La investigación forense informática en América Latina

Volumen 2

APC
por los Derechos Civiles

Área Digital
Asociación por los Derechos Civiles

Abril 2018
https://adcdigital.org.ar

Este trabajo fue realizado como parte de un proyecto financiado por Ford Foundation.

Índice

La investigación forense informática en América Latina*

I. Introducción

La ausencia de legislación específica sobre cibercrimen no es el único fenómeno que debe ser analizado. Vinculado a este, pero de forma independiente, es necesario considerar la manera en que actualmente se realizan las investigaciones que utilizan herramientas digitales para la obtención de prueba criminal. Esto es así por diversas razones.

En primer lugar, la recolección de evidencia digital es una práctica que ya existe en nuestros países. De esta manera, la poca o nula existencia de normas específicas no ha sido obstáculo para que las agencias de investigación empleen este medio cada vez con más frecuencia. Así, resulta imprescindible conocer los procedimientos utilizados para tener una idea clara de cuál es el estado actual en la región, como paso previo a una evaluación crítica.

En segundo lugar, dichas prácticas seguramente ya han producido hábitos y costumbres en aquellos que las llevan a cabo. Como tales, es posible que aún cuando eventualmente se incorpore normativa específica, la implementación de estas dependa de su correspondencia con los modos de trabajo que hoy se ejecutan. Así, examinar las prácticas actuales no implica poner solo la atención en el presente, sino que también significa pensar la influencia de las mismas en el futuro, haya o no una actualización de la legislación aplicable.

En tercer lugar, hacer foco en la práctica vigente supone analizar la manera en que las autoridades realizan una tarea de la cual dependerá muchas veces la constatación de que una persona es responsable de un delito, con la posible pérdida de su libertad por varios años. A ello, debe sumársele la novedad y complejidad de las tecnologías involucradas, lo cual requiere una amplia experticia y capacidad para su correcto manejo. Esta necesidad suele contradecirse con las falencias que los

*El presente documento fue compilado por **Eduardo Ferreyra**, analista de políticas públicas del Área Digital de la Asociación por los Derechos Civiles (ADC). Encargado de diseño y diagramación: **Leandro Ucciferri**.

países latinoamericanos -en mayor o menor medida- presentan en materia de capacitación de sus agentes públicos, volviéndose un factor preocupante y merecedor de un análisis profundo y cuidado.

Finalmente, la reciente expansión de tecnologías digitales para la investigación de delitos sumada a la ausencia de leyes o normas que la regulen específicamente ha provocado que la bibliografía sobre el tema sea todavía muy incipiente y en su mayoría proveniente de países que no pertenecen a nuestra región. De esta manera, la publicación de trabajos que den cuenta de la realidad latinoamericana se transforma en una necesidad imperiosa, a fin de impulsar la discusión con base a materiales que contemplen lo específico de nuestra problemática.

En base a estas y otras razones, desde la Asociación por los Derechos Civiles (ADC) iniciamos un trabajo de relevamiento sobre el estado actual de la investigación forense digital en América Latina. Para ello elegimos cuatro países de la región que detectamos ya cuentan con un cierto recorrido en la utilización de herramientas de recolección de prueba digital: Argentina, Chile, Colombia y México. Además, estos países han manifestado su intención de adherir al Convenio de Budapest sobre ciberdelincuencia y en algunos casos -Argentina y Chile- han sancionado leyes que cristalizan dicha adhesión. De esta manera, el estudio de las prácticas investigativas que tienen lugar en aquellos países puede darnos una imagen bastante representativa de lo que sucede en la región o, al menos, puede establecer líneas de trabajo, apuntes o perspectivas sobre las cuales continuar y profundizar la investigación.

A fin de realizar nuestra labor, en cada uno de los países seleccionados recurrimos a la ayuda de especialistas, los cuales fueron elegidos por su amplia trayectoria y conocimiento sobre el tema. Además, el vínculo con estos expertos fue la única manera de conocer lo que sucedía en la práctica, ya que conseguir información directa de las fuerzas de seguridad resultaba dificultoso. En ese sentido, cabe destacar la generosidad en brindarnos sus conocimientos, experiencias e impresiones, al menos hasta donde les fue posible, dado que en varios aspectos se encontraban limitados por acuerdos de confidencialidad. Finalmente, este análisis fue completado con actualizaciones que buscan agregar al documento aquellas preocupaciones que surgen desde la perspectiva de la sociedad civil.

El proceso de investigación comenzó con el análisis del estado de situación en Argentina por parte del ingeniero Gustavo Presman, perito informático que cuenta con un gran reconocimiento nacional y regional. Su trabajo no solo fue muy útil para conocer la práctica investigativa argentina, sino que también estableció los temas y aspectos a ser revisados y evaluados. De esta manera, sirvió como pauta homogeneizadora de las restantes investigaciones.

Así, el proceso continuó con la investigación en el resto de los países que forman parte del proyecto. Por parte de Chile, se recurrió a LICRIM Ltda. En el caso de Colombia, el encargado fue el ingeniero electrónico Giovanni Cruz Forero. Por último, el ingeniero Adolfo Grego Kibrit se dedicó a investigar la situación en México.

La versión completa de los reportes producidos puede consultarse en los siguientes links:[1]

1. Gustavo Presman (Argentina)
2. Giovanni Cruz Forero (Colombia)
3. Adolfo Grego Kibrit (México)

El presente documento tiene como objetivo ofrecer un resumen de los trabajos de los cuatro especialistas -más algunos aportes complementarios, que intentan ampliar el alcance de la investigación- y resaltar los hallazgos descubiertos en cada uno de ellos. A fin de facilitar su comprensión para aquellos interesados que no cuentan con conocimientos específicos, se ha tratado de evitar en lo posible el lenguaje técnico. En ese sentido, merecen realizarse dos aclaraciones. La primera es que, como fue mencionado, el presente reporte es un resumen. Por lo tanto, para tener una comprensión completa de los temas analizados, debe consultarse el texto completo de cada una de las investigaciones. La segunda es que cada país tiene un recorrido propio e independiente en su sistema procesal y su práctica forense, que a veces complejiza el poder establecer líneas en común con los otros países. Así, la búsqueda de regularidades se hará en tanto sea posible establecer pautas comunes, mientras que cuando no lo sea se mencionará las características especiales que presenta el país en cuestión, ya que las peculiaridades son tan importantes para el análisis como los aspectos en común.

II. Nociones preliminares de análisis forense

Las pericias informáticas pueden dividirse en dos grandes etapas. La primera es la recolección de la prueba y consiste en acceder al elemento digital, que será objeto de posterior análisis, y resguardarlo a los efectos de garantizar su contenido durante todo el proceso pericial. La segunda es el análisis de la evidencia y está constituido por el conjunto de tareas a realizar para analizar el contenido de la prueba, a fin de confirmar o refutar una hipótesis que se plantea. Como regla de buena práctica, se recomienda que ambas tareas sean llevadas a cabo por departamentos diferentes. De esta manera, la pericia tendría mayor objetividad, ya que la etapa de análisis puede descubrir irregularidades en la etapa de recolección que serían más difíciles de detectar si fuera hecha por personal de la misma división.

La regulación de estas tareas no está prevista por normas de cumplimiento obligatorio sino por diversos protocolos que reúnen las mejores prácticas conocidas y tienen la intención de suplir el vacío normativo.

[1] El aporte de LICRIM Ltda. no está publicado debido a que tiene carácter confidencial.

Entre los principales protocolos podemos mencionar: "Forensic Examination of Digital Evidence: A Guide for Law Enforcement"[2] del Instituto Nacional de Justicia (Departamento de Justicia de los Estados Unidos), "Best Practices for Computer Forensics"[3] (Grupo de trabajo científico en evidencia digital, SWGDE), el "Good Practice Guide for Digital Evidence"[4] (Fuerzas policiales de Inglaterra, Gales y el Norte de Irlanda, ACPO) y el "Identification and Handling of Electronic Evidence"[5] (Agencia Europea de seguridad de la Información, ENISA).

