CAMMINO DIRITTO
Rivista di informazione giuridica

WHATSAPP, CRITTOGRAFIA END-TO-END E SICUREZZA: RIFLESSI NEL PROCEDIMENTO PENALE

Come cambia la sicurezza dell'app di messaggistica più famosa e usata da più di un miliardo di utenti? Si può davvero parlare di tutela della privacy? Come cambiano i rapporti con l'Autorità Giudiziaria nel procedimento penale?

Stefania Serafin (redattore Angela Cuofano)
PENALE - DELITTI CONTRO LA PERSONA
Articolo divulgativo - ISSN 2421-7123

Pubblicato, Venerdì 29 Aprile 2016

Cammino Diritto
ISSN 2421-7123

Pochi giorni fa su Whatsapp è comparso il seguente testo: "*I messaggi che invii in questa chat e le chiamate sono ora protetti con la crittografia end-to-end.*"

Cosa significa? Questa speciale crittografia permette solo agli utenti (mittente e destinatario) interessati di possedere i permessi per leggere e agire sui messaggi della conversazione in comune. Si parla di sicurezza poichè con questa nuova tecnologia non è possibile intercettare un messaggio nel percorso di viaggio. Neppure WhatsApp stesso ha i permessi per agire sui messaggi di testo, vocali o qualsiasi siano loro.

Whatsapp, l'applicazione di messaggistica per smartphone che conta più di un miliardo di utenti attivi, fu creata da Jan Koum e da Brian Acton nel 2009, ed è stata successivamente acquisita da Mark Zuckerberg, il CEO di Facebook, il 19 febbraio 2014.

Perchè questa svolta?

Il percorso è stato lungo e tortuoso, e uno dei principali motivi alla base dell'introduzione di questa novità è l'adeguamento con altre app con lo stessa funzione di messaggistica istantanea, soprattutto con Telegram.

Telegram, infatti, ha incrementato notevolmente i propri utenti in pochi mesi grazie all'offerta di maggiori garanzie sulla privacy (che non sono l'unica funzione "in più" rispetto a Whatsapp, vedi i "bot").

Come funziona la tecnologia end-to-end?

Per i non esperti di tecnologia, si può esprimere il concetto di crittografia end-to-end, pensando alla sua traduzione italiana: crittografia "da punto a punto". Questo significa che esistono chiavi di lettura solo nei dispositivi dell'utente mittente e dell'utente ricevente e nel canale di scambio, perciò i messaggi scambiati tra due persone vengono cifrati fin dal momento in cui si preme invio.

Ciò non permette ai malintenzionati o alle autorità di hackerare o di rivolgersi alla piattaforma, non ottenendo alcuna informazione. Bisogna però ribadire che il protocollo appena adottato dall'app non protegge i dati quando risiedono sul dispositivo.

Per una panoramica più completa, il sito di Whatsapp e le applicazioni stesse nella sezione "sicurezza" hanno ideato una spiegazione chiara e animata anche per gli utenti che non masticano il linguaggio tecnologico.

Cosa è cambiato e cosa significa per gli utenti?

Come già accennato, la crittografia end-to-end è riservata a tutti gli utenti Whatsapp che abbiano installato sui propri dispositivi l'ultima versione dell'aggiornamento. Ciò significa che chi è in possesso di un'applicazione non aggiornata, si troverà prima o poi a dover passare alla versione più recente per essere ancora in grado di inviare/ricevere messaggi e telefonate.

La crittografia risolve davvero il problema della privacy?

A questa domanda chiave, che può essere considerato il vero cuore del problema ha risposto Luigi Martino, teaching and research assistant in ICT policies e cyber security all'Università di Firenze, in un'intervista con Cyber Affairs in cui ha dichiarato: *"[...] non significa che il contenuto del messaggio non resti a disposizione di WhatsApp, che detiene e controlla i server dove questi dati*

Cammino Diritto
ISSN 2421-7123

sono immagazzinati.". E continua con una domanda che fa riflettere: *"Ed è questo che bisognerebbe chiedersi, in una vera ottica di tutela della privacy: chi sono, oggi, i proprietari delle conversazioni e dei dati che si muovono attraverso la Rete? Noi o chi eroga i servizi?"*.

