Los delitos informáticos y la evidencia digital

Dra. Gabriela Guadalupe Valli

Secretaria del Juzgado de Primera Instancia en lo Penal de Instrucción de la 13ª Nominación. Rosario.

I. Introducción

Los avances tecnológicos y el desarrollo de las telecomunicaciones indudablemente crearon una estructura favorable para el surgimiento de un fenómeno histórico que rige nuestra sociedad, la globalización. Este fenómeno de expansión habilitó la transmisión de la información desde los centros de poder económico – político - científico, hasta los lugares más inéditos.

Nuestros tiempos, esta masificación en la comunicación sumada al deliberado capitalismo mundial sustenta, no sólo las transacciones casi instantáneas que caracterizan la economía actual, sino que a todas luces fortalecen el poder desconocido de las grandes corporaciones, generado un ámbito propicio para el nacimiento de nuevas formas y oportunidades de delincuencia, denominados en términos genéricos delitos Informáticos.[1]

No resultó una tarea fácil la inserción de la tecnología en el marco jurídico regulatorio. Hasta su regulación se generaron vacíos legales, que han colocado a infinidad de situaciónes de hecho, transacciones comerciales o relaciones contractuales en un entorno de inseguridad jurídica conllevando en el ámbito penal a que grandes ilicitudes quedaran impunes. De allí que uno de los desafíos actuales que trae el flagelo de la delincuencia cibernética es el de suministrar una respuesta jurídica expeditiva que permita combatirla eficazmente.

La sanción de la ley 26.388[2] significó un gran avance sobre este punto ya que si bien la misma requiere debate y permanente actualización en orden a la materia que trata en continuo movimiento, sin dudas implica un gran aporte a la hora de brindar respuestas jurídicas a esta nueva forma de criminalidad.

2. Tipos de delincuencia informática [3]

En la actualidad, el delito cibernético se presenta en distintas y múltiples formas, ya sea atacando a las propias tecnologías de la información y las comunicaciones, como también a los servidores, sitios Web y/o entidades comerciales, bancarias, financieras, etc.. Y si bien difieren los actores o los escenarios en términos generales podemos afirmar que comunmente el modo de comisión es a través de la manipulación de ***virus informáticos.***

Estos virus no son sino programas contenidos en otros programas que afectan directamente a la máquina que se infecta causando daños muy graves. Se denominan malware y tienen como objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos que sólo se caracterizan por ser molestos.[4]

También se distinguen **los gusanos.** Estos se fabrican de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero difiere del virus puesto que éste no puede regenerarse. En ese orden, **también aparecen las bombas lógicas o cronológicas.** ***Estas funcionan como una especie de virus que explota en un momento determinado causando daños al equipo afectado.***

Todas estas herramientas –entre otras- si bien resultan una gran hazaña en el mundo de la informática, su potencial para dañar es inconmensurable, pudiendo llegar a causar considerables perjuicios a las redes comerciales y de consumidores.[5]

El Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 18 a 25 de abril de 2005, Bangkok (Tailandia), resume las distintas tipologías en el denominado «vandalismo electrónico» y, bajo ese rótulo, ubica a todos los casos donde la actividad ilícita se dirige al blanqueo de páginas web, o a suministrar contenidos inapropiados en las mismas, o también el vandalismo típico en páginas de los propios usuarios. Otra de las formas se presenta a través del robo o fraude, por ejemplo, ataques de piratería contra bancos o sistemas financieros y fraude mediante transferencias electrónicas de fondos. En estas situaciónes las computadoras se utilizan para facilitar una amplia variedad de ventas telefónicas e inversiones fraudulentas mediante prácticas engañosas. La o la inundación de mensajes supuestamente de origen conocido ***(spam spoofing)*** es la construcción de mensajes de correo electrónico con páginas Web correspondientes, diseñadas para aparecer como sitios de consumidores existentes. Se distribuyen millones de estos mensajes fraudulentos de correo electrónico, que se anuncian como provenientes de bancos, subastas en línea u otros sitios legítimos para engañar a los usuarios a fin de que comuniquen datos financieros, datos personales o contraseñas.

