Material Imprimible

Curso Ciberdelitos y Derecho Informático

Módulo 4

Contenidos:

- Medidas procesales de evidencia digital
- Medios modernos de investigación digital
- Informe pericial
- Agente encubierto informático

Medidas procesales de evidencia digital

La criminalística es una ciencia que se va a vincular estrechamente con el resguardo de la evidencia.

El Licenciado en Criminalística argentino Carlos Guzmán, en el año 1997, expuso lo siguiente acerca de la criminalística: "En el área de la investigación criminal, la ciencia multidisciplinaria denominada criminalística ha emergido como una importante fuerza que tiene impacto en prácticamente todos los elementos del sistema judicial criminal. La misma ha sido definida 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".

Podemos decir entonces que esta disciplina nos va a dar un lugar de estudios y análisis, los cuales se van a focalizar en la reflexión intensa respecto a las evidencias y a los hechos relacionados a la escena que se esté indagando, donde se efectuaron las acciones tipificadas como delitos.

Desde la intervención, se deben desplegar un conjunto de técnicas, herramientas, estrategias, métodos y acciones para hallar en los medios informáticos la evidencia requerida para verificar e identificar las diferentes cuestiones relacionadas a hechos ilícitos y medios utilizados para la perpetuación de los mismos.

Se considera que la informática forense es un área sumamente innovadora en el mundo de la criminalística, y que si bien en un inicio se visualizó a esta disciplina de manera aislada, más vinculada a la seguridad informática, hoy en día forma parte de una rama fundamental de la criminalística, haciendo uso de los procedimientos y las técnicas de esta ciencia de manera habitual, puntualizando este vínculo respecto a las características volátiles que mantienen las evidencias digitales.

Se hace imprescindible conceptualizar y describir la terminología de manera propicia, para así colaborar en especificar el rol que mantiene un sistema informático dentro de la esfera delictiva, y para poder desarrollar de forma eficiente esta clase de

investigaciones, la adquisición de elementos indiciarios, y luego las evidencias requeridas para mantener el caso.

Con el fin de proceder eficazmente en la materia, se generaron distintas categorías, a razón de poder distinguir entre la evidencia de carácter electrónico o los elementos materiales que componen el sistema informático, es decir, el hardware, y la información mantenida en estos sistemas, digitalmente, o sea, el software. Esta diferenciación es sumamente útil para poder diseñar y desplegar los procedimientos idóneos para analizar cada clase de evidencia y generar una correlación adecuada entre una escena del crimen tangible, ubicada en un espacio físico, y la evidencia digital.

Cabe aclarar entonces que con el hardware nos referimos al conjunto de elementos físicos de los sistemas informáticos, mientras que la información que se mantiene en formato digital vienen a ser todos los programas, datos y mensajes trasmitidos a partir de la utilización de los sistemas informáticos.

Es habitual que haya confusión respecto a los términos evidencia electrónica y evidencia digital, y que esta terminología sea utilizada indistintamente. Por eso, es menester marcar la diferencia entre los dispositivos electrónicos, como los teléfonos móviles, los asistentes digitales y la información almacenada digitalmente que se hallen en ellos. Esto resulta fundamental, ya que la investigación siempre tenderá a focalizarse en la evidencia digital, teniendo igualmente en cuenta que en ciertos casos también el punto principal de análisis podrán ser los dispositivos electrónicos.

Con el objetivo de que los forenses mantengan una noción de dónde investigar respecto a la evidencia digital, ellos deberán reconocer las fuentes donde es más habitual hallar la evidencia de este tipo, posición que otorgará al analista la metodología más propicia para, posteriormente, realizar la adecuada preservación y recolección de los elementos.

Las fuentes de evidencia digital pueden ser diferenciadas a partir de tres clases de sistemas: los sistemas de comunicación, los sistemas informáticos abiertos y los sistemas afines a la informática.

Los sistemas de comunicación van a estar conformados por las redes de telecomunicaciones, el internet y las demás comunicaciones inalámbricas. Además, son una fuente que mantiene grandes cantidades de información de carácter digital.

Por otro lado, los sistemas informáticos abiertos van a ser aquellos que están conformados por las computadoras personales y todos sus dispositivos periféricos, como el mouse, el teclado, el monitor, los servidores, notebooks, etc. Hoy en día los ordenadores mantienen una amplia capacidad de almacenar grandes cantidades de información, lo que de igual forma conlleva a que sea un tipo de fuente sumamente importante.

Por último, los sistemas afines a la informática van a ser los que están conformados por los teléfonos inteligentes, las tarjetas inteligentes, los asistentes personales digitales y demás dispositivos electrónicos que mantengan información de índole digital.

La evidencia digital, al tener la característica particular de la omnipresencia, suele hallarse habitualmente relacionada a distintos hechos. Sería extraño que el delito no esté vinculado, por ejemplo, a mensajes de datos almacenados y transmitidos a partir de medios informáticos. Un analista podría distinguir el contenido de dichos mensajes para encontrar manifiesto el accionar ilícito, además de poder realizar un perfil de su actuación y vincularlo con sus víctimas.

