Tratamiento de la evidencia contenida en soportes informáticos como prueba en el proceso penal

Víctor Santelices
Profesor Ayudante Derecho Penal I
Facultad de Derecho
Universidad del Desarrollo

Profesor patrocinante: Gonzalo de la Cerda

Resumen: El tratamiento de la evidencia informática obtenida en la investigación de los ilícitos penales y las pruebas periciales aplicadas a su contenido resultan de particular relevancia al momento de acreditar la conducta ilícita ante el órgano jurisdiccional encargado de conocer y resolver la acusación formulada a su respecto. En efecto, el análisis de esta evidencia supone el cumplimiento de determinados resguardos propios de la naturaleza y volatilidad de la información contenida en dichos soportes.

Esta ponencia expone la problemática del tratamiento de la evidencia informática, la necesidad de aplicar protocolos especiales de actuación de los órganos encargados de su levantamiento, traslado, custodia y análisis, y las consecuencias posibles en el proceso penal ante el incumplimiento de los resguardos requeridos para la adecuada conservación del material informático periciado, los que inciden en la valoración de la fuente de prueba por parte del Tribunal que debe arribar la convicción acerca de la pretensión punitiva expresada en los hechos sometidos a su conocimiento.

*****

El concepto de delito informático

El avance en el uso de la tecnología en las actividades de la vida cotidiana resulta en la actualidad un asunto que no admite controversia. En este sentido, el actuar delictual se ha perfeccionado y adaptado al uso de estas nuevas tecnologías. Muchos de los engaños propios del delito de estafa actualmente son ejecutados mediante el uso de mensajería proveniente de sistemas informáticos[1], lo mismo sucede en ilícitos asociados a redes de pornografía infantil,

[1] Así, por ejemplo, la figura del *Phishing*, mediante el cual los estafadores se hacen pasar por empresas de distintos tipos y piden a los usuarios información privada. Para estos efectos utilizan correos

corrupción de menores, injurias y calumnias, entre otras figuras. Lo anterior, sin considerar la propia normativa de la Ley N° 19.223, que tipifica figuras penales relativas a la informática.

La Organización para la Cooperación Económica y el Desarrollo (OECD) define al delito informático como: "cualquier conducta no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos"[2]. Esta definición abarca dos ámbitos del delito informático, a saber: aquellas conductas consistentes en delitos tradicionales en los que la tecnología de la información es utilizada como un medio específico de comisión; como asimismo aquellas conductas nuevas no contempladas en los ordenamientos penales por su especial naturaleza, consistentes en atentados cometidos dolosamente contra los datos digitalizados y contra los programas computacionales contenidos en un sistema[3].

Los razonamientos y conclusiones contenidos en esta ponencia son válidos para ambos tipos de delitos, resultando trascendente únicamente el uso de un soporte electrónico como medio de comisión del ilícito, sea respecto de un delito tradicional o uno de carácter informático en sentido estricto. Respecto de ambos el tratamiento de la evidencia consistente en el soporte que registra la información relevante requiere un especial cuidado que permita su utilización como medio probatorio apto para producir convicción en el ente juzgador.

Tratamiento de la evidencia levantada en el sitio del suceso: la cadena de custodia

El levantamiento de los objetos y documentos relevantes para el proceso desde el lugar de comisión del delito, su posterior custodia y análisis requieren cumplir los estándares propios de toda evidencia forense.

La acreditación de estos resguardos en el levantamiento y conservación de la evidencia es realizada mediante el proceso de la cadena de custodia. Este proceso hace referencia a la seguridad y confiabilidad de las fuentes de prueba recogidas en virtud de la investigación de distintos tipos de ilícitos.

electrónicos y páginas web, donde son consultados datos como contraseñas y números de cuentas, información que ninguna empresa consulta mediante estos medios por aspectos de seguridad.

[2] Definición elaborada por un Grupo de Expertos, invitados por la OCDE a París en mayo de 1993.

