# Crittografia e app, la doppia sicurezza di Telegram

Crittografia, croce e delizia dei paladini della libertà. Perché? «Delizia» nella misura in cui protegge lo scambio di dati fra utenti dallo sguardo, spesso indiscreto, delle autorità. «Croce» poiché spesso, ahinoi, proprio le autorità sembrano fare di tutto per mettere i bastoni tra le ruote ad App e sistemi di messaggistica ove lo scambio d'informazioni sia protetto dalla crittografia *end-to-end*.

L'ultima prova in tal senso è giunta qualche settimana fa dal governo americano. Si è tenuta in particolare la riunione dei funzionari di alto livello di Donald Trump, mirata a impedire l'utilizzo della crittografia *end-to-end*all'interno delle App delle società statunitensi. I funzionari (tra cui quelli di almeno due agenzie governative come CIA, NSA o FBI) starebbero pensando di spingere il congresso a fare un passo per evitare una strategia chiamata «Going Dark»:sostanzialmente permettere che gli utenti possano nascondere dati. Da un lato, quindi, le agenzie fanno pressione affinché i dati degli utenti siano più controllabili; dall'altro però questo permetterebbe anche a malintenzionati di avere più facile accesso agli stessi.

Oggi numerose App vantano a gran voce di avere al loro attivo un sistema di crittografia: siamo certi, però, che le cose stiano sempre come ci vengono dette e presentate? Siamo sicuri che la «crittografia» in uso alle diverse App sia sempre la stessa e che non vi siano invece, magari, differenze, tali da determinare livelli diversi di sicurezza anche all'interno dell'App?

WhatsApp ad esempio sbandiera molto, a parole, la crittografia *end-to-end* con cui proteggerebbe i dati degli utenti. Abbiamo visto qui, però, come ad esempio Pavel Durov, fondatore di Telegram che, della sicurezza dei dati, ha fatto un vessillo,

ne mostri i limiti, definendola un semplice «stratagemma di marketing».




# Telegram, Cloud Chats e Secret Chats

Come stanno le cose in Telegram? Ne abbiamo parlato più volte, ma vale la pena ricordarlo. Due, nello specifico, le forme di crittografia, corrispondenti ai due diversi tipi di messaggi in Telegram: le *Cloud Chats* e le *Secret Chats*. Queste sono caratterizzate ciascuna da un diverso livello di crittografia, di sicurezza e privacy:

Che significa? Partiamo dalle *Cloud Chats*, gli scambi di messaggi tradizionali. Su questi, ben riepilogano da Telegram qui: «Noi conserviamo messaggi, foto, video e documenti dalle tue *Cloud Chats* sui nostri server, così che tu possa facilmente accedervi da ogni *device* in qualunque momento e usare il nostro motore di ricerca istantanea per rintracciar all'istante qualsiasi documento di tuo interesse». Attenzione, però: la privacy è ben più che garantita. «Tutti i dati conservati sono protetti da una crittografia a prova di bomba e le chiavi di decrittazione, in tutti i casi, sono conservate in una pluralità sterminata di parti del mondo e nelle più diverse giurisdizioni. In questo modo ingegneri, sviluppatori locali, dipendenti, o, peggio, spioni online e offline non

possono in alcun modo avere accesso ai tuoi dati».

Questo è il significato dell'espressione *client-server/server-client*: i messaggi che mandi, in partenza dal tuo *client*, arrivano al server di Telegram. Lì sono «conservati», ma in modo tale – con un tale livello di crittografia e con quel loro «frantumarsi», come frammenti di cristalli, diamanti, nel globo, tra *data center* frazionati in ogni parte del mondo – che ne rende l'accesso praticamente impossibile per chiunque. Sono come porti di mari nelle cui acque subito si disperdono: oggetti che, all'istante, divengono ceneri al vento. Senza che nessuno legga i tuoi messaggi neppure volendo. Non ci sono casseforti, non ci sono chiavi. Ciò garantisce quella velocità e funzionalità tanto importanti per aziende, per il business, ma anche sempre per la vita e la fruibilità da parte della società: mantenendo però, al contempo, il (quasi) massimo livello possibile di sicurezza e privacy che contribuiscono a rendere Telegram unica. .