Es importante señalar que la Organización Internacional de Normalización (International Organization for Standardization, ISO) ha emitido dos normas relacionadas con el análisis forense y provenientes del tronco normativo de la ISO 27000. Estas son la ISO/IEC 27037:2012 Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence , y la ISO/IEC 27042:2015 Information technology -Security Techniques - Guidelines for the Analysis and Interpretation of Digital Evidence.

Estas normas ordenan y recomiendan mejores prácticas por lo que es aconsejable que cualquier protocolo de actuación o normativa esté alineado con las mismas.

III. La situación en los países

I. Argentina

1. Peritos

La forma en que se realiza la investigación pericial en Argentina depende de si el proceso judicial en el cual va a intervenir es de naturaleza civil o penal. En el primer caso, los peritos oficiales son elegidos por sorteo, entre todos aquellos que integren la lista del Poder Judicial. Para poder formar parte de la mencionada lista, los especialistas deben poseer título habilitante vinculado a la especialidad pericial.

Por su parte, los procesos penales tienen una forma distinta de selección. Allí la función pericial suele ser encargada a un miembro de las fuerzas de la ley. Es decir, un oficial de una fuerza policial, judicial o similar. A diferencia de los que sucede en el proceso civil, no es requisito tener formación universitaria. Esta situación ha provocado que se generen planteos de impugnación debido a la falta de formación académica. Entre los motivos de esta situación, pueden esgrimirse los bajos salarios,

[2] Disponible en Forensic Examination of Digital Evidence: A Guide for Law Enforcement (último acceso:10/04/2018).

[3] Disponible en Best Practices for Computer Forensics (último acceso: 10/04/2018).

[4] Disponible en Good Practice Guide for Digital Evidence (último acceso: 10/04/2018).

[5] Disponible en Identification and Handling of Electronic Evidence (último acceso: 10/04/2018).

la rígida estructura en la cadena de mando de las fuerzas de seguridad que no incentivan el estudio y la profesionalización y el alto volumen de trabajo.

A veces, los encargados de llevar adelante las pericias pueden ser universidades -públicas o privadas- o peritos privados reconocidos. Esto puede suceder cuando la pericia requiere conocimiento avanzado o equipamiento no poseído por la fuerza o cuando, por algún motivo, la participación de la misma pueda ser cuestionada.

Entre los principales laboratorios que realizan pericias informáticas, se encuentran:

- La Policía Federal Argentina, a través de las divisiones de Apoyo Tecnológico Judicial, Delitos Tecnológicos e Informática Forense;
- La Policía de la Ciudad (Buenos Aires) mediante su Área de Cibercrimen;
- Gendarmería Nacional Argentina, desde su laboratorio de Informática Forense dependiente del Departamento de Ciberdelitos;
- Prefectura Naval Argentina, a través de su departamento de Cibercrimen;
- El Ministerio Público Fiscal de la ciudad de Buenos Aires, con su laboratorio de análisis forense informático del Cuerpo de Investigadores Judiciales;
- La Policía de Seguridad Aeroportuaria.

Por su parte, organismos de inteligencia, policías, procuraciones y poderes judiciales del resto de las provincias están formando equipos de peritos informáticos como reacción a requerimientos puntuales de casos que requieren la recolección de prueba digital.

II. Protocolos

La realización de pericias informáticas en Argentina viene haciéndose con regularidad, pero de manera dispar, desde antes de la aparición de los principales protocolos existentes. Esto significa que la existencia de laboratorios con equipamiento adecuado, cumplimiento de normas de trabajo y personal capacitados conviven con la presencia de otros que poseen recursos mínimos e inexistentes en las áreas mencionadas. Asimismo, la falta de normativa común es causa de que cada laboratorio cuente con su propio procedimiento de actuación, los cuales suelen diferir entre sí. Por ejemplo, al momento de establecer cuántas copias se deben mantener de la evidencia recolectada, algunos exigen una sola mientras otros sugieren dos o tres. En este sentido, sería recomendable un mayor orden normativo a fin de obtener más transparencia en los procedimientos utilizados.

Entre los protocolos existentes en Argentina se encuentran: el *Protocolo de Actuación para Pericias Informáticas de la Provincia del Neuquén*[6], la *Guía de obtención, preservación y tratamiento de evidencia digital*[7], elaborada por la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), y el *Protocolo general de actuación para las fuerzas policiales y de seguridad en la investigación y proceso de recolección de pruebas en ciberdelitos*[8] del Ministerio de Seguridad de la Nación. Dichos protocolos constituyen, sobre todo, una adaptación de las pautas establecidas en los documentos internacionales ya citados y, en algunos casos, adolecen de una mala redacción y de severos errores técnicos, como incluir productos comerciales de hardware y software en lugar de describir procedimientos con sustento técnico y herramientas por sus funcionalidades. Asimismo, no se han previsto planes de capacitación ni los recursos financieros necesarios para su implementación.

III. Realización de la pericia

En relación con la pericia propiamente dicha, la norma establece que en ella deben participar no solamente los peritos oficiales sino también los peritos de las partes. Esta regla puede ser dejada de lado siempre que la pericia sea extremadamente sencilla o exista peligro en la demora. En la práctica, la incorrecta apreciación de estas excepciones ha hecho que las pericias se realicen sin peritos de parte, dejándolas al borde de la nulidad.

La regla mencionada tiene como justificativo el evitar que alguno de los peritos de parte acceda a contenido de la contraparte sin el conocimiento o presencia de esta, pudiendo obtener información privilegiada y vulnerando la privacidad de las partes. Sin embargo, la introducción del sistema acusatorio ha flexibilizado este requisito en pos de una mayor celeridad en el proceso. Así, el Código Procesal Penal de la Ciudad de Buenos Aires y el nuevo Código Procesal Penal de la Nación aún no sancionado prevén que los peritos deben procurar hacer la pericia juntos sin establecer una obligación tajante.

IV. Recolección de la evidencia digital

En la etapa de recolección de la evidencia digital, debemos distinguir la recolección mediante imágenes forenses y el secuestro directo de los dispositivos.

En el primer caso se realiza una copia bloque a bloque del contenido digital almacenado, el que es autenticado mediante una función de HASH para asegurar la integridad de la prueba recolectada.

[6] Disponible en http://200.70.33.130/images2/Biblioteca/ProtocoloActuacionPericiasInformaticas.pdf (último acceso:10/02/2018).

[7] Disponible en http://www.fiscales.gob.ar/procuracion-general/wp-content/uploads/sites/9/2016/04/PGN-0756-2016-001.pdf (último acceso:10/02/2018).

[8] Disponible en http://www.minseg.gob.ar/sites/default/files/disposiciones_legales/resolucion-ciberdelito.pdf (último acceso:10/02/2018)

Las imágenes pueden obtenerse a través de un programa o un duplicador forense. Si se utiliza un programa, hay que tener cuidado en impedir la contaminación de la prueba, mediante un acceso al dispositivo que bloquee la escritura o empleando un sistema operativo que no escriba sobre el medio digital. Si se usa un duplicador forense, ya es implícito el bloqueo contra escritura y la velocidad del proceso mejora drásticamente, pudiendo producir múltiples copias.

Asimismo, está la técnica del *Triage*, que permite la recolección de prueba digital mediante el uso de criterios superficiales, a fin de identificar potenciales elementos relevantes para la investigación.

En todos estos casos, lo importante es contar con hardware y software especializado y, sobre todo, un insumo fundamental como lo son los discos rígidos necesarios para el almacenamiento de la evidencia recolectada.

A pesar de que la regla es evitar acceder al contenido de los dispositivos que contienen evidencia digital para evitar su contaminación, existen ciertas ocasiones en donde el peligro de vida o perjuicio en la demora requiera acceder al dispositivo en vivo. En estos casos, se debe solicitar autorización previa al juez y el perito debe ser muy cuidadoso en los recaudos a tomar en el procedimiento -en especial, su documentación- y circunscribirse sólo a aquellos aspectos de la investigación que han sido ordenados.

