PRUEBA ELECTRÓNICA, PRESERVACIÓN, ANÁLISIS Y VALORACIÓN

TRABAJO FINAL DE LA

CARRERA DE ESPECIALIZACIÓN EN CIBERCRIMEN

ALUMNA: CARINA ALEJANDRA BERNAL

AÑO: 2024

ÍNDICE

RESUMEN

La introducción de la prueba electrónica en el proceso penal plantea desafíos tanto legales como tecnológicos y los tribunales deben abordarlos cuidadosamente para garantizar una justicia efectiva. A menudo la prueba electrónica es presentada por las partes en forma de correos electrónicos, mensajes de texto, registros de llamadas o publicaciones en redes sociales. La tarea del perito o experto será la de conocer y estar actualizado para asegurar que la autenticidad y la integridad de estos documentos se perpetúe durante el proceso garantizando que no ha sido alterada o manipulada ya que esto será fundamental para su admisibilidad.

Palabras Claves: prueba electrónica, evidencia electrónica, criminalista, perito, investigador.

ABSTRACT

The introduction of electronic evidence into criminal proceedings raises both legal and technological challenges and must be carefully addressed by courts to ensure effective justice. Electronic evidence is often presented by the parties in the form of emails, text messages, call logs, or social media posts. The task of the expert or expert will be to know and be updated to ensure that the authenticity and integrity of these documents is perpetuated during the process, guaranteeing that they have not been altered or manipulated since this will be essential for their admissibility.

Keywords: electronic evidence, electronic evidence, criminalist, expert, investigator

INTRODUCCIÓN

El enfoque que se pretende dar a este artículo, es desde la óptica del Criminalista, como investigador y analista criminal.

Los documentos electrónicos, generados por una computadora o por dispositivos móviles en la actualidad contribuyen en muchas ocasiones a resolver hechos ilícitos, por lo que por su naturaleza es necesario que esa información con valor probatorio se asegure y resguarde.

El aporte de la prueba electrónica, es decir la información generada o almacenada en esos dispositivos o bien la información transmitida electrónicamente a través de redes de comunicación es cada vez más habitual, como así también su aseguramiento y posteriormente su análisis.

Los investigadores y criminalistas en la actualidad tienen un gran desafío: la utilización de los actuales avances tecnológicos en las tareas de investigación en los escenarios o lugares del hecho virtuales o digitales.

El autor Guzmán (2000) define a la criminalística "como la profesión y disciplina científica dirigida al reconocimiento, individualización y evaluación de la evidencia física, mediante la aplicación de las ciencias naturales, en cuestiones legales". (p.33)

En este contexto, el presente trabajo se circunscribe al estudio de la prueba electrónica, su aseguramiento y posterior análisis del investigador para coadyuvar a la tarea de resolución de casos cuyos escenarios virtuales requiere una experticia técnica en particular.

El doctor (Salt, s.f) dice que los beneficios que conlleva la utilización de evidencia digital es que las pruebas obtenidas en ese entorno contribuyen a un sistema de justicia más eficiente y moderna.

El investigador forense o el criminalista hasta hace unos años atrás, no

necesitaba más que lupas, escalimetro, cámara de fotos con lentes de aumento y luces con diferentes incidencias y alguna que otra herramienta tecnológica como un programa de edición o de gráficos, un microscopio binocular digital, para ilustrar y demostrar al Juez aquello que minuciosamente observó por más invisible o imperceptible que fuera ese indicio analizado en laboratorio y que serviría para ser introducida al proceso para luego se presenta como prueba para ser valorada por el Juez o un Tribunal.

Pero desde hace un poco más de una década y en consonancia con la introducción del internet en nuestras vidas, la cotidianidad de las personas transcurre en entornos virtuales, las relaciones interpersonales, la vida comercial, y el desarrollo de la humanidad se encuentra sumergido en esta era digital.

Por consiguiente al igual que la vida misma, se observan sofisticadas maniobras delictuales, enmascaramiento de identidades, nuevos delitos que se desarrollan en su totalidad en la virtualidad, comunicaciones encriptadas, etc.

Castillero Mimenza (2017) refiere que en este proceso de evolución y de introducción de tecnología a la vida cotidiana, el investigador debe adecuarse y aggiornarse en la interpretación de nuevos elementos perceptibles sea o no material, que resulta o se ve implicado en la escena de un crimen y que permite imaginar la existencia de una circunstancia determinada vinculada al suceso o crimen investigado.

Luego al analizar estos elementos minuciosamente si tiene relación con el hecho investigado se convierte en una evidencia y, si este indicio es digital u obtenido de entornos digitales con el manejo de herramientas tecnológicas permitirá descubrir o probar cómo sucedieron los hechos e identificar al o a los autores, expresa Contreras (2010).

Según Darahuge y Arellano González (2005) en este contexto, no lleva a una definición ampliada hacia la prueba electrónica que podemos pensar como cualquier objeto que cumpla la función de contenedor de datos informáticos que, metodológicamente investigados, nos pueden llevar a reconstruir hechos.

Es decir el investigador debe conocer y manejar los nuevos entornos virtuales para observar, asegurar preservar y analizar el indicio en el lugar o escenario donde se desarrolla un hecho susceptible de investigación.

El objetivo principal de este trabajo es demostrar que la prueba electrónica correctamente incorporada al proceso, contribuye al esclarecimiento de un hecho y a una justicia moderna, siendo los objetivos específicos la de proporcionar conocimientos específicos en investigación y análisis de evidencia digital, identificar alcances de la prueba electrónica dentro del proceso penal, diseñar guías de buena prácticas y protocolos de actuación en la obtención de evidencias en entornos virtuales.

Para el presente trabajo se tomaron de referencia diferentes autores como por ejemplo RIVOLTA (2007) donde describe que la evidencia digital puede ser considerada como elemento de prueba y como medio de prueba.

Define como elemento de prueba, al dato objetivo, en formato electrónico, que las partes obtienen e incorporan legalmente al proceso, que permite producir un conocimiento cierto probable de los hechos invocados.

La evidencia digital como medio de prueba involucra los procedimientos establecidos por la ley o por la jurisprudencia para introducir válidamente en el proceso los elementos de prueba en formato electrónico, utilizados por las partes para tornar verosímil los hechos alegados en el litigio.

El autor Quadri (2011), sostiene que:

> La prueba es un medio de verificación de las proposiciones que los litigantes formulan en el juicio o, en el caso en que la ley lo autoriza (ej. arts. 163, inc. 6°, p. 2, Cód. Proc. Civ. y Com.; arts. 200 y 201, CPC Córdoba), de acreditación de los hechos conducentes para la solución del litigio; mientras tanto, si pasamos a su análisis en el marco de un proceso concreto, prueba será —vista desde el enfoque del resultado— todo motivo o razón aportados al proceso para llevar al juez el convencimiento

> o la certeza sobre los hechos. Probar será, entonces, la acción de aportar tales razones y motivos, en orden a dejar verificada alguna de las proposiciones formuladas en juicio; y la actividad probatoria será aquella encaminada a probar (por cierto, con un resultado contingente, pues podrá —o no— lograr su objetivo. (p.17)

Para (Delle Donne, s.f) la prueba digital es todo dato o información generada por un sistema informático que se encuentra almacenada en dispositivos informáticos. La prueba digital, que puede categorizarse como prueba documental, se obtiene y se preserva de un modo diferente a todo otro tipo de evidencia porque está almacenada en un soporte electrónico. Esa circunstancia implica que la prueba electrónica tiene características particulares que exigen que las fuerzas de seguridad que intervengan en la extracción de la prueba digital cuenten con los conocimientos especiales para no contaminarla y las herramientas forenses necesarias a los fines de asegurar la recolección pertinente, la extracción correcta y la preservación adecuada. Para entender la importancia del primer acto de extracción de la prueba electrónica, debe considerarse que tiene características propias. La prueba digital es volátil, alterable o modificable y fácilmente duplicable.

Una prueba electrónica puede ser toda aquella información que se encuentra contenido en un dispositivo o que ha sido transmitida a través de los actuales canales de comunicación digitales, un correo electrónico puede ser una prueba electrónica por ejemplo, o aquellos que surjan de los sistemas de mensajería instantánea como whatsapp, son solo algunos ya que más adelante me explayaré, de más métodos probatorios para acreditar o no la ocurrencia de un hecho en un entorno digital.

La principal diferencia, y eso se intentará desarrollar en el presente trabajo, es que la prueba electrónica tiene características intrínsecas y muy propias, que por su naturaleza pueden ser inestables, intangibles y difícil de recuperar o acceder por el lugar donde se encuentra alojada la información o los datos, que permitirán luego de ser preservada y extraída, analizar su contenido genuino e íntegro y de esa manera el material probatorio que surge de esa acción técnica, pueda ser usada en el marco del

proceso para dilucidar un delito o un pleito.

Se concluye entonces, que la prueba electrónica se obtiene y se preserva de un modo diferente a otro tipo de evidencia, esta peculiaridad, exige al investigador y/o analista un conocimiento específico para la extracción, recuperación, preservación de la prueba electrónica y la admisibilidad en el proceso.

Estas situaciones ocurren a diario en las dependencias de los gabinetes periciales o en los cuerpos de investigadores en función de los requerimientos de los instructores o fiscales, por lo que lleva a reflexionar sobre las nuevas modalidades de incorporación de elementos digitales aportados de manera voluntaria por un sujeto dentro del proceso penal.

La finalidad que se persigue con la elección de este tema es aplicar los resultados obtenidos a la investigación en el ámbito de la justicia ordinaria local, ya que existe poca información registrada en cuanto a los procesos en torno a la aportación de evidencia, sin necesidad de utilizar software forense.

Ya que no toda evidencia digital puede o debe ser extraída, analizada y preservada por herramientas forenses que por la naturaleza del dispositivo que contiene esa información susceptible de recuperación y análisis, puede ser obtenida con mecanismos rápidos y de igual resultado probatorio que aquel que haya sido utilizado algún sofisticado software forense.

La aportación de una prueba electrónica en cualquier fuero y en cualquier proceso es más habitual de lo que se imagina: comentarios en redes sociales, grabaciones o filmaciones de cámaras de video vigilancia, mensajería instantánea, correos electrónicos, etc.

Esta gran variedad de fuentes probatorias deben tener acceso al proceso judicial a través de alguno de los medios de prueba legalmente previstos en nuestros Códigos.