[3] Algunos autores, a partir de esta distinción denominan delito computacional a aquella figura tradicional de Derecho Penal en la cual la forma de comisión es mediante el uso de un sistema informático, reservando la nomenclatura de delito informático solo a *"…la acción típica, antijurídica y dolosa cometida mediante el uso normal de la informática, contra el soporte lógico o software, de un sistema de tratamiento automatizado de la información"*. Ver: HERRERA BRAVO, Rodolfo (1998): "Reflexiones sobre los delitos informáticos motivadas por los desaciertos de la ley chilena Nº 19.223", en *REDI Revista Electrónica de Derecho Informático,* N° 5, [fecha de consulta 13 de septiembre de 2013] Disponible en: http://vlex.com/vid/informaticos-motivadas-desaciertos-chilena-223-107005.

La cadena de custodia ha sido definida por la Corte Suprema como

> *"un procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de administrar justicia, y que tiene como fin no viciar el manejo que de ellos se haga y así evitar alteraciones, sustituciones contaminaciones o destrucciones"*[4].

La cadena de custodia está compuesta por diversos hitos o eslabones, que dan cuenta de la manipulación de diversos agentes de la evidencia, desde su incautación hasta su devolución, destrucción o presentación al Tribunal, según sea el caso. De esta forma, el registro de cada intervención entrega garantías de integridad e inalterabilidad de esa evidencia para ser utilizada como fuente de prueba confiable. Mediante la cadena de custodia el sentenciador adquiere la certeza que la evidencia que ha sido presentada en juicio es la misma recogida en el sitio del suceso.

Si bien no existe norma legal o reglamentaria que establezca la forma en la cual se deba efectuar el tratamiento, custodia y análisis de la evidencia incautada desde el sitio del suceso, en general existen referencias a diversas etapas o fases de la cadena de custodia, a través de las cuales es posible acreditar la inalterabilidad de los elementos probatorios, estas etapas son las siguientes[5]:

1.- Hallazgo y custodia del sitio del suceso: es necesario precisar que el sitio del suceso no solo abarca el lugar principal de comisión del hecho investigado, sino también lugares relacionados y de interés criminalístico. Por ejemplo, en un homicidio no solo importa el levantamiento realizado en el lugar en el cual se cometió el delito, sino que deberá resguardarse de igual forma el sitio en el cual se halla el arma homicida, o en el cual se ocultó el delincuente en días o incluso semanas posteriores, ya que de todos ellos podrían obtenerse indicios importantes para la investigación, los que deberán estar sometidos a las mismas reglas de custodia de aquellos obtenidos en el sitio de suceso principal.

Sobre este particular, el artículo 83 del Código Procesal Penal señala que es responsabilidad de Carabineros de Chile y de la Policía de Investigaciones, aun sin orden previa del Fiscal a cargo de la investigación, el resguardar el sitio del suceso, para cuyos efectos *"impedirán el acceso a toda persona ajena a la investigación y procederán a su clausura, si se tratare de local cerrado, o a su aislamiento, si se tratare de lugar abierto, y evitarán que se alteren o borren de cualquier forma los rastros o vestigios del hecho o se remuevan los instrumentos usados para llevarlo a cabo"*.

---

[4] Corte Suprema (2010): Rol 3657-10, 23 de agosto de 2010, considerando sexto, [fecha de consulta 31 de agosto de 2013] Disponible en: www.poderjudicial.cl.

[5] LLOBET RODRÍGUEZ, Javier (1998): *Proceso penal comentado* (San José, UCI).

2.- Inspección preliminar y búsqueda de indicios: esta actividad debe estar a cargo de personal especializado, dado que la experticia del personal que participa en la diligencia es un aspecto que puede ser cuestionado en el juicio oral para restar mérito probatorio a la diligencia, por vía de sostener un inadecuado manejo del sitio del suceso.