En el segundo caso, el secuestro de dispositivos, los elementos confiscados deben ser embalados y etiquetados de manera que se resguarde el contenido y sea identificable con claridad. En el caso de los teléfonos celulares, deben ser embalados en contenedores especiales que bloqueen la interferencia electromagnética a fin de evitar que puedan ser accedidos durante el procedimiento.

v. Cadena de custodia

Un aspecto fundamental es la cadena de custodia. Es decir, el registro minucioso del movimiento de la evidencia y las personas responsables que tomaron contacto con ella. Este proceso es fundamental para demostrar la identidad, integridad, preservación y continuidad de la prueba. En la justicia argentina, los procesos judiciales son llevados en papel, en el expediente y los cuadernos de prueba. Así, la cadena puede reconstruirse a partir de la lectura y el seguimiento de estos documentos. Entre los elementos que puede contener un registro están: identificación de la evidencia, control de integridad del embalaje, los *hashes* de las imágenes forenses, nombres de las personas y fecha de contacto de la evidencia, registro de pasaje de persona y ubicación, etc.

Los cuidados en el tratamiento de la prueba digital comienzan desde la actuación en la escena del hecho. Para ello es imprescindible que la persona que interviene (Digital Evidence First Responder, DEFR) tenga la capacitación necesaria para manipular de manera correcta la evidencia. Esto es fundamental, ya que una incorrecta recolección de prueba podría generar la nulidad de la misma.

La primera decisión que se debe tomar es si la recolección tendrá lugar ahí mismo o será necesario secuestrar los dispositivos. Esta última opción se toma cuando no se disponen de los recursos necesarios o el tiempo suficiente para hacer la recolección de la evidencia o en escenarios violentos.

VI. Otros métodos de recolección

El procedimiento de recolección requiere de herramientas forenses, discos rígidos para el almacenamiento de las imágenes forenses y personal en la escena del hecho capacitada a tal fin, pero permite que se puedan conservar los recursos informáticos una vez finalizado el procedimiento de recolección de evidencia digital.

A su vez, existe la técnica de recolección por muestreo o Triage, mediante la cual se efectúa un barrido rápido empleando criterios sencillos, pero evitando profundizar las búsquedas en áreas especiales del disco o incluir elementos borrados. De esta forma se realiza un muestreo rápido bajo riesgo de dejar de lado evidencia de potencial de utilidad para la investigación privilegiando la velocidad del procedimiento.

Si la recolección debe hacerse sobre evidencia almacenada en la nube, tenemos que considerar que la misma se encuentra bajo el control de un tercero –el administrador del servicio– que muy probablemente se encuentre en una jurisdicción diferente. En Argentina, la recolección suele hacerse a través en dos modalidades. La primera consiste en la solicitud al proveedor de servicios para que conserve los datos. Dicha petición suele ser aceptada por los proveedores de servicios en la nube, si la misma es efectuada por un oficial de las fuerzas de la ley, desde una dirección de correo oficial de la dependencia a la que reporta. El segundo paso es la obtención de datos, el cual puede requerir una orden judicial o un exhorto diplomático. Todo este proceso está fuertemente influenciado por los términos y condiciones de cada empresa que presta el servicio, los cuales suelen establecer la forma en que deben ser hechos los pedidos.

Al momento de realizarse la labor pericial en el laboratorio forense, el mismo debe contar con software adecuado y licenciado a nombre de la institución, los insumos necesarios y el personal capacitado. En la práctica, es frecuente que los laboratorios de las fuerzas de la ley carezcan de alguno de estos elementos e incluso no cuenten con los recursos para adquirir los discos rígidos requeridos para la pericia. En estos casos, los discos son ofrecidos por las partes previa autorización del juez. Asimismo, en ocasiones no hay peritos de parte, lo que degrada la calidad de la pericia, debido a la ausencia de control por parte las partes.

VII. Actividades en el laboratorio

Son diversas las tareas que se llevan a cabo en un laboratorio forense. Algunas de ellas son:

- Búsquedas de contenido por criterio: búsqueda de archivos y registros mediante el uso de una palabra o frase clave provista por la autoridad judicial. En estos casos existe el riesgo de que existan "falsos positivos", es decir, archivos o registros informáticos que contienen al menos una de las palabras clave pero que manifiestamente no tienen vinculación con los hechos investigados.

- Identificación de imágenes: visualización en modo de galería de imágenes existentes en la evidencia recolectada. Este proceso es utilizado en casos de pornografía infantil y para identificación de documentos digitales o escaneados.

- Líneas de tiempo: análisis tendientes a establecer qué actividad se realizó en una fecha específica o intervalo de tiempo dado.

- Recuperación de información eliminada: incluyendo de ser posible, información sobre si el proceso fue realizado de manera automática o manual.

- Comparación binaria: permite establecer fehacientemente si dos o más archivos son idénticos entre sí, a partir de una comparación binaria de su valor de hash[9]. Es utilizado para casos de pornografía infantil y propiedad intelectual.

- Análisis de comunicaciones de correo electrónico y redes sociales: identificación de intercambio de mensajerías en redes sociales y correos. En este último caso, la autoridad judicial suele incluir la aclaración de que los correos no deben ser visualizados por el perito.

VIII. Procedimientos no contemplados legalmente

Finalmente, se deben señalar ciertos procedimientos cuyo sustento legal es débil o directamente inexistente. Así, estas actividades -aun con su correspondiente orden judicial- no son consideradas actualmente como procedimientos periciales, pues son mecanismos de vigilancia no contemplados en el Código Procesal Penal de la Nación.

Algunos de ellos son los siguientes:

- Recolección de evidencia mediante software malicioso: en este caso, se instala un malware con el objetivo de extraer información sin conocimiento del usuario.

- Recolección de evidencia mediante dispositivos de intercepción: uso de tecnología capaz de interceptar comunicaciones, permitiendo su paso hacia su destino final. Un ejemplo son los IMSI-catcher, que son torres falsas de telefonía celular a la que los dispositivos móviles objetivo se conectan para facilitar su intercepción.

[9] La Identificación de contenido binario: es el procedimiento mediante el cual se le aplica la función de HASH a un archivo o conjunto de archivos con el objeto de identificarlos en algún otro dispositivo de almacenamiento digital.

II. Chile

I. Peritos

El proceso penal en Chile se encuentra regulado por la ley 19.696 que sanciona el Código Procesal Penal[10] y es iniciado por medio del Ministerio Público (Fiscalía) o por denuncia de un particular (querellante). La investigación puede ser llevada a cabo por Carabineros de Chile o por la Policía de Investigaciones (PDI). La decisión sobre cuál fuerza intervendrá dependerá de la decisión del fiscal de turno.

Carabineros de Chile posee la Oficina de Informática Forense del Laboratorio de Criminalística, mientras que la PDI cuenta con la Brigada Investigadora de Cibercrimen, la cual tiene tres divisiones: investigación de pornografía infantil, delitos financieros e investigaciones especiales y análisis forense informático.

Luego de designada la fuerza que va a intervenir, el fiscal de turno debe solicitar las "primeras diligencias", en donde se realizará la recolección de evidencia para luego -siguiendo la cadena de custodia- ser enviada al laboratorio de la unidad policial. El perito encargado de realizar el análisis forense es designado por la institución policial dentro de alguno de los miembros de la fuerza, por lo que el fiscal no tiene la facultad de elegir al perito. Una vez terminado este proceso, el caso será derivado del fiscal de turno al fiscal específico que será el responsable de dirigir el curso de la investigación desde ese momento.

El imputado puede solicitar la intervención de un perito de su elección. Para ello puede designar uno de manera particular o de la base de datos de la Defensoría Penal Pública. Asimismo, los peritos pueden ser personas naturales o empresas prestadoras de servicios de análisis forense. Todos los peritos deben acreditar sus conocimientos mediante títulos de estudios.