Se relevarán entonces diferentes Códigos Procesales de nuestro País y

Jurisprudencia al respecto: Código Procesal Penal de la Provincia de San Luis Nº VI-0152-2021, B.O. 03/09/2021, https://www.pensamientopenal.com.ar/doctrina/.

Además, de tratarse de una evidencia que se encuentra alojada en un dispositivo que voluntariamente se aporta para el proceso, el apuro de devolver o entregar los elementos puestos a disposición, nos permite incorporar evidencia al proceso utilizando para ellos mecanismos validados.

La prueba electrónica suele ir acompañada de metadatos que pueden desempeñar un papel importante como evidencia (por ejemplo, la fecha y la hora que se escribió un documento podrían ser útiles en caso de derecho de autor. (Bielli y Ordoñez, 2019, p.93).

La estrategia metodológica que se empleará para el logro de los objetivos, será con un enfoque del proyecto de tipo cualitativo, ya que la información obtenida que permita llegar a los objetivos planteados, será a partir de la información obtenida de las diferentes casos empíricos y de las experiencias que desarrollaron otras oficinas periciales, como así también recopilar la información actualizada en materia de aportes de pruebas electrónicas en los procesos penales y como los diferentes actores resuelven diariamente situaciones similares.

La clase de proyecto de investigación documentado tendrá un alcance exploratorio ya que de esa manera permitirá familiarizarse con un fenómeno relativamente nuevo o contemporáneo, los cuales en la práctica pericial suceden a diario pero no se encuentra formalmente normado.

Para alcanzar los objetivos descritos, este trabajo se organiza en cuatro capítulos, el primero se introduce en conceptos teóricos, características y el marco legal o regulatorio de los documentos y prueba electrónica, el capítulo segundo se enfoca en los nuevos medios probatorios, whatsapp, correo electrónico y contenidos en las redes sociales.

Por su parte en el tercer capítulo se abordarán las diferentes situaciones que se presentan con el aporte de una prueba electrónica en un proceso penal, métodos

utilizados y sus resultados, herramientas forenses como Programa Espejo (desarrollo del Ministerio Público Fiscal de Chubut- Argentina), Programa Pandora (desarrollo privado de España), funciones propias de Whatsapp y de otras plataformas .

Mientras que el último capítulo explora investigaciones y diferentes autores que escribieron sobre la admisión, valoración e incorporación de la prueba digital en el proceso penal.

1) PRUEBA ELECTRÓNICA

1.1) Concepto

La incorporación de los recientes avances tecnológicos en las tareas de investigación penal por parte de las fuerzas de seguridad o de los cuerpos de investigadores judiciales es fundamental para la detección y resolución de delitos, especialmente aquellos en los que las tecnologías de la información juegan un papel crucial. Por lo tanto la aplicación de dichas tecnologías refleja el presente y el futuro en las investigaciones penales.

Para avanzar en este trabajo y abordar este apartado, se han examinado diversos autores que discuten el concepto de la prueba electrónica. Molina Quiroga (2012) prefiere hablar de documento digital, definiéndolo como aquel que es conservado en formato digital en la memoria central del ordenador o en las memorias de masa, también refiere que técnicamente, el documento digital es un conjunto de impulsos eléctricos que recaen en un soporte de computadora que, sometidos a un proceso, permiten su traducción al lenguaje natural a través de una pantalla, una impresora u otro periférico que genere un resultado equivalente.

Mientras que Ordoñez (2019) refiere que un juez valora una filmación, un mensaje de Whatsapp, una publicación de Facebook o Twitter, una página web, un mail, una fotografía, un audio o una firma electrónica, técnicamente lo que está apreciando es un documento electrónico. Esto no quiere decir que sea lo mismo un archivo de imagen que un archivo de video o de audio; o un documento no firmado que un documento signado con tecnología de firma digital o firma electrónica; o un mensaje enviado por una red local que un correo electrónico o un mensaje multimedia, existiendo distintas variables de estos instrumentos y no todas gozando de las mismas propiedades.

Vaninetti (2013) aborda este tema refiriéndose a la prueba electrónica en el marco de un proceso judicial abarcando cualquier registro generado dentro de un

entorno informático, comprendiendo este último como cualquier dispositivo físico (como computadoras, teléfonos inteligentes, tabletas, CDs, DVD, unidades flash USB, etc.) utilizado para crear, almacenar o manipular información digital o remitir o guardar a dichos registros que, producto de la intervención humana, han sido extraídos de un medio informático. Lo distintivo de la prueba electrónica es que está esencialmente vinculada a hechos o actos jurídicos ocurridos o realizados a través de medios informáticos.

El autor español Lluch (2012) se enfoca en su obra en el análisis y estudio de la prueba, siendo esta parte esencial de todo procedimiento, porque existe una relación de causa-efecto entre prueba y sentencia, como revela el viejo apotegma probare o soccombere y señala que resulta determinante que los hechos asuman una configuración informática.

Entonces, una fotografía, un video, una página web, un correo electrónico, una base de datos, en cualquier soporte (digital, magnético o informático), constituyen una prueba electrónica o documento electrónico, aun cuando su reproducción e impugnación puedan ser diferentes.

De los diferentes conceptos, coincido con el autor Quadri (2011) la prueba electrónica no es más que una prueba, no se diferencia de las demás que pudieran ingresar al proceso, la diferencia está en la forma que ingresa y la manera que se la reconoce, preserva, analiza y se presenta la juez o al tribunal.

Es posible agregar también que la prueba electrónica no es más que la acreditación de un hecho o la demostración que respalde que tal hecho no existió. En ese concepto entonces, podría decir que la prueba electrónica tiende a informar al juez para que corrobore o contraste los dichos de las partes y de esa manera arribar a una conclusión sobre los hechos y en base a eso, dictaminar.

La prueba electrónica también es conocida como evidencia digital, para hacer referencia a cualquier tipo de prueba o evidencia que se presenta en el proceso legal en formato electrónico.

1.2) Características

La relación entre la prueba en el proceso penal y la tecnología es una discusión cada vez más notable y en constante evolución en el ámbito de la investigación y el derecho que requiere una comprensión sólida de los avances tecnológicos y su impacto en el sistema legal.

Para comprender la relevancia del primer acto de extracción de la prueba electrónica debe considerarse que la realidad diaria y la cotidianidad de las relaciones humanas se encuentran documentadas electrónicamente por cualquier tipo de comunicación digital.

Por ejemplo, una publicación en una red social, un mensaje de texto, o a través de Whatsapp, una fotografía, una filmación, un audio, ese gran universo probatorio digital se ha convertido en una importante fuente de prueba que puede ser introducida al proceso tendiente a demostrar un hecho controvertido o susceptible de investigación.

La prueba electrónica, por sus características, tiene una gran facilidad para desaparecer sin siquiera dejar algún rastro digital, otras aun fuera de nuestra espectro de visión, las podemos recuperar, recordando que siempre el autor del hecho algo deja o algo se lleva de la virtualidad.

Según Ferrer (2017), una buena estrategia para probar documentos electrónico no resulta del arte de la ciencia informática, sino del hecho de que el operador jurídico comprenda cómo funciona un determinado servicio, plataforma o aplicación donde el documentó electrónico se puede visualizar y/o gestionar y, a partir de aquí, diseñar la estructura probatoria que siempre debe incluir una pericia informática debido a que el objeto es informático. (p.10)

En ocasiones el documento electrónico es la prueba y el operador judicial debe acercarse cada vez más al conocimiento técnico del experto informático, por lo que sí sabe lo que busca, entonces indica e individualiza concretamente lo que debe

pedir al perito, es decir que el operador judicial cuando sabe lo que busca en términos de evidencia digital, comunica claramente sus necesidades al perito informático, esto permite que individualice y especifique qué información necesita para su teoría del caso.

En contraste con un testimonio donde el relato queda sujeto a la memoria o los recuerdos, la prueba que surge o está relacionada con aquella información contenida o transmitida electrónicamente, si se preserva y extrae rápidamente, con las garantías establecidas en nuestras normativas y con el mandamiento judicial correspondiente, el investigador podría inmortalizar un momento determinado que permita reconstruir el hecho que investiga.

1.3) Marco Regulatorio De La Prueba Y Documentos Electrónicos

La regulación de la prueba y documentos electrónicos se refiere a leyes, normativas o marcos establecidos para regular el uso de la misma en diferentes circunstancias.

Ley 25326 de 2000 marco legal que regula la de protección de datos personales o hábeas data, protege datos de identidad, de salud o de crédito cuando son usados sin tu consentimiento. La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes entre otros aspectos. 30 de octubre de 2000.

Argentina en el año 2000 dio el puntapié inicial en la región sobre legislación en materia de datos personales, incluyendo el consentimiento informado, la finalidad específica, la calidad de los datos, la seguridad de la información y la confidencialidad.

Las pruebas electrónicas pueden involucrar el manejo de datos personales y/o de la intimidad de los sujetos que aportan un documento electrónico que servirá para el proceso, por tal razón es importante garantizar que se respeten las leyes de privacidad y protección de datos.

La ley 25.506 de 2001 donde se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley. 11 de diciembre de 2001.

Como así también en la incorporación al Código Penal de la Ley 26.388 de 2008 denominada de delitos informáticos, agrega y define a los documentos electrónicos. 24 de junio de 2008.

La ley 26388 de 2008 con respecto a la definición de documento en su artículo primero dice que comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. 24 de junio de 2008.

La ley 26.685 de 2011 marco legal donde se autoriza la utilización de expedientes, documentos, firmas, comunicaciones, domicilios electrónicos y firmas digitales en todos los procesos judiciales y administrativos que se tramitan ante el Poder Judicial de la Nación, con idéntica eficacia jurídica y valor probatorio que sus equivalentes convencionales. 30 de junio de 2011

Los operadores judiciales y el perito deben conocer y manejar la prueba electrónica para realizar exitosamente en primera medida la preservación y luego la recuperación de la información que le va a permitir al juzgador comprender y valorar esa prueba.

Así como deben conocer el marco que regula los documentos electrónicos es necesario desarrollar otros aspectos fundamentales del proceso legal y son críticos cuando se trata de pruebas electrónicas, la autenticidad, la licitud e integridad de la prueba.