El mismo artículo 83 del Código Procesal Penal señala a este respecto:

> *"personal policial experto deberá recoger, identificar y conservar bajo sello los objetos, documentos o instrumentos de cualquier clase que parecieren haber servido a la comisión del hecho investigado, sus efectos o los que pudieren ser utilizados como medios de prueba, para ser remitidos a quien correspondiere, dejando constancia, en el registro que se levantare, de la individualización completa del o los funcionarios policiales que llevaren a cabo esta diligencia"*.

3.- Fijación de la huella, muestra o evidencia: esta etapa permite determinar con exactitud la ubicación y estado de los indicios que son de interés para la investigación, y que han sido encontrados en el lugar del suceso, lo que facilita la elaboración de versiones y una eventual reconstrucción de los hechos en el relato del personal policial en el juicio oral.

De esta forma, si existen contradicciones entre el relato y la fijación efectuada de la evidencia al momento de su levantamiento, la credibilidad del testimonio se verá afectada. Por el contrario, la plena coincidencia entre ambos aspectos del relato aporta veracidad y convicción en el sentenciador al momento de valorar la prueba aportada.

El artículo 181 del Código Procesal Penal, a propósito de las actividades de investigación en relación a la evidencia, señala que:

> *"… si el hecho hubiere dejado huellas, rastros o señales, se tomará nota de ellos y se los especificará detalladamente, se dejará constancia de la descripción del lugar en que aquél se hubiere cometido, del estado de los objetos que en él se encontraren y de todo otro dato pertinente"*.

Agrega que para el cumplimiento de estos fines:

> *"…se podrá disponer la práctica de operaciones científicas, la toma de fotografías, filmación o grabación y, en general, la reproducción de imágenes, voces o sonidos por los medios técnicos que resultaren más adecuados, requiriendo la intervención de los organismos especializados"* y que luego de realizada la operación *"se certificara el día, hora y lugar en que ella se hubiere realizado, el nombre, la dirección y la profesión u oficio de quienes hubieren intervenido*

en ella, así como la individualización de la persona sometida a examen y la descripción de la cosa, suceso o fenómeno que se reprodujere o explicare".

Los medios más utilizados por los agentes policiales para proceder a la fijación de la evidencia son: la fotografía, el video, el croquis y el acta.

4.- Recolección de las huellas, muestras o evidencias: es necesario respetar los protocolos técnicos a cargo de funcionarios policiales expertos, que son quienes tienen la idoneidad para manipular las evidencias.

Las huellas o evidencias obtenidas deben ser clasificadas e individualizadas cuidadosamente a partir de criterios técnicos, es decir, inventariadas científicamente, ya que de esta manera no sólo se controla cada uno por separado, evitando, por ejemplo, contaminación de evidencia orgánica, sino que de este modo se favorece el análisis y comparación que pueda hacerse en el laboratorio, sin margen de error.

5.- Embalaje de la huella, muestra o evidencia: tiene como fin principal individualizar y garantizar la integridad de la especie, de tal forma que el embalaje debe procurar evitar la alteración, destrucción o manipulación no autorizada de la evidencia.

El embalaje deberá ser el apropiado conforme a la naturaleza de la evidencia levantada, siguiendo las recomendaciones técnicas del personal experto encargado de la diligencia, para proceder luego al sellado y el etiquetado de la especie, momento en el cual se procede a confeccionar el formulario de cadena de custodia, que deberá contener

"una descripción del objeto y del estado en que se encuentra en cada momento, actualizada – en que va dejándose constancia de cada persona que lo tuvo a su cargo, de la fecha y hora en que lo recibió, de quien lo recibió, de todas las personas que lo examinaron bajo su responsabilidad, del día y hora en que lo entregó y la persona a quien se lo entregó"[6].

6.- Traslado y entrega de la evidencia: luego de la confección de las actas respectivas, del adecuado etiquetamiento y sellado de las especies, estas pueden ser trasladadas consignando a las personas encargadas del transporte de la evidencia, así como también las fechas y los despachos en que se procede a su custodia.

[6] *Instructivo N° 19. Respecto de las funciones de la policía previstas en los artículos 83 y 90 del Código Procesal Penal,* en MINISTERIO PÚBLICO, FISCALÍA NACIONAL (2001) *Reforma Procesal Penal. Instrucciones Generales N°s 1 a 25* (Santiago, Editorial Jurídica de Chile).

