GLI SMARTPHONE

SONO PRATICAMENTE

DELLE MICROSPIE CHE CI PORTIAMO SEMPRE IN TASCA

OK, QUESTO LO SANNO TUTTI.

MA SONO POCHI, TROPPO POCHI

QUELLI IN GRADO DI SPIEGARE DAVVERO IN QUANTI E QUALI MODI

CI CONTROLLANO.

PEGGIO ANCORA:

TROPPA POCA GENTE HA DAVVERO CAPITO COSA VIEN FATTO CON I NOSTRI DATI

E I RISCHI PER IL DOMANI

MA SOPRATTUTTO NON SANNO CHE

1. A day in your life (Google lo sa)

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 sulla 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, un servizio di Google presente nella maggior parte degli smartphone, 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 perché hai mantenuto attiva la connessione WiFi, per cui conosce tutte le reti WiFi che il tuo telefono ha rilevato mentre ti spostavi. 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 di dati a cui Google ha accesso gli permette di ricostruire la vita delle persone in modi che i social network possono solo sognare.

2. Siamo un terreno di conquista commerciale

Mai, nella storia, poche aziende commerciali private planetarie erano riuscite a diventare parte della vita di miliardi di persone in modo così radicato e diffuso. Ogni minimo dettaglio della vita di miliardi di persone è per loro un terreno di conquista commerciale: così come le multinazionali del petrolio scatenano guerre per impossessarsi di terreni per estrarne l'oro nero, le *Big Tech* fanno a gara per estrarre sempre più informazioni da noi rispetto alla concorrenza e difatti la loro principale fonte di guadagno si chiama ***data mining***.

Big Tech: sono le principali multinazionali tecnologiche, tra cui Google, Apple, Facebook, Amazon e Microsoft (G.A.F.A.M.)
Data mining: cioè "minare", estrarre dati dalla miniera (la miniera siamo noi, le nostre attività, le nostre vite).
Big data: l'insieme dei dati estratti da migliaia, milioni o miliardi di persone.
Scambio sbilanciato: noi persone/utenti forniamo dati su tutto ciò che facciamo ad aziende che grazie a questi dati sviluppano tecniche e strumenti che ci legano sempre più a loro per estrarci ancor più informazioni.
Come lo fanno: con soluzioni tecniche e psicologiche più o meno note, scelte di design applicate a software che sfruttano la **gamification** o imponendosi come **standard di fatto.**

ESEMPI: per chattare si usa quasi solo Whatsapp; i documenti di testo sono quasi sempre realizzati in Word; per condividere i file si sceglie quasi sempre Google Drive, Dropbox e poco altro; per conoscere le attività di un'associazione è necessario stare su Facebook; chi apre una casella email sceglie sempre tra i soliti Gmail, Yahoo, Hotmail e poco altro.

Gamification: organizzare le piattaforme come un gioco con premi, ricompense, sfide.

ESEMPIO: Instagram è un “gioco” a chi cattura più followers. Per attirarli devi ottenere tanti likes e per farlo *devi* fare post che li attirino (devi dargli quello che vogliono) oppure far parlare di te facendoli ridere o scatenando flame (polemiche perlopiù vuote).

Effetti reali della gamification: la gamification sui social spinge a generare rumore e ciò accomuna fenomeni tipici di questi anni come la trap, M¥SS KETA, Young Signorino, Bello FiGo, Fedez, Jake & Logan Paul e tantissime altre webstar/influencer, così come blastatori, troll ma anche quelli che, adottano la strategia opposta, cercano di conquistare followers facendo di tutto per risultare simpatici a chiunque.

Internet delle cose: Con l’«*Internet of things*», non si farà che aumentare i metodi d’estrazione. In futuro potrebbe essere difficile procurarsi oggetti che *non* trasmettano informazioni alle Big Tech.