Non ci addentreremo qui nella spiegazione delle caratteristiche tecniche di tale crittografia, basata come detto sul sicuro protocollo MTProto, comunque spiegato qui. Piuttosto, che significa «end-to-end encryption», tipica delle chat segrete?

Anzitutto che i messaggi non transitano da alcun server, mai. Neanche l'ombra, nemmeno per un istante, di una «cassaforte». O meglio: la cassaforte sei soltanto tu. La «chiave» la hai solo tu: tu e la persona cui stai inviando quel contenuto. «Non c'è proprio nessun modo per noi o per chiunque altro, senza un accesso diretto al tuo *device*, di sapere che tipo di contenuto tu abbia mandato in quei messaggi. Noi non conserviamo le tue chat segrete sui nostri server. E comunque, dopo un breve periodo, non sappiamo neppure più chi o quando abbia mandato un certo messaggio in una chat segreta. Per le stesse ragioni, le chat segrete non sono disponibili nel *cloud*: tu solo hai l'accesso a quei messaggi dal *device cui* – o *da cui* – hai inviato tali messaggi. Altrettanto, quando

mandi foto, video o file via chat segreta, prima che tali contenuti multimediali siano caricati, questi sono crittografati con chiave separata sconosciuta al server. Tale chiave e il luogo del file sono poi nuovamente crittografati con chiave *ad hoc* e solo così inviati al tuo destinatario».

Questi può sì poi, naturalmente, scaricare e decifrare il file. Ciò, in qualche modo, significa che il file «è» tecnicamente su uno dei server di Telegram: all'esterno, però, non appare come null'altro se non un pezzo di un *qualcosa* assolutamente indecifrabile, inviato randomicamente nell'infinito spazio della rete. Sconosciuto a tutti tranne che a te e al tuo contatto.

«Noi non abbiamo assolutamente idea di quel che ci sia dentro o di ciò che rappresenti», concludono, «né possiamo immaginare a chi sia riconducibile quella chat. E ci prendiamo cura di ripulire periodicamente i nostri server da questi dati, onde salvare spazio sul disco».

Per questi motivi parliamo di *end-to-end encryption*: i messaggi criptati partono da un «porto in mezzo al mare» e, senza neanche far in tempo a divenire cenere – secondo la metafora usata sopra – si dissolvono, si perdono in un'altra infinità. Questa è la massima forma di sicurezza e privacy che Telegram garantisce: non la troverai né in WhatsApp né in Messenger, dove sì, si parla di crittografia end-to-end, ma l'impressione, se non la convinzione, è che i dati, una volta – forse? – crittografati ad esempio su WhatsApp, vengano poi immediatamente disseppelliti dalla cassaforte ove erano stati racchiusi, presi da qualcuno che le chiavi le ha eccome, per essere poi immediatamente trasferiti in più sicure casseforti, in ben più inaccessibili centri di controllo, destinati ad analizzare quei dati, e dunque la vita scusa uno online e offline, disegnando il destino di un tracciamento perenne, di una violazione della privacy senza fine, nella vita virtuale come in quella cosiddetta «reale».

# Perché due? Perché non render tutto segreto?

Chiariti i due diversi livelli di crittografia e sicurezza delle due forme di chat, e ricordando che tra di essi, a livello di privacy, vi è la stessa differenza che passa tra un 100% e un 1000 ‰, la domanda che a questo punto nasce spontanea è la stessa cui persino Pavel Durov si sente chiamato a rispondere giusto in occasione del quarto compleanno di Telegram. Un «Ferragosto di fuoco» ruotante intorno all'interrogativo: «Perché non rendere tutto *segreto*?». Perché differenziare in due diversi livelli di crittografia e in questo modo dare l'impressione che possa sussistere una forma di scambio messaggi non del tutto sicura al 100%?