Recomendaciones respecto a cómo manejar en primera instancia la evidencia que se halle en la escena del hecho

Antes de desplegar cualquier acción, hay que asegurar y preservar el lugar. Esto se lleva a cabo poniendo énfasis en fijar la escena con fotografías y videos y asegurando los equipos y demás dispositivos electrónicos.

Asimismo, es fundamental no manipular ningún elemento sin la utilización de guantes, ya que podría modificar, tapar o hacer borrar las improntas dactilares y demás evidencia de carácter transitorio sobre las superficies.

A su vez, si el dispositivo que se halle no se encuentra encendido, no debe encenderse, con el objetivo de evitar que se inicien programas de autoprotección. Si es factible, se

debe verificar el sistema operativo con el objetivo de dar comienzo a la secuencia de apagado y así evitar que se pierda información. Solamente se debe desconectar el dispositivo de forma inmediata si hay sospechas de que el dispositivo está destruyendo la evidencia. En cambio, si los dispositivos que se encuentran están encendidos, no se los deben apagar en el acto, ya que sería posible perder la información de carácter volátil, que es la que se borra cada vez que se apagan los dispositivos.

Recomendaciones para cuando no contamos con un técnico en la escena. Dichas recomendaciones fueron elaboradas por el abogado y profesor de Derecho Informático ecuatoriano Santiago Acurio Del Pino en el año 2009, en el Manual de Manejo de Evidencias Digitales y Entornos Informáticos.

- Primeramente, no usar el equipo informático que está siendo investigado, ni intente buscar evidencias sin el entrenamiento adecuado. Si está encendido, no lo apague inmediatamente
- Si el equipo informático tiene un mouse, muévalo cada minuto para no permitir que la pantalla se cierre o se bloquee
- Si una computadora portátil no se apaga cuando es removido el cable de alimentación, localice y remueva la batería. Una vez que esta es removida, debe guardarse en un lugar seguro y no dentro de la misma máquina, a fin de prevenir un encendido accidental
- Si el aparato está conectado a una red, anote los números de conexión, es decir, los números IP
- A su vez, fotografíe la pantalla, las conexiones y cables
- También es importante usar bolsas especiales antiestáticas para almacenar diskettes, discos rígidos, y otros dispositivos de almacenamiento informáticos que sean electromagnéticos. Si no se cuenta con estas bolsas, pueden utilizarse bolsas de papel madera
- Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática que puede destruir los datos

- Asimismo, se debe colocar etiquetas en los cables para posteriormente facilitar la reconexión
- Anota la información de los menús y los archivos activos sin utilizar el teclado, ya que cualquier movimiento del teclado puede borrar información importante
- Si hay un disco, un disquete, una cinta, un CD u otro medio de grabación en alguna unidad de disco o grabación, retírelo, protéjalo y guárdelo en un contenedor de papel
- Asimismo, bloquee toda unidad de grabación con una cinta, un disco o un disquete vacío aportado por el investigador
- A su vez, se debe sellar cada entrada o puerto de información con cinta de evidencia.
- De igual manera, deben sellarse los tornillos del sistema a fin de que no se puedan remover o reemplazar las piezas internas del mismo.
- También se debe desconectar la fuente de poder de todo hardware de red, como router, modem, swich, etc.
- Mantenga el sistema y medios de grabación separados de cualquier tipo de imán, o campo magnético
- Al llevar aparatos, anote todo número de identificación, y mantenga siempre la cadena de custodia.
- Lleve también cables, accesorios, conexiones, y si es posible, manuales, documentación, y anotaciones

En el caso de que los equipos pertenezcan a un servidor conectado a una red, como podría ser en una oficina laboral o negocio, el desconectar la misma puede tener varias consecuencias negativas, como podrían ser la irrupción ilegal del giro del negocio, un daño permanente al equipo en cuestión, y la responsabilidad civil para la fiscalía y fuerza de seguridad interviniente.

Es factible hallar gran cantidad de evidencia dentro de los Smartphone o teléfonos móviles inteligentes, entre ella, identificador de llamadas, llamadas entrantes, números

llamados, números marcados, números guardados en la memoria y en el marcado rápido, nombres y direcciones, números de acceso al correo de voz, contraseñas, números de tarjetas de crédito, información de acceso a internet y a la casilla de mail, número PIN, imágenes, grabaciones de voz, fotos, y todo tipo de información que se encuentre en la tarjeta de memoria y en el dispositivo.

