Sei proprio sicuro che WhatsApp protegga la tua privacy?

Un'inchiesta di ProPublica mostra come il servizio di messaggistica di Facebook possa scoprire moltissimo su di noi e rivelarlo alle forze dell'ordine. Nonostante i messaggi cifrati

Ogni 3 mesi, Facebook e Instagram pubblicano accurati resoconti relativi alla quantità di contenuti illeciti individuati sulle due piattaforme: come ormai noto, a occuparsi della moderazione di questi social network sono oltre 15mila persone, i cui risultati vengono promossi dalla società fondata da Mark Zuckerberg nel tentativo di arginare le polemiche che periodicamente la colpiscono.

Niente di simile avviene invece per quanto riguarda WhatsApp, che è sempre di proprietà di Facebook e nega di fare moderazione (come ha spiegato Carl Woog, direttore delle comunicazioni del servizio di messaggistica, parlando con ProPublica), perché non può cancellare alcun contenuto e soprattutto per non intaccare la reputazione di piattaforma che protegge la privacy, conquistata nel corso degli anni.

D'altra parte, come potrebbe WhatsApp moderare i suoi due miliardi di utenti se tutti i contenuti sono protetti dalla crittografia end-to-end, che permette solo ed esclusivamente al destinatario dei messaggi di decifrarli? Eppure, WhatsApp impiega oltre un migliaio di lavoratori interinali negli uffici di Austin (in Texas), Dublino e Singapore. Persone solitamente tra i venti e i trent'anni che, sedute davanti ai loro computer, passano la giornata a controllare milioni e milioni di messaggi, allo scopo di individuare quelli violenti, abusivi o peggio; portando così alla sospensione o all'eliminazione dell'utente.

Il lavoro di moderatori e intelligenze artificiali
Ma come possono vedere i messaggi di WhatsApp, se sono cifrati? La ragione è semplice: sono i milioni di messaggi che le persone, ogni singolo giorno, segnalano come abusivi. Selezionando l'opzione Segnala in fondo alle informazioni di ogni contatto, si possono inviare automaticamente a WhatsApp "i messaggi più recenti ricevuti da questo contatto", compresi video, fotografie e altro. Per quanto si tratti di azioni legittime e che hanno lo scopo di proteggere gli utenti, molti potrebbero essere sorpresi dalla facilità con cui i nostri

messaggi possono venire letti, soprattutto perché del lavoro svolto dai controllori di WhatsApp non si parla da nessuna parte.

Inoltre, questa è solo una piccola parte delle operazioni di monitoraggio svolte dalla piattaforma, quella che nell'inchiesta condotta da ProPublica viene battezzata come reattiva. C'è poi tutta una parte di lavoro proattivo, che viene principalmente gestito da intelligenze artificiali. Attenzione: dal momento che i messaggi sono cifrati, gli algoritmi impiegati da WhatsApp non possono ovviamente leggere le chat e osservare i video a caccia di materiale illecito (come invece fanno su Instagram e Facebook). Ciò di cui invece l'intelligenza artificiale si occupa è di monitorare tutti i dati non cifrati che WhatsApp raccoglie sugli utenti in cerca di comportamenti vietati (per esempio, se una persona ha inviato un'enorme quantità di messaggi è possibile che stia facendo spam).

Quali sono questi metadati? Per fare chiarezza, può essere utile un esempio analogico: i metadati sono l'equivalente delle informazioni riportate sulla busta di una lettera (il mittente, il destinatario, il luogo e il giorno della spedizione e così via), mentre il contenuto è ciò che si trova all'interno. Il limite di questa metafora è che rischia di sottostimare la quantità di informazioni che si possono raccogliere grazie ai tantissimi metadati non cifrati che trasmettiamo a WhatsApp.

Quanti segreti dentro ai metadati

Il nostro nome, la foto del profilo, ciò che abbiamo scritto sullo status, i nomi e le immagini dei nostri gruppi, l'indirizzo Ip e l'identificativo dello smartphone, il sistema operativo, ogni account Facebook o Instagram collegato, il linguaggio utilizzato e il fuso orario. Ancora: con chi abbiamo comunicato, per quanto tempo, spedendo quanti messaggi e così via. Incrociandoli, si possono ricavare informazioni talmente preziose che, secondo un ex consulente dell'Nsa, "se hai sufficienti metadati, non ti servono nemmeno i contenuti". E in effetti era proprio l'Nsa a raccogliere questo genere di elementi nel famigerato programma di sorveglianza di massa svelato da Edward Snowden.

È la ragione per cui le piattaforme predilette da chi ha più a cuore la privacy (come politici, attivisti, dissidenti, giornalisti d'inchiesta e simili) raccolgono il minor numero possibile di metadati, in modo da non poterli fornire neanche se lo volessero. È il caso di Signal, che nel 2016 venne citata in

giudizio dall'Fbi per obbligarla a fornire i dati di una persona. Poiché era in possesso solo della data di registrazione dell'utente e del suo ultimo utilizzo dell'app, la piattaforma di messaggistica fondata da Moxie Marlinspike non ha potuto divulgare altre informazioni.

E WhatsApp? "Anche all'interno di un sistema cifrato, siamo comunque in grado di rispondere alle richieste legali riguardanti metadati, compresi quelli più importanti come le informazioni sulla posizione o sull'account – ha specificato Facebook a gennaio 2020, nel corso di un'audizione alla Commissione del Senato Usa – A differenza di altri servizi cifrati, WhatsApp fornisce un sistema semplice che aiuta le persone a riferire di abusi o di preoccupazioni per la sicurezza".

Non ci sono numeri specifici sulla quantità di richieste da parte delle forze dell'ordine che sono state soddisfatte da WhatsApp. Secondo ProPublica, i 12 casi noti dal 2017 a oggi sono soltanto una parte del totale. Nel complesso, le richieste governative di ottenere accesso ai messaggi inviati tramite le varie piattaforme di Facebook sono aumentate del 276% tra il 2017 e il 2020. Nello stesso lasso di tempo, la percentuale di risposte positive da parte della società di Zuckerberg è aumentata dall'84 al 95%.

Per esempio, i dati ceduti da WhatsApp sono stati recentemente utilizzati per condannare Natalie Edwards, ex funzionaria del ministero del Tesoro che nel 2018 aveva divulgato documenti segreti, svelando sospette operazioni bancarie. I metadati relativi alle comunicazioni via WhatsApp con un giornalista di BuzzFeed News sono stati sufficienti a dimostrare che fosse lei la fonte della fuoriuscita di informazioni segrete, nonostante i messaggi fossero protetti dalla cifratura end-to-end. Niente di tutto ciò che WhatsApp fa con le informazioni che ricava su di noi è illecito o fa venire meno la protezione garantita dalla cifratura dei messaggi, l'importante è sapere chiaramente come funziona questa piattaforma, quali informazioni raccoglie e quale può essere, nei casi più seri, la posta in palio.

Andrea Daniele Signorelli

Repubblica

17 Settembre 2021