En nuestra legislación procesal la custodia y conservación de las especies incautadas corresponde al Ministerio Público, el artículo 188 del Código Procesal Penal establece: "*Las especies recogidas durante la investigación serán conservadas bajo la custodia del ministerio público, quien deberá tomar las medidas necesarias para evitar que se alteren de cualquier forma"*. Conforme lo ha sostenido el propio Ministerio Público:

> *"La conservación bajo custodia implica "guardar con cuidado y vigilancia", según la acepción del verbo custodiar del Diccionario de la Real Academia Española. A su vez, conservar significa "mantener una cosa o cuidar su permanencia", tanto como "guardar con cuidado una cosa", acepciones 1 y 4, en este segundo caso del mismo diccionario"*[7].

7.- Análisis pericial: en caso de necesitarse un pronunciamiento que requiera el conocimiento de una determinada ciencia o arte respecto de la evidencia, esta deberá ser analizada por personal especializado a efectos de rendir un dictamen pericial que incluya el resultado del análisis practicado.

Conforme lo dispuesto en el artículo 315 del Código Procesal Penal, el primer aspecto que debe contener el informe pericial es *"La descripción de la persona o cosa que fuere objeto de él, del estado y modo en que se hallare"*. De esta forma, el informe debe dar cuenta del estado en que se encontraba la evidencia cuando se recibió para su estudio, así como también el estado del embalaje, de manera tal que se posibilite cualquier confrontación con lo descrito en los registros de la cadena de la prueba o con los testimonios de quienes tuvieron bajo su custodia la misma.

8.- Devolución o destrucción de las evidencias: las evidencias recibidas en el laboratorio de criminalística deben ser custodiadas de ser posible en similares condiciones a las que fueron recibidas, por reglas general no pueden ser destruidas o alteradas, pues existe la posibilidad de que sea requerido un nuevo peritaje sobre las mismas muestras ya analizadas, lo que se denomina análisis de contramuestra[8].

9.- Registro documental de las etapas: como se señaló, el formulario de cadena de custodia debe consignar cada una de las fases del levantamiento, traslado y custodia de la evidencia de manera de permitir la reconstrucción de la ubicación de la evidencia en cada uno de sus hitos o etapas.

---

[7] *Instructivo N° 44. Sobre los objetos y las evidencias del delito en relación al nuevo proceso penal,* en MINISTERIO PÚBLICO, FISCALÍA NACIONAL (2001) *Reforma Procesal Penal. Instrucciones Generales N*os *26 a 50* (Santiago, Editorial Jurídica de Chile).

[8] El propio artículo 188 del Código Procesal Penal señala: *"Los intervinientes tendrán acceso a esas especies, con el fin de reconocerlas o realizar alguna pericia, siempre que fueren autorizados por el ministerio público o, en su caso, por el juez de garantía. El ministerio público llevará un registro especial en el que conste la identificación de las personas que fueren autorizadas para reconocerlas o manipularlas, dejándose copia, en su caso, de la correspondiente autorización"*.

El artículo 187 del Código Procesal Penal señala:

> *"Los objetos, documentos e instrumentos de cualquier clase que parecieren haber servido o haber estado destinados a la comisión del hecho investigado, o los que de él provinieren, o los que pudieren servir como medios de prueba, así como los que se encontraren en el sitio del suceso a que se refiere la letra c) del artículo 83, serán recogidos, identificados y conservados bajo sello. En todo caso, se levantará un registro de la diligencia, de acuerdo con las normas generales"*[9].

Resguardos especiales aplicables a la evidencia electrónica

Lo señalado a propósito de la cadena de custodia y sus etapas es aplicable íntegramente a la evidencia de carácter electrónico. Sin embargo, además de lo consignado, para este tipo de evidencia será necesario acreditar el cumplimiento de resguardos especiales que permitan asegurar la integridad e inalterabilidad del material obtenido.