PROBLEMA NR.1 : Più si usano i devices e le app delle big tech che fanno data mining, più diventa difficile liberarsene

3. “Sappiamo” ma non sappiamo

Sappiamo che «Google ci guarda» ma in realtà non conosciamo davvero tutti i modi in cui lo fa perché siamo in grado di usare app e devices ma solo gli smanettoni ne capiscono davvero il funzionamento.

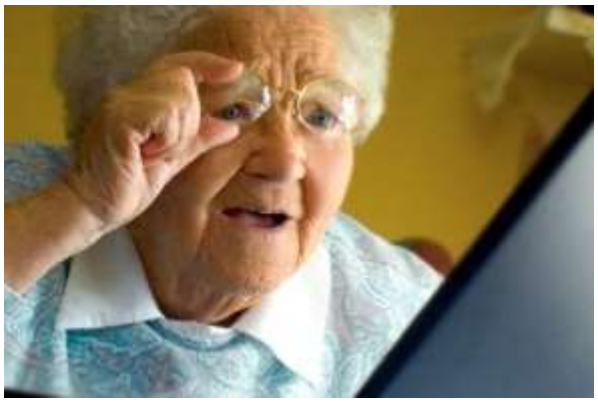
Questo è un grosso **problema**: il mondo è sempre più digitalizzato e chi non impara a comprendere come funzionano gli strumenti informatici è un po' come un analfabeta in un mondo dove tutto è scritto.
Chi non capisce come funzionano gli strumenti informatici non riesce a comprendere davvero perché il ***software libero*** è migliore (del software libero parliamo sotto).
Mica si può diventare tutti programmatori, e non si può pretendere che ognuno abbandoni di colpo tutte le app che utilizza di solito, ma è chiaro che bisogna iniziare subito ad affrontare il problema anche con piccole cose tipo sostituire browser e motore di ricerca con alternative libere.

PROBLEMA NR.2 : La maggioranza delle persone non ne sa abbastanza di informatica e usa troppo poco software libero.

4. Come è potuto succedere

Tutto il software, all'inizio era libero. Negli anni '80 ha iniziato ad esserci software proprietario e negli anni 2000, con l'aumento degli abbonamenti a internet e l'arrivo degli smartphone, il software proprietario ha preso il sopravvento.
Il software libero è più sicuro e trasparente, ma bisogna imparare ad usarlo e a volte bisogna pagarlo. Il software proprietario, invece è molto semplificato e sempre gratis.

ESEMPIO: Ci sono app per chattare libere e sicure come *XMPP* o *Riot.im* che possono fare tutte le cose che fa Whatsapp. Per usarle bisogna inserire a mano i propri contatti manualmente mentre invece Whatsapp lo installi, *si prende tutti i numeri di telefono dei tuoi contatti* e lo puoi usare subito. Whatsapp *legge e analizza tutto quello che vi scrivete* mentre XMPP e Riot.im sono fatti in modo che le vostre conversazioni siano davvero private, ma bisogna imparare come si usano.



5. Software libero vs. software proprietario

Il **software libero** è come un'automobile di cui si può aprire il cofano, vedere il motore, ripararlo, modificarlo o addirittura assemblarne uno nuovo. Essendo aperto, milioni di programmatori sparsi per il mondo collaborano a controllarlo, migliorarlo, correggere gli errori e crearne versioni alternative (ma compatibili).

Invece il **software proprietario**, quello a cui la maggior parte delle persone è purtroppo abituata, è realizzato da un'azienda che ne possiede il copyright. E' come un'automobile il cui cofano è sigillato come una cassaforte e si può solo tentar di dedurre come funzioni esattamente, senza averne mai la certezza.

Applicazioni come **Firefox**, **VLC, Kodi** o sistemi operativi **Linux** (come **Ubuntu**) sono esempi di software libero.

6. I mille tentacoli di Google

Google possiede centinaia di altre aziende e marchi e fornisce strumenti gratuiti per creare siti e altre cose ancora. Per ognuno di essi, Google ricava informazioni. Molte app gratuite in realtà guadagnano vendendo i dati a Google. Le **informazioni** che Google estrae da noi possono essere visibili o invisibili.