Hay que tener en cuenta para la valoración de la prueba electrónica que el juez no debe tener ninguna duda sobre la autenticidad, es decir que se considera genuino, legítimo y que puede ser verificado como tal, además que el contenido no ha sido alterado y que hayan sido obtenidos de manera lícita.

Entendiendo entonces cuál es la función del perito o el experto, y los nuevos desafíos investigativos a los que se enfrenta, y atendiendo que el juez necesariamente para valorar la prueba electrónica y evitar que desestime su consideración porque el perito no observó la autenticidad, integridad y licitud es necesario prestar atención a los aspectos desarrollados por IADPI, (s.f) sobre la prueba electrónica.

Autenticidad: la autenticidad, es la correspondencia entre el autor aparente y el autor real de un documento.

En el documento escrito la autoría puede acreditarse mediante la firma manuscrita o el sello comercial; en el documento electrónico, se identifica el ordenador desde el que se envía, pero no quien es su remite el ordenador desde el que se envía, pero no quien es su remitente, existiendo mayor facilidad para suplantar la identidad del remitente. Por el contrario, el documento electrónico no habilita a una efectiva identificación de autoría per se. Solo nos proporcionará los datos del dispositivo donde se ha generado y remitido.

Integridad: verificar la integridad e inalterabilidad del documento electrónico a través de un mecanismo certero que establezca la existencia o no de alteraciones de su estado original.

Haciendo una analogía con el sistema papel, en el documento escrito se pueden cotejar las modificaciones efectuadas a través de pruebas periciales. En cambio, en los documentos electrónicos, será necesario recurrir a una prueba pericial informática para establecer si esta prueba fue modificada, desde que dispositivo se produjo dicha modificación y que cambios fueron realizados.

Licitud: la licitud de la prueba se relaciona con la forma y modo de obtención de la fuente o el elemento.

Destacamos que estos elementos probatorios podrán ser llevados a juicio siempre que hayan sido obtenidos de manera lícita por quien la presenta, y que no sea de carácter confidencial, para cuyo caso es necesario el consentimiento del remitente.

Expuesto esto, es dable mencionar que si bien en nuestros instrumentos procesales no suelen encontrarse definiciones especiales sobre prueba electrónica o evidencia electrónica/digital, los magistrados podrían nutrirse de los conceptos definidos en las leyes existentes y aplicarlos por analogía.

Para finalizar este apartado entonces, y habiendo desarrollado el esquema procesal o marco legal, nos adentramos a las principales fuentes probatorias que en la actualidad representan un importante puente entre el derecho y la tecnologías, y que permiten dirimir conflictos o hechos controvertidos.

2) NUEVOS MEDIOS ELECTRÓNICOS

Seguidamente este estudio se centrará en aquellos medios electrónicos aportados como prueba con mayor frecuencia en las fiscalías. Para Bielli y Ordoñez (2019):

> Las distintas modalidades de comunicación pueden ser llevadas a juicio como prueba, siempre que la obtención de la misma se haya producido conforme a lo que establecen las mándales legales. Debe destacarse que estos elementos probatorios podrán ser llevados a juicio siempre que hayan sido obtenidos de manera lícita por quien la presenta. (p.147)

¿Pero si el que presenta la prueba es el titular del dispositivo que contiene dicha información, es parte de la comunicación sea como remitente o destinatario, podría cuestionar su legalidad?

En la actualidad existen un montón de supuestos en los que los hechos conducentes por los cuales se resolverá el fondo del juicio o pleito judicial, se presentan en soportes electrónicos y en diversos sistemas o plataformas de mensajería instantánea entre personas.

Para reforzar y avanzar en esta discusión para estos supuestos prácticos también debe considerarse la teoría del no repudio o irrenunciabilidad de la seguridad informática.

El no repudio es considerado uno de los principios fundamentales de seguridad de la información y hace referencia a la capacidad de afirmar la autoría de un mensaje o información, evitando que el autor niegue la existencia de su recepción o creación.

Existen dos tipos de no repudio:

En origen: consiste en garantizar que una persona envió un determinado mensaje. El remitente no puede negar que lo mandó, ya que el destinatario dispone de pruebas del envío.

En destino: avala que alguien recibió un determinado mensaje. El destinatario no podrá rebatir que no lo recibió porque el remitente cuenta con pruebas de la recepción.

Entonces podríamos decir que el no repudio se podría aplicar durante el proceso cuando una de las partes niega o desconoce haber recibido o enviado un mensaje, contando solo con uno de los dos extremos alcanzaría para demostrar de manera concluyente la existencia del mensaje.

Los medios electrónicos más habituales de acuerdo al delito que la fiscalía investiga pueden ser: conversaciones por mensajes de texto y aplicaciones de mensajería como whatsapp, messenger generalmente se presentan como evidencia en casos de acoso, amenazas, delitos contra la integridad sexual, violencia digital, etc.

Las fuentes probatorias surgidas de los correos electrónicos por ejemplo en casos relacionados con estafas, fraudes, delitos financieros, acoso, entre otros.

Los registros de llamadas pueden ser importantes en investigaciones criminales para establecer conexiones o vinculaciones entre personas involucradas en un caso, violación a una orden judicial en el marco de una restricción de acercamiento por ejemplo.

Publicaciones, mensajes y perfiles en redes sociales como Facebook, Twitter, Instagram, etc., pueden ser utilizados como evidencia en una amplia gama de casos, desde delitos relacionados con el discurso de odio, ciber bullying, hostigamiento y hasta casos de violencia doméstica.

Fotos, videos, grabaciones de audio y otros archivos multimedia pueden ser presentados como evidencia en casos que involucran violencia física, robos, acoso, entre otros.

Los autores Bielli y Ordoñez (2019) plantean que la informática forense tiene fundamentalmente cuatro etapas para el desarrollo eficaz de una diligencia forense: 1) La adquisición, cuya finalidad es la obtención del objeto, 2) La preservación refiriendo a la conservación del objeto, 3) La obtención, en la que se efectúan los exámenes y búsqueda de evidencia, y finalmente, 4) la presentación del informe donde se plasman los resultados obtenidos.

Y señalan que la prueba electrónica suele ir acompañada de metadatos que pueden desempeñar un papel importante como evidencia (p.ej., la fecha y hora en que se escribió un documento.

Dicho lo anterior se sugiere usar y manejar herramientas, métodos, programas o técnicas validadas y estudiadas, que permitan preservar la información contenida en un dispositivo o aquella que fue transmitida o generada por un medio electrónico, recordando que es muy volátil, irreproducible y susceptible de disiparse.

Luego, cuando a simple vista el documento electrónico no permite o habilita a una efectiva identidad de autoría, esta tarea es que la debe estar robustecida y apoyada en otras técnicas, tendientes a otorgarle una verdadera identidad a ese usuario virtual que enmascara su verdadera identidad.

El criterio técnico sin duda del experto o perito juega un rol muy importante a la hora de elegir los métodos de extracción de la información, ya que si bien existen métodos y software de alta capacidad de respuesta y éxito, la realidad es que en ese momento el técnico debe elegir cuál usarán.

En el caso de que se tratara de un hecho donde debe probarse un incumplimiento a una orden judicial (una restricción o prohibición de acercamiento) a una víctima de violencia de género por ejemplo, cuyo mecanismos de alerta (botón antipánico) se encuentran en el dispositivo de la denunciante, no será posible despojarse de esa medida de seguridad y protección por lo que es en ese momento donde el perito elegirá una técnica o método rápido y confiable y a su vez adecuada para la recuperación de la información contenida en el dispositivo.

Las herramientas modernas de procesamiento también pueden incluir software avanzados para la búsqueda y reconocimiento de elementos o de datos potencialmente relevantes o de interés para la causa.

Es esencial que los peritos y auxiliares de justicia se mantengan constantemente capacitados y actualizados en la investigación de eventos digitales. Esta preparación es fundamental para garantizar la integridad de las pruebas presentadas, sin alterar el estado original del documento, y aplicando la misma rigurosidad que se emplea para preservar cualquier otra evidencia.

2.1) Whatsapp

Según "Whatsapp" (2023) es una aplicación de mensajería instantánea propiedad de META que utiliza una versión personalizada del protocolo abierto extensible messaging and presence protocol (XMPP). Fue fundada por Jan Koum, ex empleado de YAhoo! quien fue contratado en dicha empresa en 1998 como ingeniero en operaciones y seguridad. La idea original de WhatsApp surgió cuando Koum, quien estaba lejos de su familia, encontró la manera de mantenerlos informados con las actualizaciones de estado.

Se lanzó oficialmente en enero de 2009 y hoy lidera las plataformas más usadas para comunicación. La popularidad responde por un lado a su simplicidad para su uso y por otro lado por la privacidad y seguridad de los usuarios Utiliza un protocolo de cifrado de extremo a extremo para proteger la privacidad de las conversaciones, lo que significa que solo los participantes en una conversación tienen acceso al contenido de los mensajes.

Whatsapp ha evolucionado significativamente desde su creación, incorporando nuevas funciones y mejoras para adaptarse a las necesidades de sus usuarios y mantenerse como una de las principales aplicaciones de mensajería en todo el mundo. Desde enviar mensajes de texto, imágenes, videos y audios hasta las últimas actualizaciones como comunidades, editar mensajes enviados por el usuario, canales, etc.

WhatsApp es una aplicación de mensajería gratuita que requiere un número de teléfono para registrarse a través de una conexión a internet. Para el empleo de esta plataforma se requiere contar con un número móvil de celular, que será vinculado a la cuenta de usuario de quien quiera acceder al sistema. Y aunque la aplicación se ejecuta desde un dispositivo móvil, también se puede acceder desde computadoras de escritorio o tablets por medio de WhatsApp Web.

Es decir que antes de participar en esta plataforma mediante la creación de contenido o mantener comunicación con otros usuarios, es esencial registrar una cuenta de usuario utilizando un número de teléfono móvil que quedará asociado o vinculado a la identidad digital.

Con este esquema, nos adentramos al punto donde pretendo llegar que es a este tipo de conversaciones aportadas al proceso y que son fuente de prueba.

Lo que se genera en una conversación mediante esta plataforma no es tan solo el intercambio de información, también se generan conflictos o pleitos, y cualquier tipo de contenido que coadyuva al hecho que deberá resolverse. Entonces en primer lugar el experto o el perito se encuentra frente al desafío de demostrar la autenticidad del documento electrónico. Esto implica verificar la fecha de creación, identificar al autor y asegurarse de que coincida con el emisor. Además, al investigador le corresponde realizar cruces de datos en diversas plataformas para recopilar información sobre las actividades, comportamiento y eventos del usuario, con el objetivo de construir un perfil virtual completo.

