CIBERCRIMINALIDAD

Óscar Manuel Lira Arteaga*

Sumario: I. *La cibercriminalidad en nuestro país*. II. *Investigación pericial en cibercriminalidad*.

I. La cibercriminalidad en nuestro país

En nuestro país, hoy más que en otros tiempos, la ausencia en la aplicación de procedimientos de investigación forense con relación a conductas delictivas que utilizan como medio las tecnologías de la información y comunicación (TIC), acordes a las normas de investigación establecidas por organizaciones internacionales, tales como la del Grupo de Trabajo Científico en Evidencia Digital (SWGDE** por sus siglas en inglés), apegadas a la legislación de nuestro país, provocan que la persecución de este tipo de delitos no sean resueltos en todos los casos de manera exitosa por los actores que intervienen en la administración y en la procuración de justicia (jueces, agentes del Ministerio Público, peritos y policía investigadora). Sin embargo, es importante señalar que si bien delitos como la pornografía infantil, fraude, extorsión, falsificación, el robo de información, la alteración de información, el espionaje, el secuestro, las amenazas, entre otros,

* Maestro en tecnologías de la información por la Universidad la Salle. Presidente de la Asociación Latinoamericana de Profesionales en Seguridad Informática.

** Grupo de Trabajo Científico en Evidencia Digital (SWGDE, Scientific Working Groupon Digital Evidence) *http://68.156.151.124/*

hoy se vale del uso de las nuevas tecnologías, como lo son dispositivos móviles de comunicación, telefonía celular, computadoras personales e internet, como medio para realizar las conductas delictivas antes mencionadas, se trata de delitos bien definidos en nuestra leyes, que han existido, en la mayoría de los casos, mucho antes de la invención de los medios de comunicación, procesamiento y almacenamiento de datos de manera digital en medios magnéticos, electrónicos u ópticos.

En el caso particular de nuestro país, existen vacíos legislativos importantes, específicamente en el control de los proveedores de servicios de internet, que los obliguen a almacenar los datos de conexión que permitan, a las autoridades correspondientes, realizar el rastreo de un mensaje generado y transmitido a través de Internet hasta su origen. Cabe mencionar que en países de la Comunidad Europea, como Francia, España y Alemania, entre otros, a través del Convenio de Cibercrimen, establecido a finales de 2001, la información se almacena por hasta un año, permitiendo así que los responsables de realizar investigaciones relacionadas con este tipo de conductas cuenten con el tiempo suficiente para evitar que la información que permite identificar a un delincuente a través de Internet se pierda.

Por otro lado, con relación a los fabricantes de programas de cómputo, se deben encontrar los mecanismos legales que los obliguen a generar *software* seguro, con la finalidad de evitar que el consumidor de esos productos sea vulnerable ante las amenazas que los códigos maliciosos presentan por el simple hecho de comprar dichos productos, los cuales desde su concepción implican altos riesgos de estabilidad y seguridad de los datos que procesan, dando como resultado un alto nivel de inseguridad, que al cabo del tiempo se traduce en pérdidas millonarias a los consumidores finales, ya sea a consecuencia de la pérdida de su información o por los altos costos de mantenimiento y soporte de las aplicaciones informáticas.

De lo anterior se desprende que en la actualidad los consumidores no cuentan con la transparencia y elementos suficientes,

por parte de los fabricantes de programas de cómputo, para poder realizar la elección de una aplicación con base en sus propios estándares de calidad y seguridad, y no con base en los propios de cada fabricante.

En nuestra opinión, así como al consumidor de comida se le informa del contenido calórico de los productos que consume, en el caso de programas de cómputo se le debería advertir al consumidor el grado de seguridad o, en su caso, el grado vulnerabilidad con el que cuentan los productos. Hoy el nivel de seguridad de prácticamente todos los productos que consumimos nos brindan es de 0.