Visibili: una parola cercata sul motore di ricerca o su YouTube, il contenuto di un'email, gli appuntamenti inseriti sul calendario, una città cercata su Google Earth, i pdf caricati su Google Drive, le foto ed i tracciati GPS

Invisibili: Google può intercettare tutto quello che digiti su una tastiera Android. TUTTO.

Anche se poi lo cancelli ed anche se stai digitando in una app che non è di Google. Sa tutto quello che visiti con Chrome. Registra i movimenti del dito sullo schermo e tanto altro ancora. Meno strumenti di Google utilizziamo (preferendo invece alternative libere), meno informazioni potrà collezionare.

7. Il problema non sono necessariamente i dati, ma chi li possiede e ciò che può farne

Ognuna di queste fonti di dati, da sola, può essere poco importante, ma il problema è che Google **mette tutte queste informazioni insieme** ricostruendo tutto di chiunque: gusti, opinioni, abitudini, amicizie, luoghi frequentati, dati fisiologici, voti a scuola, ecc. Può sapere pure cosa dicono alle tue spalle le persone che conosci.

"Siamo milioni, non possono certo tracciarci tutti". E invece veniamo tutti tracciati, eccome! I grossi server delle big tech utilizzano sofisticati algoritmi ottenendo misurazioni automatiche estremamente precise su milioni di soggetti.

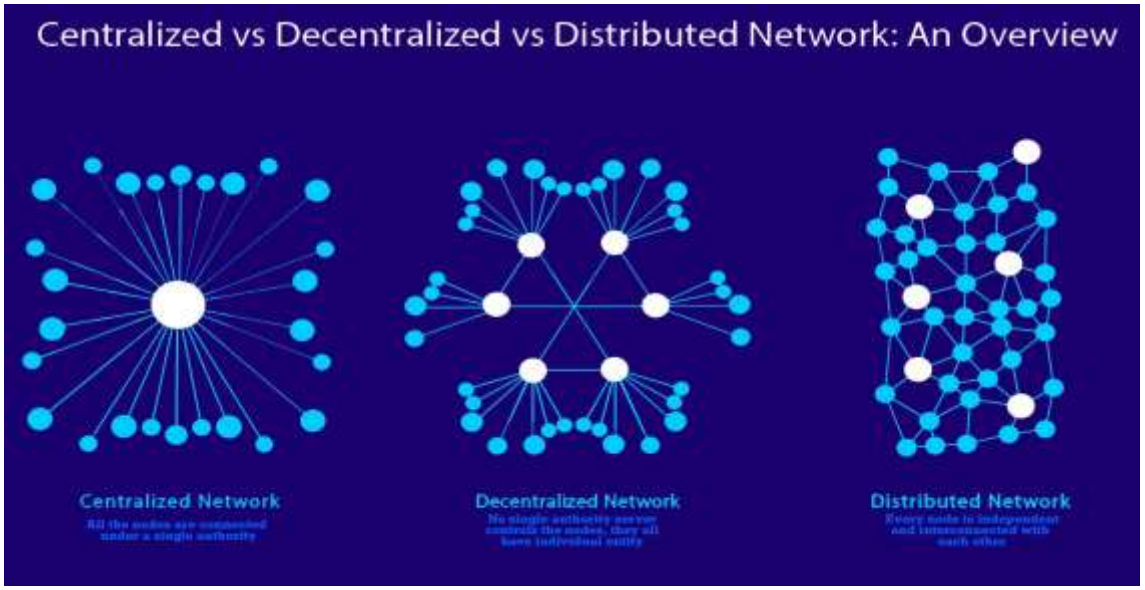
"Si ma… a Google che gliene frega di me?" Non importa se non hai nulla da nascondere, il problema è che questo *non lo decidi tu, ma lo decide chi compra i tuoi dati da Google*.