Los recaudos que hay que tener sobre estos dispositivos móviles son los siguientes:

- Si el dispositivo está encendido no hay que apagarlo, ya que puede iniciarse un bloqueo del mismo
- Se debe procurar transcribir toda la información que se pueda visualizar en la pantalla y tomar fotografías de la misma y del aparato con referencia métrica y desde varios ángulos
- También es fundamental sellar todos los puntos de conexión, entradas y salidas de, por ejemplo dispositivos de tarjetas o memorias
- Asimismo, se debe revisar la batería y anotar los datos del dispositivo, ya que el mero transporte en la evidencia puede hacer que se vaya descargando. Por las dudas que esté próximo a apagarse, es prudente llevar consigo un cargador
- De igual manera, se debe asegurar el conector electrónico y sellar los tornillos, con el fin de evitar que se muevan o se sustraigan componentes internos
- También se deben revisar todos los dispositivos de almacenamiento que puedan ser removidos, y anotarlos
- Asimismo, va a ser propicio contar con bolsas de Faraday, que son elementos para aislar las emisiones electromagnéticas. La evidencia electrónica debe guardarse y trasladarse dentro de las mismas
- Por último, cabe destacar que dada la amplia variedad y cantidad de dispositivos electrónicos que existen y se van introduciendo al mercado día a día, es fundamental que el analista indague respecto a los manuales del usuario vinculado a los aparatos hallados

Medios modernos de investigación digital

En cuanto a la recolección de evidencia digital, hay una amplia variedad de herramientas que se pueden emplear para la recuperación de información. Cada vez se hace más necesario que estas herramientas sean más sofisticadas, debido a que se multiplican en cantidad y variedad los datos que pueden estar almacenados en los dispositivos electrónicos y, a su vez, existen grandes cantidades de formatos y extensiones que podemos hallar en un mismo sistema operativo.

La información recolectada no debe ser la correcta y la requerida, sino que debe ser comprobable en cualquier momento de la investigación y posterior a la misma, y se debe poder verificar que la información recolectada no fue alterada y se obtuvo por metodologías reconocidas y aceptadas. Entonces, poder mantener estas herramientas de carácter sofisticado nos auxilian a achicar los tiempos para poder efectuar el análisis de toda la información obtenida.

Otro de los desafíos actuales es la facilidad con la que es posible borrar los archivos de los ordenadores, sumado a las herramientas de encriptación que surgen y las contraseñas.

Asimismo, una cuestión relevante para tener en cuenta es el marcado de documentos. Resulta útil una herramienta que permita hacerle marcaciones a un documento importante, lo cual es de gran relevancia en situaciones vinculadas con la sustracción de información, debido a que al marcar el documento se le puede hacer el seguimiento y detectarlo con manera sencilla.

Dentro del área de la seguridad informática se va a focalizar en la prevención de los ataques, ya que muchas empresas y sitios mantienen información de gran valor y es por eso que intentan protegerse a partir de mecanismos de validación de este estilo.

Otro punto que debemos ver es el control de computadoras y el monitoreo. Hay casos en los que se precisa saber cuál es el empleo que se le ha hecho a la computadora, previo de que se efectúe la pericia. Ante esta circunstancia, existen herramientas de control que se le instalan a las computadoras para así recopilar dicha información.

Entre las herramientas disponibles hallamos algunas muy sencillas de implementar, como las key logger, las cuales consisten en almacenar en un archivo de texto todo lo

que se teclea. De igual manera, existen intermedios que guardan capturas de la pantalla del usuario monitoreado. Por su parte, las herramientas de más complejidad llegan a permitir la toma de control total sobre la computadora, en conjunto a la observación directa de lo que realiza el usuario.

Profundizando en el hardware, se puede manifestar que la metodología de recopilación de evidencia debe ser exacta y no se debe alterar la información que se ha diseñado. A partir de este principio, se han desarrollado varias herramientas que nos van a permitir recuperar la información sin modificar los datos, ya que hoy en día seguimos teniendo como principal inconveniente que se alteren los registros de la computadora cuando la encendemos.

Programas que más se suelen utilizar actualmente para el análisis forense usadas en materia de informática forense, puntualmente para la recolección de evidencia y recuperación de datos borrados:

- Foremost es un programa que se emplea a partir de Linux y que sirve para efectuar análisis forenses. Este lee de una partición de disco o de un fichero de imagen y así puede extraer ficheros
- Advanced incident response tool consta de varias herramientas para la respuesta y el análisis ante un incidente
- Outport es un programa que va a permitir exportar los datos desde Outlook a correos
- A partir de WebJob se puede descargar un programa con http/https y ejecutarlo dentro de la misma operación
- Por su parte, Md5deep consta de varios programas con los que es posible calcular resúmenes de un número arbitrario de ficheros. Este funciona sobre Windows y Linux
- HashDig permite automatizar el proceso de cálculo de los hashes, así como su comprobación de integridad. Este va a diferenciar los ficheros conocidos de los no conocidos a partir de la comparación de una base de datos referente

- Automated Foresic Análisis es una herramienta que se utiliza para el análisis automatizado de volcados, etapa conformada por varios scripts que localizan información relevante relacionada al análisis forense
- Gpart, por su parte, es un programa que permite recuperar la información de un disco en el cual su sector 0, es decir, el registro de arranque de cualquier dispositivo de almacenamiento de datos, se encuentre dañado, haya sido eliminado o simplemente sea incorrecto, pudiendo mostrar el resultado obtenido a un fichero
- Por último, Dump Event Log es una herramienta de línea de comandos que muestra el log de eventos propios de un sistema remoto o local en un fichero de texto

Principales programas que nos permiten la recuperación de datos y, además, el estudio de los navegadores:

