TikTok, come i social ci leggono nel pensiero

Tutti, almeno una volta, abbiamo avuto l'impressione che i social ci leggano nel pensiero, quasi ci spiassero. Per capire se, e come, questo è possibile **abbiamo fatto un esperimento** eseguito dagli esperti informatici di Swascan di Pierguido Iezzi, con la supervisione scientifica di Andrea Rossetti, docente di Informatica giuridica della Bicocca, e Stefano Rossetti, avvocato per la protezione dei dati personali di noyb («None of your business», il centro europeo per i diritti digitali con sede a Vienna).

L'esperimento su TikTok

Abbiamo preso due smartphone: uno nuovo, mai usato prima e che per semplicità consideriamo intestato a Gabanelli, e uno

utilizzato abitualmente che identifichiamo come intestato a Ravizza. **Entrambi vengono collegati alla stessa rete wi-fi**. Con il telefono vergine apriamo un account TikTok, il social che in Italia oggi conta 14,8 milioni di utenti attivi al mese, e 1,2 miliardi a livello globale, di cui il 25% con un'età compresa tra i 10 e i 19 anni. Per aprire il nuovo account bisogna fornire i dati personali e creare una password. Età minima richiesta 13 anni, ma di fatto lo usano anche i bambini perché non c'è nessun tipo di controllo. Per continuare occorre accettare i termini d'uso e la policy privacy. Vediamo che cosa si accetta con la nota scritta in caratteri minuscoli e che quasi nessuno legge ma che equivale alla firma di un contratto.

I termini d'uso

Le condizioni principali che accettiamo sono due, spiegate così da TikTok:
1) «Non devi pagare per l'uso della nostra Piattaforma, ma, in cambio, veniamo pagati da terzi affinché ti possano pubblicizzare o vendere prodotti»;
2) «Quando pubblichi un contenuto sulla Piattaforma, rimani il titolare dello stesso, tuttavia, **potremo mostrarlo ad altri utenti e utilizzarlo per consentire la fruizione della Piattaforma**, così come altri utenti potranno a loro volta utilizzarlo. Laddove tu decida di rimuoverlo successivamente, copie dello stesso realizzate da altri utenti potranno comunque essere visualizzate sulla Piattaforma».
Con l'informativa sulla privacy invece autorizziamo TikTok a raccogliere tutti i contenuti che creiamo: fotografie, video, registrazioni audio, livestream, commenti, hashtag, feedback, revisioni, nonché i relativi metadati (fra cui, quando, dove e da chi è stato creato il contenuto). I testi dei messaggi e i relativi metadati (l'ora in cui il messaggio è stato inviato, ricevuto e/o letto, nonché i partecipanti alla comunicazione). Informazioni sugli acquisti. **Ci sono poi le informazioni raccolte in modo automatico**: modello del dispositivo, il

sistema operativo, gli schemi o i ritmi di battitura, l'indirizzo IP e la lingua del sistema. Localizzazione. Contenuti visualizzati, durata e frequenza di utilizzo. **Infine ci sono le informazioni dedotte**: generalità dei soggetti con cui interagisco, nonché i nostri interessi.

Le conseguenze del consenso

Noi non lo vediamo, ma ogni volta che utilizziamo TikTok, come qualsiasi altro social, si generano migliaia di file di testo con tutte le informazioni di cui sopra. A chi vanno questi dati? Dall'analisi del traffico degli esperti di Swascan si vede che i file confluiscono nei server di proprietà di TikTok e in un'immensa rete di computer (CDN) che ridistribuisce i contenuti. Da qui le informazioni che ci riguardano – lo sappiamo perché lo dichiara lo stesso TikTok – vengono inviate ai cosiddetti data broker, ossia società specializzate nelle operazioni di profilazione che classificano ogni singolo utente e lo collocano in una o più categorie. I data broker di TikTok sono 16: Adbrix Original, Adform, Adjust, Appmetrica, Appsflyer, Branch, Doubleclick, Flashtalking, Kantar, Kochava, Moat by Oracle, Mytracker, Nielsen, Singular, Sizmek, Tenjin. A questo punto si alza un muro: **cosa accade durante il data sharing (la condivisione dei dati) è impossibile da ricostruire, perché le piattaforme schermano il flusso dei dati e anche gli esperti di informatica non riescono a «bucarlo»**. È il motivo per cui abbiamo deciso di procedere con l'esperimento sul campo per un paio di settimane e vedere concretamente cosa succede sui due telefoni.