Dicho lo cual, se agrega que además de realizar tarea de buceo o exploración virtual en fuentes abiertas o herramientas forenses aplicables a este tipo de análisis de la cuenta, se deberá reforzar esta información sugiriendo o solicitando al fiscal medidas que encauce aún más la pertenencia real de esa identidad digital.

Como el usuario tiene una identidad digital asociada al número de línea, podría recabarse información de ese número utilizando herramientas para constatar a qué prestador de servicios tiene registrado esa línea, y así podría evitarse solicitar

informes a todas las empresas. En la Web de Enacom o en freecarrierlookup se puede constatar de forma online y gratis quién le presta servicio al número móvil que estamos analizando.

Cuando para acreditar los hechos que refiere una de las partes y fue motivante para la intervención del perito, presenta comunicaciones mediante sms (mensajes de texto), Whatsapp o llamadas entrantes al dispositivo puesto a disposición se deberá realizar las siguientes tareas: consignar número de teléfono vinculado a la cuenta de usuario y el código IMEI del dispositivo comunicacional, el número de teléfono vinculado a esa cuenta, compañía telefónica al cual se encuentra adherido.

En las comunicaciones mediante Whatsapp, previo a la comprobación de los datos del usuario de la línea y dispositivo objeto de la denuncia, también deberá realizarse las siguientes acciones: constatar el número de abonado asignado a ese contacto, la foto de perfil, la descripción en info, última vez de conexión, la confirmación de lectura, etc.

El documento electrónico también puede ser: un video filmado con el dispositivo puesto a disposición para su descarga y resguardo, en este caso además de las acciones ya descritas se deberá extraer las propiedades de esa filmación, día, hora, cámara que lo registra, geolocalización, etc.

Ocurre con frecuencia, la emisión de mensajes de texto gratis mediante plataformas web. En este supuesto, cada compañía debería proporcionar datos relacionados con esos números virtuales gratis, es decir, deberá solicitarle información relativa o tendiente a individualizar el usuario y autor de esos mensajes a la compañía de telefonía del abonado receptor de esos mensajes.

Continuando con el desarrollo del aporte de una comunicación mediante la plataforma de Whatsapp, una vez que se cuente con los datos registrales que a simple vista se observen o que se obtengan de las consultas en la web se procede a realizar la extracción y resguardo de esa información.

Dado que se trata de un aporte voluntario que una de las partes ofrece al proceso, y el objetivo es obtener un fragmento de comunicación o una imagen específica de la galería, no sería necesario someter al dispositivo a una extracción forense mediante herramientas especializadas para estos fines. Entonces, en resumen, si las condiciones son favorables, como el tipo de dispositivo y su estado, si las comunicaciones son claramente visibles y fácilmente identificables por la parte interesada, no sería necesario extraer toda la información del dispositivo con herramientas forenses como el UFED las cuales están diseñadas para extraer toda la información. En su lugar, el perito deberá enfocarse únicamente en los datos necesarios sin la necesidad de un proceso de extracción completo.

Ahora bien, qué aspectos se deben observar para admitir esta fuente probatoria. En primer lugar se desarrollará la Autenticidad, como lo explica Cervello Grande (2000) refiriendo que en el documento escrito, la autoría puede acreditarse mediante la firma manuscrita o el sello comercial; en el documento electrónico se identifica el ordenador desde el que se envía, pero no quien es su remitente, existiendo mayor facilidad para suplantar la identidad del remitente.

Y entiendo al igual que Bielli y Ordoñez (2019) que "El documento electrónico no habilita a una efectiva identificación de autoría *per se* sólo nos proporcionará los datos del dispositivo donde se ha generado y remitido". (p.553)

Es así que nos encontraremos en la necesidad de demostrar la autenticidad de este documento electrónico, siendo que dicha tarea se tendrá que canalizar a través de la verificación de sus atribuciones ligadas, como la fecha de generación, identificación de su autor, si la persona generadora y el emisor coinciden.

Basándonos en lo expuesto en los párrafos anteriores, podemos concluir que los mensajes de Whatsapp pueden ser utilizados para atribuir su autoría con el número de línea vinculado a la cuenta, el número de la SIM, el IMEI del dispositivo del cual se desprenden las comunicaciones susceptibles de análisis, además de complementarse con tareas inherentes a la investigación forense, como la exploración en fuentes abiertas.

En lo que respecta a la integridad del documento electrónico, en este caso la fuente de prueba consiste en comunicaciones o información que provienen de la plataforma de Whatsapp, se debe garantizar su inalterabilidad a través de algún método o técnica que permita detectar alteraciones o modificaciones. En otras palabras, implica asegurarse de que el documento permanezca completo y sin cambios a lo largo del tiempo y a través de los diferentes estadios del proceso.

Una vez que se extrae el contenido que será presentado en el proceso, es posible proteger el archivo contra cambios o modificaciones mediante técnicas como el hashing. Esto implica calcular el hash del archivo y proporcionar de manera segura en el informe.

Si alguien modifica el archivo, el hash resultante será diferente al original, lo que indicará que el archivo ha sido alterado.

Otra alternativa podría ser la de cifrar el archivo con un código sólido y que solo las personas que deban tener acceso a ese archivo cuenten con la clave.

Es posible también proteger el archivo con permisos de acceso, es decir configurar permisos para el acceso a los archivos o carpetas, limitando de esta manera quién puede ver, modificar o eliminar el archivo.

Habiendo transitado hasta acá este camino, es posible describir en consonancia con los autores citados que la licitud de la prueba electrónica se basa en varios aspectos y se relacionan con la forma y modo de obtención de la fuente o del elemento.

La evidencia digital para que cumpla con la exigencia de la legalidad debe haber sido obtenida de acuerdo con las leyes y regulaciones aplicables. Esto implica que cualquier método utilizado para recolectar la evidencia, como el monitoreo de comunicaciones, la obtención de datos de dispositivos electrónicos o la adquisición de registros electrónicos, debe cumplir con las leyes de privacidad y protección de datos.

También se debe garantizar que la evidencia digital no ha sido manipulada o

alterada de ninguna manera desde su obtención hasta su presentación o devolución en el tribunal. Es crucial mantener la integridad de los datos digitales para asegurar su validez como prueba.

Al igual que la prueba que surge del análisis de una evidencia física, se debe documentar cuidadosamente la cadena de custodia de la evidencia digital para demostrar quién tuvo acceso a la misma en cada etapa de su recolección, almacenamiento y análisis. Esto ayuda a garantizar su autenticidad y confiabilidad.

La prueba electrónica también debe ser pertinente, es decir debe ser relevante y se deben establecer conexiones claras entre la evidencia digital y los aspectos del caso o hecho en estudio.

Los metadatos asociados con la evidencia digital, como la fecha y hora de creación, modificación o acceso, son importantes para su contexto y autenticidad. La preservación de estos metadatos es crucial para mantener la integridad de la evidencia, y por último la pericia informática realizada por expertos o por peritos forenses para validar la autenticidad e integridad de la evidencia

En resumen, la licitud de la evidencia digital se basa en cumplir con los mismos estándares de legalidad, integridad, autenticidad que se aplican a la evidencia física, pero con consideraciones específicas relacionadas con la naturaleza digital de la evidencia.

Bielli y Ordoñez (2019) desarrollan que la protección otorgada a la correspondencia tradicional se puede hacer extensiva a las comunicaciones electrónicas sean los que surgen de un correo electrónico, por mensajería instantánea, así todas las formas de comunicación estarían amparadas por las mismas garantías constitucionales que se aplican a la correspondencia escrita ya que estos elementos probatorios podrán ser llevados a juicio siempre que se hayan obtenido de manera lícita, por quien la presenta.

De ser admitida es necesario establecer que no se vulnera el derecho fundamental a la intimidad, coronado en nuestra Constitucional Nacional en su

artículo 19, o también la garantía de inviolabilidad de la correspondencia, establecida en el artículo 18.

Coincido con los autores en la idea de que tanto la correspondencia tradicional como las comunicaciones electrónicas deben disfrutar de las mismas garantías de inviolabilidad y respetar el derecho a la intimidad. Esto implica aplicar de manera análoga estas protecciones a las comunicaciones virtuales asegurando que estén resguardadas contra el acceso no autorizado, la interceptación, la manipulación o el uso indebido por parte de terceros. En resumen, es fundamental que las comunicaciones electrónicas estén resguardadas de manera similar a como se protege la correspondencia física, garantizando así la privacidad y seguridad de los usuarios.

2.2) Correos electrónicos:

Una de las publicaciones científicas que utilicé como referencia para desarrollar esta sección es el trabajo de Bellorini (2013), que se centra en el estudio de documentos electrónicos, con un enfoque especial en cuestiones relacionadas con la autenticidad y el valor probatorio del correo electrónico. Este trabajo proporcionó una base sólida para abordar este aspecto, respaldado por la investigación de esta autora entre otros.

Correo electrónico se define como el "sistema de transmisión de mensajes por computadora u otro dispositivo electrónico a travé de redes informáticas" (Real Academia Española, s.f., definición 1 m)

La Comisión Nacional de Comunicaciones (2001) define al correo electrónico como "toda correspondencia, mensaje, archivo, dato u otra información electrónica que se transmite a una o más personas por medio de una red de interconexión de computadoras". (p.3)

El mensaje de correo electrónico es un documento electrónico que a su vez pertenece al género de los documentos en general. Será documento electrónico todo aquel documento elaborado por medio de una computadora, mediante el uso de técnicas informáticas

El correo electrónico no es más que una manera de intercambio de mensajes entre personas, pudiendo enviar documentos, archivos e información y podrán ser aportados al proceso cuando se quiera probar un hecho u acto jurídico.

Las principales características del correo electrónico (Vives, 2007) son: asincronismo (no necesita sincronía en envío y recepción); ubicuidad (permite su acceso en diferentes lugares); digitalización (utiliza información digitalizada).

Descriptos los significados del correo electrónico, es posible decir entonces que se asemeja al intercambio de correspondencia epistolar, pero a través de un medio electrónico.