Otra modalidad esta dada por la difusión de material ilícito y nocivo como por ejemplo la pornografía infantil. Tópico sobre el cual desde fines de los años 80 ha venido aumentando su distribución a través de una variedad de redes informáticas, utilizando una variedad de servicios de Internet, incluidos los sitios Web. Además de la utilización de la Internet para difundir propaganda y materiales que fomentan el odio y la xenofobia, hay indicios de que la Internet se ha utilizado para facilitar la financiación del terrorismo y la distribución de propaganda terrorista, entre otras.

3. Mitos y verdades de los delitos informáticos.

La Ley 26.388 ha permitido una actualización y armonización del Código Penal Argentino con el resto de las legislaciones mundiales en aras de receptar el avance de las nuevas tecnologías, pero no puede dejar de apreciarse que más allá de los llamados Delitos Informáticos actualmente la evidencia digital puede estar involucrada como elemento probatorio en cualquier clase de ilícitos.

En esa inteligencia, solo vasta echar un vistazo a los despachos para concluir lo certero de tal aseveración. Vemos a dia-

rio que nacen nuevos escenarios fácticos en los que se involucran medios tecnológicos o virtuales para la comisión de conductas ilícitas «tradicionales» pero adecuadas a la nueva realidad tecnológica.

Así aparecen amenazas, a través de medios digitales, instigación al suicidio, chantaje, coacción, corrupción de menores, estafas en sus más variadas formas, etc. En todos estos casos vemos como nota característica que el medio por el que se canaliza la intimidación, la instigación, el engaño o la sustracción, posibilita sin lugar a dudas el anonimato pudiendo quedar en la impunidad si no se actúa con precisión y en forma rápida.

Por ello entiendo que, aunque ofrezca cierta resistencia el tema, la prueba científica como especie de la prueba jurídica ocupa un papel cada vez más destacado en las investigaciones penales.

En los tiempos que corren ***es habitual que en una sola causa penal existan vinculados numerosos elementos tecnológicos de prueba que requieren de una pericia informática,*** y ello no siempre implicará que sea fruto de una investigación de delitos informáticos. De allí que resulte necesario erradicar el mito instalado que indica que la prueba tecnológica sólo es ámbito de los delitos informáticos, pues se requerirá de periciales informáticas aún para la investigación de delitos comunes.

4. Dificultades de la criminalidad cibernética.

La criminalidad informática se caracteriza por las dificultades que entraña el descubrir, probar y perseguir los delitos. Concretamente, parte del problema de reconstruir un incidente en un caso de delito cibernético es que gran parte de las pruebas son intangibles, transitorias y de difícil acceso. En lugar de pruebas físicas, las investigaciones de delitos cibernéticos procuran encontrar rastros digitales que, con frecuencia, son inestables y de corta duración.

Una de las razones de la inestabilidad es que algunos tipos de información sobre direcciones y rutas electrónicas (es decir, los «datos sobre el tráfico») no se almacenan de manera permanente. Esa información puede quedar sólo en la memoria de un sistema de computadoras por un período corto y luego se le superpone otra ruta de información. **En sentido similar ocurre cuando se trata de acceder** a la evidencia digital protegida en muchos casos mediante mecanismos criptográficos, en tanto suele ocurrir que los laboratorios periciales se vean imposibilitados de acceder a la evidencia por no contar con el soporte específico para sortear esos programas. Esa imposibilidad o demora en la labor pericial es nociva para la investigación, por cuanto privará a la misma de sustanciosa información que en muchas ocasiones hará pender de ella la suerte del proceso. De allí que resulte necesario contar no sólo con el experto capacitado sino también con el soporte que habilite a sortear las trabas tecnólogicas predispuestas por los ciberdelincuentes para acceder, en rigor, a la prueba tecnológica.

