Diálogo Forense
Num. 2, Vol. 2, 2020
ISSN: 2707-8477

Conversaciones de la aplicación **WhatsApp** y ejemplos de su valor probatorio como evidencia digital en la legislación guatemalteca

Fredy Emanuel Sánchez Gálvez
Laboratorio de Informática Forense
Instituto Nacional de Ciencias Forenses de Guatemala –INACIF-
frsanchez122@gmail.com

Recibido: 24 de agosto 2020
Aceptado: 30 de septiembre 2020

Palabras clave: WhatsApp, mensajería, conversación, delito, evidencia, cifrado asimétrico.

Key words: WhatsApp, messaging, conversation, crime, evidence, asymmetric encryption.

RESUMEN

WhatsApp es una aplicación móvil de mensajería instantánea que tiene 1,500 millones de usuarios activos a nivel mundial, de los cuales 2.6 millones se encuentran en Guatemala (datos obtenidos hasta el año 2019). Esta permite a los usuarios mantener una conversación en tiempo real, por mensajes de texto, notas de voz o por llamadas telefónicas utilizando internet, aplicando el cifrado extremo a extremo, el cual permite que ninguna persona ajena a la comunicación tenga acceso a esta o intercepte y lea los mensajes, incluso ni la propia empresa tiene acceso a esos datos, debido a este sistema de cifrado denominado cifrado asimétrico. Es posible que las conversaciones que se generan en esta aplicación puedan ser valoradas como pruebas en distintas ramas del derecho, entre las que se pueden mencionar: contratos civiles, derecho mercantil a través del comercio electrónico y puede ser mayormente aceptado en el derecho penal cuando se demuestre o fundamente la comisión de un delito. Es importante hacer mención que solamente un juez o un tribunal de justicia pueden brindarle valor probatorio o legal a estas comunicaciones generadas a través de medios electrónicos.

ABSTRACT

WhatsApp is a mobile instant messaging application that has 1.5 billion active users worldwide, of which 2.6 million are in Guatemala. This allows users to start a conversation in real time, through text messages, voice notes or telephone calls using the internet, applying end-to-end encryption, which allows no person outside the communication to have access to it or intercept and read the messages, even the company itself does not have access to that data, due to this encryption system called asymmetric encryption. The conversations that are generated in this application, it is possible that they can be valued as evidence in different branches of law, among which we can mention, civil contracts, commercial law through electronic commerce and can be widely accepted in criminal law when the commission of a crime is proven or supported. These are some of the examples of the legal value that could be given to the data and messages that are shared in this mobile application. It is important to mention that only a judge or a court of law are the only ones who can provide probative or legal value to these communications generated through electronic means.

INTRODUCCIÓN

WhatsApp es una aplicación de mensajería instantánea que se instala en dispositivos móviles como teléfonos inteligentes, tabletas electrónicas, entre otros.

Con esta aplicación no solamente se tiene la ventaja de enviar mensajes de texto de un usuario a otro, sino que también, tiene la capacidad de crear grupos de hasta doscientos cincuenta y seis miembros, a quienes se les puede enviar el mismo mensaje en tiempo real.
Actualmente, WhatsApp es la aplicación en este ámbito que tiene la mayor cantidad de usuarios activos a nivel mundial; se ha hecho famosa debido a su facilidad de uso, sus distintas opciones y el nivel de seguridad que proporciona. En Guatemala, existen 2.6 millones de suscriptores activos por debajo de Facebook Messenger que cuenta con 4 millones. (Prensa Libre, 2019)

El uso de dicha aplicación, según la actividad que se genere a través de ésta, puede significar en algún momento una acción ilícita tal como: extorsión, violación a la intimidad sexual, posesión y/o distribución de pornografía infantil, entre otros. Además puede ser utilizada como evidencia en derecho penal, civil y mercantil; sin embargo, solamente los juzgadores tienen la potestad de valorar la información obtenida de esta aplicación.

¿Qué hace a WhatsApp una aplicación interesante?

Según el informe Digital Yearbook 2019, la aplicación WhatsApp tiene 1,500 millones de usuarios activos a nivel mundial (imagen 1), mientras que 2.6 millones, son los usuarios activos en Guatemala, según el artículo presentado por Prensa Libre en el mes de septiembre de 2019 (imagen 2).

Pero ¿a qué exactamente se debe que muchas personas utilicen este servicio y qué lo hace interesante?

Como ya muchos de los lectores han experimentado, esta aplicación de comunicación personal tiene las siguientes capacidades:

a. Mensajería de texto
b. Distribución de contenido grupal
c. Realizar llamadas
d. Realizar videollamadas
e. Compartir imágenes, videos, mensajes de voz y documentos
f. Transmisión en tiempo real
g. Cifrado extremo a extremo
h. Otras

