AI e sorveglianza di massa

RIVOLUZIONE ONLINE – 02 MARZO 2026

Una giornata normale.

AI e sorveglianza di massa.

Sofia, 36 anni. Milano.

Sofia si sente al sicuro. Ogni mattina clicca “Accetta tutto” sui **banner** dei cookie per inerzia: il tasto per rifiutare è piccolo, grigio e nascosto. Mentre legge le notizie, il suo **browser** comunica un **fingerprint** unico: non solo il sistema operativo, ma il livello di carica della batteria e la velocità con cui si scarica. Il sistema registra perfino come l’accelerometro reagisce alle micro-vibrazioni del dispositivo mentre lo tiene in mano. È un identificatore univoco, quasi impossibile da mascherare anche con una VPN.

La sua vita è organizzata su **Google Calendar** (visite mediche, appuntamenti, impegni) e passa per **Gmail**. Anche se usa una chat cifrata, i metadati di **Messenger** e **WhatsApp** (chi sente, quando e da dove) sono a disposizione delle autorità su richiesta. Nel frattempo, **Netflix** registra orari, abitudini e scelte di visione: sa se soffre d’insonnia, inferisce stati d’ansia, e dai contenuti che seleziona costruisce un’ipotesi sui suoi orientamenti politici e culturali.

Tutto questo finisce in un report di "**affidabilità comportamentale**" che un broker vende alla banca quando **Sofia chiede un mutuo.** Il sistema incrocia le ricerche mediche, gli orari irregolari, le frequentazioni digitali. Il responso è un tasso d'interesse più alto perché il suo "profilo di resilienza" è considerato basso.

Sofia pagherà di più per colpa di un algoritmo che ha interpretato i suoi dati come segnali di instabilità. Non saprà mai perché.

Marcus, 43 anni. Chicago.

Marcus parla con la sua **AI** e le confessa lo stress per il lavoro, le chiede consigli su come gestire l'ansia, le racconta i suoi dubbi esistenziali. Non sa che quelle conversazioni sono dati processati per estrarre il suo **stato emotivo e psicologico**. Il sistema analizza le parole, il tono della voce, i pattern temporali e mappa i suoi picchi di stress con precisione crescente.

Quando esce di casa e sale in auto, il sistema di sorveglianza fisica prende il testimone. Lungo i viali di Chicago, le **telecamere ambientali** montate sui semafori e sulle auto della polizia leggono la sua targa migliaia di volte al giorno. Ogni passaggio è un timestamp: il sistema sa a che ora Marcus è uscito, quale percorso ha fatto e, incrociando i dati, sa quali altre targhe si muovono spesso "in colonna" con la sua. Se l'auto di un attivista politico è parcheggiata regolarmente vicino alla sua, il database crea un legame associativo automatico, anche se i due non si sono mai scambiati un messaggio.

Mentre guida, il suo **telefono** aggancia le celle dell'operatore telefonico ricostruendo ogni spostamento. Nei centri commerciali e nelle piazze, il **Bluetooth** intercetta il segnale dello smartphone anche se non è connesso a nulla. Questo permette una **mappatura di rete** chirurgica: il sistema sa che Marcus incontra regolarmente le stesse venti persone in un seminterrato ogni martedì sera. Le telecamere esterne confermano che le loro auto sono tutte parcheggiate nello stesso raggio di 200 metri.
Anche se nessuno di loro ha mai dichiarato un'affiliazione politica, l'AI li ha già classificati come **gruppo organizzato ad alto indice di attivismo**.

Marcus non viene arrestato. Semplicemente, il suo nome finisce in una query della **polizia predittiva**.

Quando l'ufficio delle tasse deve decidere chi sottoporre a un controllo fiscale aggressivo, il sistema sceglie lui.

Non perché abbia sbagliato i conti, ma perché il suo profilo (costruito tra confidenze all'AI, targhe riprese per strada e segnali Bluetooth) lo colloca in una rete sociale considerata **"poco collaborativa"** con le istituzioni.

Elena, 20 anni. Roma.