5. El quid de la prueba: *corpus instrumentorum.*

Como mencionara en líneas anteriores, en materia de delitos informáticos resulta sumamente difícil delimitar el conocimiento, en tanto por la versatilidad de la **disciplina no posee límites definidos,** ***lo que demanda mayor sutileza y cuidados no sólo en la recolección del material probatorio sino también en la manipulación del material sujeto a pericia.***

Desde el mismo momento del allanamiento o secuestro del objeto informático a peritar, se exige supremo respeto a fin de obtener el corpus instrumentorum.

Por ello la actividad del experto también requerirá detectar y analizar el entorno para llevar a cabo la pesquisa. ***Es de vital importancia que el investigador indague qué contacto tuvieron los usuarios con el sistema o efecto involucrado en el incidente. Y resulta de gran utilidad llevar un registro detallado de la escena y de las entrevistas que se realicen y de ser posible procurar la registración fílmica o fotográfica ya que podrían relevarse a través de la misma detalles de utilidad en la investigación.***

Puede suceder que se requiera el experto con anterioridad a la realización del allanamiento y/o procedimiento a fin de que sirva informar al magistrado requirente las medidas a adoptar, la disponibilidad de equipos y personal técnico en el momento de la diligencia como asimismo determinar si la labor pericial puede llevarse in situ o bien cuáles serían las posibles consecuencias de diferir su tratamiento en cuanto a tiempo y lugar de realización.

Justamente por la rapidez en que se puede esfumar la prueba tecnológica del delito es que los métodos tradicionales de búsqueda y el hallazgo de evidencia resultan ineficaces.

Debemos tener en claro que si de mecanismo u objeto informático se habla, cualquiera sea, lo incautado debe ser exactamente lo que llegue al ámbito del perito para su análisis y dictamen, pues no escapa a la lógica más simple suponer que, al procederse al diligenciamiento de una orden de allanamiento, quienes resultan afectados y, de alguna manera se saben partícipes de una actividad delictual, intentarán por todos los medios evitar que los funcionarios intervinientes obtengan elementos probatorios que pudieren incriminarlos. De allí que sea necesaria la asistencia de expertos si lo que no se quiere es frustrar la investigación.

En una etapa posterior, sea ámbito judicial o policial, resultará preciso ser cuidadoso en la custodia de los efectos, en tanto la experiencia nos demuestra que ante tales situaciónes no faltan los curiosos que no pueden vencer sus pasiones y sumidos en la curiosidad proceden a desplegar su supuesta experticia manipulando de algún modo la evidencia. Dicha actividad es altamente perjudicial para la investigación, en tanto puede generar la frustración de material dirimente para la solución del caso. Por ello, considero que en estos supuestos la labor del Secretario es importante tanto a la hora de enfrentar un procedimiento

como de procurar la correcta cautela y custodia de los efectos secuestrados.

Un buen ejemplo de que puede ser vital para un proceso la buena manipulación del material informático lo constituye el caso ***«Perel». En el mismo pudo determinarse que ningún otro medio hallado en el lugar podía aportar datos tan concretos sobre las últimas horas de la victima. Sin embargo,*** **labor pericial en forma directa sobre el ordenador secuestrado en la escena del crimen, sin realizar copias de resguardo de su disco rígido pudo determinarse más tarde introdujo cambios o alteraciones insalvables para la investigación.**

Este ejemplo sirve para ilustrar lo dicho y de como la ausencia de observación de los recaudos esenciales puede ser vital para la suerte de la investigación.

Ahora bien, los problemas en el ámbito de los ciberdelitos tampoco escapan al juzgador, en tanto si bien el principio general de que el conocimiento del perito debe sustentarse en un sistema verificable ordenado sobre pautas o hechos es totalmente aplicable a la totalidad de la actividad pericial, la incidencia ***de la falibilidad en cuanto a la valoración jurisdiccional de los resultados*** adquiere especial relevancia sea porque existe un generalizado desconocimiento respecto de las modificaciones tecnológicas, sea porque irroga un elevado nivel de abstracción y terminología técnica en la exposición de sus resultados, o por la inexistencia de apoyo jurisprudencial suficiente que permita al juez moverse sobre bases más o menos seguras, fundadas en la experiencia judicial, tal como ocurre con otras disciplinas criminalísticas.