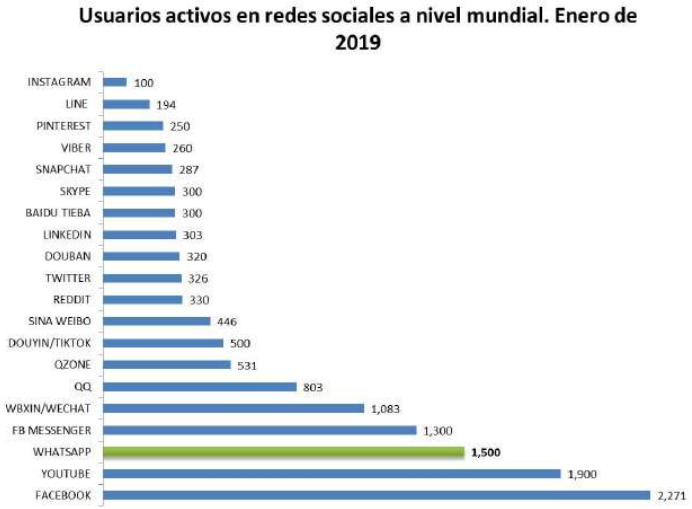

Imagen 1. Usuarios activos en redes sociales a nivel mundial. Obtenido de: We Are Social & Hootsuite (2019)

Esta aplicación tiene una interfaz bastante simple que hace que cualquier persona la pueda utilizar, todos sus servicios se realizan a través de los datos móviles del teléfono o mediante una conexión Wifi.

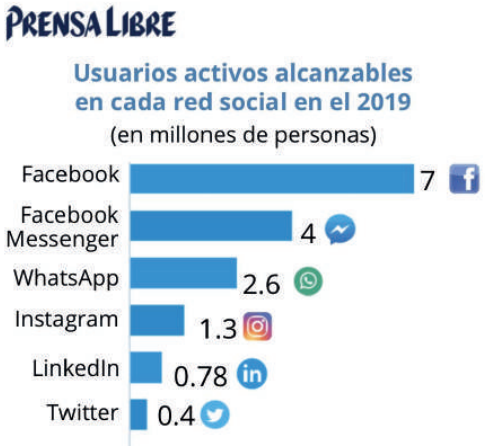

Imagen 2. Usuarios activos en Redes sociales en Guatemala. Fuente Prensa Libre

Como ya se ha indicado, WhatsApp es una aplicación de comunicación personal, la cual permite a los usuarios establecer comunicación con otras personas mediante las opciones de mensajería de texto, llamadas locales e internacionales o notas de voz con cualquier otro dispositivo que tenga instalada dicha aplicación.

La comunicación mediante esta aplicación se realiza en tiempo real, por lo que, independientemente del país en donde se encuentren los interlocutores, siempre que tengan una conexión a internet estable se podrán comunicar fácilmente sin que la distancia represente una limitante.

Otro de los puntos por los cuales esta aplicación es bastante popular se debe a su seguridad. Para muchos de los usuarios de esta aplicación es totalmente transparente la seguridad que aplica WhatsApp a los mensajes, llamadas y a toda comunicación con otros contactos.

El cifrado de extremo a extremo, garantiza que solamente el emisor y el receptor, puedan ver lo que ambos están compartiendo, lo que evita que terceras personas, fuera de la conversación, tengan acceso a dicho contenido.

Para generar un cifrado de extremo a extremo el emisor y el receptor deben contar con dos llaves: una pública y otra privada, por cada uno de ellos.

El proceso de cifrado y transmisión de los mensajes se genera de la siguiente manera:

1. Se crea un mensaje y se envía a un receptor
2. El contenido del mensaje se cifra o encripta utilizando la llave pública del receptor y se firma con la llave privada del emisor.
3. El mensaje es enviado a través de un medio de transmisión, encriptado y firmado.
4. El mensaje es recibido y validado, utilizando la llave pública del emisor, y es descifrado utilizando la llave privada del receptor.
5. El contenido del mensaje se vuelve legible para el receptor.

En consecuencia, cabe destacar que al utilizar el cifrado de extremo a extremo, a través de la criptografía asimétrica como un método de seguridad en la transmisión de información, ninguna persona puede leer el contenido de los mensajes, incluyendo a WhatsApp como empresa, debido a que las llaves privadas se encuentran en cada uno de los dispositivos móviles y es única por cada uno de estos.

Actividad en WhatsApp que puede suponer un delito

Ya se ha hablado de las bondades que tiene esta aplicación de mensajería personal, por lo que también es importante hablar del mal uso que se le puede dar, lo cual podría suponer un delito según la legislación guatemalteca.

Inicialmente, hay que mencionar que en la legislación guatemalteca, a la fecha, no existe una ley que regule delitos informáticos, únicamente en el Código Penal hace referencia a los siguientes: destrucción de registros informáticos, alteración de programas, reproducción de instrucciones o programas de computación, registros prohibidos, manipulación de información y uso de información..

Cabe destacar que mucha de la actividad que se pudiera generar en WhatsApp podría causar algún tipo de inconveniente para las personas que lo utilizan, a continuación se muestran algunos ejemplos, de los cuales, algunos pueden estár catalogados a nivel internacional como ciberdelitos.

a) Las conversaciones en donde se puedan sustentar pruebas como algún tipo de contrato verbal, conspiración o la planificación de algo ilícito.

b) El compartir imágenes íntimas a través de esta u otra aplicación es denominado como sexting, lo cual no es un delito, debido a que es algo íntimo de las personas; sin embargo, si uno de los interlocutores fuera un menor de edad podría tomarse como acoso de menores, o bien, como producción de pornografía infantil.
c) Extorsión sexual, ésta se deriva del sexting y se genera mediante el chantaje de compartir imágenes intimas de la víctima, a otras personas, a cambio de algo.
d) Extorsión o intimidación a través de este medio de comunicación, a cambio de dinero.
e) Regularmente en los grupos de WhatsApp, entre los integrantes del mismo, se comparten todo tipo de contenido, incluyendo:

- Documentos protegidos por derechos de autor.
- Mensajes o imágenes incentivando el bullying a través de medios informáticos.
- Videos o imágenes con contenido sexual infantil.