L'intercettazione informatica e telematica nel procedimento penale.

L'intercettazione telematica è diretta ad apprendere la trasmissione di un flusso di comunicazioni in forma riservata nel pieno rispetto delle garanzie previste dall'art. 15 Cost. e dall'art. 8 CEDU.

Le intercettazioni di comunicazioni informatiche e telematiche sono disciplinate all'art. 266-*bis* c.p.p. che recita: «Nei procedimenti relativi ai reati indicati nell'art. 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi», e può essere esteso anche a tutti quei reati commessi mediante l'impiego di tecnologie informatiche. La perquisizione informatica, introdotta nel codice di procedura penale dall'art. 8 comma 2 della legge 48/08, disciplinata dall'art. 247 comma 1-*bis* c.p.p., dispone che: «Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

Prima di procedere alla perquisizione, l'art. 247 comma 1-*bis* c.p.p., impone di adottare delle "misure tecniche" dirette ad "assicurare la conservazione dei dati originali e ad impedirne l'alterazione", al fine di garantire l'acquisizione e la conservazione dell'elemento di prova. Prima di poter utilizzare tale strumento di ricerca della prova bisogna adottare ogni garanzia diretta a tutelare l'inviolabilità del domicilio "informatico", inteso come "spazio contenitore" di tutti i dati informatici appartenenti alla persona e a questo si estende la tutela della riservatezza della sfera individuale.

Quindi, alla luce delle novità introdotte, le conversazioni scambiate tra gli utenti di Whatsapp non potranno più essere utilizzate per fini probatori.

Crittografia end-to-end e rapporti con l'autorità giudiziaria.

Crittografia end-to-end significa, quindi, che lo stesso Whatsapp e terze parti non possono leggere messaggi o ascoltare chiamate e messaggi vocali. Cifrare le comunicazioni oggi può essere vitale per quelle persone che vivono in paesi controllati da regimi totalitari e violenti, Paesi in cui l'intercettazione di messaggi non graditi determinano il rischiare la vita o l'incarcerazione.

Con la crittografia end-to-end WhatsApp non potrà più svelare i contenuti dei messaggi, anche qualora le autorità lo richiedessero, perciò in questo modo il privato cittadino ha una protezione maggiore dai crimini informatici. Tuttavia, secondo Andrea Zapparoli Manzoni, membro del Clusit, l'associazione italiana per la sicurezza informatica, "*Bisogna ricordare che la protezione del dato 'in transito' è solo una delle componenti di una strategia complessiva di sicurezza, e che la cifratura dei messaggi di per sé non è in grado di garantire la sicurezza assoluta delle comunicazioni*", poiché "*Ci sono altri due elementi da considerare: la sicurezza del device (fisso o mobile) sul quale gira l'applicazione e la sicurezza dell'applicazione stessa. Verso di loro esistono minacce concrete, che non sono minimamente mitigate dall'adozione della crittografia sul canale di trasmissione*".

Non mancano però le eccezioni. In un articolo di Repubblica del 1 marzo 2016 si legge, infatti, che BlackBerry non si è allineata alla scelta di Apple e Whatsapp e ha consegnato ai giudici di Torino le chat che incastrano alcuni criminali. Si tratta di chat scambiate attraverso l'applicazione "interna" di BlackBerry, cioè un'app che può essere usata solo tra utenti in possesso di dispositivi di questo

Cammino Diritto
ISSN 2421-7123

marchio. Il problema che si è posto, però, è che queste, secondo i legali che difendono una banda di narcotrafficanti, non possono essere utilizzate perchè non sono state "intercettate" direttamente dall'autorità giudiziaria.