6. Del material probatorio. «Una evidencia sin alteraciones». La intervención del experto.

Si de evidencia se trata, no puede soslayarse que pueden diferenciarse algunas situaciónes tejidas en relación al objeto sometido a pericia. Sin perjuicio de ello, se trate de un objeto obtenido como fruto de un allanamiento o de un ofrecimiento realizado por las propias partes del proceso en mismo ámbito del tribunal, se debe convocar siempre al experto.

Ahora bien, si el hallazgo o secuestro se realiza en el ámbito de un allanamiento, en tal caso se deberá convocar a personal técnico especializado para la realización de la medida[6] y deberá estarse también al cumplimiento de las formalidades propias de la medida conforme el digesto procesal santafesino[7].

Como primera medida se deberá disponer el alejamiento de toda persona que se halle en presencia de los computadores, servidores o tableros de suministro eléctrico, para proceder inmediatamente a desconectar la totalidad de los teclados hasta que cada uno de los terminales sea examinados por los expertos.

Se sugiere explicar claramente a los testigos cada una de las tareas que se realizan en el marco del procedimiento y, en el caso de realizarse pericial *in situ,* se deberá explicar a los presentes la finalidad de las aplicaciones que utiliza el experto, velando por la exacta transcripción de sus especificaciones en el acta respectiva. La toma de vistas fotográficas y soporte fílmico de la medida desde el inicio hasta su culminación resultaran altamente ilustrativas por cualquier vicisitud que plantee el mismo procedimiento.

En rigor, *la labor del experto se reduce a recoger la información relevante teniendo especial cuidado para no modificarla. Asimismo, por la naturaleza volátil de algunos medios de almacenamiento, se recomienda tomar un duplicado forense (copia bit a bit)[8]. Para llevar a cabo el análisis de la evidencia se debe contar con herramientas útiles y acordes al objeto que se secuestra a fin de no afectar la evi-*

dencia digital original. ***¡El punto clave es recolectarla sin alterarla¡.***

Se procura asegurar que el contenido de las unidades de almacenamiento (discos rígidos, CD, diskettes u otros) al momento del secuestro sea el mismo que se someterá a dictamen pericial posterior. Por ello se requiere un procedimiento prolijo, detallado y cauteloso.

Si lo que se pretendiere secuestrar fueran soportes de almacenamiento, se recomienda listarse todos los directorios o carpetas, según el sistema operativo de que se trate, de modo que quede expresamente consignado el nombre del archivo, su extensión, su tamaño, fecha y hora de su última modificación y atributos de accesos[9].

Resulta conveniente asegurar la medida con la rúbrica de los presentes, procediendo luego a asegurar con cinta adhesiva o elemento similar las entradas de acceso a toda unidad de almacenamiento (siendo un cpu se deberá proceder a franjar conexiones de entrada y salida, ya sea de datos, periféricos o energía y los accesos a unidades de discos flexibles, rígidos removibles, o unidades de **back-ups,** ***evitando la posibilidad de que se desmonten sus partes componentes, todo ello con la rúbrica de funcionarios y testigos.*** Luego se procede al secuestro de los objetos y traslado al Tribunal o lugar que ordene el Juez que extendiera la medida.

Idéntico tratamiento se aconseja para los discos flexibles u elementos menores que deberán ser colocados preferentemente en cajas debidamente aseguradas para su traslado. En la medida que todos los elementos permanezcan bien conservados, no se albergarán dudas sobre su contenido.

7. Consideraciones técnicas

En el sentido apuntado, y visto que uno de los mayores cuestionamientos en materia probatoria lo constituye la cadena de custodia del elemento tecnológico a peritar, es que se debe procurar el respeto de las formas, procurando participación de las partes del proceso en la pericial y extremando los recaudos para llevar a cabo una adecuada recolección, cautela y custodia de la evidencia.