En cuanto se refiere a videos e imágenes con contenido sexual infantil, es importante hacer mención que la aplicación cuenta con la opción de descarga automática de archivos, en la cual, al estar activas las distintas opciones, descarga todo tipo de archivos compartidos. En algunos casos, si bien es cierto, el receptor no ha tenido la intención de reproducir los videos o ver las imágenes que recibió, pero al tener dicha opción de descarga activa, se almacenarán los archivos, automáticamente en la memoria del dispositivo, representando un problema para el receptor debido a que al estar almacenados en este se puede catalogar como posesión de material pornográfico de personas menores de edad, lo cual está tipificado como delito en el Artículo 42 de la Ley contra la violencia sexual, explotación y trata de personas.

WhatsApp y la pornografía infantil

El proteger las comunicaciones de extremo a extremo a través de un cifrado asimétrico, garantiza que nada podrá ser interceptado y leído por personas ajenas a dicha comunicación y, como se ha mencionado anteriormente, ni la propia empresa WhatsApp puede leer u observar el contenido de lo que sus usuarios comparten.

En el uso de la aplicación, la seguridad es clave para muchos de los usuarios pero también es la clave que llevará a entender el problema, debido a que la misma herramienta que sirve para proteger a personas respetuosas de la ley y preocupadas por sus registros digitales, sirve también para proteger y ocultar actos ilícitos.

Si Facebook e Instagram, a través de su sistema de inteligencia artificial para la detección de desnudos infantiles, tienen la capacidad para bloquear y/o eliminar publicaciones con contenido pornográfico ¿por qué WhatsApp no puede aplicar filtros similares? la respuesta está en el cifrado asimétrico, lo que ya se ha enfatizado anteriormente, en la cual ni la propia empresa tiene acceso a las llaves privadas de los usuarios y pretender reducir este nivel de seguridad en los algoritmos de cifrado en algunos grupos mayoritarios afectaría a todos los usuarios en general, trayendo consigo consecuencias graves para estos y para la propia empresa.

Aplicaciones FAKE de WhatsApp

Debido a la popularidad de WhatsApp y los chats que se pueden generar en esta, se han desarrollado aplicaciones que son utilizadas para crear y simular conversaciones falsas con el fin de jugar bromas a otras personas.

Muchas de estas aplicaciones tienen la capacidad de simular chats, cambiar estados, agregar marcas de verificación (enviado, entregado, leído), simular llamadas, videollamadas, envío de notas de voz, entre otras opciones.

Estas aplicaciones se han vuelto bastantes realistas por la facilidad de falsificar elementos y los detalles tan acertados a la aplicación original. Dichas aplicaciones se encuentran disponibles en la tienda virtual de Google Play y App Store, algunas de ellas son:

- Fake Chat Whatsapp
- WhatsFake Chats falsos
- Fake Chat Conversations
- Create Fake WhatsChat Conversation

A simple vista pareciera ser divertido simular chats para hacer bromas; sin embargo, estas simulaciones también podrían ser el origen de un problema, o bien, servirían para iniciar o simular ciberbullying, o crear conversaciones falsas con el objetivo de dañar a otras personas. Por ejemplo, que un usuario de estas aplicaciones, a modo de venganza, cree una conversación falsa y haga una o varias capturas de pantalla de dicha conversación para hacer creer que uno de sus contactos lo está acosando, o en el peor de los casos, amenazando de muerte.

A partir de lo anterior nace la pregunta ¿cómo hacer para demostrar que una conversación es real?

Existen varios factores mediante los cuales se puede determinar si una conversación es o no real, lo cual debe ser demostrado por un perito en informática forense.

Firma electrónica

La firma electrónica puede ser catalogada como un grupo de datos que son enviados adjuntos a un mensaje generado de manera electrónica y que tiene como fin indiscutible identificar al firmante como su único e inequívoco autor, así como garantizar que el mensaje no haya sido alterado.

La firma electrónica en Guatemala está regulada por el Decreto 47-2008 del Congreso de la Republica, el cual regula temas relacionados al reconocimiento de las comunicaciones electrónicas, firmas electrónicas, comercio electrónico, entre otros.

La firma electrónica se genera a través de una infraestructura de llave pública (PKI por sus siglas en inglés), la cual genera dos certificados digitales o electrónicos: 1) sirve para firmar, autenticar mensajes y documentos y, 2) para descifrar el contenido cifrado o encriptado de los mensajes que recibe.

Por lo tanto, la firma digital se genera a través del cifrado asimétrico, tal como se genera el cifrado de extremo a extremo de la aplicación WhatsApp.
En el caso de la firma electrónica se digitalizan los datos de las personas, su huella dactilar y en algunos casos, su firma manuscrita, para generar la llave pública.

