

Così i tuoi spostamenti sono spiai e venduti di Milena Gabanelli e Simona Ravizza

(Fonte: <https://www.corriere.it/> 10 novembre 2025)

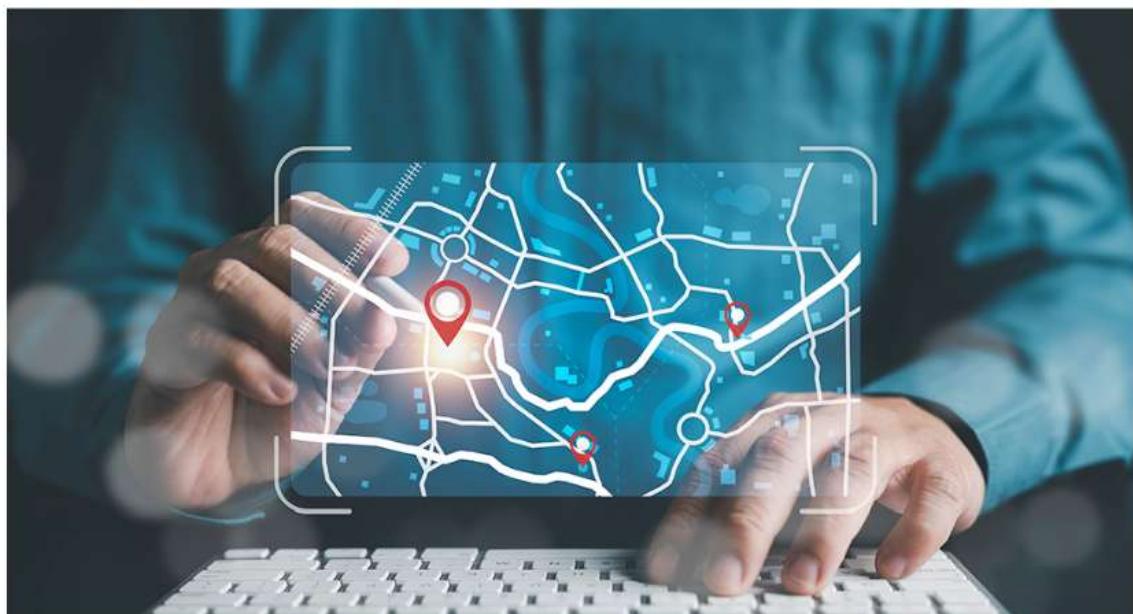


«Dimmi dove vai e dirò chi sei». Gli interessati a sapere chi siamo sono proprio tanti. Con un tocco sullo schermo del nostro smartphone e un'autorizzazione che concediamo senza pensarci, tutti i nostri spostamenti e dunque la nostra vita si trasformano in un prodotto in vendita. Le informazioni su dove abitiamo, dove lavoriamo, chi frequentiamo, come ci curiamo e dove, possono finire nelle mani di una compagnia di assicurazioni, di aziende di marketing, di un avvocato, un investigatore privato o un ricattatore. **Basta pagare, e chiunque può conoscere movimenti, abitudini, luoghi, orari.**

Il consenso alla geolocalizzazione

Quando si acquista uno smartphone la prima operazione è quasi sempre quella di aprire *Impostazioni*, poi *Privacy e sicurezza*, e attivare la localizzazione. Serve a rintracciare il telefono in caso di furto o smarrimento, per accedere a **Google maps**, per seguire gli spostamenti dei figli, per vedere il meteo, conoscere l'oroscopo, fare incontri galanti, giocare a carte, ecc. Occorre concedere l'accesso alla propria posizione e il dare consenso all'informativa sulla privacy, che nessuno legge, e dove di solito è indicato – in modo non del tutto chiaro – che i nostri dati possono essere ceduti a terzi. **Il risultato è che la nostra posizione esatta, minuto per minuto, può essere registrata e archiviata nei server di società che di mestiere raccolgono, confezionano e rivendono dati personali.** In gergo queste aziende si chiamano **data broker**. Lo smartphone sa sempre dove siamo perché determina la posizione tramite il *Gps*, che utilizza i segnali dei satelliti; le celle telefoniche a cui si connette attraverso le antenne; e le reti *Wi-Fi*

circostanti. Inoltre, nelle app che scarichiamo, gli sviluppatori possono includere nel codice un modulo software chiamato **Sdk (Software Development Kit)**, che **consente ai data broker di raccogliere direttamente i dati di localizzazione di milioni di telefonini**.