Los trabajos de los peritos de la querella y del imputado no se mezclan y por ende, no existe trabajo en conjunto. Cada trabajo es presentado al expediente, en donde se abre una segunda instancia llamada metapericia, en la cual se realiza una revisión crítica y exhaustiva de la pericia de la parte contraria.

II. Normativa

No existe una norma vinculante específica para el manejo de evidencia digital. En la práctica, las fuerzas de seguridad siguen las buenas prácticas establecidas por guías como la normativa ISO 27.037 pero la observancia no es total y absoluta, al no haber una norma que así lo disponga. Asimismo, no hay mención de un tratamiento especial para las evidencias digitales en la formación

[10] Disponible en https://www.leychile.cl/Navegar?idNorma=176595 (último acceso:10/02/2018).

inicial de los policías. No obstante, las unidades especializadas en cibercrimen tienen programas de formación y capacitación para sus peritos. También es normal que se contrate a técnicos o ingenieros en informática para realizar labores de laboratorio.

III. Cadena de custodia

La cadena de custodia está prevista en el Código Procesal penal (art. 184) y en su desarrollo en general intervienen: la Policía de Investigaciones de Chile, Carabineros de Chile, Gendarmería de Chile, Servicio Médico Legal, el Ministerio Público y el Ministerio de Salud. Para el registro de la prueba, se cuenta con un formulario que posee un NUE (número único de evidencia), es foliado y consta de dos partes: un rótulo-formulario único de cadena de custodia y la cadena de custodia propiamente dicha. En el primero se deben completar los siguientes datos: día, hora, lugar en que se levanta la evidencia, breve descripción de la evidencia, observaciones al respecto si es que existieran, nombre, Rol Único Nacional (RUN), cargo y firma de quien selecciona el elemento que se convertirá en evidencia.

Esta persona es la que dio origen a la cadena de custodia de la evidencia (levantó la prueba). Las personas que entregan la evidencia a otro y quienes la reciben para traslado, custodia o análisis de esta, deberán dejar registrados sus datos: día, hora, lugar, nombre, RUN, cargo y firma en la hoja de la Cadena de Custodia, las veces en que se haya procedido, todas las veces que sea necesario. La normativa no establece ningún tratamiento especial para la evidencia digital. En estos casos, se siguen los lineamientos sobre cadena de custodia de evidencia digital establecidos en la normativa ISO 27.037[11].

IV. Recolección y análisis de evidencia

La pericia informática también comprende las dos etapas de recolección y análisis. En la primera, lo común es que las policías realicen el acceso al dispositivo en el laboratorio para evitar la contaminación de la información. Para ello, el procedimiento estándar involucra el apagado e incautación de los dispositivos, así como su inclusión en la cadena de custodia, indicando marca, modelo, color, número de serie si estuviera disponible, así como cualquier otro dato que facilite la individualización de la evidencia. El retiro de los equipos requiere una orden de allanamiento y secuestro por parte del juez, salvo en aquellos casos de flagrancia o delitos de terrorismo.

[11] Esta guía dispone que *"El registro de la cadena de custodia debería contener al menos la siguiente información: Identificador de evidencia único; Quién accedió a la evidencia, cuándo sucedió y desde dónde: Quién revisó el ingreso y la salida de la evidencia desde las instalaciones de preservación de la evidencia y cuándo sucedió: Por qué la evidencia fue revisada (en qué caso y el propósito) y la autoridad pertinente: si corresponde; y Cualquier cambio inevitable en la evidencia digital potencial, así como también el nombre del responsable individual y por consiguiente la justificación para la introducción del cambio..."*

Respecto al análisis, las tareas dependerán de lo encargado por el fiscal. Los estándares a seguir están delineados por la norma ISO 27037 (Norma Chilena: Tecnología de la información - Técnicas de seguridad - Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital. Documento validado por el Instituto Nacional de Normalización), que es idéntica a la versión en inglés de la Norma Internacional ISO/1 EC 27037:2012.

v. Manejo de videncia digital

Esta norma establece dos roles en el manejo de la evidencia digital: el primer responsable de la evidencia digital (encargado de actuar primero en la escena del hecho) y el especialista en evidencia digital (quien tiene un conocimiento específico para manejar una amplia gama de dificultades técnicas). En la práctica, el levantamiento de evidencia digital es realizado por personal no especializado, por lo que la prueba pasa directamente a manos de un especialista en evidencia digital.

La norma ISO 27037 establece 3 principios fundamentales para el manejo de la evidencia:

- Principio de relevancia: el material adquirido debe ser pertinente a la investigación.
- Principio de confiabilidad: los procesos involucrados en el manejo de evidencia digital deben ser auditables y repetibles.
- Principio de suficiencia: la evidencia recolectada debe ser la suficiente para propiciar una correcta investigación.

Para asegurar la confiabilidad (auditabilidad y repetibilidad) el investigador debe generar una copia de la evidencia digital, la cual debe estar autenticada por una función HASH[12], a fin de asegurar que la copia es idéntica al original. Las copias pueden ser generadas mediante software de duplicación que no tenga permisos de escritura -para no modificar el contenido original- o mediante hardware especializado de duplicación, el cual es un método más rápido y fiable pero también más costoso.

vi. Otros métodos de recolección de evidencia

Asimismo, también existe la recolección mediante el método *Triage*, el cual permite la recolección de evidencia que normalmente se pierde mediante el método tradicional de apagado del equipo, como ser la información volátil (usuarios con sesión abierta, contenido del portapapeles, información del tráfico de red, información de procesos abiertos, servicios ejecutándose en segundo plano, contenido de la RAM, etc.). El método *Triage* es adecuado para la recolección de información de un sistema "vivo"

[12] Las funciones HASH son algoritmos que consiguen crear a partir de una entrada una salida alfanumérica que representa un resumen de la información que se le ha dado.

(encendido) y es necesario para su funcionamiento el conectar un dispositivo externo que contenga las aplicaciones forenses para el análisis en sitio. La elección de este método queda a criterio del oficial a cargo de las diligencias en el terreno. En caso de que se decida llevar adelante, las fuerzas policiales cuentan con apoyo de personal experto en crimen informático, forenses - ingenieros en la materia y además cuentan con peritos de su laboratorio para efectuar dichas actividades, sin embargo y pese a lo anterior, pueden requerir apoyo de privados en estas materias.

A pesar de no existir estadísticas, en la mayoría de los casos las fuerzas utilizan el método de apagado de equipo, usando la investigación en "vivo" para el caso de los servidores, ya que la desconexión de éstos puede ocasionar más problemas y daños que beneficios.

Por otro lado, la evidencia en la nube plantea nuevos desafíos técnicos y legales, ya que la recolección de evidencia se debe efectuar de manera remota, al estar ubicada en un servidor externo. En estos casos, la solicitud de acceso es hecha por el tribunal, ya que la mayoría de los proveedores de servicios en la nube sólo entregan información mediante orden judicial. En ese sentido, muchas empresas proveedoras de servicios tienen sus propias políticas de entrega de información a las autoridades.

En cuanto a la prueba recopilada desde perfiles públicos de las redes sociales, son tratadas como información pública y al existir libertad de prueba, basta que estas sean fotografiadas y presentadas al tribunal. Por el contrario, si se trata de un perfil privado, se requiere de una orden judicial para obtener los datos o hacer uso de un agente encubierto.

Entre las tareas más comunes para el analista forense, figuran:

- Acceso y respaldo de datos: resguardando la integridad de la información y la cadena de custodia.
- Recuperación de datos eliminados: recuperación de archivos que han sido eliminados del dispositivo de almacenamiento.
- Búsqueda de contenido por criterio: a través de patrones de búsqueda como tipo de archivo, rango de fechas de escritura, palabras clave, peso, etc.
- Búsqueda e identificación de contenido multimedia: como ser imágenes, video, audio u otros.
- Líneas de tiempo: registro cronológico de las actividades desarrolladas en el sistema de archivo.
- Comparación binaria: permite establecer si dos o más archivos son idénticos entre sí a partir de la comparación de su valor de hash.
- Análisis de comunicaciones de correo electrónico y redes sociales: identificación de intercambios de mensajería en redes sociales y correos electrónicos.