Como se ha mencionado, lo anterior no significa, de ninguna manera, que nuestro país se encuentre en estado de indefensión con relación a los delitos cometidos a través de tecnologías de la información, ya que existen leyes que interpretadas de manera adecuada permiten advertir la tipificación y persecución de todos los delitos cometidos a través de las tecnologías de la información y comunicación. La Constitución Política de nuestro país, el Código Penal Federal, el Código Federal de Procedimientos Penales, la Ley Federal de Telecomunicaciones, entre otras, son normas que aplicadas de manera correcta permiten la persecución y castigo de todo tipo de conductas delictivas, cometidas a través de las tecnologías de la información y de la comunicación, erróneamente identificadas como ciberdelitos.

Pretendemos mostrar la situación actual, alcances y limitantes, así como los retos que enfrentan en nuestro país aquellos que forman parte del engranaje que conforma la procuración de justicia con relación a la problemática antes expuesta, con la finalidad de aportar soluciones que brinden la posibilidad de realizar los ajustes necesarios para que todos los responsables de realizar una investigación en el área de la TIC cuenten con los elementos necesarios para desarrollar su trabajo de manera eficaz y eficiente, cumpliendo con las expectativas de todos aquellos que esperan justicia, cuando se ven afectados por las conductas de este tipo de delincuentes.

En este momento la pregunta obligada sería: ¿de dónde vienen o qué factores propician los ciberdelitos?, y ¿cómo se combaten este tipo de conductas?

Bien, ante la constante evolución tanto de la sociedad como de su entorno ideológico, económico, social y tecnológico, surgen a la par de ella, distintas tendencias y conductas delictivas cometidas por mentes criminales, que de alguna manera encuentran la forma de adaptarse o aprovecharse de la candidez del momento, con la finalidad de obtener un beneficio violentando las garantías individuales de terceras personas. Como respuesta y en auxilio a las autoridades responsables de la procuración y aplicación de justicia, surge una ciencia, la cual busca, mediante la aplicación de metodología aplicada a la investigación, reconstruir la verdad histórica de los hechos después que se ha cometido un "presunto acto delictuoso": la criminalística.

Sin embargo, como abordaremos a lo largo de este trabajo, el criminalista forma parte de un equipo de trabajo dependiente, que partiendo de las circunstancias de los hechos en torno a un delito, necesitará de la pericia de los involucrados, tanto en materia legal como en ciencias físicas y naturales. Al día de hoy, los medios y los métodos utilizados para cometer un delito han evolucionado a la par de la sociedad, y hoy, más que en otras épocas, las nuevas tecnologías y su capacidad para procesar, comunicar y almacenar de manera masiva datos e información, e inclusive controlar sistemas vitales, han sido testigos del nacimiento de un nuevo perfil criminal, el cual hace uso de ellas para burlar las medidas de seguridad implementadas aun en los corporativos que nunca pensaron estar al alcance de un criminal; sin embargo, es importante no perder la objetividad del delito; esto es, el hecho de poder cometer un fraude financiero, mediante la falsificación de un documento elaborado mediante técnicas de impresión cerigráficas o a través de la red informática, aprovechando las diferentes vulnerabilidades de los sistemas electrónicos bancarios, no hace diferencia en cuanto a la tipificación del delito de fraude. En otras palabras, el robo, el engaño, el asesinato, la explotación y la

prostitución de menores, entre otros, han existido, seguramente, desde que nuestros primeros antepasados formaron grupos sociales en los cuales se albergaron los primeros individuos con mentes criminales.

Desafortunadamente, como demostraremos en esta investigación, nuestro país no ha sido la excepción con relación al incremento de conductas delictivas, cometidas mediante el uso de tecnologías de información y comunicaciones (TIC), sobre todo en relación con secuestros, extorsiones, robo de identidad y fraudes financieros, cometidos a través de Internet. De lo anterior se desprende la necesidad de tomar en cuenta los fundamentos de esta rama de la ciencia, con la finalidad de establecer una nueva especialidad criminalística dedicada al estudio, investigación y esclarecimiento de actos probablemente delictivos que utilizan como medio y objeto las TIC. Con el planteamiento anterior, se busca conjuntar los elementos necesarios para que el perito en esta materia se encuentre capacitado para dar fundamento técnico, acorde a la legislación de nuestro país, a las posibles evidencias que en su oportunidad serán presentadas por el agente del Ministerio Público ante un juez.