En este punto, si bien resultan de aplicación las normas de procedimiento del digesto procesal penal santafesino y, supletoriamente, las disposiciones del Código Procesal Civil y Comercial, las

mismas resultan estrechas ante la nueva casuística delictiva. De allí que deberían ser objeto de una actualización pues el análisis de la evidencia técnica digital -está claro- escapa a cualquier previsión que haya hecho el legislador.

En ese orden y de algún modo para sanear esas lagunas es que resulta hoy necesario que tanto las agencias policiales, de seguridad o judiciales tengan como prioridad la utilización de una metodología adecuada y herramientas jurídicas robustas para aplicar al proceso de investigación y de prevención de la ciberdelincuencia.

Por ello entiendo que resulta de interés superlativo definir políticas y diseñar protocolos de actuación y/o estándares de operación tanto sea para ser utilizados en la recolección como en el análisis de la evidencia, ya que su errada manipulación, como vimos, puede costar el éxito del juicio.

Sobre este punto la Asociación de Oficiales Jefes de Policía del Reino Unido ha publicado cuatro principios básicos aplicables al procedimiento estándar de operación que merecen su reproducción:
1) no deberá alterarse los datos almacenados en un medio digital.
2) sólo en casos excepcionales se podrá acceder a los datos originales. La manipulación sólo por técnicos y llevar registro de sus acciones documentando y explicando su proceder.
3) crear y preservar un registro de secuencia de eventos. Un tercero podrá examinar esos resultados y lograr los mismos resultados.
4) el investigador es responsable de asegurar que la ley estos principios sean cumplidos.

8. El Análisis del material informático. «Triage»

Debido a las dificultades propias de la materia en su mayoría las pericias se practican en laboratorio, siendo dificultoso -sino imposible- realizar tareas periciales en el lugar del hecho. Las instituciones policiales no cuentan con personal capacitado ni con recursos para realizar triage (clasificación y priorización) para lograr una reducción y selección de posibles fuentes de prueba digital y aunque ello fuera posible las inspecciones digitales en el lugar del hecho requieren un tiempo excesivo, bajo presión, y deben ser realizadas en un lapso temporal limitado -momento del allanamiento-, lo que no permite poder arribar a conclusiones certeras e induce a errores.

La técnica de triage fue desarrollada en el ámbito de la medicina, para lograr la optimización de recursos. Las inspecciones digitales -conocidas habitualmente como «triage» forense-, deben ser realizadas utilizando métodos forenses estándares y válidos, para evitar que la evidencia no sea dañada, modificada o contaminada. Como resultado de este proceso automatizado se obtiene una predicción sobre la verosimilitud de localizar evidencia relevante a la causa en un determinado dispositivo. La utilización de la técnica de triage con esta nueva herramienta forense es sumamente útil para intentar mitigar las listas de espera en un laboratorio pericial, pudiendo ser aplicada en casos que tienen varios elementos informáticos para ser analizados. No obstante – en atención a los costos- no hay señales de su utilización por estos tiempos.

9. Conclusión

Estamos frente a una nueva realidad, un entorno fáctico distinto, con valores cambiantes que apenas llegamos a comprender. Aún así la dinámica del proceso penal y la legislación de fondo permanecen inmóviles frente a estas nuevas prácticas delictivas. En este orden de ideas, todo esfuerzo resulta estéril si no

es acompañado por la adopción de políticas de seguridad orientadas a combatir y prevenir delitos informáticos.

La actividad pericial informática, aparece, en nuestro país, desdibujada, en tanto no solo no se invierte en instrumentos idóneos para la realización de la labor pericial, sino que tampoco se cuenta con personal especializado idóneo en el rubro.

Los profesionales del derecho, en su carácter de legisladores, jueces, fiscales o defensores no pueden permanecer ajenos a esta realidad. Tampoco puede desconocerse que no es necesario estar ante un delito informático para toparse con pruebas digitales.

