# ¿Por qué ahora usamos Telegram y dejamos atrás WhatsApp?

**Autor:** Adolfo Morán Cavero*

**Publicado:** 20/01/2021**

En las últimas semanas hemos podido leer diversos titulares alertándonos sobre el cambio o "actualización" de las políticas de privacidad de la popular aplicación de mensajería instantánea WhatsApp.

Hasta aquí nada nuevo, una compañía más que informa a sus usuarios sobre el tratamiento de sus datos personales. En resumen, lo nuevo de esta actualización es que (i) WhatsApp compartirá datos (ej. número de teléfono, idioma, zona horaria, IP) con Facebook y compañías vinculadas[1], y (ii) la información que compartas con cuentas de empresa WhatsApp Business podrá ser compartida a Facebook o terceras empresas que les presten servicios a estas cuentas.[2]

Sin embargo, para mala suerte de Mark y compañía, la noticia del cambio en la política de privacidad de WhatsApp ha traído una airada reacción de los usuarios. Animados por personajes públicos de gran relevancia mundial, entre ellos Elon Musk (Tesla) y Jack Dorsey (Twitter), millones de usuarios han decidido descargar Telegram y -en menor cantidad- Signal.

De acuerdo con Pável Durov (apodado el Zuckerberg ruso), quien creó junto con su hermano Nikolái la aplicación Telegram, solo en la primera semana de enero se habrían descargado esta aplicación alrededor de 25 millones de usuarios de todo el mundo. Según sus cálculos, 21% de los nuevos usuarios provienen de Latinoamérica.

En mi caso, yo soy usuario de Telegram desde hace un poco más de un año y he podido verificar que durante los últimos días muchos de mis contactos se han creado una cuenta en esta aplicación (incluso algunos me invitaron a descargarla sin saber que ya la venía usando). La razón exacta: ¿No la hay?

De hecho, para Durov la masiva migración de hace unos días se debe directamente a que los usuarios de WhatsApp están "indignados" con los últimos cambios a la Política de Privacidad, que resultaría perjudicial para la privacidad de los usuarios. En síntesis, para él Telegram respeta el tratamiento de datos de sus usuarios, WhatsApp no lo hace.

Yo me pregunto ¿la mayoría de "exusuarios" de WhatsApp (y ahora usuarios de Telegram) conocía el tratamiento de sus datos personales? ¿Tenían al menos una idea clara de lo que sucedía con las fotos y videos que enviaban en sus chats grupales? ¿Estaban seguros de que nadie podía escuchar sus llamadas o videollamadas con sus amigos? Y la pregunta más importante ¿Por qué ahora se sienten más seguros con Telegram que con WhatsApp?

---

1 En realidad esto no es del todo nuevo. Los usuarios de WhatsApp comparten datos con Facebook desde hace unos años. La única diferencia es que antes existía la posibilidad de rechazar esta acción, ahora sería obligatorio ya que si no aceptas tendrás que eliminar la aplicación. Lee la Política de Privacidad de WhatsApp aquí: https://www.whatsapp.com/legal/updates/privacy-policy/?lang=en

2 Aunque no será el tema de este artículo, aquí estaría el posible peligro en caso estas cuentas tengan practicas inadecuadas en el tratamiento de datos personales. Lee aquí: https://wabetainfo.com/are-our-chats-and-calls-safe-with-new-terms-of-service/

Sabemos que normalmente poca gente lee los Términos y Condiciones o las Políticas de Privacidad antes de comenzar a utilizar una nueva aplicación móvil. Entre varios factores, Mapi Segura ha destacado que esto se debería a un uso inadecuado de jerga legal y de palabras complicadas que haría que leer una política de privacidad sea igual de difícil que leer la Crítica a la Razón Pura del filósofo Immanuel Kant.

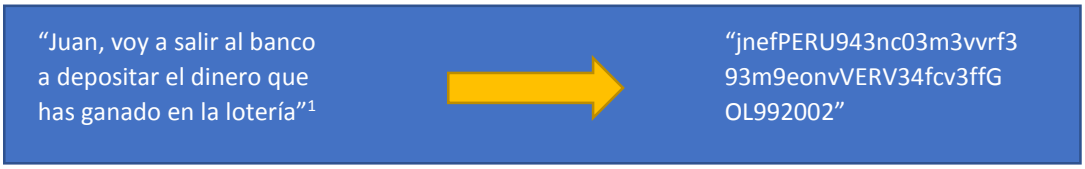
Por eso, dudo mucho que la mayoría de mis contactos (y estoy seguro de que no soy el único que piensa igual) haya leído si quiera la Política de Privacidad de Telegram y concluido que le conviene por sobre WhatsApp en términos de calidad y seguridad. Llamémoslo claro, en este caso ha habido un efecto manada o *herd behaviour*; en simple, "me descargo Telegram y lo comienzo a usar porque ahora todos mis amigos lo hacen".