Como dice Somer (2004), es innegable que en mayor o menor medida ninguna Nación escapa a este proceso. Este término inicialmente se vincula principalmente con lo económico, pero se extiende a diversos aspectos de nuestra vida cotidiana, incluyendo lo social, cultural, ideológico, político, científico y tecnológico. Actualmente, nos encontramos inmersos en un "microcosmos electrónico", donde el uso generalizado de internet permite que una persona en cualquier parte del mundo pueda comunicarse instantáneamente con otras ubicadas en cualquier otro lugar del planeta.

Y siguiendo en la misma dirección que estas reflexiones se agrega, que cuando tratamos a los correos electrónicos como fuente de prueba, nos encontramos ante un elemento probatorio de carácter indiciario y complejo, dado que requiere de una producción conexa y acumulativa de pruebas para verificar su veracidad, integridad, autoría y contenido, con el objeto de que pueda procurar formar convicción en el juez.

Bielli (2018) refiere que los correos electrónicos constituyen una fuente de prueba, ya que a través de esta metodología de comunicaciones generadas por vía electrónica, se produce un intercambio de información. Se originan controversias y se crean contenidos que podrían ser importantes para demostrar algo en un proceso a fin de crear la necesaria convicción hacia el juzgador sobre la ocurrencia o no de un hecho

controvertido.

Coincido con ambos autores, el flujo de comunicación y el intercambio de información que se genera en un correo electrónico, podrá ser presentado durante el proceso ya que tanto el correo postal como el correo electrónico son dos maneras distintas de comunicación entre un receptor y un emisor del mensaje, lo que varía claramente es el medio que se utiliza.

Y como explica Vives (2007), los mensajes de correo electrónico agregan, a la sencillez y comodidad de uso, la imagen de certeza que transmite la palabra escrita.

Bielli y Ordoñez (2019) exponen que una vez cumplida con las constataciones delineadas, se podrá sostener que el envío y recepción de distintos documentos electrónicos a través de plataformas de correo, tales como archivos, fotografías, videos son susceptibles de ser valorados como elementos probatorios en un proceso judicial, bajo la premisa de que cualquier evidencia electrónica puede corroborar un hecho o situación derivada del intercambio de mensajes e información dirigidos o enviados a un individuo.

La autoría gráfica o el patrimonio escritural de quien estampa una firma en un documento dudoso puede ser establecida mediante una pericia caligráfica, de esa manera se determina si es genuina o apócrifa. Sin embargo, cuando se trata de un correo electrónico o mail, el enfoque para establecer la autoría puede diferir debido a la naturaleza digital del medio. En un correo electrónico o mail se requiere un enfoque más amplio que tenga en cuenta aspectos técnicos y digitales para determinar la autenticidad y la autoría.

Gallo (2016) refiere que en materia de correos electrónicos, ciertamente deberemos establecer dos pilares apuntaladores de la fuente, que serán la respectiva autoría, autenticidad e integridad de los contenidos intercambiados, a fin de procurar convicción sobre los mismos.

Y también describe que la autenticidad se prueba con la identificación del remitente constatando nombre de usuario, cuenta de correo y dirección, la trazabilidad

es decir los diferentes servicios o agentes que intervienen en la comunicación y los datos del remitente.

Es así que se deberá constatar los datos del remitente de la cuenta de correo y dirección IP, la presencia del documento electrónico en el dispositivo emisor y/o en el servidor del ISP del emisor, la trazabilidad, analizar el destinatario, su nombre de usuario, cuenta de correo y dirección IP y el contenido.

Además la experiencia iindica que se pueden implementar diferentes técnicas para verificar la autenticidad y la autoría:

Los correos electrónicos poseen metadatos como por ejemplo la dirección IP del remitente, la hora y la fecha de envío. Además, el examen del contenido de un correo electrónico, el estilo de redacción, el lenguaje empleado y el contexto, podría proporcionar indicios sobre su origen y el remitente involucrado. También considerar que las cuentas de correo electrónico suelen estar vinculadas a dispositivos móviles a efectos de enviar mensajes de confirmación o bien, para el recupero de contraseñas, en el caso de que estas sean olvidadas, perdidas o bloqueadas por sus usuarios.

Quadri (2015) dice que "la doctrina ha considerado que, si un determinado documento fue enviado desde una cuenta de correo electrónico que está vinculada a una persona física o jurídica por su nombre de usuario y la denominación del servidor, ello constituirá un indicio grave en contra de esa parte, acerca de la autoría de los contenidos". (p. 696)

Bielli y Ordoñez y (2019) explican que se bien es cierto y real que en ocasiones coinciden los nombres con la denominación del usuario que posee la cuenta de correo electrónico, para la identificación digital efectiva o la identidad real del titular es necesario recurrir a otros elementos probatorios para determinar la autenticidad de las comunicaciones y un análisis más exhaustivo a los fines de obtener información del ISP, del dominio, realizar una pericia informática, etc ya que nada impide que una persona pueda crear una cuenta con otro nombre.

Coincidiendo con estos autores, la pericia informática sobre los mails puestos

a disposición, podría contribuir a dar respuesta sobre la autenticidad y la integridad de un correo electrónico cuyo contenido puede constatar la ocurrencia de hechos o de un acto jurídico generado mediante el intercambio de un mensaje o de un archivo.

Una dirección de correo electrónico se compone de un nombre de usuario, el signo @ y el dominio detrás. La información pública asociada a ese dominio se puede ver por ejemplo a través a través a cualquier servicio público de WHOIS, en su página www.whois.com, en este sitio webs cuyos contenidos son libres es posible obtener información del dominio bajo el cual se creó el correo electrónico.

También es posible obtener más información sobre la identidad digital de un correo electrónico ya que se usan en la asociación y vinculación de dispositivos electrónicos a cuentas en línea, proporcionando datos validados de identidad digital.

Solicitar a la empresa proveedora del dominio información relacionada con la dirección IP, datos de conexión o logins. Conociendo ese dato puede solicitarse con una orden judicial a la ISP que provee del servicio de internet los registros de tráfico respecto de su cliente para ir desentramando la identidad digital del correo electrónico como así también datos registrales de su cliente.

Conforme a lo desarrollado en este apartado sostengo que identificar o individualizar la autoría del contenido invocado en torno a un pleito judicial es posible mediante la investigación forense y de los procedimientos técnicos que se utilicen ya que de los datos obtenidos permitiría acreditar los hechos manifestados. Aun así es importante destacar que esta fuente probatoria como las descritas en este trabajo, se robustecen al analizar en forma integral todo el caudal probatorio en torno al hecho que se investiga, siendo positiva su valoración dentro de un conjunto de probanzas o medidas indiciarias**.**

2.3) Contenidos En Redes Sociales

Bielli y Ordoñez (2019) en su capítulo sobre redes sociales en general definen a las plataformas de internet como facilitadoras de intercambio de comunicaciones entre individuos de una misma estructura social denominándose redes sociales

virtuales.

También puede definirse como un espacio digital que permite a los ciudadanos compartir información personal a través de imágenes y videos.

Por su parte Quadri (2015) sostiene que "se ubican en un espacio digital que permite aglomerar gran cantidad de información de cada uno de los usuarios, a la vez que ofrece la oportunidad de intercambiar entre ellos, todos aquellos elementos que se deseen compartir". (p.630)

Y Veltani (2012) describe y asocia a la red social como plataformas de intercambio de mensajes sumamente favorables para la comunicación inmediata, otorgando opciones a los ciudadanos para que puedan transmitir de manera privada mensajes escritos, notas de voz, archivos de audio y de video, imágenes y fotografías, y en general, cualquier tipo de documento electrónico.

Dicho lo cual se puede decir que una red social es una plataforma online que permite crear perfiles o usuarios y mantenerse comunicados o conectados intercambiando mensajes en forma de audios, videos o simplemente de texto. Estas plataformas facilitan la interacción entre personas con intereses similares, ya sea a nivel personal o profesional.

Facebook es una de las redes más populares y pionera ya que dio lugar al surgimiento de otras plataformas, es propiedad de META y cuenta con más de 2.320 millones de usuarios registrados en todo el mundo

Una de las características de esas redes es que los usuarios tienen la capacidad de configurar la privacidad de su perfil y contenido según sus preferencias. Esto les permite controlar quién puede ver su información, sus publicaciones y actividades. También se puede restringir el acceso al perfil, limitar quién puede ver publicaciones o establecer permisos de privacidad aún más estrictas para mantener conversaciones privadas.

En cuanto a una característica que tiene por ejemplo Facebook de acuerdo a

la descripción que Bielli y Ordoñez (2019), es que el contenido vertido en redes sociales no es generalmente estático. Cuando una persona accede a su perfil, la aplicación genera lo que ve en función de sus acciones, interacciones con otros usuarios y datos proporcionados, siguiendo las normas y preferencias del consumidor. Además, la esencia de las redes sociales se resume en una palabra: compartir.

La accesibilidad de Facebook ha llevado a que las personas lo integren en su vida diaria, ya que les permite compartir sus experiencias de manera constante, pero también se emplea para difamar, acosar, hostigar e incluso se utiliza como medio para la comisión de un delito.

En un supuesto práctico donde el motivo del aporte fuera una publicación en una red social, deberán además arbitrarse todos los mecanismo de solicitud de preservación de datos de las cuentas en cuestión, consignando correctamente (Url, ID) la identificación del usuario o perfil, fecha y hora, aclarando que esta medida salvo que se solicite la extensión del plazo, será por el término de 90 días, por lo cual antes de su caducidad, se deberá solicitar mediante los mecanismos jurídicos específicos, información de datos registrales de la cuenta.

Y es que cuando se comparte una publicación en una red social, su impacto y expansión pueden ser significativos dependiendo de varios factores, como la calidad del contenido, el alcance de las conexiones y de la participación que genera. Una publicación bien recibida puede alcanzar a una amplia audiencia a través de acciones como compartir o darle "me gusta", lo que puede generar un efecto de amplificación y aumentar su visibilidad, alcanzando la visualización de miles de usuarios.

Al momento de crear una cuenta en la plataforma de Facebook es necesario ingresar datos de registración que luego serán de interés en el supuesto que se requiera información de un perfil desde el cual se viraliza una noticia falsa o una manifestación de odio o desde el cual un adulto se comunica con un menor con intenciones claramente sexuales.