Si bien la prueba digital posee características propias como su volatilidad, lo que demanda procesos específicos en lo que atañe a la recolección, cautela y custodia la misma. Así, se debe ser cuidadoso en su recolección y manipulación en tanto una desprolijidad podría frustrar el éxito de la investigación. Y para poder cumplir con ello se requiere de la colaboración de técnicos y, en lo posible, de procedimientos previamente definidos de actuación (creación de protocolos), y la sanción de leyes dinámicas que propicien la incorporación inmediata de las innovaciones tecnológicas.

No puede resultarnos ajena esta nueva realidad. Por ello es que resulta necesaria la capacitación de los funcionarios, fiscales, jueces, operadores judiciales y policiales para hacer frente a este nuevo escenario delictivo ■

Referencias bibliográficas:

- Kelsey Galloway «Cybercrime and Policing: The Continuous Online Game of Cat and Mouse», 2011.

- Gabriel H. Tobares Catalá y Maximiliano J. Castro Arguello «Delitos Informáticos». Ed. Advocatus, Cordoba 2009.

- 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal Salvador (Brasil), 12 a 19 de abril de 2010.

- Daniel A. Torres, Sandra J. Rueda Jeimy J. Cano Colombia.«Algunas consideraciones técnicas y de procedimiento para la investigación de delitos informáticos», ponencia, Reunión Española sobre Criptología y Seguridad de la Información, 2004.

- 11ºCongreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 18 a 25 de abril de 2005, Bangkok (Tailandia).

- XI Encuentro de Asociación Argentina de Profesores de Derecho Penal, Facultad de Derecho de la UNR, Rosario, Pcia. De Santa Fe, Junio 2011.

- Leopoldo Sebastián M. Gómez, »El protocolo de actuación para peritajes informáticos en el ámbito judicial» Revista de Derecho y Nuevas tecnologías – Revista de Derecho Informático, ISSN 1681-5726, 2006 . Alfa-Redi Disponible en: *http://www.alfa-redi.org/rdi- articulo.shtmlx=6216.Fernández, C.;*

- «Prueba Pericial. Delitos y tecnología de la Información. Características y valoración en el Proceso Penal Argentino», en Delitos Informáticos.com, 2002. Disponible en: «http://www.delitosinformaticos.com/delitos/prueba.shtml»http://www.delitosinformaticos.com/delitos/prueba.shtml

[1] Gabriel H. Tobares Catalá y Maximiliano J. Castro Arguello «*Delitos Informáticos*». Ed. Advocatus, Cordoba 2009. Convenio de Ciberdelincuencia del Consejo de Europa, podemos definir los delitos informáticos como: los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos.

[2] Sancionada el 4/06/2008, publicada en Boletín Oficial el 25/06/2008.

[3] Según Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 18 a 25 de abril de 2005, Bangkok (Tailandia).

[4] De las referencias de las periciales informáticas extendidas por la uriI Rosario.

[5] Entre los ejemplos históricos: se encuentra el virus melissa que en marzo de 1999 causó más de 10 millones de dólares en daños solo en los eeuu y el virus I love you en marzo 2000 daños en 7.0000 millones y 10.000 millones de dólares y que infectó hasta 45.000 computadores en el mundo.

[6] Que en nuestro ámbito sera el Gabinete de Pericias Informáticas Unidad Regional II.

[7] Art. 218 del cppsf cctes. Y sgtes.

[8] Algunas consideraciones técnicas y de procedimiento para la investigación de delitos informáticos, ponencia, Reunión Española sobre Criptología y Seguridad de la Información, 2004 por Daniel Torres,Sandra Rueda, Jeimy Cano(Colombia).

[9] Prueba Pericial,Delitos y tecnología de la Información Características y valoración en el Proceso Penal Argentino,Dr. Claudio Alejandro Fernández, 17,11,2002, Disponible en: *http://www.delitosinformáticos.com/delitos/prueba.shtml.*