Stagista in una grande azienda, lavora con la suite **Microsoft 365**. L'azienda utilizza: strumenti di **analytics**, come Viva Insights, che analizzano metadati (numero di email, tempo in riunione, ampiezza della rete interna, tempi di risposta. Non leggono i contenuti, ma misurano i pattern di interazione), e tecniche di Organizational Network Analysis che mappano come circolano relazioni e competenze.
Formalmente è tutto conforme all'art. 4 dello **Statuto dei Lavoratori**: gli strumenti sono presentati come necessari all'organizzazione del lavoro e al benessere aziendale, e i dipendenti sono informati del trattamento dei dati.
Elena consegna puntuale, ma comunica poco. Scrive meno email della media, interviene raramente nelle chat, partecipa solo alle riunioni necessarie. Nei **report HR** risulta con **bassa centralità relazionale** e compare tra i profili a possibile "rischio di turnover", un indicatore a supporto delle valutazioni manageriali. L'HR verifica poi anche i suoi profili social pubblici.
E a fine stage non viene confermata. Nel verbale si legge: "Limitata integrazione nella rete collaborativa e bassa proattività comunicativa."

Non c'è un algoritmo che la epura.
È un sistema che la misura non per quello che fa realmente, ma per quanto assomiglia al profilo atteso.

Cosa è cambiato.

Per decenni la **re-identificazione**, ovvero risalire a una persona specifica partendo da dati apparentemente anonimi, è stato un processo lungo, costoso, che richiedeva tecnici specializzati, accesso a più fonti, settimane di lavoro. E quindi veniva fatto solo quando c'era una ragione precisa: un'indagine, un sospetto, un mandato. La sorveglianza era costosa, quindi selettiva. I dati personali erano frammentati, archiviati in sistemi separati, difficili da incrociare.

Poi abbiamo cominciato a **produrre e lasciare traccia di centinaia di segnali al giorno**: posizione, acquisti, ricerche, relazioni, stati emotivi inferiti.
Questi **dati** vengono ceduti attraverso termini di servizio che nessuno legge, **venduti** da chi li raccoglie **a broker di primo livello**, **rivenduti ad aggregatori di secondo livello** che costruiscono profili con fino a 10.000 attributi per persona. Società come Acxiom, LexisNexis, Experian hanno profili su miliardi di individui.
I dati sono "pubblici" nel senso che sono stati **ceduti volontariamente a soggetti privati**: e questo basta a farli uscire dalla protezione costituzionale.

Infine è arrivata l'AI: l'**aggregazione** e la **re-identificazione** sono diventate **automatiche**, **istantanee** e applicabili **su scala di massa**.
Un sistema di AI non costruisce il profilo di una persona specifica su richiesta: costruisce il profilo di tutti, e poi risponde a interrogazioni.

> "Dammi tutti i residenti di Milano che hanno frequentato una moschea negli ultimi tre mesi."
> "Dammi tutti i candidati a un concorso pubblico con un profilo di attivismo politico superiore a una certa soglia."

L’interrogazione richiede secondi e nessun mandato, perché i dati sono già stati acquistati da soggetti privati.

La zona grigia è esattamente qui: tra chi raccoglie (le app, le piattaforme), chi vende (i broker di primo livello), chi aggrega (i broker di secondo livello), e chi compra il profilo finale (lo Stato, le banche, le assicurazioni). Nessun singolo passaggio è tecnicamente illegale. Il risultato finale è una sorveglianza capillare e preventiva su chiunque, senza che nessuno abbia fatto nulla che potesse anche lontanamente giustificarla.

Sofia, Marcus, Elena non erano indagati.
Erano semplicemente nel database.
Come tutti.

Il rischio che l’intelligenza artificiale diventi il braccio armato di una sorveglianza di massa senza precedenti è uno dei due motivi che ha spinto **Dario Amodei (Anthropic)** a rompere con il Pentagono. L’intelligenza artificiale non deve diventare un’infrastruttura per la **sorveglianza automatizzata e universale**.