Esos datos vinculantes a la identidad digital del usuario son por ejemplo el nombre y el apellido del titular de la cuenta, correo electrónico y número de celular los cuales son validados, es decir, se confirma la autenticidad de la dirección de correo electrónico o número de celular proporcionada por el usuario durante el proceso de registro o creación de una cuenta. La validación del correo electrónico es un paso importante para asegurarse de que la dirección de correo proporcionada realmente pertenece al usuario que está intentando registrarse y de esa manera se confirma que no está utilizando una dirección de correo electrónico falsa o inválida. Dicho esto, en el marco de una investigación al solicitar estos datos registrales a META permitirá acercarse al usuario real de la cuenta ya que los datos que la plataforma requiere para su creación deben ser validados para confirmar su identidad digital.

Una vez creada la cuenta los usuarios también pueden personalizar el perfil, es decir describir preferencias, lugar de residencia, ocupación, estado civil. También es posible configurar la privacidad del perfil para que el público en general tenga acceso a esos datos y a su lista de amigos, fotos, publicaciones.

Lo cierto es que si bien la red social Facebook permite que las personas puedan conectarse, compartir publicaciones y contenido, mantenerse informadas y entretenerse, en la actualidad y desde hace unos años, esta plataforma permite enmascarar la identidad de un usuario y crear perfiles falsos para lograr la comisión de un delito.

Es en esos casos cuando el investigador tiene que lograr inmortalizar esa publicación o comunicación usando técnicas de preservación de la cuenta denunciada, como primer paso.

Para esas situaciones META tiene un portal de requerimientos legales para las fuerzas de la ley, donde permite solicitar que los datos de una cuenta sean preservados o congelados y requerirles luego, aun cuando esta se haya eliminado o dado de baja.

Esto permite al investigador, ganar tiempo hasta que se obtenga una orden legal para solicitar datos registrales y de conexión de la cuenta, ya que conociendo estos datos permitiría acercarse a la identidad real de quien realizó la publicación o envió un mensaje.

Las circunstancias desarrolladas en el presente trabajo, permite afirmar sin lugar a dudas que el investigador, sea las fuerzas de seguridad, el informático o criminalista que intervenga en la extracción de la prueba digital cuenten con los conocimientos especiales para no contaminarla y las herramientas forenses necesarias a los fines de asegurar la recolección pertinente, la extracción correcta y la preservación adecuada.

3) MECANISMOS, ETAPAS Y HERRAMIENTAS DE EXTRACCIÓN Y PRESERVACIÓN

La finalidad del aporte de una prueba electrónica al proceso y que ésta se introduzca a través de un informe pericial garantiza la originalidad, la autenticidad e integridad de la información que se presenta como evidencia digital. Por lo tanto será muy útil en los casos donde exista un gran volumen de información a extraer y analizar o bien cuando la prueba electrónica es la principal o incluso en algunos casos, la única disponible.

Es aquí donde el especialista o el perito debe recabar toda la información alojada o contenida en el dispositivo electrónico puesto a disposición, cuyos resultados los plasmará en un informe pericial el cual contendrá las operaciones realizadas y a la conclusión que arribó.

Dicho esto, los peritos o expertos designados serán los encargados de analizar la evidencia digital aportada por las partes con la finalidad de dilucidar el marco conflictivo.

De acuerdo a las experiencias recolectadas, colegas de otros Ministerios Públicos y la propia, es posible identificar 4 etapas o momentos del aporte de una prueba electrónica en cuanto a su tratamiento técnico pericial.

La primera consiste en la recepción del elemento de prueba.

En esta etapa el perito realiza un examen extrínseco del dispositivo que contiene la prueba electrónica y describe las características que observa como por ejemplo, marca y modelo, color y estado general, acto seguido deberá contrastar si estas circunstancias son coincidentes con el objeto de prueba y la descripción que realiza la fiscalía o juzgado.

Es fundamental que se coteje el contenido de la orden judicial como así también el elemento que se pone a disposición para verificar que exista una

correspondencia entre lo que se recibe y lo que refleja el oficio.

Una manera de inmortalizar o fijar el estado en que se recibe el elemento es con fotografías que serán agregadas al informe a los fines de demostrar y documentar todos los pasos que se realizaron desde el momento de la recepción del mismo. Es habitual la filmación como método de fijación en algunas dependencias de diferentes Ministerios Públicos del país.

Acto seguido, el perito deberá individualizar la información que se aporta a la causa y procederá a la extracción u obtención de la misma.

Si bien este trabajo está orientado a la prueba electrónica que se aporta al proceso siendo las más comunes aquellas que surgen por ejemplo de una conversación a través de Whatsapp, Messenger, una publicación en una red social o de un correo electrónico es factible también que por la complejidad o el tamaño de la información a extraer el perito deberá estimar la utilización de software y hardware específicos a fin de salvaguardar la integridad de la prueba. El perito preserva la información que se encuentra alojada en el dispositivo que actúa como contenedor del objeto de pericia, para evitar la pérdida o alteración de la información.

Ahora bien, identificada la información sujeta a extracción, el perito elegirá de acuerdo a lo que observa que técnicas o métodos utilizara.

En Whatsapp si las conversaciones o chats tienen un límite temporal, está relacionada con un número reducido de usuarios y se encuentra visible es posible llevar adelante la siguiente tarea:

WhatsApp permite hacer copias de seguridad en la nube como Google Drive (en Android) o iCloud (en iOS).

Entonces en el supuesto que la información a extraer no está visible, se podría instalar la aplicación en el mismo dispositivo y con la misma cuenta de Google o iCloud según corresponda, levantar y/o restaurar las últimas comunicaciones siempre y cuando fueran anterior a la copia de seguridad.

Si las comunicaciones están visibles y no son tan extensas la plataforma ofrece la posibilidad de exportar el chat. Seleccionando el chat en cuestión sobre los tres puntitos del extremo superior derecho, opción más y exportar chat.

Esta conversación se exporta en formato TXT y las imágenes y videos van en archivo separado del texto plano de la conversación. Esta es una opción amigable y permite enviarla por correo electrónico y en caso de no tener internet se puede exportar por bluetooth.

Si la información aportada se trata de un chat de messenger es posible realizar las siguientes técnicas de recuperación: Desde la aplicación del mismo dispositivo, el aportante va a la conversación que se desea extraer, manteniendo presionado el dedo sobre el mensaje o la conversación identificada, y selecciona la opción “guardar” o “guardar chat”.

Dependiendo del dispositivo y la versión de la aplicación, es posible que también pueda exportar el chat como archivo de texto o enviarlo por correo electrónico.

En el supuesto que el aportante se presenta en las oficinas periciales sin el dispositivo, se puede facilitar una computadora para que ingrese a su perfil desde la versión web de Messenger y desde ahí elige la conversación que desea extraer, luego cliquea sobre el icono de engranaje en la esquina superior derecha de la ventana de chat, selecciona la opción "más" y luego "descargar".

El chat se descargará como un archivo HTML que se puede abrir con cualquier navegador web.

Es interesante remarcar, que en estas situaciones donde el aportante voluntario de una prueba electrónica nos permite acceder a una comunicación, fotos y/videos o publicaciones, al igual que con Whatsapp, es importante respetar su privacidad y obtener el consentimiento de las personas involucradas antes de extraer y compartir las conversaciones, como peritos debemos limitarnos a extraer solo el objeto de pericia identificado o individualizado por la parte aportante de la prueba.

El perito asignado deberá extraer la comunicación en pleito, mediante técnicas de recuperación forense o a través de los diferentes programas pagos o incluso aquellos libres existentes en la web o propios de la plataforma en cuestión que por sus características técnicas permite exportar estos archivos y resguardarlos como los descriptos hasta aquí.

Brevemente se desarrollarán otros métodos o técnicas de extracción que se usan y se conocen en la actualidad en los Ministerios Públicos del país.

El UFED es una herramienta de extracción forense que de acuerdo a los modelos de los dispositivos y la información que se pretenda extraer permite obtener buenos resultados.

Se trata de una herramienta forense digital desarrollada por la empresa Cellebrite que se utiliza para extraer y analizar datos de dispositivos móviles y otros dispositivos electrónicos como tablets, tarjetas de memoria, etc. El UFED es utilizado por distintas fuerzas policiales, profesionales de gabinetes periciales para investigaciones criminales, análisis forense y recuperación de datos. Ofrece capacidades para extraer una amplia gama de datos, incluyendo llamadas, mensajes de texto, correos electrónicos, contactos, imágenes, vídeos, registros de llamadas, ubicaciones GPS, aplicaciones instaladas y otros datos almacenados en dispositivos móviles.

El UFED es una herramienta potente y robusta muy requerida por sus resultados. La cantidad de causas que requieren este tipo de extracción forense, sobrepasan la capacidad técnica y operativa de los laboratorios forenses del país, por lo tanto suele ser una pericia que puede demandar mucho tiempo de espera.

En la actualidad casi todas las causas tienen evidencia digital, las cuales en su mayoría de acuerdo a la complejidad de la causa y de las medidas llevadas adelante por las fiscalías, son las que surgen de una orden de allanamiento y secuestro de dispositivos electrónicos. En ese contexto los efectos secuestrados suelen ser numerosos y en algunas oportunidades impertinentes.

Entonces este tipo de tecnología forense para extracción de información contenida en un dispositivo, se podría reservar para causas donde por las características del efecto, de la información, del volumen y de la urgencia entre otras, requiera un tratamiento y procesamiento especial.

En todos los casos, independientemente de la técnica o método, el perito deberá identificar el archivo o la información a extraer y luego deberá realizar una copia del mismo para su posterior análisis y búsqueda si fuera el punto de pericia, y si no, se deberá resguardar el archivo obtenido en su estado original, generando y certificando la originalidad e inalterabilidad a través de un código hash, es decir el archivo generado en la exportación o en la extracción de la prueba se le deberá consignar el nombre o identificación original que le da el programa, extensión, o plataforma exportadora, y sobre cada uno de esos archivos logrados, se obtendrá su huella hash, es decir el ADN del documento generado.

El experto informático trabajará sobre la copia, ya que en el proceso de análisis, puede ocurrir que se altere, modifique y por consiguiente pierde su estado original, al igual que en el tratamiento de una muestra biológica, se estudia sobre una muestra, para que de ser necesario y solicitado se pueda repetir el análisis.