Está bien, el éxito de una aplicación se debe principalmente al número de usuarios que la utiliza, más aún cuando se trata de una aplicación de mensajería instantánea que involucra la interacción entre éstos; sin embargo, quiero hacer un llamado a que reflexionemos con quién queremos compartir realmente nuestra información personal y ser conscientes de que en internet no hay nada "gratuito".

Esto va más allá de WhatsApp y Telegram, se trata de la forma en la que interactuamos en internet y los datos que vamos dejando cada vez que hacemos *click* en un enlace. A mis contemporáneos (los famosos *millennials*), que hemos crecido con un celular en la mano durante nuestra adolescencia, los invoco a informarse y ser responsables con su actividad digital.

Definitivamente, este artículo quedará muy corto para todos los temas que se pueden tratar en torno a la privacidad en internet y al tratamiento de datos personales; sin embargo, aprovechando el escándalo que ha ocasionado WhatsApp, quiero tratar -muy brevemente- un tema que todos debemos conocer (al menos lo básico). Me refiero a la encriptación o cifrado.

En términos simples, el cifrado se refiere al proceso a través del cual convertimos un texto legible (*plaintext)* a un texto cifrado (*cyphertext*). ¿Cuál es la relevancia de esto? **Que el texto cifrado es ininteligible.** Es decir, que cualquiera que tenga acceso a dicho texto cifrado no entenderá su contenido. Esto se podría graficar así:




Sin entrar a mucho detalle, lo importante por ahora es saber que la idea detrás de usar un método de cifrado es que el contenido del mensaje encriptado sea solo conocido por el remitente y el destinatario. En otras palabras, el único que debería poder descifrar el mensaje y enterarse de que van a depositar el dinero que ha ganado en la lotería es Juan (no el gobierno, no Facebook, no Movistar, etc.).

Hago una pausa aquí y pregunto al lector ¿alguna vez te has preguntado si tus mensajes están cifrados? Si la respuesta es un no, pues deberías. Podrías estar compartiendo más información con terceros de la que quisieras.

Hablar en simple sobre el cifrado y cómo esto es importante para nuestra privacidad y el ejercicio de nuestros derechos resulta esencial hoy en día. ¿Acaso compartirías

información sobre el ambiente laboral en tu trabajo o sobre tu estado de salud si supieras que cualquiera puede leer tus mensajes por chat?

En efecto, el cifrado es vital para el ejercicio de nuestro derecho a la libertad de expresión en la era digital. No podríamos comunicarnos libremente si hay personas observando o escuchando lo que decimos o compartimos con nuestros contactos.

Volviendo al tema en particular de este artículo, ¿qué cifrado utiliza Telegram y WhatsApp? De acuerdo con sus políticas de privacidad (ven lo importante de leerlas), ambos utilizan cifrado de extremo a extremo, pero no de la misma manera.

Cuando decimos que WhatsApp o Telegram utilizan el cifrado de extremo a extremo nos referimos precisamente a que el contenido del mensaje solo puede ser leído entre los usuarios que se comunican. En otras palabras, **si en la Política de Privacidad de un servicio de mensajería instantánea se señala que utiliza cifrado de extremo a extremo, entonces la compañía detrás de este servicio está garantizando que no tiene acceso al contenido de los mensajes de sus usuarios.**

En consecuencia, los mensajes (fotos, videos) serán ininteligibles para cualquier tercero, incluido los directivos de la compañía de mensajería, funcionarios del gobierno, etc. En simple, solo los usuarios conocen el contenido de la información que comparten a través de los chats.

Seguramente uno pensaría que aplicar cifrado de extremo a extremo es el estándar y que por defecto todas las aplicaciones la utilizan. Sin embargo, esta suposición está muy lejos de la realidad.

Ahora bien, lo cierto es que como dijimos WhatsApp y Telegram sí usarían cifrado de extremo a extremo según sus políticas de privacidad, pero de diferentes maneras.

Por un lado, WhatsApp – que ha implementado el cifrado de extremo a extremo recién en el 2016[3] - lo aplica por defecto para todas las comunicaciones. Es decir, el usuario no tiene que hacer nada para que sus comunicaciones estén cifradas *end-to-end*.