- iDetect Toolkit es un programa que auxilia al investigador forense en el análisis de la memoria de un sistema que se encuentre comprometido
- Srprint es un programa que permite mostrar el contenido de los ficheros de log del beneficio de restauración del sistema de Windows XP. Esta clase de logs nos auxilian a averiguar la fecha de surgimiento y borrado de ficheros que ya no se encuentren en el sistema
- Por su parte, Pasco es un programa que permite analizar los ficheros de registro de la actividad en la web utilizando Internet Explorer
- Rifuiti es un mecanismo para el análisis forense de la información que se encuentra en la Papelera de Reciclaje de un sistema de Windows
- Reg Viewer sirve para la navegación de ficheros de registro pertenecientes a Windows. Este va a operar de forma independiente a la plataforma en la que se opere
- ProDiscover Basic Edition es un programa que brinda un entorno muy completo para el análisis forense de sistemas que se encuentren en Windows. Este va a

auxiliar en la realización de imágenes, análisis, preservación y realización de informes de los datos contenidos en el aparato en el cual se esté efectuando el análisis.

- FTK Imagen es un programa gratuito que nos va a permitir efectuar imágenes de un dispositivo que se encuentre comprometido. Entre sus características también se encuentra el cambio entre los distintos formatos de imagen
- Por su parte, Allimage es un programa que está diseñado para Windows y que nos brinda la posibilidad de generar imágenes bit a bit en cualquier clase de dispositivo de almacenamiento de información.
- PlainSight es un programa que mantiene un entorno sumamente completo para el análisis forense respecto a sistemas. Este se utiliza bajo el sistema Linux y se puede ejecutar desde un CD.
- Por último, PyFlag es un programa muy avanzado en materia de análisis forense de imágenes de log y grandes volúmenes de información en general. Fue creada por el lenguaje de programación Python y posee una interfaz sencilla de acceder a partir del navegador web. Una de sus características es que facilita el análisis de la memoria física que corresponde a los sistemas Windows.

Cuando hablamos de técnicas anti-forenses nos referimos a metodologías que buscan frustrar las pericias, a las herramientas forenses y a los peritos en sí.

Una de las maneras empleadas es el ocultamiento de evidencia digital. La criptografía, que es una técnica que consiste en escribir claves o procedimientos de forma secreta para que lo escrito solo pueda visualizarse por quien sepa cómo descifrarlo, asegura la protección de los datos y genera un canal para comunicarse de forma segura ante un análisis forense. Por su parte, a partir de la esteganografía, que es la aplicación y estudio de técnicas que nos permiten ocultar mensajes, se esconde la información de tal manera que el analista forense no observa el envío de los datos secretos.

Otra posibilidad va a ser el ocultamiento de datos en lugares no convencionales del sistema, en donde ciertas metodologías eliminan información almacenada para así

lograr destruir la evidencia digital. La limpieza de un disco puede ser analógica, lógica, criptográfica o digital.

Sin embargo, hay metodologías más drásticas, como lo son la devastación física del dispositivo de almacenamiento. Estas metodologías son denominadas anti-concepción de datos, las cuales van a operar a partir de la evitación de la creación de datos. Generalmente se efectúan llamadas al sistema de un proceso lejano, o bien, se ejecutan los procesos de forma completa para no dejar rastros directamente en la memoria.

También hay técnicas llamadas "de ofuscación", que intentan confundir la investigación y desviarla hacia diferentes caminos. Lo que se suele hacer es sobrescribir metadatos de los archivos y aplicar ciertas maniobras en el envío de correos electrónicos para que no se pueda detectar de forma sencilla el receptor o emisor.

Actualmente está preponderando como técnica el ataque a softwares forenses, particularmente sobre la validación de datos, provocando denegación de servicio o modificando la integridad del hash. Ciertos autores cuestionan, en función a esto, las distintas fases de los procesos forenses empleados para la recolección y análisis de la evidencia digital.

Podemos decir que existe un vínculo estrecho entre los crímenes informáticos, las técnicas anti-forenses y el hacking. La tecnología evoluciona más rápidamente que la legislación en vigencia, por lo que continuamente nos enfrentamos a vacíos legales que pueden ser aprovechados. Esta actividad, al sobrepasar los límites de los Estados, configura delitos muy complejos de juzgar.

En cuanto a la normativa de la República Argentina, existen ciertas insuficiencias en función al Convenio sobre Ciberdelincuencia. Sin embargo, en comparación a otros Estados de América Latina, se encuentra relativamente actualizada.

El hacker ético puede emplear técnicas anti-forenses con el objetivo de mejorar el software y las metodologías forenses sin que esto sea considerado un ilícito.

Los especialistas en el área de la seguridad informática emplean varias técnicas a fin de salvaguardar los sistemas y dispositivos de cualquier tipo de intrusión o ataque efectuados por hackers, y así precaver que estos obtengan o alteren la información. Una de las metodologías que emplean es el Ethical Hacking, o hacker ético, que mencionamos previamente.

El fin principal de este es explotar las vulnerabilidades que mantienen los sistemas, realizando diversas pruebas de intrusión, que van a ayudar a evaluar y verificar la seguridad, tanto lógica como física.

