CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

WHATSAPP, EL CIFRADO DE EXTREMO A EXTREMO Y LA SEGURIDAD: REFLEJOS EN EL PROCESO PENAL ITALIANO

¿Cómo va a cambiar la seguridad de la aplicación de mensajería más popular y utilizada por más de mil millones de usuarios? ¿Se puede hablar realmente de protección de la confidencialidad? ¿Cómo cambiarán las relaciones con la Autoridad Judicial en los procesos penales?

di **Simone Lonchiar**
IUS/17 - DIRITTO PENALE
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Raffaele Giaquinto

Pubblicato, Venerdì 1 Luglio 2016

CamminoDiritto.it
ISSN 2421-7123

Hace unos días en Whatsapp ha aparecido el texto siguiente: 'Los mensajes enviados en este chat y las llamadas están ahora protegidos con el cifrado de extremo a extremo ".

¿Qué significa? Este cifrado especial sólo permite a los usuarios (emisor y receptor) interesados, en tener permisos para leer y actuar sobre los mensajes de la conversación. En términos de seguridad, esta nueva tecnología permite al mensaje de no ser interceptado durante toda la duración de la transmisión. Ni siquiera WhatsApp tiene permiso para actuar sobre los mensajes de texto, voz o cualquier otro tipo.

WhatsApp es la aplicación de mensajería para smartphones que tiene más de mil millones de usuarios activos. Esta aplicación fue creada por Jan Koum y Brian Acton en 2009, y fue adquirida posteriormente por Mark Zuckerberg, el Director ejecutivo de Facebook, el 19 de Febrero de 2014.

¿Por qué este cambio?

El camino ha sido largo y sinuoso. Una de las principales razones de la introducción de esta nueva característica es el ajuste con otras aplicaciones con la misma función de mensajería instantánea, especialmente con Telegram.

Telegram, de hecho, ha aumentado significativamente sus usuarios en pocos meses ofreciendo mejores garantías de confidencialidad. Estas nuevas garantías no son las únicas funciones adicionales (véase también el "bot") que Telegram ofrece más de WhatsApp.

¿Cómo funciona la tecnología de extremo a extremo?

Para los no especialistas, se puede expresar el concepto de cifrado de extremo a extremo pensando a la"red punto a punto": las claves de lectura se encuentran sólo en los dispositivos del transmisor y del receptor en el canal de cambio, así que los mensajes de ida y vuelta entre dos personas están codificados desde el momento en que se pulsa Intro.

Esta tecnología no permite a los malintencionados o a las autoridades de piratear o de contactar la plataforma, por tanto, impidiendo la adquisición de cualquiera información. El protocolo adoptado por la aplicación no protege los datos almacenados en el dispositivo.

Para una mejor visión de conjunto, el sitio de Whatsapp y las mismas aplicaciones en la sección "Seguridad" han ideado una explicación clara y animada, incluso para los usuarios

CamminoDiritto.it
ISSN 2421-7123

que poseen un conocimiento limitado del lenguaje tecnológico.

¿Qué ha cambiado y qué significa para los usuarios?

Como se mencionó anteriormente, el cifrado de extremo a extremo es para todos los usuarios de WhatsApp que han actualizado la aplicación. Esto significa que los que poseen una versión no actualizada, deben sustituirla con la última versión, para poder enviar y recibir los mensajes y las llamadas.

¿El cifrado ha realmente resuelto el problema de la confidencialidad?

A esta pregunta clave, que puede ser considerada el verdadero meollo de la cuestión, respondió Luigi Martino, asistente de investigación en políticas de TIC y seguridad cibernética, de la Universidad de Florencia. En una entrevista con Cyber Affairs, él afirmaba que: " [...] no significa que el contenido del mensaje no se queda a disposición de WhatsApp, que posee y controla los servidores donde se almacenan estos datos». Martino continúa con una pregunta que hace reflejar: «Esto es lo que habría que preguntarse, en una verdadera óptica que tutele la privacidad de los usuarios: quiénes son, hoy, los dueños de las conversaciones y de los datos que se mueven a través de la Red? Nosotros o el proveedor de los servicios? ".

La interceptación de datos informáticos y la interceptación telemática en el proceso penal italiano.