Para lograr lo anterior, será necesario estandarizar metodologías y técnicas de investigación de este tipo de delitos, con la finalidad de que la identificación, fijación, preservación, manejo y análisis de posible evidencia digital se conviertan en una norma que permita a la autoridad competente utilizarlas, como prueba irrefutable, en la persecución y castigo de este tipo de delincuentes; asimismo, se deberán aplicar los cambios legislativos que permitan no solo definir delitos que se cometen a través de estos medios, sino establecer los mecanismos para controlar los medios que sirven de enlace o que permiten la comunicación entre un dispositivo emisor y un receptor, así como a los responsables de su administración, para que la información que queda registrada en ellos, y que permite establecer el origen y destino de una comunicación, a través de una red informática y/o de telecomunaciones, pueda ser almacenada, con la finalidad de que los responsables

de una investigación cuenten con los elementos necesarios que brinden la certeza para localizar al responsable de cometer un acto delictivo.

II. Investigación pericial en cibercriminalidad

1. *Cibercrimen*

El término "cibercrimen" se encuentra aún en la mesa de debate en cuanto a la legislación de muchos países del mundo, incluyendo a México; sin embargo, a partir del atentado del 11 de septiembre de 2001 contra las Torres Gemelas en la cuidad de Nueva York, en los Estados Unidos, que fue planeado y ejecutado a través del uso y aprovechamiento de las tecnologías de la información y comunicaciones, así como de la amenaza global de terrorismo digital, dirigido al ataque de sistemas financieros, sistemas de defensa, bases de datos, difusión de virus, entre otros factores, trajo como consecuencia que en la actualidad se trabaje de manera seria y globalizada en la generación y aplicación de leyes enfocadas a castigar conductas delictivas cometidas mediante la utilización de equipos de cómputo y sistemas de comunicación, ya sea como fin o como medio.

2. *Definición de investigación forense aplicada a TIC*

Es la rama de la criminalística que se aplica en la búsqueda, tratamiento, análisis y preservación de indicios relacionados con una investigación, en donde, tanto equipo de cómputo y/o telecomunicaciones han sido utilizados como fin o como medio para realizar una acción presuntamente delictiva.

El objetivo de la investigación forense en esta materia es auxiliar a la autoridad solicitante en el descubrimiento de la verdad histórica de los hechos relativos a un presunto acto delictuoso, en donde han sido utilizados como medio o fin:

— Equipo y programas de cómputo
— Dispositivos digitales de almacenamiento de datos
— Equipo electrónico y/o
— Equipo o dispositivos de telecomunicaciones con la finalidad de identificar al o a los autores del hecho.

En el desarrollo de esta investigación forense aplicada a las TIC encontramos varios tipos de intervenciones:

1. Informática
   a) Identificación de acceso y/o uso no autorizado a equipos de cómputo
   b) Robo, alteración o copia de información contenida en equipos de cómputo
   c) Falsificación de documentos mediante equipos de cómputo
   d) Identificación de fraudes financieros a través de una red informática
   e) Ataques informáticos a servidores
   f) Robo de programas de cómputo
   g) Identificación de correos electrónicos
   h) Recuperación de información en dispositivos digitales de almacenamiento
   i) Ataques informáticos a redes de cómputo
   j) Rastreo de servidores
   k) Recuperación de información publicada en internet
   l) Análisis de licitaciones y/o contrato en sistemas y equipos de cómputo
   m) Clonación de bandas magnéticas y/o chips de tarjetas
2. Telecomunicaciones
   a) Identificación de dispositivos y/o equipos de telecomunicaciones
   b) Recuperación de información almacenada en dispositivos de telecomunicaciones
   c) Identificación de intervención de líneas telefónicas

d) Identificación de ataque o daño a una red de comunicación
e) Identificación de robo de flujo electromagnético (TV, Cable).
f) Identificación de uso indebido de frecuencias de comunicación.

3. Electrónica

a) Identificación y funcionamiento de dispositivos y/o equipo electrónico
b) Identificación de principio y funcionamiento de circuitos electrónicos
c) Análisis de diagramas esquemáticos
d) Alteración de cajeros automáticos