La interceptación de comunicaciones son parte de la investigación criminal, si y sólo si son autorizadas por un Juez de Garantía. En estos casos, los organismos llamados a esta función son por conectividad las operadoras o ISP, y en las centrales de inteligencia las propias agencias policiales con equipamiento preciso para dicha función. Los peritos no toman parte de esta actividad ya que no es una función pericial, sin embargo, de acuerdo al debido proceso, es menester que sean entregadas a los peritos de las partes para su análisis, estudio y validación conforme dictámenes.

Por último, el escándalo de la Operación Huracán[13] puso el alerta sobre la utilización de la ley de inteligencia para producir prueba en el proceso penal, salteando la regulación establecida en el código procesal. A través de la ley 19.974 de inteligencia, Carabineros pudo solicitar directamente al tribunal la interceptación de comunicaciones de los sospechosos, sin el control de la Fiscalía. La ausencia de supervisión facilitó la fabricación de pruebas adulteradas y generó una fuerte incertidumbre en Chile acerca de la forma en que sus fuerzas de seguridad llevan adelante sus investigaciones.

III. Colombia

I. Peritos

De acuerdo a lo establecido por las normas procesales penales, pueden ser peritos, en general, aquellas personas que cuenten con título legalmente reconocido o, en circunstancias diferentes, personas de reconocido entendimiento en la materia aunque carezcan de título. Con relación al manejo de evidencia digital, este conocimiento rara vez es tratado en las materias de grado y la preparación del posgrado es insuficiente para producir expertos. De esta manera, personas con título reconocido en ciencias relacionadas con la actividad pericial muy posiblemente no tendrán las habilidades para llevar adelante un análisis forense digital.

Asimismo, la ausencia de comprobación de la idoneidad de los peritos más la falta de una definición de las competencias necesarias para ser un analista forense digital lleva a que se realicen técnicas de recolección y análisis de evidencia digital que luego no pueden ser presentadas en un proceso judicial debido a las fallas en los procedimientos ejecutados.

Otro problema es la brecha existente entre el lenguaje técnico utilizado por los peritos y el lenguaje manejado a nivel legal. Por un lado, es difícil desde la perspectiva legal comprender los términos técnicos utilizados por los peritos al momento de realizar los procedimientos. Por el otro, la comprensión

[13] La Operación Huracán fue una investigación de Fiscalía y Carabineros que implicó la detención de ocho comuneros mapuches acusados de ser autores de una serie de ataques incendiarios. Como prueba, se aportaron conversaciones supuestamente interceptadas de los celulares de los imputados, las cuales fueron difundidas en los medios de comunicación. Finalmente, la Fiscalía descubrió que dichas conversaciones habían sido introducidas en los celulares de los acusados luego de que los móviles hayan sido incautados, generando fuertes sospechas de que todo se habría tratado de un montaje policial. Cfr. Viollier, Pablo. *Cómo el gobierno de Chile ha dado rienda suelta a sus policías*. Derechos Digitales, disponible en https://www.derechosdigitales.org/11916/como-el-gobierno-de-chile-ha-dado-rienda-suelta-a-sus-policias/ (último acceso: 22/03/2018)

de las reglas y procedimientos judiciales resulta abrumadora para los peritos. Así, es necesario establecer un lenguaje común y claro entre las dos perspectivas a fin de poder ejecutar un procedimiento exitoso.

II. Instituciones que realizan análisis forense

En relación a las instituciones con capacidad para hacer análisis forense, diferentes entidades del estado ya cuentan con laboratorios forenses, con diferentes capacidades, con la posibilidad de prestar servicios para sus necesidades propias, entre los que se puede enumerar los de la Fiscalía General de la Nación, el Ejército Nacional de Colombia, la Policía Nacional de Colombia, la Procuraduría General de la Nación, la Contraloría General de la Nación, la Superintendencia de Industria y Comercio. Asimismo, existen diferentes empresas privadas dedicadas a la venta de servicios forenses digitales en sus laboratorios. Al igual que en el sector público, es posible identificar diferentes capacidades instaladas y ofertas variadas de servicios, que sirven como apoyo a un mercado que muchas veces no entiende en su totalidad el funcionamiento de un servicio de análisis forense digital, pero sabe que puede servirle en ciertas ocasiones para dar solución a problemas que afectan a la información que las empresas almacenan en sus bases de datos.

III. Cadena de custodia

En julio de 2016, la Fiscalía General de la Nación lanzó el manual de procedimientos de cadena de custodia elaborado bajo la dirección del Cuerpo Técnico de Investigación (CTI) de la Fiscalía y con el apoyo de la Policía Nacional, el Instituto Nacional de Medicina Legal, la Embajada de los Estados Unidos, entre otras entidades. Este documento de carácter general busca unificar conceptos para todas las fuerzas de policía judicial y por ser generado por el órgano de indagación e investigación de Colombia (Artículo 200 del Código de Procedimiento Penal Colombiano), con el apoyo del órgano técnico - científico (Artículo 204 del Código de Procedimiento Penal Colombiano), tiene toda la validez y relevancia para ser usado como documento guía para el manejo de evidencia digital.

Dentro de lo que se puede resaltar en el documento para evidencia digital, es el tipo de embalaje que se debe realizar para los contenedores de este tipo de evidencia. Adicionalmente se encuentra información de un esquema de procedimientos según el elemento material probatorio o evidencia física, donde se encuentra información específica relativa a Computadores (Servidores, de escritorio y portátiles), dispositivos de almacenamiento digital y celulares. Se incluye dentro del manual resúmenes de procedimientos específicos para dichos elementos y precauciones a tener en cuenta cuando se realiza un estudio que busque la recuperación y extracción de información, el análisis de código malicioso, la identificación de cuentas de usuario, sistema operativo, programas instalados, el cruce de información entre dispositivos o el análisis de comunicación.

IV. Normativa

A pesar del intento recién comentado, todavía no existen procedimientos realmente unificados en el país, es más, en diversas unidades de análisis forenses no existen procedimientos documentados en absoluto, y si bien los investigadores suelen tener en claro las tareas que deben llevar a cabo, las mismas no están cristalizadas en algún documento estructurado.

De acuerdo con la norma ISO 27037, resulta conveniente la presencia del primer respondiente, quien se encuentra autorizado, entrenado y calificado para atender la escena del incidente y realizar la recolección y adquisición de evidencia digital con la responsabilidad del manejo de dicha evidencia. Sin embargo, en la práctica esta figura no existe en la mayoría de los casos. La falta de la asignación de dicho rol, la falta de conocimiento del mismo, o la transferencia de la responsabilidad de las actividades que debe realizar el primer respondiente a los usuarios que sufren el incidente o a la mesa de ayuda[14] de las organizaciones, hace que la evidencia muchas veces se encuentre viciada o se pierda desde ese primer instante en el que se interactúa de forma errónea con ella. A pesar de esto, la fiscalía cuenta dentro de su grupo de delitos informáticos con personal capacitado que puede realizar las tareas requeridas al primer respondiente.

V. Recolección de evidencia

El Código de Procedimiento Penal colombiano[15] prevé ciertas facultades de la Fiscalía relacionadas con la obtención de evidencia digital. Así, el art, 235 sostiene que el fiscal podrá ordenar de manera fundada y por escrito la interceptación de comunicaciones que contengan información de interés para la investigación. Los órganos encargados de cumplir con la orden tienen la obligación de realizar la tarea inmediatamente después de haber sido notificados y de guardar la debida reserva. Por otro lado, el art. 236 faculta al fiscal a ordenar el secuestro de computadoras, servidores y otros dispositivos de almacenamiento para que luego sean analizados por expertos en informática forense. El secuestro será autorizado cuando haya motivos razonablemente fundados de que existió transmisión de información relevante y se limitará exclusivamente al tiempo necesario para la captura de la información contenida.