Las pruebas pueden realizarse sobre redes de computadoras, sistemas de información, bases de datos, aplicaciones Web, servidores, entre muchos otros. Si a partir de esta técnica es factible acceder, se puede demostrar que el sistema es vulnerable y a qué aspectos. A partir de los datos recabados por estos especialistas, es posible tomar medidas de prevención en contra de posibles ataques.

A partir de esto podemos definir al **Hacker Ético** como el individuo especialista que efectúa pruebas de penetración.

El hacker ético va a ser idóneo en redes de datos y en distintos dispositivos, va a saber de qué manera es posible realizar los ataques a los sistemas de seguridad y los va a efectuar en nombre de los empleadores, únicamente con la motivación de indagar y hallar vulnerabilidades, procediendo de manera similar y empleando las mismas técnicas que utilizaría un hacker con fines maliciosos. Básicamente vulneran e ingresan a los sistemas de las empresas que los contratan para reportar qué vulnerabilidades mantienen, en vez de borrar o alterar la información.

A partir de estas evaluaciones de penetración se permite probar vulnerabilidades, brindar recomendaciones, categorizar y analizar las debilidades halladas, en función, además, a las prioridades de la empresa. Luego se trabajará en la erradicación de dichas vulnerabilidades.

En cuando a las garantías que ofrece esta técnica, enumeramos a las siguientes:

- Demuestra configuraciones no propicias para las aplicaciones que se hayan instalado
- Disminuye el esfuerzo y el tiempo necesarios para afrontar este tipo de situaciones
- Identifica qué sistemas requieren actualizaciones
- Brinda un panorama respecto a las vulnerabilidades encontradas para ver cómo proceder ante las mismas

Hay un vínculo estrecho entre las técnicas anti-forenses y las técnicas de los hackers. Las metodologías empleadas en materia forense, así como cualquier programa, mantiene vulnerabilidades o fallas respecto al diseño y precisan mejorarse. Respecto a este punto es donde adquieren relevancia los trabajaos realizados por los hackers éticos, ya que estos especialistas pueden desplegar técnicas anti-forenses o puntualizar en los defectos de los programas forenses.

Asimismo, hay ciertos códigos de ética informática que pueden emplearse de base para los profesionales en esta materia. Estos conceptos conllevan a evitar delitos informáticos, robo o intrusión y fraude desde la moral y no aplicando la normativa de la legislación.

Respecto a cómo evadir o sobrepasar un análisis forense, el infractor informático deberá entender el actuar desde el lugar del perito forense y saber cómo se emplean y se desarrollan las técnicas y metodologías forenses. De forma mutua, el analista forense tendrá que analizar las últimas herramientas anti-forenses para establecer si la pericia informática servirá y qué esfuerzo podría conllevar.

Por todo lo informado, podemos decir que el analista forense y el delincuente cibernético son dos figuras que, si bien se encuentran enfrentados, se han retroalimentado recíprocamente a través de los años para así mejorar sus metodologías, ya sean anti-forenses o forenses.

Informe pericial

Por prueba pericial entendemos al informe realizado por un individuo ajeno al proceso, que cuenta con conocimientos científicos y/o técnicos respecto a la materia que se precisa para el interrogante pericial. A partir de un proceso metodológico deductivo, y en base a sus saberes específicos, el individuo aplica conocimientos al caso concreto y brinda su opinión de manera fundamentada con los elementos que surgen a partir del análisis.

El perito que se designe por parte del Poder Judicial va a ser un auxiliar del órgano respectivo que, de acuerdo a su idoneidad, va a contribuir a dilucidar el caso en las cuestiones técnicas y científicas que no sean propias del saber del juez.

En su rol, el perito va a tener que cumplir con ciertas características:

- En primer lugar, conocimiento, ya que se requiere que el individuo posea una formación de experticia, la cual puede estar reglamentada o provenir de la experiencia de sus labores, conocimientos científicos, artísticos, técnicos, especializados o prácticos respecto a la temática que se precise en el dictamen del caso concreto
- En segundo lugar, objetividad, debido a que es fundamental que se trate de un individuo ajeno al proceso en el cual se lo requiera y, además, debe tener absoluta imparcialidad respecto al caso concreto
- Por último, voluntariedad, ya que el individuo debe aceptar desempeñarse en su función sin ningún tipo de coacción.

Asimismo, es necesario distinguir ciertos principios que se deben regir en los informes periciales:

- Se deben ordenar los pensamientos, respondiendo adecuadamente los puntos de pericia que se requieren
- Nunca se deberá admitir nada como verdadero o falso sin mantener la evidencia apropiada que lo respalde y corrobore
- Y se sugiere hacer recuentos integrales y revisiones exhaustivas a fin de reforzar que no se omita nada.

