

Come la polizia USA sfrutta i dati di Google per ottenere informazioni sugli utenti

L'utilizzo dell'ecosistema digitale di **Google** è senza dubbio conveniente. Il motore di ricerca del *brand* è diventato un vero e proprio punto di riferimento nel settore, il suo servizio di posta elettronica è tra i più apprezzati dell'intero internet e Google Maps viene comunemente adoperato per navigare le viuzze delle città di tutto il mondo. Tuttavia una simile comodità non è esente da inconvenienti. Per conformarsi alle leggi vigenti, le Big Tech non esitano a **condividere i dati** dei loro utenti con le **forze dell'ordine** e con i Governi che dispongono dei mandati giudiziari appropriati, una peculiarità che sta generando nuovi stratagemmi di **sorveglianza e investigazione**.

Recentemente, [Bloomberg](#) ha pubblicato un report in cui ha esplicitato l'esistenza di una pratica poliziesca che si appoggia sui dati di **geo-fencing** accumulati delle varie imprese tecnologiche. In termini semplici: le autorità costringono le aziende a comunicare quante e quali dispositivi sono **transitati in una specifica** area geografica durante un lasso di tempo ben definito. Queste informazioni, spesso eccessivamente dispersive, vengono successivamente raffinate richiedendo a Google di tracciare le informazioni di coloro che hanno effettuato determinate ricerche sul web. Coloro che si trovano nei punti di contingenza delle due liste finiscono spesso con l'essere indagati, poco importa che la loro presenza in loco fosse innocente o casuale.

Una simile pratica deve necessariamente esplorare in maniera indiscriminata le informazioni personali di persone estranee ai fatti, pertanto viene formalmente considerata un'*extrema ratio* da scomodare esclusivamente nei casi di assoluta necessità. La sua immediatezza sta tuttavia facendo sì che questo percorso sia scelto fin troppo spesso come via preferenziale ancor prima che tutte le altre opzioni a disposizione si siano dimostrate inefficaci. Nel 2021, in risposta a un articolo del [The Guardian](#), Google [ha rivelato](#) di aver ricevuto tra il 2018 e il 2020 ben **21.000 mandati** di richiesta per i dati di *geo-fencing* solamente dalle autorità degli Stati Uniti. Stando a quanto riporta [Bloomberg](#), nel 2022 le richieste sono lievitate a **60.472** e l'80% di queste sono state accolte. Il 20% circa dei mandati riguarda per altro reati poco emergenziali quali furti o vandalismo, crimini che difficilmente giustificano un'invasione nella privacy che può coinvolgere in una sola volta decine di migliaia di persone.

Dal punto di vista legale, le Big Tech non possono sfuggire alle norme vigenti, eppure possono comunque compiere scelte consapevoli al fine di prevenire pratiche che rasentano l'abuso di potere. Un esempio viene fornito da Apple, la quale ha deciso di non conservare quel genere di informazioni tanto care alle polizie, sminuendo così alla sorgente l'efficacia delle pratiche di *geo-fencing*. Google non ha però intenzione di seguire questa strada: la commercializzazione delle inserzioni legate a questo genere di dati rappresenta **l'80% del suo fatturato** e l'azienda si guarda bene dall'anteporre gli interessi del pubblico a quelli

Come la polizia USA sfrutta i dati di Google per ottenere informazioni sugli utenti

dei suoi investitori. Questo approccio consapevole è stato reso ancora più trasparente da alcune [recenti rivelazioni](#) in cui il vicepresidente finanziario di Google, Michael Roszak, ha candidamente ammesso che il popolo di internet sia ormai tanto dipendente dai suoi servizi che la Big Tech può concretamente permettersi di **accantonare gli interessi degli utenti** per concentrarsi sulla monetizzazione dei beni digitali.

Il rapporto sulla trasparenza [pubblicato](#) da Google rivela che negli ultimi cinque anni le autorità italiane hanno inoltrato **più di 1.200 richieste ogni semestre** per ottenere informazioni la cui natura non è mai opportunamente specificata, tuttavia gli europei possono comunque consolarsi sapendo che, almeno per il momento, il regolamento generale sulla protezione dei dati (**GDPR**) ostacola l'uso delle pratiche di *geo-fencing*. Per accedere alle informazioni, gli investigatori dovrebbero ricevere il consenso esplicito del consumatore.

[di Walter Ferri]