Cosa compra chi acquista

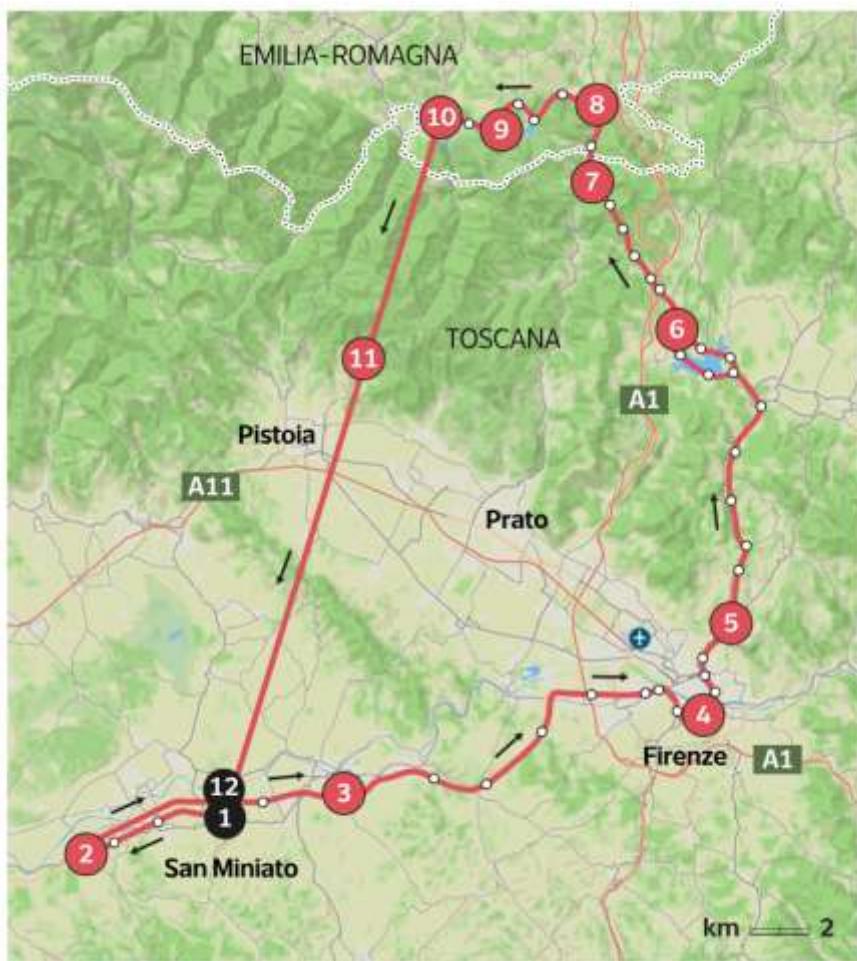
Chi acquista i dati di localizzazione da un data broker ottiene file con milioni di righe di informazioni: ciascuna contiene il **Maid (Mobile Advertising ID)**, ossia un codice alfanumerico che - come una targa dell'auto - non indica il nome dell'utente ma identifica in modo univoco il dispositivo; e poi il **sistema operativo** (Android o iOS); l'ora, la durata e il Paese di connessione; le coordinate esatte della posizione; e l'indirizzo IP utilizzato in quel momento. Siccome il servizio è costoso un data broker ha fornito a un potenziale cliente di una società di marketing un singolo campione di dati a titolo gratuito per mostrare come funziona. Il campione fotografa in media gli spostamenti di oltre due milioni di persone al giorno tra **Milano, Firenze, Roma e Napoli** durante 2 settimane nel mese di giugno 2025. Cosa succede a questo punto possiamo dimostrarlo per la prima volta in Italia.