Test numero 1

Sullo smartphone vergine di Gabanelli decidiamo di seguire 20 brand tra i più noti e seguiti: Adidas, Balenciaga, Chiara Ferragni, Dior, LuisaviaRoma, Nike, Zalando, Zara, ecc. **Ebbene, su Instagram del telefono di Ravizza, dove non è stata eseguita nessuna ricerca, compare la pubblicità degli**

stessi brand di cui è diventata follower Gabanelli. È la conferma pratica che tramite i data broker almeno tre informazioni essenziali passano da TikTok di Gabanelli a Instagram di Ravizza: indirizzo IP, user agent e geolocalizzazione. Il risultato è che **in base all'indirizzo Ip che indica il wi-fi a cui io sono collegata, chi è vicino a me e collegato alla stessa rete, riceve pubblicità su quello che interessa a me**.

Test numero 2

Sul telefono vergine cerchiamo su Google informazioni su un noto brand di tecnologia, Samsung, e accettiamo tutti i cookies. Su TikTok di Gabanelli compare in tempo reale la pubblicità di Samsung. Il perché sta nell'analisi del traffico dei dati: per le campagne social Samsung manda le informazioni alla società Sprinklr, che a sua volta è partner di TikTok.

Test numero 3

Sempre su TikTok del telefono usato abitualmente da Ravizza compare la pubblicità di VGP, un'agenzia di videogames. Dall'analisi del passaggio di informazioni si vede che TikTok fornisce al data broker Adjust i dati degli utenti, che in base alla loro profilazione possono diventare giocatori. Siccome Adjust è anche socio di VGP, grazie alle informazioni ricevute può fare pubblicità mirata su TikTok individuando gli utenti più inclini a spendere soldi all'interno dell'app. Il team di marketing di VGP riceve poi notifiche in tempo reale da TikTok su chi clicca, chi scarica e chi acquista. In questo modo il Roas di VGP, che è l'indice di redditività che misura l'efficienza degli investimenti pubblicitari, è passato dal 15 al 30%. Ma come ha fatto Ravizza a finire classificata come potenziale giocatrice? **È stato sufficiente fare qualche ricerca sulle società di game per scriverci un articolo. Ogni click viene registrato e quindi diventa possibile protocollare l'intera vita**.

Le tracce digitali

Per dare un'idea della precisione dei dati raccolti su ciascun individuo, si può osservare il recente caso della «lista Xandr», uno dei principali data brokers. La lista permette di conoscere il grado di dettaglio con cui queste società operano. Per esempio, se utilizzate il vostro cellulare con una frequenza superiore alla media, sarete etichettati come «Mobile addicts». Una certa tendenza a comprare farmaci online vi collocherà nella categoria «Addiction medicine». Se fai ricerche online sull'aborto diventi sostenitore dell'«Abortion Rights». Poi ci sono le categorie sull'etnia (italiani, ispanici, ecc.), le classificazioni di classe («Sophisticated hispanic»), situazione finanziaria («Very poor»), e stato di salute. Gli «Xandr files» dimostrano che le informazioni si stratificano nel tempo e non sono utilizzate solo per le annunciate finalità pubblicitarie. Le stesse informazioni sono infatti usate, per fare qualche esempio, per valutare il merito creditizio, nella ricerca del personale e per il microtargeting politico (qui la fonte).

Shufa, un'azienda tedesca privata che raccoglie dati di natura economica e finanziaria di cittadini e imprese a vantaggio di agenzie di credito e dei loro partner commerciali, **possiede i dati di circa 66 milioni di cittadini tedeschi**. Quella Usa di analisi di big data **Acxiom dispone dei dati di circa 300 milioni di cittadini americani, cioè quasi tutti**. Il suo quartier generale nell'Arkansas è protetto da cancelli strettamente sorvegliati, come fosse un edificio del Servizi Segreti, ed è probabile che abbia più informazioni sugli americani della stessa Fbi.

Il **filosofo sudcoreano Byung-chul Han** nel saggio «Nello sciame» la sintetizza così: **«L'analisi dei big data permette di conoscere modelli di comportamento che rendono possibili anche delle previsioni**: al posto dei modelli basati su ipotesi subentra il confronto diretto dei dati. E quindi la teoria è superflua. La società della sorveglianza digitale, che ha accesso all'inconscio collettivo, al futuro comportamento

delle masse, sviluppa tratti totalitari: ci consegna alla programmazione psicopolitica e al controllo».