*Informática forense, protocolo de actuación**

Sofía González de la Calleja**

La presente obra de Herlinda Vite resulta ser de suma importancia en el mundo del Derecho principalmente, a partir del ya no tan nuevo proceso penal acusatorio y no sólo en el área del Derecho Penal, sino en otras áreas.

El uso masivo de las llamadas tecnologías de la investigación y las comunicaciones permite almacenar y procesar grandes volúmenes de información digital, incluyendo información personal de los usuarios, ya sean personas físicas o jurídicas; sin embargo, dicha información es altamente vulnerable y de fácil transmisión. Es importante señalar que la informática jurídica tiene diversas definiciones, por ejemplo, "aquella Ciencia que tiene por objeto adquirir, preservar, obtener datos procesados electrónicamente a fin de dar certeza real y técnica a las diversas autoridades que así lo soliciten, así como a todos aquellos titulares de dicha información".

La reforma del sistema de justicia penal, que, como es sabido, busca también optimizar y agilizar los procesos penales, se auxilia en gran parte por esta ciencia o disciplina, con el fin de generar certidumbre en sus resoluciones, particularmente en la etapa de la investigación en la que se deberán establecer los indicios que permitan el esclarecimiento de los hechos que puedan ser actos delictivos. Por tal motivo, los actos de investigación deberán llevarse a cabo mediante técnicas o instrumentos tecnológicos que puedan no sólo preservar la información, sino también otorgar mucha más confiabilidad a los interesados, de que dicha información no sólo está resguardada, sino que es confiable. De tal suerte que resulta de gran trascendencia conocer en la obra de Vite la importancia de estos instrumentos al servicio del Derecho.

La evidencia digital tiene particularmente dos características que la hacen sensible: su vulnerabilidad y, desde luego, el gran volumen de información y almacenamiento de los dispositivos. Para que esta información sea válida y admitida jurídicamente se consideran los siguientes conceptos: autenticidad, confiabilidad, completitud o suficiencia, conformidad con las leyes y la administración de justicia, es decir, conforme a derecho.

** Profesora Investigadora en la Facultad de Derecho y Ciencias Sociales de la Benemérita Universidad Autónoma de Puebla, México. (sofiadelacalleja@hotmail.com)

La autenticidad se refiere a la no alterabilidad de la información original, la confiabilidad en cuanto a las fuentes creíbles y verificables, y que sean útiles al proceso; la suficiencia se refiere principalmente a que la información sea suficiente o que realmente aporte o sirva para complementar otras pruebas, ya que la falta de suficiencia comúnmente es factor de dilación o pérdida del proceso o del juicio; la conformidad con las leyes hace referencia a que dichas pruebas sean aceptadas para la recolección, el aseguramiento y el análisis como evidencia digital.

En materia de medios digitales existen criterios internacionales como los de la IOCE, la Convención de Cibercrimen, presentada por la Comunidad Europea, entre otros, en donde se establecen lineamientos y parámetros que sirven para afianzar el tratamiento de evidencia en medios electrónicos.

El proceso de registro que marca el Código Nacional de Procedimientos Penales (CNPP), en su artículo 227, que tiene como fin garantizar la no alteración o no contaminación de los indicios, tendría que ser suficiente para otorgar esa certeza jurídica. En el procedimiento de cuidado o embalaje de los indicios digitales, es importante decir que existen bolsas antiestáticas para su cuidado; desde luego, la autoridad —suponemos— sabrá también cómo manejar dicha evidencia.

El método de la informática forense básicamente se organiza de la siguiente manera: identificación, preservación, análisis y presentación de resultados; esto, desde luego sugiere que se trata de mucha información que, a juicio de la autoridad, podrá seleccionarse partiendo del planteamiento del problema, la adquisición de copias o reproducciones, el análisis, la extracción e interpretación de los datos contenidos y, por último, la documentación y el dictamen, es decir, el soporte documental o dictamen pericial. Los rastros informáticos son en extremo sensibles; se recomienda, a fin de prever un ataque digital, evitar apagar computadoras, encender un equipo apagado, ejecutar aplicaciones, realizar búsquedas, desconectar dispositivos de almacenamiento y abrir archivos en el equipo de cómputo.

Actualmente, la mayor parte de las TIC son dispositivos altamente intrusivos, por lo que se recomienda que el profesional en informática forense actúe con respeto a los derechos humanos y con respeto a los usuarios, tal como lo indica el Código de Procedimientos Penales en su artículo 251, que indica:

Actuaciones en la investigación que no requieren autorización previa del juez de control:

1. Inspección del lugar del hecho o del hallazgo.
2. Inspección del lugar distinto al del hecho o hallazgo.
3. Inspección de personas.
4. La revisión corporal.
5. Inspección de vehículos.
6. Levantamiento e identificación de cadáver.
7. La aportación de comunicación entre particulares.
8. Reconocimiento de personas.
9. La entrega vigilada y las operaciones que autoricen los protocolos emitidos para tal efecto por el procurador.
10. La entrevista a testigos, y
11. Las demás en las que expresamente no se prevea control judicial.

Respecto al punto nueve, las actuaciones deberán estar autorizadas por el procurador. Con excepción de los actos mencionados, se requiere de autorización del juez de control para todos los actos de investigación que impliquen una afectación a los derechos constitucionales.

Algunos procedimientos recomendados en Informática Forense: (RAM) Memoria de acceso aleatorio de imágenes. La recolección y análisis de la RAM puede revelar las claves de encriptación de los sistemas de archivos o carpetas, programas, confecciones a redes, etc. Incluso accesos remotos a la computadora, una vez que se apaga el equipo se pierde la información ya que solo se almacena en la RAM.

Los ruteadores también son computadoras que pueden almacenar información importante sobre todas las computadoras con acceso a Internet mediante ese ruteador, y pueden indicar computadoras conectadas desconocidas, almacenamientos remotos y otros dispositivos.

La identificación de usuarios conectados en la terminal o de manera remota puede ayudar a identificar a la persona responsable de la actividad o en la computadora. Saber quién está conectado podría revelar cuentas de usuarios en riesgo, cuentas no autorizadas, etc.

Respecto a las aplicaciones, el VOIP (protocolo de voz sobre Internet, en español) es una tecnología que permite a la gente hacer llamadas "telefónicas" y conferencias de audio o video en Internet. Aplicaciones como Skype,

Vonage y otros programas de VOIP con frecuencia tienen bitácoras sobre la computadora que documenta la actividad. Esta información podría revelar a quiénes están asociados con actividad delictiva e información importante para la investigación.

Newsgroups es una plataforma en línea para la comunicación e intercambio de información de algún tema, se usan para intercambiar archivos y mensajes entre los inscritos en esta plataforma; por lo general, se utiliza por parte de los agentes de la policía de investigación.

Es inmenso el uso de herramientas informáticas al servicio del Derecho, tales como las hojas de cálculo, los algoritmos útiles para investigaciones de pornografía infantil, las rutas de archivo, los proveedores de servicio, las redes sociales, los programas Peer to Peer, las direcciones IP, programas ajustados para correr automáticamente y comandos ejecutados, etc.

Todas estas tecnologías de información útiles para los profesionales de la informática forense deben apegarse, como ya se comentó, a derecho, contar con todas las herramientas legales establecidas en el CNPP y cuidar que su actuación se apegue en todo momento al estricto respeto a los derechos humanos de los usuarios de estas tecnologías.

Por lo tanto, resulta de suma importancia que se conozca la informática forense al servicio el derecho y, en particular, al nuevo proceso penal acusatorio, en donde la adecuada preservación y recolección de los indicios será determinante como medios de prueba.