
WhatsApp, ora i messaggi sono crittografati

Autore: Daniela Baudino

Fonte: Città Nuova

I creatori della app annunciano la novità: conversazioni protette con la crittografia end-to-end per salvaguardare la privacy degli utenti. Considerazioni e interrogativi

Tanti di noi, utilizzando **WhatsApp** in questi giorni, si saranno accorti della comparsa nelle conversazioni e nei gruppi in cui siamo inseriti di un piccolo box giallo contenente un avviso, forse ai più, è proprio il caso di dirlo, criptico: «I messaggi che invii in questa chat e le chiamate sono ora protetti con la **crittografia end-to-end**».

La crittografia è una particolare tecnica che permette di cifrare un messaggio attraverso una chiave che deve essere conosciuta e condivisa da mittente e destinatario, rendendo così la loro comunicazione illeggibile da altri che non siano in possesso di quel particolare codice interpretativo.

Come funziona la trasmissione di un messaggio su WhatsApp

Quando inviamo un messaggio attraverso WhatsApp esso viene prima registrato sui server di WhatsApp (e lo vediamo quando viene visualizzata la prima spunta) e poi successivamente inoltrato sul dispositivo del destinatario (seconda spunta). La “semplicità” di questo tipo di trasmissione dei messaggi ha permesso, in passato, che fossero creati particolari programmi che, attivati su una connessione Internet, consentivano di intercettare i messaggi scambiati con dispositivi collegati su quella stessa Rete.

Cosa cambia?

Con l'introduzione della crittografia end-to-end, WhatsApp si è ora dotata di un livello di protezione aggiuntivo che **impedisce che le comunicazioni effettuate tramite l'app possano essere controllate e lette da terzi** rendendo, sulla carta, le nostre comunicazioni lontane da occhi indiscreti. E questo senza che noi dobbiamo far niente, perché la condivisione e la comprensione del codice crittografico è affare dei dispositivi che utilizziamo per inviare e ricevere messaggi, foto, video e chiamate con WhatsApp. L'unica differenza è che ora i messaggi risiedono sui server in modo criptato e **WhatsApp diventa un semplice postino** senza poter leggere cosa c'è dentro la busta che trasporta.

Perché utilizzare la crittografia end-to-end

Secondo i creatori di WhatsApp, **«quando mandi un messaggio, l'unica persona che può leggerlo è la persona o il gruppo a cui lo hai mandato**. Nessun altro può vedere cosa c'è nel messaggio. Non i criminali informatici. Non gli hacker. Non regimi oppressivi. Nemmeno noi. La crittografia end-to-end aiuta a rendere le comunicazioni fatte con WhatsApp private, come quelle che si fanno di persona».

La motivazione dietro alla mossa di WhatsApp **ha probabilmente due radici** diverse. **La prima riguarda questioni di mercato**, perché dopo l'inglobamento della app nell'ecosistema **Facebook** una sempre maggiore fetta di utilizzatori di WhatsApp si sta progressivamente spostando verso l'utilizzo di altre app, come ad esempio **Telegram**, che offrono comunicazioni più sicure da sempre.

La seconda tocca aspetti più politici, dopo il braccio di ferro che coinvolge negli Stati Uniti da una parte **le società legate alla tecnologia** e dall'altra **le autorità** di Stato, soprattutto dopo l'episodio che ha coinvolto l'**Fbi**, che in seguito alla **sparatoria di San Bernardino** del dicembre 2015 aveva avanzato la richiesta di accesso ai dati dell'**iPhone** del killer, permesso invece negato da **Apple** in nome della scelta di non diffondere dati dei propri utenti per proteggere la loro privacy.

Interrogativi

Due sono gli interrogativi che ci si può porre, guardando questa novità da una prospettiva più ampia. Il primo riguarda **Facebook** (che è proprietaria di WhatsApp): **davvero rinuncerà**, come sembra promettere, **ad analizzare le nostre conversazioni e telefonate**, perdendo così dati (i nostri) commercialmente fondamentali per profilarci e per vendere, di conseguenza, la pubblicità, motore economico del famoso sito di social network?

Il secondo riguarda la reale sicurezza. Perché, come scrive il giornalista **Arturo Di Corinto**, elementi di debolezza o punti di attacco sono sempre presenti, anche nei sistemi che si presentano come i più sofisticati.

E allora, nel dubbio, ecco il consiglio, semplice ed efficace: **se una cosa non vuoi che si sappia, non scriverla.**