Il rischio è il passaggio definitivo dall’indagine sul singolo alla **neutralizzazione preventiva** della massa: un mondo in cui non sei più un cittadino protetto da diritti, ma una query in attesa di essere filtrata da un algoritmo.

I tuoi dati.

Quali tracce di te lasci, chi le raccoglie, le vende, le compra e cosa ci fa.

Tracciamento totale

USA vs Europa

Le leggi europee dicono una cosa, i server americani ne fanno un’altra.
Una tabella per orientarci e svelare il “loophole” tecnico tra il diritto alla privacy e la realtà della sorveglianza di massa.

legenda

nessuna tutelaNessuna protezione reale.

zona grigiaFormalmente vietato, accade lo stesso.

legge esisteEsiste una norma, applicazione debole.

tutela realeProtezione concretamente applicata.

1 — FONTI DI RACCOLTA DATI

APP TELEFONO

USA

NESSUNA TUTELA

SDK di data broker integrati nel codice: raccolgono posizione GPS ogni pochi minuti anche in background. Modello di business reale delle app gratuite.

EUROPA

ZONA GRIGIA

Vietato dal GDPR senza consenso esplicito. I dark pattern sui banner portano il 90% degli utenti ad accettare tutto. Le app europee installano SDK americani e trasferiscono i dati oltreoceano.

BROWSER E RICERCHE

USA

NESSUNA TUTELA

Ogni ricerca Google: timestamp, dispositivo, posizione. Cookie di terze parti su milioni di siti. Fingerprint del browser: sistema operativo, font, livello batteria, velocità scarica, risposta accelerometro — identificatore univoco, resistente a VPN.

EUROPA

ZONA GRIGIA

Stesso fingerprinting tecnico. Il GDPR richiede consenso per i cookie ma il consenso viene ottenuto tramite dark pattern. Le ricerche su Google transitano su server USA.

SOCIAL MEDIA

USA

NESSUNA TUTELA

Like, post, tempo di visualizzazione per ogni contenuto, contatti importati dalla rubrica. Cambridge Analytica deduceva i Big Five della personalità dai like. TikTok: tempo di stop su ogni video.

EUROPA

ZONA GRIGIA

Meta ha sede UE in Irlanda. Sanzione record 1,2 miliardi€ nel 2023 (= 4 giorni di fatturato). I dati europei transitano su server USA per processing.

E-COMMERCE E PAGAMENTI

USA

NESSUNA TUTELA

Amazon: ogni prodotto visto, cercato, comprato. Carte di credito: ogni transazione con merchant, importo, orario, posizione. Gmail estrae ricevute d'acquisto automaticamente.

EUROPA

ZONA GRIGIA

Stessa raccolta tecnica. Le banche europee integrano dati da app fintech collegate e navigazione (se hai accettato i cookie sul loro sito).

TELECOMUNICAZIONI

USA

NESSUNA TUTELA

Operatore: posizione antenna ogni pochi minuti, numeri chiamati, durata, SMS. Metadati disponibili all'NSA senza mandato individuale (programmi FISA).

EUROPA

LEGGE ESISTE

Metadati conservati per 6-24 mesi in Europa (fino a 6 anni in Italia per reati gravi).

Accessibili con autorizzazione giudiziaria. In pratica: scambiati con partner intelligence USA attraverso accordi bilaterali.

EMAIL E CLOUD

USA

ZONA GRIGIA

Third-party doctrine (se dai i tuoi dati a una terza parte, perdi il diritto alla privacy previsto dal IV Emendamento): i dati su cloud perdono la protezione costituzionale. Gmail scansiona voli e acquisti; Messenger non è cifrato (accesso gov). Chiavi di cifratura in mano alle Big Tech, non all'utente.

EUROPA

ZONA GRIGIA

Server fisici in UE, ma il CLOUD Act USA scavalca i confini. Accordi legali fragili: dopo il crollo dei primi due (casi Schrems), il terzo è già sotto ricorso. Accesso USA garantito "de facto".