Una herramienta usada para casos de aportes voluntarios de una prueba electrónica se denomina Espejo Chubut, consiste en un sistema desarrollado por el Departamento de Informática Forense de los Equipos Técnicos Multidisciplinarios de la Procuración General de la provincia de Chubut, Argentina. Ministerio Público Fiscal de Chubut [MPF]. 2023)

Se trata de una herramienta diseñada para realizar capturas en forma de imágenes o video en tiempo real de la pantalla de dispositivos Android conectados mediante USB, no genera archivos en el dispositivo, solo espeja la pantalla.

El programa Espejo es un desarrollo argentino y en resumen lo que hace este tipo de herramientas es capturar imágenes de lo que se pretende aportar, validando

dicha información generando un código hash

En el manual que proporciona la Procuración General de la Provincia de Chubut se establecen ciertas condiciones para el uso de la herramienta que los peritos deben saber para operar con este programa.

Antes de iniciar el programa de captura se debe habilitar el "Modo Desarrollador" en el teléfono aportado y la conexión del mismo a la computadora a través de la activación de la "Depuración USB". Para iniciar este modo (que puede variar de un modelo a otro de teléfono) normalmente se debe acceder primeramente a las configuraciones y ajustes del aparato. Posteriormente al apartado "Acerca del teléfono" e "Información de software", luego teniendo en vista el acceso "Número de compilación", tocar el mismo siete veces hasta activar el "Modo desarrollador". Se debe acceder al apartado desbloqueado "Opciones de desarrollador" o similar. Activar el mismo y la denominada "Depuración de USB". En estas condiciones ya se puede iniciar el programa de captura para el dispositivo aportado.

Otra herramienta de España usada para este tipo de pruebas aportadas contenidas en un dispositivo se llama Pandora, es un programa similar a Espejo, y se trata de un Software realizado por la unidad I+D+I: Escolta Digital. Es una herramienta para las investigaciones y certifica lo que hay publicado en la web en un determinado tiempo como así también capturar conversaciones o todo aquello que se encuentre en el dispositivo y que sea de interés.

Según (Escolta Digital, s.f.) PANDORA protege las evidencias para ser utilizadas en sede Judicial, permite la recopilación de evidencias para un traslado posterior a los juzgados con plenas garantías y poder demostrar su autenticidad. Las evidencias se almacenan cifradas con las máximas garantías con algoritmo criptográfico SHA256 para cumplir con la cadena de custodia necesaria en los procesos judiciales.

Se trata de un Software realizado por especialistas con amplia experiencia en el campo de la ciberinteligencia e informática forense by Escolta Digital.

3.1) Modelo De Presentación De Informe

Volcar en un dictamen las operaciones realizadas, los fundamentos en los que se basó el experto y a las conclusiones que arribó será también de gran importancia. El perito o investigador no debe olvidar que un dictamen debe ser COMPLETO, CONCISO, CORRECTO Y CONCRETO.

El informe o dictamen deberá contener la descripción detallada de las pruebas electrónicas aportadas por las partes interesadas, la fijación del momento en que se recepcionaron los elementos denotando el estado en que se recibieron, así como la descripción minuciosa de las tareas u operaciones realizadas. Además, se requiere un fundamento técnico y científico en el que se basa para arribar a las conclusiones.

El dictamen o informe pericial deberá contener un encabezado de presentación, (nombre, apellido, función del perito designado y los autos caratulados) el objeto de pericia (transcribirá textualmente los puntos de pericia a dilucidar), los elementos ofrecidos (en este aparato podría describirse el estado general o una descripción que surja de la observación extrínseca de los elementos puesto a disposición para peritar) los fundamentos técnicos o científicos (describir en que se funda científicamente para dar respuesta a los solicitado como punto de pericia y además explicar los alcances de la ciencia criminalística o informática forense para resolver estas cuestiones) operaciones realizadas (desarrollar la tarea pericial, describiendo paso a paso los métodos, técnicas, es el núcleo de la pericia) conclusiones (categóricas, claras, y si la respuesta fuera muy extensa se puede observar y remitir al punto de pericia desarrollado ut supra) se cierra el dictamen, con una elevación de la actuación y devolución de los elementos que le fueran concedidos para peritar o en préstamo.

Al momento de pretender probar un hecho con un documento electrónico aportado, será necesario incorporarlo con un dictamen pericial realizado por un experto en la materia para que pueda brindar la información necesaria dentro de un proceso. Es necesario entender que la prueba electrónica sin importar el formato en el que esté contenida, su incorporación correcta al proceso permitirá que ningún efecto

esencial se pierda o pierda valor probatorio.

Bielli (2021) refiere que la finalidad del aporte de una prueba electrónica mediante un informe pericial permite resguardar las garantías de originalidad, autenticidad e integridad de la información obtenida.

Darahuge (2016). Expresa que:

> En cuanto a los recaudos de la pericia, la misma deberá contener la explicación detallada de las operaciones técnicas realizadas y de los principios científicos en que se funde (art. 472, Cód. Proc. Civ. y Com.); la doctrina señala que los deberes impuestos al perito implican: 1. descripción clara y precisa de lugares y oportunidades de recolección de la prueba; 2. de ser necesaria descripción, con documentación fotográfica y planimétrica de los locales inspeccionados y la ubicación física de los lugares de acceso a la prueba; 3. descripción exhaustiva de los equipos informáticos involucrados en la tarea, en lo posible con sus especificaciones técnicas; 4. Descripción exhaustiva de los programas utilizados para realizar la tarea; 5. Explicación detallada de las relaciones detectadas entre los componentes descritos; 6. elementos entregados al experto por parte del tribunal para realizar la pericia; 7. Si estos elementos son entregados sin la correspondiente cadena de custodia, dicha circunstancia se debe indicar de manera explícita, para deslindar responsabilidades por parte del experto.(p.69)

(Morales Vallez, s.f) dice que los mensajes de Whatsapp la tarea del perito radica en el análisis del dispositivo suministrado por las partes, determinar que el contenido almacenado no ha sido objeto de alteración o manipulación y poseer los conocimientos pertinentes en la materia, emitir dictamen sobre los "hechos o circunstancias relevantes en el asunto o adquirir certeza sobre ellos.

Y al respecto sobre el perito informático (Picón Rodríguez, s.f) escribe que dispone de conocimiento y herramientas necesarias para extraer el contenido original

del dispositivo como así también para certificar y mantener la cadena de custodia de esta prueba, es decir que un perito informático se encarga de 1) extraer conversaciones originales de WhatsApp (o cualquier otra aplicación), 2) certificar y 3) custodiar la cadena de custodia.

En este apartado desarrollado comparto la opinión de estos autores cuyas ideas son relevantes en esta investigación, además se agrega que el informe o dictamen de un experto es crucial dentro del proceso porque, proporciona conocimientos técnicos y especializados en cuestiones específicas que están más allá del alcance del conocimiento de la fiscalía o del juez, ayuda a aclarar un hecho complejo y puede respaldar una decisión judicial al proporcionar una opinión objetiva y fundada sobre aspectos técnicos o científicos, ya que los expertos deben mantener la imparcialidad y ser neutrales en su evaluación, esto le da robustez y credibilidad a sus conclusiones.

4) ADMISIÓN Y VALORACIÓN DE LA PRUEBA ELECTRÓNICA

A lo largo de este camino transitado se observa que no existen pautas concretas y específicas para encuadrar la admisibilidad que tienen las pruebas electrónicas aportadas y su fuerza probatoria, ya sea legislativamente, es decir normativa específica que regule su ofrecimiento y producción, o desde la perspectiva de la práctica judicial, en razón de una falta de conocimiento certero acerca la prueba electrónica y sus características propias. Lo cierto es que para que el magistrado pueda realizar una íntegra valoración de esta prueba, en primer lugar debe poseer una relación directa o indirecta con el hecho controvertido objeto del pleito, siendo que una vez admitida, deberán aplicarse las reglas de la sana crítica racional para determinar su autor, autenticidad, integridad, trazabilidad y licitud, a través de una apreciación íntegra de los medios de prueba producidos por las partes para establecer la necesaria convicción.

Con extrema claridad dice Vaninetti (2013) que lo informático debe ser considerado como un indicio adicional que debe coincidir y confluir con otros indicios. Además, debe existir una relación directa y certera entre el hecho investigado y los indicios.

Como bien observó Devis Echandía (2002) por valoración o apreciación de la prueba judicial se entiende la operación mental que tiene por fin conocer el mérito o valor de convicción que puede deducirse de su contenido. (p. 273)

Al respecto en un fallo de la Cámara Civil y Comercial de Córdoba.4ª.Ceballos, Eduardo N. y otro c. Municipalidad de Córdoba. 24/11/2005. Se pronunció expresando que la valoración de la prueba es el análisis crítico e integral del conjunto de elementos de convicción reunidos y definitivamente introducidos en el proceso con la actividad práctica anteriormente cumplida.

Conforme a estos autores y en consonancia con sus ideas opino que las

pruebas electrónicas aportadas deben ser analizadas en su conjunto con el resto de las pruebas que forman parte de la teoría del caso de la fiscalía que será presentada ante el Juez, las cuales deberán ser valoradas en su totalidad. Devis Echandía (2002) al respecto el citado autor señala que mediante la valoración de la prueba se trata de determinar la eficacia o influencia que los datos o elementos probatorios aportados al proceso, mediante los oportunos medios de prueba, tendrán en la formación de la convicción del juzgador.(p.177)

Ciertamente el aporte de prueba electrónica en la actividad probatoria ha revolucionado el proceso judicial, proporcionando nuevas herramientas y métodos para la obtención, presentación y valoración de la evidencia. Este proceso inicia generalmente por denuncia de la víctima o denuncia de oficio por parte de la fiscalía, y una de las partes para afirmar o desmentir un hecho presenta voluntariamente una información electrónica. El rol del perito es fundamental ya que tendrá la responsabilidad técnica de observar la autenticidad y la integridad de la evidencia electrónica para que sea admitida, estas características son esenciales debiéndose preservar a lo largo de todo el proceso penal, ya que permiten afirmar que la información no se adulteró en ninguna de sus particularidades y propiedades.

Otro aspecto fundamental para que la evidencia digital tenga eficacia probatoria y permita que a través de su valoración los jueces elaboren su convencimiento acerca de la comisión o no de un hecho delictivo, es la cadena de custodia. La preservación de la prueba a través de la cadena de custodia asegura que la prueba es la misma que se secuestró y que no se alteró durante la extracción, en el examen pericial o en ninguna etapa de la instrucción del caso hasta su presentación en el juicio. Ese objetivo se alcanza a través de la aplicación de las buenas prácticas en la recolección de evidencia digital que requiere que tanto el personal de las fuerzas de seguridad como los peritos intervinientes cuenten con el conocimiento suficiente y utilicen las herramientas informáticas forenses apropiadas.