Por otro lado, Telegram tiene configurado el cifrado de extremo a extremo únicamente para sus *secret chats* (chats secretos). Este es un tipo especial de chat[4] que tiene que ser activado por el propio usuario para conversaciones con una persona (no está disponible para chats grupales).

Así es. Telegram no tiene configurado por defecto el cifrado de extremo a extremo. Esto quiere decir que no hay garantía de que el contenido de las conversaciones sea solo conocido por los usuarios, salvo que utilices *secret chats*.

---

[3] En efecto, antes de implementar el cifrado de extremo a extremo, la aplicación tuvo muchos problemas de seguridad. Por ejemplo, se descubrió en el 2011 que las sesiones de usuarios podían ser "secuestradas" y que era posible que un usuario pudiera cambiar el estado de otro usuario de WhatsApp.

[4] Las características de los chats secretos de Telegram son: (i) usan cifrado de extremo a extremo; (ii) no dejan rastro en el servidor; (iii) tienen autodestrucción de mensajes; e (iv) impiden reenviar mensajes.

¿Entonces que sucede con la información transmitida a través de los chats en Telegram? Esta es almacenada y cifrada en la nube (cliente-servidor/servidor-cliente). En tal sentido, en teoría Telegram podría acceder al contenido de tus conversaciones. [5]

Por lo tanto, a primera vista para un usuario promedio WhatsApp resultaría más conveniente en cuanto a la privacidad del contenido de sus mensajes. ¿Es así realmente?

Ahora, sería un poco ingenuo en estos tiempos (PRISM, WikiLeaks, Cambridge Analytica) creer que las grandes compañías y los gobiernos no tienen intención de acceder al contenido de nuestras conversaciones cifradas. Las principales razones que aducen para ello son económicas y de seguridad ciudadana. Por ello, si queremos ser verdaderamente diligentes con la seguridad de nuestras comunicaciones en línea debemos ir más allá y buscar información adicional.

De hecho, las denuncias contra Facebook, compañía que adquirió WhatsApp en el 2014, son bastante conocidas. En cuanto a WhatsApp en específico cabe resaltar que el mismo cofundador de esta aplicación Brian Acton, quien renunció a su puesto en Facebook en 2017, ha señalado en una entrevista para Forbes que el cifrado de extremo a extremo siempre fue un obstáculo para el modelo de negocio de Facebook y que se buscaban formas de monetizar WhatsApp con los datos personales de sus usuarios. Asimismo, se ha especulado que la renuncia del otro cofundador de WhatsApp en el 2018 se debió a que se intentó debilitar el cifrado de WhatsApp para fines comerciales.

Por otro lado, Telegram tampoco estaría libre de manchas. Por ejemplo, se descubrió hace unos años que la Oficina Federal de Investigación Criminal de Alemania (BKA, por sus siglas en alemán) llevaba años monitoreando las comunicaciones de usuarios de Telegram. Asimismo, para algunos expertos en criptografía las razones por las que Telegram no configura el cifrado de extremo a extremo por defecto no son nada convincentes.

En fin, las controversias en torno al uso de nuestros datos personales y la privacidad en las comunicaciones en línea están muy lejos de acabar. Sin embargo, somos – y seguiremos - vulnerables frente a terceros mal intencionados si no nos informamos bien sobre las verdaderas implicancias de usar determinado servicio de mensajería instantánea (y no tomemos las medidas de seguridad adicionales en caso corresponda).

Algunos consejos para estar debidamente informados:

1. Leer los Términos y Condiciones (principalmente, la Política de Privacidad)

2. Investigar en internet sobre temas relacionados a los servicios de mensajería instantánea (cifrado, *encryption backdoors*, información de los fundadores, fuentes de financiamiento, 5-Eyes Alliance, etc.).

3. Leer foros o blogs especializados (reddit, medium, etc.).

Ten en cuenta que hay mucha información falsa y equivocada. Por eso, es importante que formes tu propio criterio a partir de la lectura de diversas fuentes. No te quedes solo con las comunicaciones emitidas por los canales oficiales de WhatsApp o Telegram.

---

[5] Al respecto, señalan en su Política de Privacidad que las llaves para descifrar el contenido de los mensajes se encuentran distribuidas en diferentes jurisdicciones, lo que dificultaría cualquier acceso no autorizado.

Finalmente, algunas páginas que podrían ser de ayuda:

- https://www.securemessagingapps.com/
- https://ssd.eff.org/en/module/what-should-i-know-about-encryption
- https://www.internetsociety.org/issues/encryption/

*** Co-fundador y Director Ejecutivo de la Asociación Lawgic Tec.**

**** Artículo recibido el 18/01/2021**