ASSISTENTI AI

USA

NESSUNA TUTELA

Alexa, Google Assistant, ChatGPT: ogni comando vocale archiviato con timestamp. I pattern linguistici e il tono della voce permettono inferenza dello stato emotivo, livelli

di stress, vulnerabilità psicologica.

EUROPA

ZONA GRIGIA

Stessi sistemi, stesso processing. Il GDPR richiede consenso ma i termini di servizio degli assistenti AI sono accettati come blocco unico. Dati processati su server USA.

AUTO CONNESSE

USA

NESSUNA TUTELA

GPS continuo, frenate, uso cinture, peso sui sedili e battito cardiaco dal volante. I produttori vendono i profili di guida ai broker assicurativi. Le colonnine di ricarica (Tesla Supercharger, Electrify America) registrano identità, posizione esatta e durata della sosta, profilando le abitudini di sosta e consumo.

EUROPA

ZONA GRIGIA

L'AI Act classifica l'uso assicurativo come "alto rischio" ma non lo vieta. I gateway telematici proprietari bypassano il controllo dell'utente: i dati fluiscono verso i produttori USA (GM, Ford, Tesla) e da lì direttamente ai broker. Le reti di ricarica UE (Enel X, Ionity) raccolgono dati identici: il GDPR tutela il pagamento, ma la posizione e i tempi di ricarica sono trattati come dati operativi necessari, spesso trasferiti ai partner USA.

SMART TV E STREAMING

USA

NESSUNA TUTELA

ACR (Automatic Content Recognition) campiona ogni pochi secondi tutto ciò che appare sullo schermo, anche da dispositivi HDMI esterni. Netflix inferisce insonnia, stati d'ansia, preferenze culturali dai pattern di visione.

EUROPA

ZONA GRIGIA

Stessa tecnologia. Il GDPR richiede opt-in esplicito per ACR ma molti produttori lo attivano di default. Enforcement frammentato per paese.

IOT DOMESTICO

USA

NESSUNA TUTELA

Termostati Nest: orari di presenza in casa. Serrature smart: ogni apertura/chiusura. Alexa/Google Home: comandi vocali archiviati. Tutto accessibile all'azienda e alle autorità su richiesta.

EUROPA

LEGGE ESISTE

Il GDPR si applica. Ma in pratica i dispositivi IoT trasmettono dati su cloud americani. L'enforcement è minimo perché i dispositivi sono distribuiti e i produttori sono quasi tutti extra-UE. Nessuno controlla cosa invia una lampadina smart prodotta in Cina o USA.

TELECAMERE

USA

NESSUNA TUTELA

Le reti ALPR private (Vigilant Solutions, Flock Safety) vendono i dati di posizione ai broker senza restrizioni. Il riconoscimento facciale è vietato solo in alcune città (San Francisco, Boston).

EUROPA

ZONA GRIGIA

Il GDPR richiede base giuridica per il trattamento biometrico, ma l'AI Act vieta il riconoscimento facciale in tempo reale negli spazi pubblici solo con eccezioni ampie (sicurezza nazionale, terrorismo). Il riconoscimento retrospettivo (su registrazioni) è permesso con autorizzazione.

WEARABLE

USA

NESSUNA TUTELA

I dati sanitari dei wearable non sono coperti dall'HIPAA se il dispositivo non è prescritto da un medico. Già venduti a broker assicurativi e datori di lavoro.

EUROPA

ZONA GRIGIA

Il GDPR classifica i dati biometrici e sanitari come categorie speciali (art. 9), richiedendo consenso esplicito. In pratica, i termini di servizio di Apple, Garmin, Fitbit/Google ottengono quel consenso in blocco. Dati processati su cloud USA.

CARTE FEDELTÀ E PROGRAMMI LOYALTY

USA

NESSUNA TUTELA

I dati di acquisto sono proprietà dell'azienda e vendibili liberamente. Broker come Acxiom li incrociano con profili sanitari e finanziari.

