


NUOVA PRIVACY DI WHATSAPP

COSA C'È DA SAPERE?



Whatsapp annuncia
modifiche sui termini **privacy**
dei propri utilizzatori.

Riflessioni e valutazioni
tecniche per capire se
la nostra privacy è
realmente a **rischio**

Un recente avviso di Whatsapp, relativo ai nuovi termini dell'informativa della privacy che entreranno effettivamente in vigore a partire dall'8 febbraio 2021, ha scatenato molti dubbi da parte dei suoi utilizzatori, risvegliando nei Social Network i leoni da tastiera, pronti a seminare il panico e a diffondere notizie incomplete e superficiali.

Il messaggio, per chi non l'avesse ricevuto o non gli avesse dato particolare importanza, recitava: "Stiamo aggiornando i termini e l'Informativa sulla privacy di WhatsApp. Per maggiori informazioni su queste modifiche, consulta questa pagina".

Ma ad accrescere la perplessità, alla stessa velocità istantanea con cui si invia un messaggio, è stato un dettaglio, non passato inosservato al popolo di Whatsapp.

La comunicazione, infatti, invitava ad accettare i nuovi termini e regole sulle privacy per poter continuare ad utilizzare l'applicazione di messaggistica, vincolo che ovviamente ha suscitato non pochi dubbi sulla condotta etica di Whatsapp e generato estrose teorie complottistiche.

Cerchiamo di capire cosa implica questo aggiornamento e cosa è realmente cambiato

Il punto cruciale della questione afferisce allo scambio e condivisione di dati ed informazioni personali tra le due piattaforme Whatsapp e Facebook.

L'interazione tra queste due app è sempre stata oggetto di forte attenzione per gli organi di tutela della privacy, tanto che **quella comunicata da WhatsApp, come modifica contrattuale unilaterale ai termini e alle condizioni del servizio, non ha valenza per i paesi membri dell'Unione Europea, Italia compresa.**

L'Europa in fatto di protezione della privacy è molto rigorosa, da ultimo l'entrata in vigore nel 2018 del GDPR. Tale contesto di particolar tutela normativa, di conseguenza, impedisce a WhatsApp di poter condividere i dati degli utenti europei con Facebook e, come spiega un portavoce di WhatsApp:



non ci sono modifiche alle modalità di condivisione dei dati di Whatsapp nella Regione europea, incluso il Regno Unito, derivanti dall'aggiornamento dei Termini di servizio e dall'Informativa sulla privacy. Non condividiamo i dati degli utenti dell'area europea con Facebook allo scopo di consentire a Facebook di utilizzare tali dati per migliorare i propri prodotti o le proprie pubblicità.



A prova di quanto affermato dal portavoce, i due enti che gestiscono i dati di Whatsapp sono infatti differenti: WhatsApp Ireland per gli utenti europei e WhatsApp Inc per il resto del mondo.

Cosa cambia invece fuori dall'UE?

Situazione ben diversa invece per gli utenti di Whatsapp che risiedono fuori dall'UE, dove la condivisione delle informazioni tra le due piattaforme online avviene già da tempo, ma con l'entrata in vigore delle recenti modifiche contrattuali, tali informazioni verranno utilizzate non solo per migliorare o commercializzare i servizi di WhatsApp, ma anche per personalizzare offerte e prodotti di Facebook. Un esempio: suggerire all'utente amici, gruppi o contenuti interessanti per il suo profilo.

Quindi, Whatsapp è davvero una minaccia per la nostra privacy?

Abbiamo capito che agli utenti WhatsApp che abitano in Europa si applica una policy a parte per la privacy e rimane invariato il fatto che WhatsApp non possa condividere i loro dati con Facebook.

La normativa europea, quindi, ci tutela ed è dalla nostra parte sul tema privacy; ma lo stesso non si può dire quando è un nostro malsicuro e rischioso utilizzo di Whatsapp o di altre applicazioni di messaggistica a mettere in discussione la nostra protezione e la nostra sicurezza.

Su questo fronte, siamo solo noi i custodi della nostra privacy.

Quali alternative abbiamo a Whatsapp?

Nel caso volessimo provare ad utilizzare un'applicazione di messaggistica diversa da Whatsapp, potremmo valutare di installare nel nostro smartphone Telegram o Signal, due app molto in voga e di cui si sta discutendo molto ultimamente.

Se vogliamo scegliere con cognizione di causa perché la nostra privacy ci sta particolarmente a cuore, di seguito un'attenta comparazione tra le tre app di messaggistica istantanea al momento più scaricate ed utilizzate: **Whatsapp – Telegram – Signal.**



Whatsapp

Proprietà: Facebook.
Sede di origine: California.
Sede attuale: California e Irlanda.

Crittografia End-to-end:
Conversazioni e file vengono crittografati end-to-end. Il protocollo di cifratura di Signal e Whatsapp è lo stesso: sottoposto a peer review, è considerato uno dei migliori protocolli end-to-end.

Crittografia metadati*:
non presente.

Client Desktop:
presente e supporta la crittografia end-to-end.

Plus:
Conversazioni e file transitano sui server Whatsapp ma non vengono salvati.



Telegram

Proprietà: Telegram LLC, senza fini di lucro.
Sede di origine: Russia
Sede attuale: Dubai

Crittografia End-to-end:
non presente di default nelle chat utilizzate normalmente e nei gruppi, è presente solamente nelle chat segrete.