Le scuole migliori (privatizzate) potrebbero rifiutarti perché in base alle analisi preventive acquistate dalle big tech non rientri nei loro standard; enti di vigilanza potrebbero metterti in una lista di persone da controllare perché usi spesso certe parole o perché hai visitato una sola volta un certo sito che a *loro* non piace; le assicurazioni potrebbero importi polizze salatissime perché in base ai *loro* criteri ti considerano più a rischio d'infarto perché fai poco sport oppure perché fai skate, che a *loro* non piace perché ci si ammacca spesso. Potresti non trovare lavoro perché le aziende, vedendo che hai due amici a *loro* non graditi, ti mettono automaticamente più in basso nelle liste d'assunzione.

Questo sta già succedendo, anche se in modo ancora molto soft. In **Cina** invece la cosa è più avanzata. Attraversi le strisce pedonali col rosso? Una telecamera con riconoscimento facciale collegato ai tuoi social mostra il tuo volto e il tuo nome su dei megaschermi bollandoti come trasgressore in modo che chiunque possa insultarti sui social. Non hai pagato una multa o una bolletta? I tuoi dati vengono trasmessi a diverse attività (compagnia ferroviaria, hotel, ecc) obbligandoli ad aumentarti i prezzi. Hai partecipato ad una manifestazione in piazza contro le politiche del governo che il governo stesso non aveva voluto autorizzare? Ti possono togliere tutti i punti della patente.

8. Decentrare, federare, adottare standard aperti

Negli anni 2000 le Big Tech hanno convinto la maggior parte delle persone che l'unico modello possibile è quello fatto da piattaforme chiuse gestite ognuna da una sola grande azienda centrale che ne detiene il controllo. Ma non è affatto vero.



Il mondo del software libero preferisce invece realizzare network di software e piattaforme di diverso tipo basate però su *standard aperti* condivisi.

ESEMPIO: L'email è una piattaforma basata su standard aperto che viene condiviso da diversi fornitori (provider). Difatti se usi Gmail puoi scambiare messaggi anche con chi ha un indirizzo Hotmail.

Anche le linee telefoniche sono una piattaforma basata su uno standard aperto: se hai Tim puoi chiamare Vodafone e viceversa!

Whatsapp invece è una piattaforma chiusa: per chattare con chi usa Whatsapp *devi* per forza usare anche tu Whatsapp e l'app ufficiale… non puoi più toglierti altrimenti perdi tutti i contatti Whatsapp! La stessa cosa vale per Instagram, TikTok, Facebook, Snapchat, ecc.
Tutte queste piattaforme si impongono grazie a grandi capitali che possono usare per promuoversi e diventare così grandi da essere degli *standard di fatto* perché usati dalla maggioranza delle persone.

Una piattaforma basata su standard aperto ed è fornita da diversi provider forma ciò che vien definito un *network decentralizzato* (o "federato").

ESEMPIO: Mastodon è una piattaforma simile a Twitter ma è decentralizzata e libera. Anzichè una sola app ufficiale ce ne sono diverse, tutte diverse fra loro e puoi scegliere quella che preferisci.

Anche per registrarsi non c'è un'unico sito ma tanti ed ognuno ha le sue regole personalizzate e la sua community, come **mastodon.bida.im** o **mastodon.cisti.org** ma se ti registri su uno di questi siti puoi comunque interagire con chi si è registrato su un sito Mastodon diverso.

Gli standard aperti non riguardano solo le app, ma anche i files. Usare solo files basati su standard aperti impedisce di creare il monopolio di una sola app.

ESEMPIO: I file di testo sono quasi sempre **.doc**, che è un formato di Microsoft. Questo fa sì che tutti scrivano i testo usando l'applicazione Word (che è di Microsoft, appunto).

Al contrario, i files **.odt** (OpenDocument) sono un formato aperto utilizzabile da qualsiasi applicazione.