EUROPA

LEGGE ESISTE

Con lacune. Il GDPR richiede consenso esplicito e finalità dichiarata. In pratica il consenso è bundled nell'iscrizione (obbligatorio per avere lo sconto) e le finalità sono formulate in modo vago. Gli acquisti in farmacia rivelano patologie senza essere trattati come dati sensibili.

RETI WI-FI PUBBLICHE

USA

NESSUNA TUTELA

Il tracciamento MAC address è prassi standard nei centri commerciali e aeroporti, venduto a broker di location intelligence senza restrizioni.

EUROPA

ZONA GRIGIA

Il GDPR si applica al MAC address come dato personale, ma l'enforcement è quasi assente perché il tracciamento avviene passivamente, senza che l'utente si connetta, e i responsabili del trattamento sono difficilmente identificabili.

EDUCAZIONE (SCUOLE)

USA

LEGGE ESISTE

Ma debole. Il FERPA protegge i record accademici formali, ma non copre i dati comportamentali raccolti dalle piattaforme LMS (Canvas, Google Classroom, Turnitin). Le edtech vendono pattern di apprendimento a broker terzi.

EUROPA

LEGGE ESISTE

Il GDPR e le normative nazionali sulla protezione dei minori impongono vincoli più stringenti. In pratica, le piattaforme (Google, Instructure) trasferiscono comunque i

dati su server USA per "manutenzione".

DATI ELETTORALI

USA

NESSUNA TUTELA

I registri elettorali sono pubblici in quasi tutti gli stati e vendibili legalmente. Incrociati con dati comportamentali permettono profilazione politica granulare (base tecnica delle operazioni Cambridge Analytica).

EUROPA

LEGGE ESISTE

I dati di partecipazione al voto sono dati sensibili sotto il GDPR (art. 9). I registri elettorali non sono pubblici e non sono commercializzabili. Restano accessibili ai servizi di intelligence nazionali e, indirettamente, ai partner americani.

2 — CHI COMPRA I DATI E COME LI USA

GOVERNO E FORZE DELL'ORDINE

USA

NESSUNA TUTELA

Data broker loophole: il Quarto Emendamento vieta perquisizioni senza mandato, ma

non si applica ai dati ceduti a terzi privati. NSA, FBI, DIA comprano profili già aggregati senza mandato. Con l'AI: interrogazioni su milioni di persone in secondi. Polizia predittiva su quartieri e individui.

EUROPA

ZONA GRIGIA

Il GDPR non si applica alla sicurezza nazionale. I servizi di intelligence nazionali operano con leggi diverse e scarsa supervisione parlamentare. Scambiano dati con NSA/CIA: se non possono raccoglierli direttamente, accedono alle analisi prodotte dai partner americani che li hanno processati dopo il transito su server transatlantici. **Stesso loophole, vestito europeo.**

ASSICURAZIONI

USA

NESSUNA TUTELA

Comprano report comportamentali da Acxiom/LexisNexis. Variabili: orari di guida, stile di frenata (dall'auto connessa), acquisti notturni, dati biometrici da wearable, CAP di residenza. Premio aumenta senza incidenti, senza spiegazione, senza possibilità di contestare.

EUROPA

ZONA GRIGIA

L'AI Act classifica il risk scoring assicurativo come "alto rischio" ma non lo vieta. Le

compagnie incrociano dati da wearable e abitudini d'acquisto. La legge vieta discriminazioni per patologie genetiche, ma non per "stile di vita poco resiliente" dedotto algoritmicamente.

BANCHE E CREDITO

USA

NESSUNA TUTELA

Credit scoring alternativo: oltre al reddito, il profilo include negozi frequentati, orari degli acquisti, ricerche online su temi legali/medici, reti sociali. Mutuo negato o a tasso più alto. La decisione è "algoritmica" e non contestabile nel dettaglio.

EUROPA

ZONA GRIGIA

Il GDPR vieta decisioni automatizzate con effetti significativi senza revisione umana. In pratica: la revisione umana ratifica quasi sempre il punteggio algoritmico. Le banche integrano dati di navigazione e fintech. Diritto di spiegazione teoricamente garantito, raramente esercitabile.