Il codice alfanumerico in vendita



Cosa sanno di noi

Dispositivo n. 1): Tizio parte da via Rovani a **San Miniato Basso** (dove abita) poco dopo le 6 del mattino, 7.26 **Montopoli in Val d'Arno**, 7.42 **Empoli**, 8.06 **Firenze**, 9.27 **Fiesole**. Poi si dirige a **Barberino di Mugello**, passa per **Montepiano**, alle 11.25 è a **Castiglione dei Pepoli**, poi **Bagnone**, e 12.06 giro intorno al **lago di Suviana**. Ritorna a casa alle 20.28.



Esempio n.1

Partenza da casa

- 1 6.00 → Via Rovani a San Miniato (provincia di Pisa)
- 2 7.26 → Montopoli in Val d'Arno
- 3 7.42 → Empoli
- 4 8.06 → Firenze
- 5 9.27 → Fiesole
- 6 Barberino di Mugello
- 7 Montepiano
- 8 11.25 → Castiglione dei Pepoli
- 9 Bagni
- 10 12.06 → Lago di Suviana
- 11 Dati parziali perché il campione è gratuito
- 12 20.28 → Ritorno a casa

Dispositivo n. 2) Caio abita in via Di Camerino a **Reggello** (Firenze), dove esce di casa alle 3.29 e passa la notte spostandosi per **Incisa in Valdarno**, dove si ferma poi qualche ora in via Roma, alle 10.34 del mattino riparte, torna a casa, e alle 13.46 è al circolo ippico, poi di nuovo a casa dalle 17.08.



Esempio n.2

Partenza da casa

- 1 3.29 → Via Di Camerino a Reggello (Firenze)
- 2 10.34 → Passa la notte spostandosi per Incisa in Valdarno, dove si ferma poi qualche ora in via Roma
- 3 13.46 → Reggello, al circolo ippico
- 4 17.08 → Ritorno a casa

Dispositivo n. 3) Sempronio esce di casa in via Di Taccino a **Fucecchio** (Firenze) alle 7.24, si sposta nel quartiere, poi si dirige verso **Pistoia** dove arriva alle 12.48 e si ferma in via Padre Ippolito Desideri per circa un'ora. Alle 14.04 prende viale Adua per la Statale che lo porta alle 16.20 a **Lizzano in Belvedere**, alle 19.27 ritorna in centro a **Pistoia**, dove si ferma fino alle 21.15 e risulta di nuovo a casa alle 23.08.



Esempio n.3

Partenza da casa

- 1 ORE 7.24 → Via Di Taccino a Fucecchio (Firenze) Si sposta nel quartiere
- 2 12.48 → Pistoia (si ferma in via Padre Ippolito Desideri per circa un'ora)
- 3 14.04 → Prende viale Adua per la Statale
- 4 16.20 → Lizzano in Belvedere
- 5 19.27 → Pistoia (si ferma fino alle 21.15)
- 6 23.08 → Ritorno a casa

Il prezzo dei dataset completi, cioè tutti i dati di posizione delle app relativi a un determinato territorio, possono variare dai 3 ai 5 mila dollari mensili. Chi compra questi dati non ottiene il nome del soggetto, ma un codice che permette di identificarlo (**Maid**). Con 5 centesimi in più per 100 contatti ci sono poi data broker che forniscono il Maid associato a nome, cognome, indirizzo e-mail. A questo punto l'acquirente può conoscere tutti i dati funzionali a quello che succede in una determinata area, ma anche associare i nostri spostamenti ai dati anagrafici, e quindi sapere chi sta facendo trattamenti sanitari, chi frequenta il circolo ippico, la sede di un partito, o chi entra al Ministero della Difesa.