Andiamo con ordine. Anzitutto, questo è il solo ma vincente modo con cui Telegram può andare a risolver non solo un problema ma due. Massimizzare cioè la velocità nello scambio messaggi, la loro fruibilità, da parte ad esempio dei membri di team piccoli e grandi, dei clienti esterni di quella o quest'azienda – in ottica business, dunque, in vista di quella ottimizzazione della *Employee Experience* e della *Customer Experience* già citate – garantendo però al contempo la massima sicurezza. Il tutto in una convenienza unica, a costo quasi zero.

Eliminare del tutto i *data center* – peraltro frantumati in ogni parte del globo – implicherebbe:

- Meno disponibilità e, dunque, velocità di reperimento contenuti per l'utente;
- Un possibile campanello d'allarme per i governi, che penserebbero si abbia chissà che da nascondere.

Ora:

- Le Chat Cloud «normali» sono già sicure al 100%.

- Le Chat Segrete lo sono al 1000 per 1000.

Perché sacrificare velocità, immediatezza, possibilità di accedere all'App da ogni device scambiandosi qualsiasi contenuto, di qualsiasi dimensione, Supergruppi ormai quasi illimitati, di decine di migliaia di persone, e Canali con membri illimitati, in nome di una «presunta maggiore sicurezza» che già c'è?

Telegram così risolve invece non solo un problema ma due: massimizza la velocità nello scambio messaggi, la loro fruibilità, da parte di team piccoli e grandi, clienti, ottimizzando per una compagnia *Employee Experience* e *Customer Experience*, ma anche garantisce al contempo massima privacy. Certo ancora accentuata nelle chat segrete che però, se uniche, imporrebbero limiti alla piattaforma. Questo insomma è il modo, unico ma vincente, per ottimizzare in modo irrintracciabile altrove, il rapporto qualità-prezzo, a costo quasi zero.

Non basta? Leggiamo questo post, pubblicato da Pavel Durov giusto il 14 agosto 2017, nel quarto compleanno di Telegram, rilanciato anche tramite il suo canale e quelli affiliati all'App, in cui oltre a spegnere le candeline si sono festeggiati risultati record: 700.000 nuovi utenti al giorno e una crescita globale di oltre il 70% annuo, per 200 milioni di utenti attivi al mese.

Il titolo è illuminante: «Perché Telegram non ha crittografia *end-to-end* di default?». Che è poi la domanda già presente nelle FAQ: «Perché non rendere tutte le chat segrete?».

Quello di Durov nasce come chiarimento definitivo a una *quaestio* sin troppo *vexata*, con riferimento specifico all'interrogativo postogli da un utente: «Perché Telegram non ha un sistema di crittografia *end-to-end* di default, mentre svariate altre App popolari lo hanno?».

«Telegram è in assoluto la via più sicura di comunicazione»,

sintetizza Durov: «lo è stata, lo è e lo sarà sempre». *Cloud Chats in primis*. Eliminare i *data center* su cui poggiano i messaggi "normali" porterebbe con sé non un giustificato e positivo aumento della sicurezza, bensì i rischi di cui dicevamo poco sopra, in termini di minor disponibilità e, dunque, velocità di reperimento contenuti per l'utente, nonché di pre-allarme per i governi. Perché, dunque, sacrificare velocità, immediatezza, possibilità di accedere all'App da ogni device scambiandosi qualsiasi contenuto, di qualsiasi dimensione, o ancora godere del *plus* di Supergruppi e Canali con membri illimitati, in nome di una «presunta maggiore sicurezza» che già c'è? Telegram invece così:

- Massimizza la velocità nello scambio messaggi, la loro fruibilità, da parte di team piccoli e grandi, ottimizzando per una compagnia *Employee Experience* e *Customer Experience*;
- Garantisce però, al contempo, massima privacy. Certo, come detto più volte, ancora maggiore nelle chat segrete che però, se uniche, imporrebbero limiti alla piattaforma.
- Questo è il modo, unico ma vincente, per ottimizzare il rapporto qualità-prezzo a costo quasi zero. Per avere un network esclusivo, senza barriere all'ingresso, essendo Telegram un servizio non commerciale, gratuito. Per ottenere dunque, potenzialmente, un ROI al 100%.

