUG!!!

Da dove cominciare: 5 passi per stasera

01

Installa uBlock Origin

due minuti, e metà dei tracker
sparisce

02

Cambia motore di ricerca

DuckDuckGo, Startpage o SearXNG

03

Rivedi i permessi

a partire da posizione e microfono

04

Porta un amico su Signal

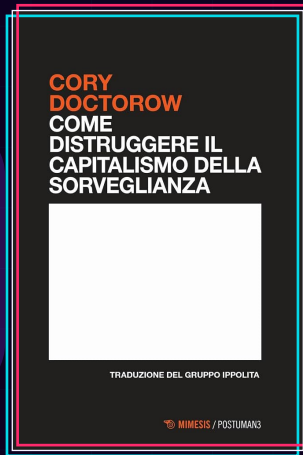
la privacy si fa in due

05

Chiedi i tuoi dati

con Google Takeout o con "Scarica le
tue informazioni" di Meta

CONCLUSIONI



Compiti per casa

- i dati crescono più in fretta della nostra capacità di capire chi li usa
- il problema non è la tecnologia, ma un **modello economico** che vive di previsioni sul nostro comportamento
- quel modello ha bisogno di opacità, abitudine e monopolio
- il FLOSS risponde con trasparenza, libertà e comunità
- difendersi è possibile: strumenti, metodi, e soprattutto pratiche collettive

OWN YOUR DATA