La integración de la prueba electrónica en la actividad probatoria ha aportado numerosas ventajas al sistema judicial, aunque también plantea desafíos

significativos. La evolución continua de la tecnología y la legislación es crucial para asegurar que estas pruebas se utilicen de manera justa y efectiva, garantizando al mismo tiempo la protección de los derechos fundamentales de las personas involucradas.

5) CONCLUSIÓN

Resolver un caso es entonces dependiente de la habilidad de los investigadores para juntar todas las piezas de las evidencias para así acreditar los hechos que motivaron su participación pericial. Se encuentra orientada a lograr la convicción del Juez sobre un hecho que puede revestir complejidad y que por su naturaleza técnica se requirió de los conocimientos del perito o investigador.

Así como en un hecho donde se investiga un homicidio con arma de fuego, el balístico sabe y conoce qué indicios del lugar se deberán relevar para así poder realizar pericias o una reconstrucción, en el caso de una estafa digital, o de acoso virtual, una amenaza o restricción de acercamiento, el perito o técnico que asiste al operador o investigador judicial en la tarea de resolución del hecho, necesariamente deberá conocer estos nuevos desafíos a los que se enfrenta.

En ese camino de tránsito y evolución permanente de las relaciones humanas, en que la tecnología y el mundo digital nos invaden por completo, el investigador tiene y debe estar a la altura de esas circunstancias.

La Prueba electrónica necesariamente nos alcanza y debemos conocer los métodos y técnicas para que su incorporación dentro del proceso se encuentre revestida de toda legalidad, por los carriles que expresamente se encuentran establecidos en nuestra legislación.

Las circunstancias desarrolladas en el presente trabajo, permite afirmar sin lugar a dudas que el investigador, sea las fuerzas de seguridad, el informático o criminalista que intervenga en la extracción de la prueba electrónica cuenten con los conocimientos especiales para no contaminarla y las herramientas forenses necesarias a los fines de asegurar la recolección pertinente, la extracción correcta y la preservación adecuada.

Para que la prueba electrónica tenga eficacia probatoria y permita que a través de su valoración los jueces elaboren su convencimiento acerca de la comisión o no de un hecho delictivo, desde el primer momento que se la obtiene debe ser correctamente preservada asegurando que la prueba es la misma que se secuestró y que no se alteró durante la extracción, en el examen pericial o en ninguna etapa de la instrucción del caso hasta su presentación en el juicio.

Ese objetivo se alcanza a través de la aplicación de las buenas prácticas en la recolección de evidencia digital que requiere que tanto el personal de las fuerzas de seguridad como los peritos intervinientes cuenten con el conocimiento suficiente y utilicen las herramientas informáticas forenses apropiadas.

Luego de analizar y estudiar técnicas, métodos e investigaciones sobre la prueba electrónica en el proceso penal, se concluye, sin lugar a dudas, que para garantizar el éxito en la investigación de hechos en entornos virtuales es fundamental conocer y seleccionar las herramientas y técnicas forenses adecuadas según el tipo de evidencia electrónica, aplicar procedimientos de cadena de custodia sólidos para preservar la integridad de la evidencia durante todo el proceso, documentar exhaustivamente todos los pasos del proceso de investigación, utilizar software especializado para la extracción, análisis y recuperación de datos electrónicos de acuerdo al caso que se presenta, mantenerse actualizado sobre las últimas herramientas y técnicas forenses disponibles.

Este nuevo panorama tecnologico exige una adaptación integral del escenario investigativo, tanto en el ámbito jurídico como en el técnico a la óptica digital/tecnológica. Es decir la eficacia probatoria de los documentos electrónicos o prueba electrónica dependerá de que sea posible probar su autoría, integridad y licitud a través de los mecanismos de seguridad propios de la tecnología que empleen y que deben ser conocidas por las fuerzas de seguridad, criminalistas, técnicos, por empleados, funcionarios y magistrados judiciales.

Este estudio también resalta la importancia de los informes o pericias para una adecuada valoración de la prueba, ya que las conclusiones a las que arriba el

experto proporciona conocimientos técnicos y especializados en cuestiones específicas que están más allá del alcance del conocimiento de la fiscalía o del juez, asiste en la tarea de aclarar un hecho complejo y puede respaldar una decisión judicial al proporcionar una opinión objetiva y fundada sobre aspectos técnicos o científicos.

En consonancia con lo expuesto, mi análisis también pone de relieve la necesidad de contar con marcos normativos adaptables a las nuevas tecnologías y de reconocer el uso de los nuevos medios de comunicación que surgen del avance tecnológico. Si bien por analogía podría emplearse el marco que regula las pruebas tradicionales en general, las pruebas electrónicas presentan una mayor probabilidad de manipulación o alteración, tal situación exige que el perito o experto ostente con el conocimiento suficiente para acreditar la autenticidad e integridad de la prueba.

Las nuevas tecnologías no solo modifican la forma en que nos comunicamos, trabajamos y en las relaciones comerciales sino que también generan nuevos desafíos y oportunidades para el sistema jurídico.

En un mundo en constante progreso donde la tecnología avanza a pasos agigantados, la justicia tiene que adaptarse a las nuevas realidades tecnológicas porque es una necesidad imperiosa para garantizar su vigencia y efectividad.

6) REFERENCIAS

BIELLI Y ORDOÑEZ. (2019) La Prueba Electrónica- Teoría y Práctica. Editorial Thomson Reuters – La Ley.

BIELLI, G. E. (2018) Los mensajes de WhatsApp y su acreditación en el proceso civil.

CASTILLERO MIMENZA, O (2017) Recuperado de https://psicologiaymente.com/forense/diferencia-indicio-prueba-evidencia.

CERVELLÓ GRANDE, J.M (2000) La prueba y el documento electrónico. Derecho de Internet, contratación electrónica y firma digital. Editorial Aranzadi, Pamplona

COMISIÓN NACIONAL DE COMUNICACIONES (2001). Resolución Nº 333/01 de la Secretaría de Comunicaciones. Ley Protección de correo electrónico. https://www.enacom.gob.ar/normativas

DARAHUGE, M. E. Y ARELLANO GONZÁLEZ, L. (2005). Manual de Informática Forense. Buenos Aires, AR: Errepar.

DELLE DONNE, C. (s.f), La extracción de prueba electrónica de teléfonos celulares y la garantía de defensa en juicio, Recuperado de file:///C:/Users/Invitado/Downloads/dossier-el-desafio-de-la-prueba-electronica%20(1).pdf.

DE GALLO, B. P. Pericias en correos electrónicos. Recuperado https://www.researchgate.net/profile/Beatriz_Gallo2/publication/308917364_Pericias_

en_Correos_Electronicos/links/57f76ac008ae280dd0bca81c/Pericias-en-Correos-Electronicos.pdf.Refiere

ECHANDÍA, D. H (2002) Teoría general de la prueba judicial, tomo I, quinta edición, Editorial Temis, S. A., Bogotá.Colombia.

ECHANDÍA, D.H (s.f) Compendio de la prueba judicial. Editorial Rubinzal Culzoni.

FERRER, F.M. (2017) La prueba de autoría de los contenidos publicados en redes sociales. Revista de Derecho Laboral, Rubinzal - Culzoni.

GUZMÁN, C. (2000) Manual de Criminalística, Buenos Aires, Argentina, Ediciones La Rocca.

INSTITUTO ARGENTINO DE DERECHO PROCESAL INFORMÁTICO (IADPI) Prueba Electrónica.

LLUCH, X. A. (2012). Derecho probatorio . EDITOR. J.M. BOSCH

MINISTERIO PÚBLICO FISCAL DE CHUBUT. (28 de abril 2023). Espejo Chubut se presentó ante los Procuradores en Mendoza. https://www.mpfchubut.gov.ar/centro-de-noticias/puerto-madryn/espejo-chubut-el-software-creado-en-chubut-que-permite-validar-a-los-chat-y-audios-de-whatsapp-en-juicios

MOLINA QUIROGA, E. (2010) Ley de expedientes digitales y notificaciones electrónicas judiciales. La Ley

MORALES VALLEZ, C (2016) La validez probatoria del WhatsApp y su incorporación al procedimiento". Recuperado de *http://ala.org.es/la-validez-probatoria-del-whatsapp-y-su-incorporacion-al-procedimiento/*.

MTRO. O. A. ROMÁN CONTRERAS (2010) Criminalística. Preservación y conservación del lugar de los hechos. México.

PAZ BELLORINI, G. (2013). La era de la Tecnología y los nuevos medios probatorios. El correo electrónico y su valor probatorio. Ratio Iuris. Revista De Derecho ISSN: 2347-0151, 1(1). Recuperado a partir de https://publicacionescientificas.uces.edu.ar/index.php/ratioiurisB/article/view/50

PICÓN RODRÍGUEZ, E. (2017) ¿Por qué no es válida una conversación de WhatsApp en juicio? Recuperado https://elderecho.com/por-que-no-es-valida-una-conversacion-de-whatsapp-en-juicio

REAL ACADEMIA ESPAÑOLA,(s.f). Correo Electrónico. En Diccionario de la lengua española. Recuperado 2023. De https://dle.rae.es/correo#N9wNw54

SOMER M. P. (2004). Documento electrónico. SJA 3/3/2004, JA 2004-I- p. 1029.

VANINETTI, H.(2013) Dossier prueba informática en el derecho penal. Preservación y valoración de la prueba informática e identificación de IP. Recuperado https://www.thomsonreuters.com.ar/content/dam/openweb/documents/pdf/arg/white-paper/pdf_descargable_dossier_prueba_informatica.pdf

VELTANI, J.D. (2012) El uso de las 'redes sociales' en el ámbito laboral. La Ley

VIVES, J.M. (2007) Valor probatorio de los mensajes de correo electrónico no firmados digitalmente. La cuestión en el marco de las relaciones contractuales interempresarias. Buenos Aires

WHATSAPP. (20 de noviembre de 2023).Wikipedia https://es.wikipedia.org/w/index.php?title=Discusi%C3%B3n:WhatsApp&oldid=155502282