Sucedería similar con WhatsApp, en donde en lugar de digitalizar los datos de personas, se capturan los datos de identificación del dispositivo. Por ejemplo, el código de país, el número telefónico y el número de IMEI, lo cual hace único al dispositivo móvil a nivel mundial.

La infraestructura de clave pública (KPI) brinda los siguientes aspectos:

- **Confidencialidad:** Con este tipo de cifrado se garantiza que las conversaciones son totalmente secretas y que ninguna persona ajena a la comunicación va a tener acceso a esta.

- **Integridad:** Garantiza que cualquier persona que logre capturar los mensajes a través de la red, no los pueda leer y mucho menos modificar. Dicho de otro modo, evita la alteración del contenido de los mensajes.

- **Autenticación:** Garantiza que el emisor y receptor de una comunicación, sean realmente las personas quienes deben tener acceso a los datos y que previamente tienen una identidad electrónica definida y verificada.

- **No repudio:** Garantiza que el emisor de un mensaje no pueda negar el envío y el receptor no pueda negar la recepción.

Estos cuatro aspectos son básicos para la seguridad del comercio electrónico.

Principio de no repudio

En la seguridad informática existe un término denominado principio de no repudio, mediante el cual es posible probar la participación de las distintas partes que componen o establecen una comunicación, utilizando medios electrónicos.

Esto es posible a través del cifrado asimétrico, en donde el emisor no puede negar que envió un mensaje debido a que el receptor tiene registros de quien emitió dicho mensaje y el receptor no puede negar que recibió un mensaje debido a que el emisor tiene pruebas o registros de la recepción. Esto es denominado como no repudio en origen y no repudio en destino.

En la aplicación WhatsApp existen mecanismos en los que se puede observar cuando el receptor recibe un mensaje debido a las dos marcas de verificación o cheques en donde el primero indica que se ha enviado el mensaje, el segundo significa que lo ha recibido y el cambio de color, representa que lo ha visto o leído. Esta última opción puede modificarse para evitar el cambio de color, sin embargo, no interfiere en la recepción del mensaje.

En la recepción de un mensaje, se puede observar el número telefónico de quién envió el mensaje, la fecha y la hora de envío.

En consecuencia, no existe manera de repudiar o negar una comunicación utilizando la aplicación WhatsApp.

1. MARCO LEGAL

Las conversaciones y mensajes de la aplicación WhatsApp, pueden ser utilizados como pruebas en un proceso judicial, siempre que estas sean extraídas siguiendo procesos adecuados o forenses, que permitan al juez hacerlas admisibles. En materia penal todo lo que constituya una prueba puede ser válida, siempre que ésta haya sido obtenida legalmente.

Hay que tomar en cuenta que hacer una captura de pantalla de la conversación e imprimirla, para presentarla como prueba, puede que no sea aceptada por el juez, debido a que no se certifica la procedencia de la misma, ni se garantiza que sea una conversación real, generada en WhatsApp, a menos que se pueda demostrar directamente en la aplicación.

1.1. Prueba pericial

La informática forense se divide en varios ámbitos para el análisis de distintos dispositivos electrónicos, entre los cuales se pueden mencionar los siguientes:

a) Cómputo forense: Es el análisis de datos, registros obtenidos de computadoras y dispositivos de almacenamiento externo. Se realiza a través de preservación, adquisición, análisis y presentación de los resultados.
b) DVR forense: Se refiere al análisis de dispositivos de grabación de video, no se considera directamente como cómputo forense debido a los distintos sistemas de archivos que utilizan para la grabación continua.
c) Móvil forense: Se refiere a la obtención y análisis de datos de dispositivos móviles utilizando dispositivos y programas forenses.

El objetivo de muchos peritajes de informática forense es la extracción y el análisis de los registros de llamadas, correos electrónicos, archivos activos y eliminados, análisis de metadatos, obtención de las bases de datos de mensajería instantánea tales como WhatsApp, debido a que como se ha mencionado a lo largo del presente artículo, el uso de esta aplicación puede contener información de valor en un proceso judicial.

Cabe destacar que, según la guía para la recopilación de evidencia digital y su almacenamiento (RFC3227), en sus consideraciones legales, establece que la evidencia digital debe ser

a) Admisible: La evidencia debe ser obtenida a través de métodos legales y apegados a la legislación local previo a ser presentado ante el tribunal.
b) Auténtica: Se refiere a que la evidencia digital obtenida debe permitir la vinculación con el hecho.
c) Completa: Es la información relacionada a los hechos, la cual debe ser clara, en el caso particular de la evidencia. La información que se brinde sobre esta no debe ser una perspectiva particular de quien la presenta.
d) Confiable: Se refiere al uso de metodologías y procedimientos aprobados para la obtención de la evidencia, la cual debe garantizar la confiabilidad de los resultados, siendo claros y evitando la ambigüedad.
e) Creíble: Los resultados deben ser fácilmente creíbles y comprensibles por los juzgadores.

1.1.1. Obteniendo una conversación

De ser una conversación específica la que se necesita para demostrar un hecho ante un juez, esta se puede obtener a través de las opciones que brinda la propia aplicación.

Para este procedimiento es necesario que el dispositivo se pueda conectar a internet utilizando los datos móviles del mismo o bien a través de una conexión Wifi, seguidamente se debe ingresar a la conversación en cuestión y exportarla mediante el correo electrónico hacia una cuenta de correo oficial (del perito).