Il mercato dei dati

QUANTO COSTA UN DATASET COMPLETO



dai **3** ai **5.000** dollari mensili

+

5 centesimi

per 100 contatti si risale a: **nome, cognome, indirizzo e-mail**

LE INFORMAZIONI



chi sono



dove abito



dove lavoro



che posti frequento

CHI LI PUÒ COMPRARE



compagnia
di assicurazioni



un avvocato



uno spione
o un ricattatore

I rischi

I pericoli legati alla vendita dei nostri dati di posizione sono enormi. A livello personale, chiunque può acquistare la nostra routine quotidiana e usarla a fini di **ricatto** o **stalkeraggio**. A livello aziendale e statale, si aprono le porte allo **spionaggio industriale** e a minacce per la **sicurezza nazionale**, monitorando gli spostamenti di dipendenti, funzionari o militari.

Un'[inchiesta](#) di *le Monde* ha rivelato come attraverso una nota **app di fitness** venivano tracciati gli spostamenti del presidente **Macron**, mentre una [indagine recentissima](#) condotta insieme ai colleghi belgi di *L'Echo* e altre testate mostra il monitoraggio di funzionari Ue fino alle loro abitazioni. Un rischio gravissimo che riguarda anche lo **Stato di diritto**. In Italia, un **magistrato** deve ottenere l'**autorizzazione** di un **giudice** per poter tracciare un **telefono**, con limiti precisi di tempo e di finalità. Questo sistema di garanzie viene completamente

aggirato: chiunque, pagando, può acquistare un tracciamento molto più capillare. Nel nostro Paese la divulgazione o diffusione illecita di dati personali, sensibili e non cedibili, costituisce reato ai sensi degli articoli 167 e 167-bis del Codice in materia di protezione dei dati personali (D.lgs. 196/2003 [qui](#)). Tuttavia il consenso, che regolarmente viene prestato in modo inconsapevole, legittima il trattamento dei dati da parte dei broker, che peraltro operano per lo più all'estero. Di conseguenza, perseguire penalmente questi soggetti risulta difficile, se non impossibile. Alla luce di tutto ciò, l'intera architettura burocratica sulla privacy - se non accompagnata da un adeguato controllo del **Garante, delle Procure, delle Forze dell'Ordine** e più in generale di tutti gli organi competenti, è in grado di garantirci una tutela effettiva?

La reazione della Commissione Ue

È una domanda che interella direttamente il legislatore. Risponde attraverso il suo portavoce il Dipartimento Dg Justice, che presso la Commissione Ue si occupa del **Regolamento generale sulla protezione dei dati** (*General Data Protection Regulation*): «La Commissione è consapevole dei risultati preoccupanti emersi da queste inchieste. Siamo preoccupati per il commercio dei dati di geolocalizzazione dei cittadini e dei funzionari della Commissione, un mercato di cui molti di noi e molti cittadini europei non sono consapevoli. Nella Ue disponiamo già di una legislazione solida, in particolare il Gdpr: qualsiasi dato personale può essere raccolto solo per finalità esplicite e legittime. Spetta alle autorità di vigilanza nazionali determinare se le norme europee in materia di protezione dei dati siano state violate. La Commissione è pronta a cooperare con tali autorità. Un importante promemoria: **dobbiamo prestare molta attenzione quando le app e i servizi online ci chiedono di fornire il consenso**, anche per tracciare la nostra posizione o la nostra attività su altre app e siti web a fini pubblicitari. Dopo aver appreso dell'indagine, la Commissione ha emanato nuove linee guida per il proprio personale sulle impostazioni di tracciamento pubblicitario nei dispositivi aziendali e privati, e ha informato altre istituzioni dell'Unione e i team di risposta agli incidenti informatici degli Stati membri».

Come possiamo difenderci? Pierguido Iezzi, direttore cyber di *Maticmind - Zenita Group*: «La geolocalizzazione racconta abitudini, relazioni, momenti privati. Nel quotidiano digitale la posizione va concessa solo quando serve davvero, bisogna capire perché un servizio la chiede e per quanto la userà, ed evitare di installare app concedendo *tutto* senza sapere cosa stai concedendo.

In pratica:

- 1) vai su impostazioni, poi su *Privacy e sicurezza, e localizzazione*.
- 2) Scorri l'elenco delle app e per ciascuna seleziona il livello di condivisione:
 - a) **consenti solo mentre l'app è in uso;**
 - b) **chiedi ogni volta;**
 - c) **non consentire».**