Además, los puntos que deben estar siempre en todos los dictámenes que se emitan son:

- Una descripción pormenorizada de todas las operaciones efectuadas en el informe y sus conclusiones
- La correcta descripción del objeto, cosa material o individuo sujeto a análisis, así como también, la forma y el estado en el que se encuentran al momento de efectuar la pericia
- También las conclusiones a las que se arriban, redactadas de manera clara y comprensible
- Y los principios técnicos o científicos en los que se basan para emitir la pericia

La abogada argentina Estelly Mary Díaz Fernández, señaló en el año 2016 en un artículo de la Revista In Iure lo siguiente. "La labor pericial contribuye a aportar cierta información al sentenciante, en una actividad de asesoramiento, a los fines de facilitar la formación de una opinión fundada acerca de los puntos que fueron objeto de dictamen. Pero luego, una vez que el juez ha formado su opinión fundada, en parte pero no exclusivamente por conducto de ese asesoramiento a cargo del experto, será el magistrado quien, evaluando la prueba pericial no aisladamente, sino en conjunto con la totalidad de la prueba incorporada al proceso, conforme a las reglas de la sana crítica, emitirá su juicio a partir de la convicción o certeza moral acerca del acontecer histórico de los hechos materia de juzgamiento; juicio que se concretará en la construcción de

una norma individual cuyo objeto es plasmar el valor de lo justo para el caso particular, conforme al derecho vigente y a una noción de equidad."

A partir de lo recapitulado, se aclara la sumatoria de las características sine qua non de los dictámenes periciales:

- El fin principal va a ser transmitir la información obtenida de manera clara y objetiva, ya que, habitualmente los que lean y hagan uso del informe, van a ser legistas que no necesariamente saben respecto a la especialidad respectiva
- Pueden ser varios los modelos que se incorporan en el informe, incluso existe el concepto de contra pericia cuando un tema es sujeto a debate por las partes
- Asimismo, el informe no va a ser una demostración de las capacidades del perito, ya que eso no será lo importante para la causa
- Será preciso remarcar la condición independiente del especialista
- A su vez, la pericia, en su totalidad, debe de ser comprensible por cualquier persona que no sepa del tema. Para eso, será sugerente utilizar métodos pedagógicos para hacer más sencilla la comprensión
- Además, el dictamen no podrá estar condicionado y bajo ningún aspecto tendrá información que no corresponda con los resultados objetivos adquiridos en el proceso de investigación
- Toda la información obtenida debe justificar cuestiones vinculadas a los interrogantes periciales
- Asimismo, los objetivos solicitados deben ir en línea con el desarrollo de la pericia
- La pericia deberá seguir una estructura bien definida y organizada
- Y por último, el dictamen no podrá exponer cuestiones que se encuentren resueltas de manera adecuada

Particularmente, la pericia informática se va a referir, como indica la palabra, a la investigación y estudios relacionados a la adquisición de una evidencia electrónica de aplicación en un caso judicial o extrajudicial para que auxilie a decidir respecto a distintos interrogantes que surgen en la causa.

Agente encubierto informático

El Tribunal Supremo de España ha descrito a esta figura en su sentencia 1140/2010, del 29 de diciembre del 2010, de la siguiente forma: "El término undercorver o agente encubierto, se utiliza para designar a los funcionarios de policía que actúan en la clandestinidad, con identidad supuesta y con la finalidad de reprimir o prevenir el delito. Agente encubierto, en nuestro ordenamiento, será el policía judicial, especialmente seleccionado, que bajo identidad supuesta, actúa pasivamente con sujeción a la Ley y bajo el control del Juez para investigar delitos propios de la delincuencia organizada y de difícil averiguación cuando han fracasado otros métodos de la investigación o estos sean manifiestamente insuficientes para su descubrimiento. Permite recabar información sobre su estructura y modus operandi, así como obtener pruebas sobre la ejecución de hechos delictivos, debiéndose aclarar que es preciso diferenciar esta figura del funcionario policial que, de forma esporádica y aislada y ante un acto delictivo concreto, oculta su condición policial para descubrir un delito ya cometido."

Respecto a las medidas que se toman, son numerosos los derechos fundamentales que pueden afectarse, entre ellos el derecho a la intimidad, el derecho a la protección de datos, el derecho al secreto de las comunicaciones, el derecho a la inviolabilidad del domicilio, entre muchos otros.

Actualmente, los avances del día a día en materia tecnológica han aportado a lo referente de la investigación criminal nuevas metodologías para la persecución de los delitos y la identificación de los delincuentes.

Se considera al agente informático como una manera de agente encubierto, pero, a diferencia del carácter presencial del tradicional, hará su despliegue a partir de canales cerrados de la comunicación.

Los agentes encubiertos informáticos se describen como funcionarios que operan a partir de una identidad distinta en comunicaciones desplegadas en canales de comunicación cerrados, lo que podemos comprender como lo vinculado a las redes sociales o a otras formas de conexión de la web, con el objetivo de esclarecer los ilícitos efectuados por estos medios. Se puede decir entonces que se entiende como una medida puntual de investigación informática focalizada en el descubrimiento y persecución de los delincuentes informáticos.

Si bien el ámbito de actuación del agente encubierto tradicional va a ser sumamente objetivo, el agente encubierto informático mantiene un marco de actuación mucho más abarcativo. A raíz de esto, a continuación se describen las competencias objetivas de las distintas modalidades de agentes encubiertos.