Esta conversación se envía con sus archivos adjuntos, de manera comprimida, para garantizar que no se modifican datos en la transmisión.

El siguiente paso es certificar este archivo a través del valor hash, que es un valor hexadecimal que garantiza la identidad e integridad del archivo digital.

Este procedimiento es de cierta manera riesgoso ya que debe estar conectado a la red de telefonía local o a internet, lo que podría permitir que el usuario de este, de manera remota, realice el bloqueo del dispositivo, el bloqueo de las cuentas o incluso envíe una instrucción de borrado de datos.

1.1.2. Obteniendo la base de datos

En los dispositivos móviles es complejo realizar la adquisición de datos para el análisis forense, inicialmente por el bloqueo del dispositivo a través de los distintos factores de autenticación que existen, seguidamente por los sistemas de seguridad propios

de los sistemas operativos o de los parches de seguridad que se instalan en las distintas actualizaciones que ponen a disposición los desarrolladores de equipos móviles.

Después de haber superado esta barrera, la cual en muchos de los casos es casi imposible de evadir, se procede a la configuración del dispositivo para hacerlo accesible mediante las herramientas forenses de adquisición.

Se puede hablar de dos métodos para la obtención de la base de datos siendo estos:

a) Rooteando el dispositivo: Rootear un dispositivo es un método que permite al usuario tener privilegios de administrador, en el cual se puede tener acceso a todos los archivos del sistema operativo incluyendo los archivos que almacenan las contraseñas de acceso al teléfono, el archivo que almacena la información de la huella dactilar y, lo que más interesa, el archivo que contiene la llave que desencripta la base de datos de WhatsApp.

   Al rootear el dispositivo no se altera la partición que contiene los datos de los usuarios, lo que se consigue a través de este método es similar a tener que ingresar a una vivienda en la cual se ha cometido un asesinato, en donde no se puede ingresar, pero que es necesario hacerlo para obtener el cuerpo y todo indicio que permita iniciar la investigación. Es decir que, rootear un teléfono únicamente abre la puerta del dispositivo que permitirá obtener información relacionada a un hecho.

   WhatsApp almacena la base de datos cifrada, la cual se identifica como msgstore.db.crypt12, misma que se localiza en la carpeta SDCARD/WhatsApp/Databases/.

   Ya con el dispositivo rooteado, es necesario buscar el archivo KEY que se genera para desencriptar las conversaciones y la base de datos. Este archivo se encuentra en la partición USER DATA del sistema operativo, en la siguiente ruta: Data/Data/-com.Whatsapp/files/.

   Después de obtener la base de datos y la llave, se debe utilizar un programa que permita realizar el descifrado y leer el contenido, cabe hacer mención que la base de datos de esta aplicación está desarrollada en SQLite, que es un sistema de gestión de base de datos utilizado por varias aplicaciones móviles.

   Utilizando el programa WhatsApp Viewer o SQLite Browser, es posible leer el contenido de las conversaciones y todos los registros referentes a la comunicación. WhatsApp Viewer tiene la capacidad de mostrar las conversaciones de forma ergonómica, asimismo permite cargar la base de datos wa.db que contiene información de los contactos con los que se ha tenido comunicación.

b) Degradando la versión: Este método consiste en realizar una degradación de la versión actual de la aplicación, a una versión que permita realizar un backup local.

   Como se ha mencionado anteriormente, las bases de datos de WhatsApp están cifradas lo que evita que se puedan analizar de forma directa.

   Las conversaciones y los registros de llamadas o videollamadas utilizan el cifrado AES-256 (Estándar de cifrado avanzado), sin embargo, los archivos de multimedia como videos, imágenes y audios se almacenan sin ningún tipo de cifrado.

   La degradación de la versión de la aplicación puede generar en algún momento la pérdida total de la información, debido a que consiste en desinstalar la versión actual sin perder los datos remanentes del usuario.

   Posteriormente se debe instalar una versión antigua que permita realizar respaldos locales sin ningún tipo de cifrado.

   WhatsApp v.2.11.431 es la última versión de esta aplicación sin cifrado de respaldo forzado, con la cual se puede realizar un backup utilizando la consola de depuración de Android (ADB) y obtener la base de datos sin cifrado para su respectivo análisis forense.

   Similar al proceso anterior, se puede abrir la base de datos utilizando el programa SQLite Browser u otro similar.

   Aunque existen dispositivos y programas forenses que permiten la obtención de la base de datos de forma automatizada y la presentación de resultados de mejor manera, no es garantía de que esta se pueda obtener debido a los sistemas de seguridad,

propios de los dispositivos, las actualizaciones de los parches de seguridad en los sistemas operativos y otros programas que pueden cifrar aplicaciones.

Para la obtención de la base de datos, al igual que en la obtención de correos electrónicos, mensajes de texto e incluso los registros de llamadas, de acuerdo a la legislación guatemalteca, se debe contar con una orden de juez competente en la cual permita el allanamiento del dispositivo, la extracción de los datos, el análisis de estos y por último la reproducción de los resultados.