A chiarimento definitivo, ecco alcuni passaggi del **post di Durov**, per finirla con la storia che WhatsApp sarebbe «e2e-encrypted by default» e che per questo, di conseguenza, sarebbe più sicura di Telegram. «Le App che ignorano di fare backup (come Wickr, Signal, Confide)» e «altre App sicure restano una nicchia», afferma. «Le App popolari come WhatsApp, Viber e Line conservano su Apple iCloud e Google Drive lo storico messaggi dei loro utenti e prevengono così problemi, qualora questi perdano ad es. lo smartphone». Che significa però? Che i *backup non* sono criptati con crittografia *end-to-*

*end* come invece si crede e possono essere decriptatiogni volta che qualcuno compra un nuovo smartphone e ripristina i dati».

Che significa? Che la presunta crittografia *end-to-end*, tanto sbandierata, semplicemente non esiste. «Tu credi di essere al sicuro? In realtà hai trasparenza zero. Se davvero credi alla crittografia sicura e che nessun'altra terza parte possa accedere ai tuoi messaggi, ti sbagli di grosso. I tuoi dati privati sono, infatti, vulnerabili per gli hacker come non mai e i governi possono accedervi in qualunque momento». E continua: «I messaggi finiscono non crittografati con e2e nel *cloud* senza che tu te ne accorga. Non puoi in alcun modo sapere ciò che è crittografato con e2e e ciò che è sottoposto a backup. Ti affidi alla crittografia e2e e ti fidi del mantra *Nessun terzo può accedere ai miei messaggi*, ma i tuoi dati personali sono esposti agli hacker e ai governi che possono accedervi tramite il *cloud storage*. La maggior parte delle chat *e2e-encrypted* su WhatsApp è stata salvata e archiviata nel *cloud*, non crittografata con e2e».

In una parola «la maggioranza delle chat che WhatsApp ti dice criptate in forma *end-to-end*, semplicemente, non lo sono. Una situazione che invalida il 99% delle conversazioni private su WhatsApp e applicazioni analoghe».

Per tirare le somme: il fatto che i messaggi nelle Chat Segrete usino la crittografia *end-to-end*, mente le *Cloud Chats* quella *client-server/server-client*, e siano archiviate in maniera crittografata nel Cloud di Telegram, permette ai messaggi *Cloud* di essere sia sicuri che facilmente accessibili da tutti i dispositivi, e «puoi anche cercarli facilmente usando la ricerca su server – che risulta spesso molto utile». «L'idea alla base di Telegram sta nell'offrire qualcosa di più sicuro per le masse, che non si intendono di sicurezza e non ne vogliono sapere nulla. Essere solamente sicuri non basta per raggiungere i nostri obiettivi – bisogna essere anche veloci, potenti e *user-friendly*. Questo permette a Telegram di essere utilizzato massivamente in ampie cerchie, non solo da

attivisti e dissidenti, così il semplice fatto di usare Telegram non marchierà gli utenti come obiettivo per un’elevata sorveglianza in alcuni Paesi».

Ecco perché, già da queste prime informazioni, è possibile concludere: «Telegram risulta come SMS ed email combinati – e si occupa di tutti i tuoi bisogni di messaggistica, personale o aziendale». Risultato? Massimizzazione dei risultati per tutti, sia sul piano professionale sia personale, economico e sociale, istituzionale e educativo.

https://www.key4biz.it/crittografia-e-app-la-doppia-sicurezza-di-telegram/267587/