- Su participación como testigo durante el despliegue del juicio oral presume una alteración, debido que la identidad falsa no debe ser expuesta en el plenario y puede conservarse cuando los funcionarios que hayan obrado amparados en ella, testifiquen en dicho proceso que pueda emanarse de los hechos en los cuales han efectuado intervenciones, siempre que así establezca por resolución judicial motivada
- Asimismo, solo pueden desplegarse como agente encubierto funcionarios públicos de fuerzas de seguridad en sentido estricto y solamente podrán hacerlo de manera voluntaria.

Una cuestión a tener en cuenta es que el agente va a estar exento de responsabilidad penal en su accionar, siempre y cuando mantenga la debida proporcionalidad con el desarrollo de la actividad encomendada y no se manifieste como una provocación al ilícito.

Respecto a la naturaleza de esta exención, en primer lugar, puede manifestarse como una causa de justificación, eximiendo de responsabilidad al que infringe la normativa en el cumplimiento de los deberes a su cargo o en el ejercicio legítimo de sus funciones, o también, siendo el caso, por operar bajo un estado de necesidad. Y, en segundo lugar, puede considerarse como una excusa absolutoria, fundamentado en cuestiones de política criminal. En tal caso, impacta en la punibilidad del hecho que, como consecuencia, es injusto, apareciendo la responsabilidad civil por los daños ocasionados y que se establece sobre aquellos en quienes concurra.

El agente informático, mientras mantenga la autorización específica respectiva, podrá realizar las siguientes acciones:

- Adquirir imágenes y grabar conversaciones que puedan darse en los encuentros pensados entre el agente y los individuos a indagar, aunque se lleven a cabo en el interior de la vivienda
- Estudiar los resultados de los algoritmos utilizados para la identificación de los archivos ilícitos respectivos
- Y enviar por sí mismo o intercambiar archivos delictivos a razón de su contenido

La autorización judicial que habilita dichas operaciones tiene que reunir las condiciones esenciales de legitimidad conforme a la constitución de las medidas que limitan los derechos fundamentales. Con esto se manifiesta que deberá existir una proporcionalidad adecuada que ha de disponer toda afectación legítima de estos derechos, alegando la idoneidad de la medida, su debido equilibrio, su necesidad y el beneficio que se obtendrá del mismo respecto de las circunstancias específicas que circundan la investigación penal vigente.

En cuanto a la regulación en Argentina podemos manifestar que la ley 27319 de Investigación, Prevención y Lucha de los Delitos Complejos define al agente encubierto en su artículo 3 de la siguiente manera. “Será considerado agente encubierto todo aquel funcionario de las fuerzas de seguridad autorizado, altamente calificado, que presta su

consentimiento y ocultando su identidad, se infiltra o introduce en las organizaciones criminales o asociaciones delictivas, con el fin de identificar o detener a los autores, partícipes o encubridores, de impedir la consumación de un delito, o para reunir información y elementos de prueba necesarios para la investigación, con autorización judicial."

Por su parte, el artículo 4 expone lo siguiente: "Dispuesta la actuación por el juez, de oficio o a pedido del Ministerio Público Fiscal, su designación y la instrumentación necesaria para su protección estará a cargo del Ministerio de Seguridad de la Nación, con control judicial. El Ministerio de Seguridad tendrá a su cargo la selección y capacitación del personal destinado a cumplir tales funciones. Los miembros de las fuerzas de seguridad o policiales designados no podrán tener antecedentes penales."

Si bien todavía no está regulada la figura del agente encubierto informático, existe un proyecto de ley presentado en el año 2017 en la Cámara de Diputados, donde en el artículo 2 figura lo siguiente: "Incorpórese al artículo 3 de la Ley 27.319 de Delitos Complejos el siguiente párrafo, el cual quedará redactado de la siguiente manera: 'Será considerado agente encubierto informático todo aquel funcionario de las fuerzas de seguridad autorizado, altamente calificado, que presta su consentimiento y ocultando su identidad interactúe, se relacione, participe, a través una identidad supuesta en grupos de internet, redes sociales y plataformas de intercomunicación on-line ,con el fin de identificar o detener a los autores, partícipes o encubridores, de impedir la consumación de un delito, o para reunir información y elementos de prueba necesarios para la investigación, con autorización judicial.'

El artículo 7 de la ley hace referencia a las regulaciones comunes, y allí se explicita que "La información que el agente encubierto, el agente encubierto informático y el agente revelador vayan logrando, será puesta de inmediato en conocimiento del juez y del representante del Ministerio Público Fiscal interviniente en la forma que resultare más conveniente para posibilitar el cumplimiento de su tarea y evitar la revelación de su función e identidad."

Asimismo, el artículo 8 expone que "El agente encubierto, el agente encubierto informático y el agente revelador serán convocados al juicio únicamente cuando su testimonio resultare absolutamente imprescindible. Cuando la declaración significare un riesgo para su integridad o la de otras personas, o cuando frustrare una intervención ulterior, se emplearán los recursos técnicos necesarios para impedir que pueda identificarse al declarante por su voz o su rostro. La declaración prestada en estas condiciones no constituirá prueba dirimente para la condena del acusado, y deberá valorarse con especial cautela por el tribunal interviniente."