Esta orden emitida por el juez garantiza que el perito en informática forense realice su trabajo en el marco de lo legal y evita que este cometa un delito al realizar una acción inconstitucional, regulada en el Artículo 24 de la Constitución Política de la República de Guatemala, el cual sanciona la secretividad de la correspondencia y de las comunicaciones que se realizan utilizando la tecnología moderna.

1.2. Principio de equivalencia funcional

Pietterly (2015) indica que el principio de equivalencia funcional es transmitirle el mismo valor, tanto jurídico como probatorio, a las actividades que en la actualidad se realizan utilizando tecnologías de información y que anteriormente se realizaban a través de medios tradicionales.

Por su parte, Polanco (2017), indica que el principio de equivalencia funcional hace que los datos transmitidos en forma de mensaje, posea valor legal en condiciones similares concernientes al comercio electrónico.

A partir de estas dos aseveraciones se puede tener claro que este principio avala legalmente las acciones que se realizan a través de medios electrónicos, por lo tanto, lo que anteriormente era el correo postal ahora es el correo electrónico y lo que anteriormente eran mensajes a través de telégrafo ahora se puede traducir a mensajes de texto o mensajería instantánea y, referente al comercio electrónico, toda comunicación tendrá también un valor jurídico.

Este principio permite que las acciones que se realizaban a través de métodos tradicionales y que en la actualidad se realizan a través de medios electrónicos, conserven su mismo valor legal. A continuación se muestran algunas:

a. Firma electrónica
b. Correo electrónico
c. Comercio electrónico

Así como este principio apoya las acciones para el comercio electrónico y el desarrollo de otras actividades, también restringe cierta actividad como leer el contenido de conversaciones y correos electrónicos de otras personas o irrumpir en la privacidad de las llamadas telefónicas.

Por lo tanto, no es factible que un perito en informática forense de oficio o nombrado, o bien alguien con conocimientos técnicos, pueda acceder a un dispositivo móvil y extraer todo lo referente a correos electrónicos, conversaciones, registros de llamadas, entre otros.

Si por otra situación se llegara a realizar un peritaje informático sobre un dispositivo para la obtención de las conversaciones como WhatsApp, sin tener el respaldo de una orden de juez, llevaría hacia la doctrina del fruto del árbol envenenado. Dicha doctrina es una metáfora desarrollada en el Tribunal Supremo de Estados Unidos en la que indican que la fuente para obtener una prueba es el árbol y, por el hecho de estar envenenado, la prueba que sería el fruto, de igual manera estará envenenada y por consiguiente esta prueba es totalmente inadmisible.

1.3. El valor probatorio de las conversaciones de la aplicación WhastApp

Tomando como base que la evidencia, o prueba, debe obtenerse a través de métodos forenses apegados a la legislación local para que sea admisible en un proceso judicial y comprendiendo el concepto del principio de equivalencia funcional, cabe la posibilidad que un juez o un tribunal de justicia brinden valor probatorio a las conversaciones de WhatsApp, en cualquiera de las áreas del derecho en las que se pueda aplicar, tal como el área civil, área mercantil o el área penal. A continuación se muestran algunos ejemplos:

a) **Valor Probatorio en el derecho civil:** En el derecho civil se regulan las relaciones entre las personas o las relaciones del tipo patrimonial.

   Esta rama del derecho se define a través de distintas normas o pautas. Tal es el caso del derecho de las obligaciones y contratos, los cuales rigen y controlan los actos y negocios jurídicos y sus consecuencias.

   Como un ejemplo de la aplicación y valoración de conversaciones de WhatsApp en el derecho civil, se puede mencionar el caso en donde un Juez del municipio de Vigo, España, consideró valorar las

conversaciones desarrolladas a través de la aplicación WhatsApp como un contrato verbal.

Este caso trató de un arrendamiento en donde el arrendatario tuvo comunicación con el inquilino a través de mensajes de texto de WhatsApp, negociando las condiciones del trato. Estando de acuerdo las partes, el inquilino se comprometió a pagar las mensualidades y las facturas de los servicios básicos, incluso envió fotografías de su documento de identificación y el número de cuenta bancaria.

El inquilino dejó de cancelar las facturas, lo que llevó a los arrendantarios a iniciar un juicio en contra de este. El juez recibió las pruebas de las conversaciones, las aceptó y le dio la figura de contrato verbal.

En la legislación guatemalteca, el capítulo III del Código Civil, establece la forma de los contratos pero específicamente el Artículo 1574 regula las distintas formas en que las personas pueden contratar y obligarse, entre estas se pueden mencionar: "a través de correspondencia" o "de manera verbal".

Tal como se menciona anteriormente en el principio de equivalencia funcional, el correo electrónico tiene el mismo valor jurídico que el correo postal o la correspondencia tradicional y, por otra parte, las conversaciones de WhatsApp pueden ser valoradas jurídicamente a través de la figura de un contrato verbal.

b) Valor Probatorio en el derecho mercantil: El derecho mercantil rige y acompaña los actos comerciales de bienes y servicios y sus implicaciones legales.

En las conversaciones de WhatsApp se pueden generar actos mercantiles a través de lo estipulado en la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

No está de más recordar que la firma electrónica se genera a través de certificados de cifrado asimétrico que cuentan con autenticación, integridad confidencialidad y no repudio, tal como se generan los certificados y la comunicación de la aplicación WhatsApp.