En los dos supuestos, el fiscal deberá comparecer dentro de las 24 horas de realizada la medida ante el juez de control de garantías para que se desarrolle la audiencia de control de legalidad. Durante el trámite de la audiencia sólo podrán asistir, además del fiscal, los funcionarios de la policía judicial y los testigos o peritos que prestaron declaraciones juradas con el fin de obtener la orden respectiva, o

[14] La mesa de ayuda es la parte una organización empresarial encargada de dar respuestas y soluciones a los clientes o a los empleados de la empresa. Generalmente su propósito es resolver problemas acerca de computadoras, equipos informáticos y software.

[15] Disponible en http://www.pensamientopenal.com.ar/system/files/2014/12/legislacion30901.pdf (último acceso: 02/04/2018)

que intervinieron en la diligencia. El juez podrá, si lo estima conveniente, interrogar directamente a los comparecientes y, después de escuchar los argumentos del fiscal, decidirá de plano sobre la validez del procedimiento. En relación con la práctica, existen dudas sobre la preparación para asegurar, embalar y custodiar la evidencia digital. Muchas veces, el personal designado para hacer dichas tareas no se encuentra totalmente preparado ni tiene el conocimiento necesario de las herramientas adecuadas para su labor. Esto produce que varios de los procedimientos se lleven a cabo de manera artesanal, ya que no se quiere hacer la inversión exigida para capacitar al personal o adquirir las herramientas requeridas. Además, se debe revisar la preparación de las empresas que almacenan información en sus servidores, en cuanto a su infraestructura para permitir la recolección de evidencia digital de una manera correcta.

En definitiva, el análisis forense en Colombia es de carácter reactivo y no existe una preparación que permita a los peritos acceder a la información necesaria. Asimismo, el mal manejo de los contenedores ha producido casos en los cuales la información recolectada carece de validez legal, como fue el renombrado caso de las computadoras de Raúl Reyes[16], donde la evidencia perdió su validez legal, después de realizar un incorrecto manejo de la cadena de custodia y una incorrecta manipulación de los archivos.

Un tema álgido es la obtención de evidencia alojada en servidores externos. Actualmente no existen procedimientos para la fijación de dicha prueba y este vacío normativo puede ser causa de que la evidencia no sea aceptada en una instancia judicial. Algunas soluciones intentadas han sido obtener contenedores de los servicios, con los cuales se puede hacer una fijación de los datos. Sin embargo, suele ser difícil comprobar la integridad de aquellos, ya que no existe la posibilidad de hacerlo contra la fuente.

VI. Análisis de evidencia

Acerca del análisis de la evidencia recolectada, es difícil que se realice la inversión en herramientas forenses, lo cual genera problemas cuando se trata de demostrar los resultados del proceso del análisis con software no licenciado en cabeza del organismo a cargo de la realización de la pericia. En ese sentido, debe resaltarse que la credibilidad de las pericias se basa en la herramienta utilizada o las licencias adquiridas para el servicio. Desde esta perspectiva, es necesario hacer entender que el valor de una pericia se extiende más allá de las herramientas utilizadas y comprende la experiencia y pericia misma de la persona que realiza el análisis, la comprensión de las estructuras dentro de las que realiza búsquedas específicas con el fin de encontrar evidencias dentro de datos.

Bajo este panorama, puede citarse un caso que, si bien no puede considerarse representativo de toda

[16] Raúl Reyes fue un guerrillero de las Fuerzas Armadas Revolucionarias de Colombia (FARC) que murió en Ecuador durante una operación militar de las fuerzas armadas colombianas. En la misma operación se encontraron sus computadoras, que revelaban información acerca de sus actividades en las FARC.

la práctica que se lleva a cabo en Colombia, sí sirve como ejemplo de las cosas que pueden mejorarse en el proceso de investigación. En un allanamiento, se realizó la incautación de todos los equipos que se encontraban en la habitación de la persona. Al afectado no se le dejó copia de la orden de allanamiento ni le fue informada la causa de la investigación. Ocho meses después del suceso, no se le entregó información alguna sobre el avance de la investigación y hubo que hacer dos reclamos judiciales para que se le devuelven los equipos, necesarios para que la persona pudiera hacer sus actividades laborales. Finalmente, la investigación fue cerrada y nunca pudo obtenerse información sobre el proceso.

Este caso deja varias lecciones: el proceso de recolección debió hacerse en el lugar de los hechos o al menos el análisis en el laboratorio no debió haber insumido mucho tiempo, si la fiscalía hubiera encontrado evidencia en el caso, sería necesario que el acusado pudiera haber hecho una contrapericia, entre otras.

VII. Actividades forenses utilizadas

Entre los procedimientos utilizados en Colombia, figuran los siguientes:

- Evidencia digital de almacenamiento: es uno de los procedimientos más utilizados e involucra diversas tareas como: la búsqueda de contenidos por criterio, la creación de líneas de tiempo para la identificación de posibles actividades realizadas que involucren el borrado voluntario de información o la modificación de archivos que puedan ser usados en temas de espionaje industrial, análisis de contenedores de correo electrónico y recuperación de información eliminada.
- Evidencia digital de memoria RAM: se utiliza cuando el equipo se encuentra afectado por malware y se enfoca en credenciales de acceso, información de cifrado, información que se está manipulando en el momento de captura del contenedor.
- Evidencia digital de tráfico: si bien no es muy utilizado en Colombia, puede ser un componente muy valioso en las investigaciones. Sin embargo, debe tenerse cuidado en que el almacenamiento de grandes cantidades de datos pueda generar afectaciones a la privacidad.
- Evidencia digital de dispositivos móviles: su uso se ha incrementado últimamente debido a la gran cantidad de información que puede encontrarse en ellos. Los inconvenientes con este procedimiento están dados por la falta de herramientas especializadas de obtención y la imposibilidad de realizar copias físicas de los dispositivos.
- Evidencia almacenada en servidores externos: los procedimientos de este tipo se enfocan en la recolección de información de compañías, en búsqueda de fuga de información o comunicaciones que puedan demostrar la participación en actividades de espionaje industrial. Los

contenidos más analizados están relacionados con difamación, material de abuso sexual de niñas, niños y adolescentes, casos de phishing y estafas.

- Recolección de evidencia de manera remota: procedimiento muy poco utilizado, se recurre a él en ambientes corporativos para proteger la evidencia de posibles agentes internos involucrados en hechos objeto de investigación. La policía judicial no lleva a cabo este procedimiento.
- Procedimientos realizados por organismos de inteligencia: actualmente, en pocas agencias de inteligencia existen profesionales que puedan realizar la recolección forense de evidencia.

IV. México

I. Un sistema procesal en transición

El reto más importante para México se encuentra en la transición de un sistema penal inquisitivo a uno acusatorio. El cambio más importante es que con el nuevo sistema se privilegia a la evidencia como mecanismo de demostración de acusaciones o argumentos de defensa, en vez de las confesiones que eran utilizadas de forma más frecuente en el sistema penal anterior. De esta manera, los peritos especialistas en Cómputo Forense se encuentran bajo una carga de trabajo dual, atendiendo casos en ambos sistemas penales de forma paralela y teniendo además que actualizarse constantemente en las capacidades técnicas que demanda la profesión. Dentro de este contexto, se encuentran capacidades técnicas dispares entre los mismos peritos no solo entre los ámbitos federales y locales, también entre los peritos de las mismas instituciones.

II. Marco legal vigente

Entre el marco normativo relevante para el tratamiento de evidencia digital, es conveniente comenzar con la Constitución mexicana, que establece el principio de la inviolabilidad de las comunicaciones privadas (art. 16) y que sólo la autoridad judicial federal puede autorizar una intervención. Entre los órganos facultados para solicitar una intervención se encuentran: el Centro de Investigación y Seguridad Nacional (CISEN, órgano de inteligencia del Gobierno Federal Mexicano), la Policía Federal o los estados a través de cada Ministerio Público. El órgano encargado de llevar adelante las intervenciones es la Procuraduría General de la República, quien debe contar con un cuerpo técnico de control que será el encargado de determinar los requerimientos técnicos y de equipamiento necesarios para llevar a cabo las interceptaciones no sólo de comunicaciones privadas sino también de datos o informáticas.