Crittografia metadati*:
non presente

Client Desktop:
presente ma non supporta la crittografia end-to-end.

Plus:
In Telegram sia nei gruppi che nelle altre tipologie di chat è possibile tenere nascosto il proprio numero di telefono ed essere rintracciati tramite Nickname.



Signal

Proprietà: Signal Foundation, un'associazione non profit.
Sede di origine: California.
Sede attuale: California.

Crittografia End-to-end:
presente in tutte le tipologie di chat. Il protocollo di cifratura di Signal e Whatsapp è lo stesso: sottoposto a peer review, è considerato uno dei migliori protocolli end-to-end.

Crittografia metadati*:
presente.

Client Desktop:
presente e supporta la crittografia end-to-end.

Plus:
Ha ideato ed implementato **Sealed Sender**. Permette di non sapere, nemmeno a Signal chi sta messaggiando a chi, garantendo la massima privacy.

Signal per impostazione predefinita **crittografa tutti i file locali** con una passphrase di 4 cifre.

Supporta anche le **chiamate di gruppo crittografate**.

Lo sapevi che Whatsapp e Signal utilizzano lo stesso protocollo di crittografia end-to-end?

Protocollo che è stato sviluppato da **Open Whisper Systems**, il gruppo software no profit che sviluppa progetti open source collaborativi, tra questi la stessa Signal.

Nel novembre 2015, **Snowden** ha twittato:
"io utilizzo Signal ogni giorno"



Quali dati raccoglie ciascuna app?

Di seguito l'elenco dei dati che ciascuna aziende **dichiara** di raccogliere.

Whatsapp

- Numero di cellulare.
- Nome del profilo.
- Immagine del profilo e informazioni in "Info".
- I numeri di telefono dei contatti presenti in rubrica.
- Appartenenza a gruppi Whatsapp.
- Stato dell'utente.
- Dati di pagamento e transazioni per servizi Whatsapp, se usati.
- Diagnostica e prestazioni.
- Iterazioni con i servizi Whatsapp e con altri utenti (data di accesso, durata, orari).
- Modello del dispositivo, versione del sistema operativo, stato della batteria,
- Potenza del segnale, versione dell'app, informazioni sul browser e sulla rete mobile.
- Informazioni sulle connessioni, l'operatore mobile o il provider ISP, la lingua, il fuso orario e l'IP.
- Identificatore univoco per altri servizi Facebook associati allo stesso account.
- Posizione, previa autorizzazione dell'utente.
- Messaggi e allegati, solo fino ad avvenuta consegna.

Telegram

- Numero di cellulare.
- Nome del profilo.
- Immagine del profilo e delle informazioni in "Info".
- I numeri di telefono dei contatti presenti nella sua rubrica, previa autorizzazione dall'utente.
- Indirizzo email, se attivate specifiche funzionalità.
- Messaggi e allegati per sempre (crittografati).

Signal

- Numero di cellulare.

Attenzione!

Nel caso di comunicazioni aziendali, utilizzando la versione **Whatsapp Business**, le cose cambiano un po'.

In questo caso non è più Whatsapp che gestisce i dati degli utenti, bensì l'azienda che offre il servizio, in tal caso diventa essa stessa la responsabile del trattamento delle informazioni e di come queste vengono utilizzate.

Per maggiori info: <https://www.whatsapp.com/business/api>



Riassumendo

	WHATSAPP	TELEGRAM	SIGNAL
Privacy dati utente	 Raccoglie molti dati sugli utenti	 Raccoglie pochi dati sugli utenti	 Non raccoglie alcun dato sugli utenti
Privacy conversazioni	 Crittografia end-to-end di default: nessuno, al di là del mittente e del destinatario, potrà vedere il contenuto del messaggio	 Il contenuto dei messaggi potrebbe potenzialmente essere letto da Telegram, a meno di non utilizzare la funzionalità chat segreta	 Crittografia end-to-end di default: nessuno, al di là del mittente e del destinatario, potrà vedere il contenuto del messaggio
Esperienza utente	 Usabilità semplice ed interfaccia grafica accattivante, ma poco personalizzabile	 Usabilità semplice, interfaccia grafica accattivante e molto personalizzabile	 Usabilità semplice ma interfaccia grafica poco accattivante, ridotta personalizzazione

Lo sapevi che, dopo la notizia della modifica di WhatsApp ai suoi termini sulla privacy, Telegram in 72 ore ha registrato 25 milioni di nuovi utenti?

Lo ha dichiarato il suo fondatore **Pavel Durov**, nato in Russia.

Un'altra chat che ha registrato una forte impennata di download è Signal, raccomandata anche da **Elon Musk**, attualmente l'uomo più ricco del mondo e patron di Tesla e Space X.



IMQ Intuity propone un approccio diverso alla Cybersecurity modificando lo status quo che vede nella soluzione tecnologica l'unico modo di affrontare il problema, quest'ultimo invece sempre più legato all'uomo ed al contesto sociale in cui esso opera.

La sicurezza informatica deve essere approcciata da un punto di vista Culturale, mettendo al centro le persone nel processo di sicurezza aziendale: **People-Centric Security**

www.intuity.it



IMQ INTUITY S.r.l.

Soggetta ad attività di direzione e coordinamento di IMQ Group S.r.l.

Sede operativa

via A. Ceron, 2 35129 Padova
049 817 0850 | info@intuity.it

Sede legale

via Quintiliano, 45 20138 Milano
admin@pec.intuity.it