En el Artículo 5, de la ley en mención, se reconocen las comunicaciones electrónicas, en donde indica que no se negará valor jurídico y validez a contratos o comunicaciones electrónicas.

Para contratar o adquirir un bien o servicio es importante mencionar que debe existir un consentimiento por parte de la persona que desea adquirirlo, esto obliga a ambas partes a cumplir con lo pactado.

Traducido a medios digitales, la contratación realizada por medios electrónicos también necesita de un consentimiento, pero este debe ser electrónico.

El consentimiento electrónico es una declaración de la voluntad de una persona, en el cual, utilizando tecnologías de información y comunicación, manifiesta la aceptación de una propuesta u oferta recibida electrónicamente.

Este consentimiento puede hacerse mediante sistema de aceptación por declaración, el cual consiste en que con un simple mensaje el aceptante declara su conformidad, sin necesidad de otros requisitos o formalismos, ante el oferente. Por otra parte, puede hacerse también mediante el sistema de aceptación por recepción, en el cual, la plataforma electrónica brinda la información de que la respuesta de aprobación por parte del aceptante, llegó al oferente.

El sistema de mensajería de la aplicación WhatsApp, mediante su plataforma tecnológica y su sistema de seguridad, proporcionan estas condiciones para poder llevar a cabo actos mercantiles. Es importante insistir que este tipo de comunicaciones tienen reconocimiento jurídico, admisibilidad y valor probatorio, gracias a la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas.

c) Valor Probatorio en el derecho penal: El derecho penal pauta y crea las capacidades de castigo que se reserva el estado para las personas que violentan las leyes y normas de conducta.

En esta rama del derecho es más factible que una conversación de WhatsApp sea admisible por un juez, siempre que cumpla con lo establecido en el marco legal del país.

Las conversaciones de WhatsApp pueden ser aceptadas como prueba, por ejemplo:

1. Delitos contra la vida: En donde es capturado el autor de un asesinato y en sus conversaciones se demuestre relación directa con el hecho, tales como conversaciones premeditando el acto, según el Artículo 132 del Código Penal guatemalteco.

2. Conspiración y asociación ilícita: Lo cual está relacionado de cierta manera con el numeral anterior, este se puede ejercer cuando en las conversaciones o en los archivos compartidos, se demuestre actividad para cometer uno o más delitos. Según lo estipulado en los Artículos 3 y 4 de la Ley Contra la Delincuencia Organizada.

3. Delitos de Extorsión: En el caso que se demuestre mediante las conversaciones generadas en la aplicación WhatsApp, que uno de los interlocutores solicite dinero o beneficios de forma obligada a otra persona, a cambio de no hacerle daño. Según el Artículo 11 de la Ley Contra la Delincuencia Organizada.

4. Difamaciones y Publicaciones de ofensas: En las que se utilicen los medios informáticos para la difusión de contenido que provoque el descredito de las personas, injuria o calumnias, según los Artículos 164 y 165 del Código Penal.

5. Posesión y distribución de contenido sexual infantil: Como se mencionó anteriormente, en la aplicación WhatsApp se puede compartir contenido de todo tipo, tal como archivos con contenido sexual infantil, lo cual puede ser catalogado como producción, distribución o posesión de material pornográfico infantil, este delito está regulado en la Ley Contra la Violencia Sexual, Explotación y Trata de Personas, según los Artículos 41 y 42.

6. Violación a la intimidad sexual: En WhatsApp se puede compartir todo tipo de contenido, sin filtro alguno, en donde se puede llevar a cabo la practica denominada sexting, la cual consiste en el intercambio de imágenes o videos íntimos y, a partir de este, puede compartirse dicho contenido con otras personas por venganza o solamente por compartir este material. De momento no está tipificada la extorsión sexual o la porno-venganza, sin embargo puede penarse esta actividad a través del Artículo 34 de la Ley contra la Violencia Sexual, Explotación y Trata de Personas.

2. CONCLUSIONES

La aplicación de mensajería instantánea WhatsApp, hasta el año 2019, ha sido de la aceptación de muchos, en específico de 1,500 millones de personas a nivel mundial aproximadamente, gracias a sus distintas opciones y sobre todo al nivel de seguridad que brinda a sus usuarios a través del cifrado asimétrico.

Las conversaciones de esta aplicación pueden ser utilizadas como medio o fin para cometer un delito; asimismo, pueden generar un valor legal dependiendo el área del derecho en donde sea enmarcado.

En el derecho civil, es posible la aceptación de las conversaciones de WhatsApp, como un contrato verbal o un contrato a través de correspondencia, debido al valor jurídico que tiene la mensajería, gracias al principio de equivalencia funcional.

En el derecho mercantil, es posible realizar comercio electrónico a través de esta aplicación, debido a que se sabe quiénes interactúan en una conversación y no es posible repudiar la recepción o envío de un mensaje.

Asimismo, cabe destacar que los certificados de la firma electrónica se crean de la misma manera que los certificados de la aplicación WhatsApp, utilizando algoritmos para el cifrado asimétrico, con la diferencia que en la firma electrónica se vincula directamente a una persona, mientras que en la aplicación se vincula el dispositivo, mediante el número telefónico, el IMEI, entre otros.