La interceptación telemática está dirigida a obtener la transmisión de un flujo de comunicaciones en forma confidencial, de acuerdo con las garantías previstas por el artículo 15 de la Constitución Italiana y el artículo 8 del CEDH.

Las interceptaciones de las comunicaciones informáticas y telemáticas están reguladas para el art. 266-bis del Código de Procedimiento Penal italiano (CPP) que dice: «En los procedimientos relativos a los delitos previstos en el art. 266, así como los delitos cometidos mediante el uso de tecnología informática y telemática, se autoriza la interceptación del flujo de las comunicaciones relacionadas con los sistemas informáticos y telemáticos entre múltiples sistemas». Este articulo se puede también extender a todos los crímenes cometidos mediante el uso de tecnología informática. El registro de material informático es introducido en el CPP art.8, apartado 2 de la ley 48/08, que está regulada por el art. 247 apartado 1-bis del CPP. Este articulo establece que: «Cuando hay razones para creer que los datos, las informaciones, los programas informáticos o las pistas pertinentes del delito se encuentran en un sistema informático o telemático, aunque

CamminoDiritto.it
ISSN 2421-7123

protegido por medidas de seguridad, se dispone el registro. El registro utilizará medidas técnicas destinadas a garantizar la conservación de los datos originales y para evitar la manipulación indebida».

Antes de emprender el registro, el artículo 247 apartado 1-bis CPP, requiere la adopción de "medidas técnicas" destinadas a "garantizar la preservación de los datos originales y para evitar la manipulación indebida ", con el fin de garantizar la adquisición y la preservación del elemento de prueba. Antes de utilizar esta herramienta de búsqueda de la prueba es necesario tomar cada garantía directa para proteger la inviolabilidad del domicilio " informático", entendido como "espacio contenedor" de todos los datos informáticos que pertenecen a la persona. Esto se extiende también a la protección de la confidencialidad de la esfera individual.

Por lo tanto, a la luz de las novedades introducidas, las conversaciones intercambiadas entre los usuarios de WhatsApp ya no serán utilizadas con fines probatorios.

El cifrado de extremo a extremo y las relaciones con la autoridad judicial

El cifrado de extremo a extremo significa, por tanto, que el mismo Whatsapp y las terceras partes no pueden leer los mensajes o escuchar las llamadas y los mensajes de voz. Actualmente, cifrar las comunicaciones puede ser vital para las personas que viven en países controlados por regímenes totalitarios y violentos, dónde la interceptación de mensajes no deseados por el régimen determina el riesgo para la vida o el encarcelamiento.

Con el cifrado de extremo a extremo, WhatsApp no podrá revelar el contenido de los mensajes, incluso si las autoridades lo requieren; de esta manera el ciudadano privado tiene una mejor protección contra los delitos informáticos. Sin embargo, de acuerdo con Andrea Zapparoli Manzoni, miembro de la CLUSIT, la Asociación Italiana para la Seguridad de la Información, "Hay que recordar que la protección de los datos ‘en tránsito’ es sólo un componente de una estrategia global de seguridad, y que el cifrado de mensajes por sí mismo no es capaz de garantizar la seguridad absoluta de comunicaciones ", ya que " Hay otros dos elementos que deben ser considerados: la seguridad del dispositivo (fijo o móvil) que se ejecuta en la aplicación y la seguridad de la aplicación misma. Hacia ellos hay amenazas reales, que son de ninguna manera mitigadas por la adopción del cifrado en el canal de transmisión ".

Sin embargo, hay excepciones. En un artículo del periódico italiano 'La Repubblica del 1° de marzo de 2016 se lee, en efecto, que BlackBerry no se ha alineado con la elección de Apple y Whatsapp: Black Berry entregó a los jueces de la corte de Turín, las

CamminoDiritto.it
ISSN 2421-7123

conversaciones que encajan algunos delincuentes. Se trata actualmente de conversaciones intercambiadas a través de la aplicación "interna" de BlackBerry, que se puede utilizar sólo entre los usuarios con dispositivos de esta marca. El problema que ha surgido, sin embargo, es que las conversaciones, de acuerdo con los abogados que defienden la banda de traficantes de droga, no se pueden utilizar porque no han sido 'interceptadas' directamente por la autoridad judicial.