9. Informazione targhetizzata

La gran mole di dati che Google raccoglie su ognuno di noi permette di eseguire analisi psicologiche, sociali ed economiche estremamente minuziose su ogni singola persona.
Questi analisi possono essere vendute (ma anche rubate da) a chiunque, basta che paghi. L'analisi può essere utilizzata per realizzare post e contenuti *specifici per te*.
Questi post e contenuti oggi vengono scritti da esseri umani e diffusi tramite bot (account automatici), ma negli ultimi anni stanno progredendo rapidamente le capacità delle Intelligenze Artificiali (I.A. oppure A.I.) che sono capaci di generare post, testi e commenti di risposta sempre più indistinguibili da quelli umani.
Nel giro di pochissimo tempo sarà **impossibile distinguere utenti reali ed I.A. che scriveranno come noi**, genereranno dei finti selfie di sé stessi, avranno una voce e appariranno in video totalmente generati al computer ma che sembreranno al 100% reali.

Queste I.A., avendo accesso ai tuoi dati, *sapranno tutto di te* e potranno parlarti, chattare con te e farlo in modo assai subdolo per fare in modo che tu ti convinca di quel che vogliono in modo estremamente persuasivo.
Oggi ci sono le *fake news* (notizie false) e i

troll ma domani potresti essere circondata da “amici” online che ti consiglieranno film, ti daranno opinioni su vestiti ma anche su notizie ed idee politiche e lo faranno in modo convincente, amichevole e piacevole, ma saranno appunto degli strumenti controllati da chi ha più interesse e soldi per alterare l’opinione pubblica.

10. Alcuni strumenti liberi suggeriti

DuckDuckGo, SearX e **Qwant** sono motori di ricerca alternativi a quello di Google

Firefox è un browser estremamente personalizzabile alternativo a Chrome, Safari ed Internet Explorer

Openstreetmap.org è una mappa online dettagliatissima e alternativa a quella di Google. Da smartphone può essere usata con decine di applicazioni, tra cui **OsmAnd** (Android) e **Pocket Earth** (iOS)

Protonmail e **Tutanota** sono alternative sicure a Gmail.

Riot.im è una app di messaggistica sicura che assomiglia un po Whatsapp che può collegarsi a Discord e a Jitsi

Gimp è un’applicazione per modificare le immagini simile a Photoshop

LibreOffice è una suite da ufficio simile a Windows Office

Mastodon è l’alternativa libera e decentralizzata a Twitter

Audacity è un’applicazione per registrare/modificare audio e creare podcast

Jitsi è un software per videoconferenze simile a Skype

Calibre serve per organizzare la propria collezione di ebook, mentre per i fumetti/manga digitali c'é **YacReader**

Etherpad e **Framapad** sono strumenti per scrittura collaborativa che permettono a più persone di scrivere contemporaneamente uno stesso testo

VLC è in assoluto il miglior software per guardare video

Thunderbird é un'ottima app per email

Kodi è un mediacenter estremamente potente e personalizzabile

Joplin è una app per segnarsi gli appunti e sincronizzarli su più dispositivi

Bitwarden e **Keepass** sono delle "cassaforti" in cui segnarsi tutte le password

NextCloud è un software per spazio cloud simile a Google Drive e iCloud

DOMANDE

1. Leggi il paragrafo 1. Cosa ne pensi? (rispondi brevemente).
2. Secondo il paragrafo 2, un problema è la "Gamification" Prova a descrivere questo processo.
3. L'articolo sostiene che più si usano applicazioni o prodotti delle delle big tech, più diventa difficile liberarsene. Secondo te è così? Motiva la tua risposta.
4. Quali software liberi usi/hai usato?
5. Perché, secondo l'articolo, non si può considerare giusta una risposta come "non ho nulla da nascondere, guardino pure i miei dati"?
6. Che legame c'è tra Intelligenze Artificiali (AI) e "Fake news", secondo l'articolo?
7. Pensi di cambiare, concretamente, i tuoi comportamenti dopo queste informazioni? Motiva la risposta.
8. Invia il riassunto del testo all'insegnante di italiano.