DATORI DI LAVORO E PUBBLICA AMMINISTRAZIONE

USA

NESSUNA TUTELA

Nessuna legge federale vieta l'uso di profili comportamentali nelle assunzioni. Il profilo

include attivismo sui social, associazioni, donazioni politiche. Polizia predittiva fiscale: l'IRS può ricevere segnalazioni algoritmiche basate sul network sociale del contribuente.

EUROPA

ZONA GRIGIA

Il GDPR e l'AI Act limitano l'uso di profiling per decisioni di assunzione. In pratica: i concorsi pubblici non usano profili acquistati direttamente, ma broker di "affidabilità comportamentale" vengono usati da enti appaltanti privati. I dati di partecipazione a manifestazioni restano negli archivi per anni.

3 — COSA PRODUCE L'AGGREGAZIONE

PROFILO INDIVIDUALE

USA

Dove abiti e lavori, relazioni sentimentali, fede religiosa, medici frequentati, situazione finanziaria, orientamento politico, partecipazione a manifestazioni. Non dichiarato: inferito dai pattern comportamentali.

EUROPA

Stesso profilo, costruito con dati europei trasferiti su infrastrutture americane. Meno accessibile allo Stato nella forma diretta, ma disponibile attraverso broker e

cooperazione intelligence.

RE-IDENTIFICAZIONE

USA

AUTOMATICA E MASSIVA

L'87% degli americani è identificabile univocamente con data di nascita + sesso + CAP. Con l'AI servono ancora meno elementi. Dataset "anonimi" vengono de-anonimizzati in automatico su tutti, non solo su obiettivi specifici.

EUROPA

ZONA GRIGIA

Stessa tecnica. Il GDPR impone pseudonimizzazione, ma i dataset pseudonimizzati vengono de-anonimizzati dai broker americani che li ricevono tramite SDK.

MAPPATURA DI RETI

USA

NESSUNA TUTELA

Due telefoni nello stesso posto nello stesso momento = incontro registrato. Ripetuto = relazione. Venti telefoni ogni martedì = gruppo organizzato. Classificato automaticamente senza indagine formale.

EUROPA

ZONA GRIGIA

Beacon Bluetooth, celle telefoniche e telecamere comunali permettono la stessa mappatura. L'AI Act non vieta il riconoscimento biometrico retrospettivo (solo quello in tempo reale negli spazi pubblici).

ATTRIBUTI INFERITI

USA & EUROPA

NESSUNA TUTELA – VALIDO PER ENTRAMBI

Stato di salute fisico e mentale, orientamento sessuale, vulnerabilità finanziaria, stato emotivo in tempo reale, opinioni politiche, fede religiosa: nessuno di questi attributi viene dichiarato. Tutti vengono dedotti dai pattern comportamentali e archiviati nel profilo.

4 — IL CAMBIAMENTO STRUTTURALE

RE-IDENTIFICAZIONE

PRIMA

Processo manuale. Richiedeva tecnici specializzati, accesso a fonti multiple, settimane di lavoro. Si faceva solo su obiettivi specifici con motivazione e spesso con mandato.

ORA

Automatica, istantanea, applicata su tutti in parallelo. Il profilo esiste prima che ci sia un sospetto. Non serve mandato perché i dati sono stati acquistati da privati.

SCALA	
PRIMA	Sorveglianza costosa = sorveglianza selettiva. Il costo operativo fungeva da freno de facto alla sorveglianza di massa.
ORA	Sorveglianza quasi gratuita a qualsiasi scala. Il freno economico è scomparso. Si costruisce il profilo di tutti e poi si interroga il database.

CHI RACCOGLIE	
PRIMA	Lo Stato, con atto formale e spesso con supervisione giudiziaria.
ORA	Aziende private (app, piattaforme, broker). Lo Stato compra il risultato finale senza atto formale. La catena: raccoglitore → broker L1 → broker L2 → acquirente finale. Nessun passaggio è illegale. Il risultato è sorveglianza di massa.