En derecho penal, todo elemento que pueda constituir una evidencia, puede ser admitida como prueba siempre que la misma sea adquirida legalmente. Por lo tanto, es posible presentar mensajes, imágenes, videos, audios o registros de toda actividad que se genere o se comparta en esta aplicación, siempre que su obtención se encuentre en el marco de lo legal, para evitar que la prueba sea inadmisible, tal como lo describe la doctrina del árbol envenenado.

Existen aplicaciones que pueden crear supuestas conversaciones falsas de WhastApp, de las cuales, aparentan ser reales, por lo que no es recomendable que un juez de valor a una imagen, a menos que se confirme que la conversación esté almacenada en la base de datos de esta aplicación.

El principio de no repudio permite al emisor, ver cuando un mensaje fue enviado y recibido por el receptor, asimismo el receptor, tiene los registros del contacto que emitió el mensaje. Con este principio que se da a través del cifrado asimétrico, nadie que utilice la aplicación, puede negar que envió o recibió un mensaje o un archivo.

Estas comunicaciones electrónicas pueden servir como evidencia en un proceso legal, sin embargo, solamente los juzgadores tienen la potestad de darle el valor jurídico correspondiente a la información obtenida de esta aplicación.

AGRADECIMIENTOS

Agradezco a Dios por iluminarme y permitirme realizar este artículo; a las personas que me apoyaron directa e indirectamente para desarrollar cada uno de los temas, gracias por compartir sus ideas, consejos y experiencia; a mis expertos en la legislación guatemalteca, a mis expertos en el análisis informático forense, a las personas que colaboraron en la revisión de este documento y al Instituto Nacional de Ciencias Forenses de Guatemala por darme la oportunidad de crecer profesionalmente y aportar conocimiento de valor para muchas personas.

BIBLIOGRAFÍA

We Are Social & Hootsuite (2019), DIGITAL 2019, consultado el 30/10/2019, disponible en: https://www.juancmejia.com/wp-content/uploads/2019/03/Digital-2019-WeAreSocial-y-HootSuite.pdf

Gándara, N. (25 de septiembre 2019). Prensa Libre. Consultado el 30/10/2019, disponible en: https://www.prensalibre.com/economia/estudio-redes-sociales-ilifebelt-2019-guatemala-centroamerica-y-latinoamerica/

Barrios, Omar. Licenciado en Ciencias Jurídicas y Sociales. Entrevista realizada el 25 de octubre 2019.

Decreto 09-2009, Ley contra la Violencia Sexual, Explotación y Trata de Personas (2009). Guatemala.

Pérez Colomé. España. (10/01/2019). Diario El País, Consultado el 06/11/2019, disponible en https://elpais.com/tecnologia/2018/12/22/actualidad/1545435648_287351.amp.html?__twitter_impression=true

Herrera, I. Guatemala (10/09/2019). Diario Digital El Periódico, Consultado el 14/11/2019, disponible en https://elperiodico.com.gt/gente/2019/09/10/impulsan-la-firma-electronica-en-guatemala/

Cordón, Elizabeth. Licenciada en Ciencias Jurídicas y Sociales, Abogada y Notaria. Entrevista realizada el 21 de octubre 2019.

Grupo de trabajo de red D. Brezinski (2002), Solicitud de comentarios 3227 (RFC 3227), consultado el 13/11/2019, disponible en https://www.ietf.org/rfc/rfc3227.txt

Pérez Martín, D. Ingeniero, Director Técnico en el CERT AIUKEN, Santiago de Chile, Ex Perito forense de la Policía Judicial de España. Entrevista realizada el 20/10/2019.

SalvationData (08/02/2018). Consultado el 30/10/2019, disponible en: https://blog.salvationdata.com/2018/02/08/whatsapp-forensics-decryption-of-encrypted-databases-and-extraction-of-deleted-messages-on-non-rooted-android-devices/

Constitución Política de la República de Guatemala, Art. 24.

Pietterly, A. (SF) Lindeco, consultado el 31/10/2019, disponible en https://lideco.com/download/CERTIFICADO%20DIGITAL1.pps

Berbell & Rodriguez. España. (05/08/2018), consultado el 14/11/2019, disponible en https://confilegal.com/20180805-que-es-la-doctrina-del-arbol-envenenado/

Rafino, M. (02/03/2019). Derecho Civil, consultado el 14/11/2019, disponible en https://concepto.de/derecho-civil/

Yúbal-FM. XATAKA (27/09/2019). Consultado el 15/11/2019, disponible en https://www.xataka.com/aplicaciones/juez-vigo-sentencia-que-dicho-whatsapp-puede-ser-considerado-contrato-verbal-vinculante

Rafino, M. (29/11/2019). Derecho Mercantil, consultado el 14/11/2019, disponible en https://concepto.de/derecho-mercantil/

Rincón Cárdenas, E. (2006). Manual de derecho de comercio electrónico y de internet. Bogota, Colombia: Centro Editorial Uiversidad del Rosario.

Rafino, M. (29/11/2019). Derecho Penal, consultado el 14/11/2019, disponible en https://concepto.de/derecho-penal/

Mejía, Carlos. Licenciado en Ciencias Jurídicas y Sociales, Abogado y Notario. Entrevista realizada el 21 de octubre 2019.