Por otro lado, el Código Nacional de Procedimientos Penales (CNPP) establece los principios que deben guiar el trabajo forense. Respecto a quién puede ser perito, se establece que los peritos

deberán poseer título oficial en la materia relativa al punto sobre el cual dictaminarán y no tener impedimento alguno para el ejercicio profesional, siempre que la ciencia, el arte, la técnica o el oficio sobre el que vaya emitirse el peritaje esté reglamentada. En caso de no estarlo, deberá designarse a una persona que pueda demostrar conocimientos profundos de forma idónea relativa a la actividad sobre la que se vaya a emitir el peritaje.

III. Peritos

En México el documento oficial que debe presentar como base el perito en informática forense es la Cédula Profesional. Este documento se tramita a los profesionistas que se han titulado en diferentes carreras profesionales. Un Ingeniero en Sistemas Computacionales o un Licenciado en Sistemas de Cómputo cuentan con este documento.

En el caso de las Fiscalías y Procuradurías, existen los cuerpos de Servicios Periciales (pueden ser coordinaciones, áreas forenses, etc.). Los profesionales adscritos a Servicios Periciales sí tienen que acreditar su carrera profesional, ya sea como Criminalistas, Médicos, Ingenieros, Licenciados, etc. Finalmente, estos peritos son los que firman los peritajes y, por ende, son los responsables de los mismos.

IV. Cadena de custodia y trabajo pericial

Otro aspecto a tener en cuenta es la cadena de custodia. El CNPP establece que la cadena de custodia deberá de contener los siguientes elementos: identidad de la prueba, estado original, condiciones de recolección, preservación, empaque y traslado, lugares y fechas de permanencia, así como los cambios que en cada custodia se hayan realizado. Se deberá registrar el nombre y la identificación de todas las personas que hayan estado en contacto con la evidencia.

Específicamente, los peritos en Informática Forense tienen el reto de demostrar que los procedimientos que han seguido para la recolección, resguardo y análisis de la evidencia cumplan con los preceptos de las diversas leyes, códigos y reglamentos.

Aquí es donde se aplican las prácticas recomendadas a nivel internacional o las normas estandarizadas que son publicadas por cuerpos reconocidos internacionalmente como la International Standards Organization (ISO), las directrices del FBI o las recomendaciones emitidas por cuerpos policíacos especializados.

En el caso específico de México existen normas que son publicadas bajo el auspicio de la Secretaría de Economía a través de NYCE S.C. La Norma Mexicana relativa a los procedimientos de Cómputo Forense es la NMX-I- 289-2016 titulada "Tecnologías de la Información - Metodología de Análisis Forense de Datos y Guías de Ejecución". Esta norma es la referencia de facto para demostrar que

se han seguido las prácticas recomendadas para la recolección, preservación y análisis de evidencia digital. Además, muchos investigadores siguen las recomendaciones emitidas por cuerpos internacionales como el FBI, las guías del NIST para la evaluación de herramientas forenses, ENISA en Europa y otras guías con prácticas recomendadas.

Con la llegada del nuevo sistema penal acusatorio, las fallas metodológicas y la falta de capacitación de los investigadores pueden poner en duda la evidencia recolectada en el momento de ser presentada en el juicio oral. Así, los peritos deben ser especialmente claros en la emisión de las conclusiones producto de su análisis. Se requiere de una contundencia irrefutable para la presentación de los resultados. Uno de los puntos más importantes que debe evitar un perito es el de no emitir conclusiones de carácter legal, ya que de él solo se requiere la elaboración de conclusiones técnicas y científicas.

Las actividades realizadas por el perito deberán quedar plasmadas en el Dictamen Pericial, documento que debe presentar de forma clara las actividades realizadas por el perito sobre los indicios con el fin de explicar cómo fue que identificó las pruebas que presenta y que soportan sus conclusiones. La sección más importante del Dictamen Pericial es la de conclusiones, donde el perito deberá presentar de forma clara cada una de ellas.

La estructura del documento del Dictamen Pericial deberá ser estandarizada por la institución a la que pertenezca el perito. En caso de que se trate de una práctica privada, lo recomendable es que se mantenga una estructura uniforme y que sea consistente con los procedimientos de operación.

Una de las mejores referencias que se pueden tomar como base para establecer dicha estructura recomendada por el Manual de Procedimientos del Departamento de Informática y Telecomunicaciones de la Coordinación General de Servicios Periciales de la Procuraduría General de la República. De acuerdo con el índice que utiliza dicha institución es:

1. Fecha de emisión del Dictamen Pericial.
2. Nombre de la persona solicitante.
3. Planteamiento del problema (Antecedentes). Se recomienda incluir de forma textual los planteamientos con los que deberá de trabajar el perito.
4. Observación del lugar. Esto aplica para los casos de investigación en campo.
5. Análisis y consideraciones técnicas. Aquí se documentan los detalles del análisis realizado, incluyendo técnicas, manuales, herramientas y procedimientos utilizados.
6. Glosario. Es necesario para que las conclusiones puedan ser entendidas por personal no técnico, con el fin de ayudar a explicar los términos técnicos que aparezcan en el Dictamen.
7. Conclusiones. Aquí el perito presenta su opinión técnica con respecto al planteamiento que se le haya realizado. Deberá de ser clara, precisa y contundente.

8. Firma de los peritos responsables de haber realizado el estudio solicitado.

v. Entidades que realizan análisis forense

Respecto a las instituciones con capacidad de investigación en Cómputo Forense, a nivel federal existe la Policía Federal, que cuenta con un cuerpo de policía cibernética dependiente de la división científica de la institución. En varios de los estados de la República Mexicana se han establecido cuerpos de policía cibernética que dependen de las policías estatales. Estos cuerpos han iniciado en muchos casos sus operaciones para intentar mantener a las instituciones a la vanguardia en la lucha contra la delincuencia. Sin embargo, los marcos normativos no han sido siempre suficientes para garantizar una correcta actuación.

Otra de las actividades que es visible por parte de estos cuerpos policíacos son los llamados "ciber patrullajes", donde los miembros de las fuerzas realizan revisiones de distintas redes sociales con el afán de detectar delitos y proteger a la ciudadanía. Estas labores pueden llegar a ser difíciles de mediar en cuanto a sus alcances, pues están supeditados a las políticas de acceso y uso aceptable establecidos por las empresas que proveen el servicio de las redes sociales. Ha habido algunas intervenciones en contra de bandas relacionadas con la pornografía infantil, así como operativos coordinados a nivel internacional donde las fuerzas policiales han participado.

Los equipamientos, funciones y atribuciones difieren mucho entre fuerzas policiales y los diversos estados mexicanos. Ninguna ciber policía tiene capacidad de compra autónoma y dependen siempre del presupuesto asignado a la institución de la que depende el cuerpo. Sin embargo, la llegada del nuevo Sistema Penal Acusatorio está influyendo vertiginosamente la actuación de estos cuerpos. En ese sentido, es necesario estandarizar las policías científicas del país para poder hacer frente a los juicios orales dentro del nuevo sistema penal acusatorio. Las policías cibernéticas deberán actuar como peritos para presentar pruebas durante los procedimientos penales y por supuesto, como se ha desarrollado en este documento, durante las audiencias. Aquí es donde la situación se complica. En estos momentos, el presupuesto es una de las grandes barreras para que los cuerpos se estandaricen en la totalidad de los estados.

vi. Influencia del sistema acusatorio en el trabajo pericial

En lo que se refiere a la investigación de delitos cibernéticos como parte de las labores de las fiscalías y procuradurías, tanto estatales como a nivel federal, existen cuerpos de peritos en tecnología y cómputo forense. Estas áreas de peritos son las que presentan mayores contrastes en cuanto a su equipamiento y capacidades. Aquí existe una dependencia directa en cuanto al estado de la república al que pertenecen, si la entidad federativa ya terminó su transición hacia el nuevo sistema penal

a través de la implementación de una Fiscalía o si siguen operando bajo el paradigma de una Procuraduría.