Según el artículo 9, "No será punible el agente encubierto, el agente encubierto informático o el agente revelador que como consecuencia necesaria del desarrollo de la actuación encomendada, se hubiese visto compelido a incurrir en un delito, siempre que éste no implique poner en peligro cierto la vida o la integridad psíquica o física de una persona o la imposición de un grave sufrimiento físico o moral a otro."

De acuerdo al artículo 10, "Cuando el agente encubierto, el agente encubierto informático o el agente revelador hubiesen resultado imputados en un proceso, harán saber confidencialmente su carácter al juez interviniente, quien en forma reservada recabará la pertinente información a la autoridad que corresponda. Si el caso correspondiere a las previsiones del artículo anterior, el juez lo resolverá sin develar la verdadera identidad del imputado".

Por su parte, el artículo 11° afirma que "Ningún integrante de las fuerzas de seguridad o policiales podrá ser obligado a actuar como agente encubierto, el agente encubierto informático ni como agente revelador. La negativa a hacerlo no será tenida como antecedente desfavorable para ningún efecto."

Asimismo, el artículo 12 manifiesta que "Cuando peligre la seguridad de la persona que haya actuado como agente encubierto, el agente encubierto informático o agente

revelador por haberse develado su verdadera identidad, ésta tendrá derecho a optar entre permanecer activo o pasar a retiro, cualquiera fuese la cantidad de años de servicio que tuviera. En este último caso se le reconocerá un haber de retiro igual al que le corresponda a quien tenga dos grados de escalafón mayor por el que cumpliera su función." Dicho artículo prosigue manifestando que de ser requerido, deben adoptarse las medidas de protección que sean propicias, dentro de los alcances contemplados en la legislación, de imputados y de testigos. Además, la adquisición de los enunciados que se contienen en el proyecto tendrán que estar sujetos a una evaluación con criterio restrictivo y razonable, en el que el jurista tendrá que analizar la no factibilidad de usar una medida más propicia para dilucidar los hechos que incentivan la investigación o la localización de los infractores.

Esta iniciativa correspondiente a la propuesta de este proyecto inicia con la necesidad de otorgar más instrumentos a la justicia cuando han de investigarse ilícitos vinculados al crimen organizado. En la Argentina contamos con la Asociación Argentina de Lucha Contra el Cibercrimen, que se focaliza en esta temática y que ha planteado la posibilidad de contemplar una transformación en nuestra normativa que proporcione una respuesta efectiva ante el avance persistente de la ejecución de estos tipos de ilícitos.

La aparición continua de nuevas tecnologías ha posibilitado el surgimiento de modernos instrumentos de ataque a partir de la utilización de estos medios, teniendo en cuenta que cada vez es más habitual, como ya lo hemos hablado, la perpetración de ilícitos por medio de la web. Actualmente son millones los individuos que utilizan internet, debido a que, en primer lugar, hace más sencillas las comunicaciones entre personas, otorgando diversos beneficios; pero además, es cierto que la internet conlleva a la facilitación de comisión de ciertos delitos a través de este medio, que de otra manera no se habrían perpetuado debido a la posibilidad que mantienen los autores de adquirir otra identidad para aproximarse a sus víctimas, y así mantener el anonimato.

Existen diversos casos que podemos visualizar a diario respecto a la influencia que mantienen las redes. Esto nos interpela a razón de modificar las normativas existentes y nos traslada a una continua revisión de nuestro sistema penal, que precisa de una evolución a la par de la actividad criminal para brindar las respuestas precisas a las nuevas exigencias en materia de seguridad que precisa la sociedad actual.

El medio tecnológico por parte del gobierno cumple, actualmente, un doble rol en función al proceso penal: en primer lugar, ayuda al perfeccionamiento de los medios analíticos para investigación, obteniendo de esta forma, resultados más confiables; y en segundo lugar, ayuda a la persecución de los ilícitos vinculados directamente con los medios tecnológicos. Como ejemplo podemos citar a España, que avanzó en la temática y en su nueva regulación respecto a la Ley de Enjuiciamiento Criminal, en el artículo 282 bis, donde describe al agente encubierto informático en relación a investigaciones que afecten a actividades propias de la delincuencia organizada.
El proyecto argentino intenta incorporar al agente encubierto informático con motivo de generar una nueva herramienta para la justicia ante los nuevos casos que va afrontando. Recordemos que, como describimos anteriormente, la figura del agente encubierto ya está regulada en nuestra legislación, y a partir del proyecto, lo que se busca es darle mayor especificidad y alcance, contemplando lo ya dispuesto por la ley.

Si bien se está trabajando desde lo tecnológico y jurídico día a día, también cambian y evolucionan las técnicas delictivas. Por eso, lo que se remarca como fundamental es la organización estatal desde el ámbito institucional.

El periodista mexicano Javier Sicilia plantea que "Si no tenemos policías, jueces, abogados, fiscales, honestos, valerosos y eficientes; si se rinden al crimen y a la corrupción, están condenando al país a la ignominia más desesperante y atroz."