Estos cuerpos y sus peritos son quienes sentirán de forma inmediata la transición al nuevo sistema de justicia penal, ya que deben de cambiar su forma de operar para alinearse a los requerimientos del CNPP. Asimismo, los peritos también representan la brecha más importante de referentes a conocimientos y capacidades técnicas. Se tienen dos grandes grupos: aquellos que son verdaderamente expertos y aquellos que requieren de mucha capacitación y mentoreo para lograr la experiencia necesaria.

En este sentido, los aspectos a mejorar en México son los siguientes:

- Falta de mantenimiento y actualización en los recursos utilizados.
- Rotación de personal debido a falta de interés, frustración o traspaso al sector privado.
- Personal que no cumple con los perfiles técnicos necesarios.
- Ausencia de dominio del idioma inglés, que es el lenguaje predominante de las soluciones tecnológicas.
- Marcos normativos y de actuación insuficientes para las actividades operativas.
- Complejidad al interactuar con otras áreas para perseguir delitos más complejos.

Por último, organizaciones de defensa de los derechos humanos de México han denunciado prácticas de vigilancia sistemática sobre periodistas y defensores de derechos humanos a través de un sofisticado software llamado Pegasus, el cual permite tener acceso a los archivos del dispositivo así como tener control de la cámara y el micrófono, entre otras facultades.[17]

IV. Puesta en común y conclusiones

A partir de la descripción de las experiencias existentes en los países objeto de investigación, podemos descubrir ciertas problemáticas que son compartidas por aquéllos y que establecen un conjunto sobre el cual se puede empezar a trabajar para mejorar las investigaciones de informática forense en nuestra región.

[17] Para profundizar en las investigaciones y denuncias, consultar el reporte *"#GobiernoEspía: vigilancia sistemática a periodistas y defensores de derechos humanos en México"*, elaborado por Article 19 Oficina para México y Centroamérica, R3D: Red en Defensa de los Derechos Digitales y SocialTIC, disponible en https://r3d.mx/gobiernoespia (último acceso: 10/04/2018).

Marco normativo insuficiente: Los países reseñados carecen de normativa obligatoria específica referente a la recolección y análisis de evidencia digital. Para mitigar esta carencia, se ha recurrido a dos alternativas. La primera es la aplicación -vía interpretación, analogía, etc.- de las reglas tradicionales de los códigos procesales penales en tanto sea posible. Esta tendencia se ve especialmente al momento de determinar las condiciones exigidas para ser peritos o para establecer los lineamientos generales acerca de la forma en que deben practicarse las pericias. La segunda vía es recurrir a reglas de buena práctica, las cuales se encuentran cristalizadas en protocolos o guías de actuación. Dentro de éstas, las más utilizadas son las normativas ISO 27000 sobre recolección y análisis. De esta manera, estas herramientas se vuelven una pauta a seguir por los investigadores aunque su falta de obligatoriedad hace que su influencia dependa de la voluntad de aquellos a los que pretende regular.

Problemas en la profesionalización de los peritos: Otro aspecto a resaltar fueron los defectos en la preparación y capacitación de los peritos integrantes de las fuerzas de seguridad. Entre las causas citadas se encuentran: la no exigencia de título universitario, la falta de enseñanza de contenido específico en la educación de pregrado o posgrado, la permanente rotación de personal o la ausencia de incentivos para capacitarse. Esta tendencia se profundiza en aquellos países con sistema federal -como Argentina, Colombia y México- en los cuales existen grandes diferencias de preparación entre las fuerzas de seguridad de las diversas provincias o estados.

Equipamiento no actualizado: En varios casos, las herramientas utilizadas para recolectar evidencia son mínimas o están desactualizadas. En otros casos, existe falta de mantenimiento o se hace uso de herramientas no licenciadas. Detrás de estos fenómenos, aparece la falta de financiamiento por parte de las autoridades públicas, ya sea en la inversión en equipos o en el mejoramiento de las condiciones económicas de los miembros de las fuerzas.

Recolección de evidencia: La adquisición de evidencia digital suele realizarse a través de la obtención de imágenes duplicadas o mediante el secuestro de los dispositivos. Asimismo, existe un incremento en la utilización del método Triage, que permite una búsqueda rápida en el lugar del hecho y es muy conveniente para casos en que se precisa de manera urgente la información.

Cadena de custodia: Todos los países cuentan con procedimientos de cadena de custodia, los cuales están basados en lo dispuesto de manera general por los códigos procesales penales y en las guías de la normativa ISO. Los inconvenientes se presentan al momento de ponerlas en práctica, ya que su buena implementación dependerá de la capacitación e idoneidad de los operadores intervinientes.

Actividades practicadas en los laboratorios: Entre los procedimientos más utilizados figuran aquellos que operan sobre evidencia digital de almacenamiento, tales como búsqueda de con-

tenidos por criterio, creación de líneas de tiempo recuperación de información eliminada o análisis de correos electrónicos y mensajes en redes sociales.

Mecanismos de acceso remoto: La utilización de mecanismos de acceso remoto sin el conocimiento del usuario - a través del uso de malware- plantea serias dudas sobre su legalidad. En este sentido, se ha señalado la peligrosidad del malware para ejercer vigilancia sistemática contra periodistas y defensores de derechos humanos, debido a su capacidad para infectar computadoras y teléfonos móviles con distintos tipos de software malicioso, lo cual permite a las autoridades extraer información de los dispositivos e incluso tomar control del mismo para convertirlo en un dispositivo completo de vigilancia.

Evidencia en la nube: Hay una creciente atención en el aprovechamiento de los servicios de la nube para la obtención de prueba digital. Sin embargo, se remarca que la falta de un marco normativo impacta de manera especial en este tema, ya que las autoridades se ven obligadas a llevar acuerdos con cada una de las empresas privadas (mayormente extranjeras) proveedoras de servicio o incluso a ajustarse a las condiciones unilaterales impuestas por aquellos.

En conclusión, más allá de las diferencias particulares de cada país, existen ciertas problemáticas en común que parecen ser producto de la falta de una reacción apropiada a la aparición del fenómeno de las tecnologías digitales. Es como si la repentina disponibilidad de tantos recursos hubiera entusiasmado a las autoridades debido a los beneficios prometidos, y alentados por ese entusiasmo, se dispuso su rápida utilización sin realizar diagnósticos mínimos de situación y sin evaluar la necesidad de contar -y en su caso crear- las condiciones normativas, técnicas y presupuestarias indispensables para lograr su correcto uso.

Así, la oportunidad de llevar adelante investigaciones eficaces se vuelve riesgosa debido a la probabilidad de errores en los procedimientos que vuelvan inválida la prueba recolectada. Además, las garantías y derechos de las personas investigadas se encuentran en peligro ya que la utilización de estas técnicas -sin las debidas salvaguardas- tiene el potencial de afectar su privacidad o revelar información personal. Finalmente, este panorama amenaza con perjudicar las garantías procesales que todo sistema democrático debe tener para asegurar que las personas sean acusadas -y eventualmente condenadas- luego de una investigación independiente, imparcial y lícita.

En ese sentido, todo intento por encauzar el fenómeno debe tener una aproximación múltiple. Esto significa que los esfuerzos por generar normativa específica deben estar acompañados por una mejora en la capacitación de los operadores -incluida una fuerte enseñanza en derechos humanos- y una actualización en las herramientas utilizadas, en el sentido de elegir aquellas que brinden garantías de respeto a la privacidad, los datos personales y las salvaguardas procesales. Dentro de este contexto, toda incorporación de tecnología debe evaluarse no solamente en base a los beneficios que brinda a los investigadores sino también en base a las potencialidades de aquellas herramientas para incurrir en actividades de vigilancia masiva y control sobre las conductas e información de los individuos.