En este sentido, una primera complejidad de este tipo de evidencia surge al delimitar el concepto del sitio del suceso. En estos casos podrían darse diferentes ubicaciones geográficas en las cuales sea posible levantar evidencias de carácter electrónico, pasando a ser parte de lo que se podría denominar "sitio del suceso informático". Por ejemplo, el lugar en el cual el delincuente utilizó un computador con el cual ejecuta el delito; el lugar donde se encuentra el computador que recibe un ataque cibernético que permite perpetrar una sustracción de dinero o valores; los sitios en los que un sujeto pueda alojar páginas web, dar el servicio de foros, tener un servicio de correo electrónico o en general donde puedan alojarse y compartirse archivos. Igualmente relevante resultan los proveedores de conexión a Internet para los delitos en que el medio utilizado es precisamente la red, por ejemplo la dirección IP de los clientes para determinar la identidad del imputado. Todo ello, independiente de otros lugares en los que se podrían encontrar dispositivos que pudiesen tener mantener información de relevancia.

En todos los sitios anteriormente nombrados se podrán encontrar distintos dispositivos electrónicos en los que pudiere haber evidencia, como cámaras digitales, discos duros, cintas magnéticas, tarjetas de memoria, CD, DVD, dispositivos USB (como *pendrives* o discos externos), o dispositivos de almacenamiento electrónico en general.

[9] La norma se complementa con lo dispuesto en el artículo 221 del Código Procesal Penal: *"De toda diligencia de incautación se levantará inventario, conforme a las reglas generales. El encargado de la diligencia otorgará al imputado o a la persona que los hubiere tenido en su poder un recibo detallado de los objetos y documentos incautados. Los objetos y documentos incautados serán inventariados y sellados y se pondrán bajo custodia del ministerio público en los términos del artículo 188"*.

Así, a efectos de acreditar los hechos constitutivos de un delito informático, es de importancia tanto el resguardo de los dispositivos que pueden ser levantados desde el sitio del suceso (*hardware*) como la información que se contiene en los mismos, correspondiente a archivos, imágenes, correos electrónicos, entre otros.

Aunque, como se señaló, nuestra normativa procesal penal no contempla reglas estrictas de conservación y tratamiento de la evidencia, la naturaleza de la evidencia electrónica y la volatilidad de la información que se encuentra almacenada en los distintos soportes exigen un especial cuidado de parte del personal experto encargado de su levantamiento, custodia y posterior análisis.

De esta forma, las distintas etapas de la cadena de custodia que ya han sido expuestas en esta ponencia, en el caso de evidencia electrónica presentan las siguientes particularidades[10]:

En lo que respecta al resguardo del sitio del suceso, el personal experto o de apoyo debe asegurar que todas las personas sean apartadas del área inmediata de la cual se obtendrán las evidencias. En efecto, cualquier actividad que sea efectuada sobre los equipos computacionales, incluso a distancia (ingresando, por ejemplo, al servidor de correo electrónico desde un teléfono con conexión a Internet) puede alterar la evidencia. Es igualmente importante que al arribar al sitio del suceso, el personal que toma contacto con la evidencia no encienda ni apague ningún equipo electrónico, así como tampoco moverlo, hasta la llegada de personal especializado, a menos que existan indicios de manipulación del sistema informático.

La inspección preliminar en este caso debe poner especial atención en identificar provisoriamente todos los dispositivos que pudiesen ser fuente de evidencia presentes en el sitio del suceso; entre ellos, se cuenta con el gabinete del computador, discos duros, CDs, DVDs, dispositivos USB, tarjetas de memoria, cámaras digitales, disquetes, entre otros.

A continuación, en lo que respecta a la fijación de la evidencia, el funcionario encargado debiera efectuar el procedimiento de etiquetado de los distintos

[10] Algunos de los protocolos o criterios de actuación en materia de levantamiento, custodia y análisis de evidencia informática cuyo contenido se resume en esta ponencia puede ser encontrado en: ACURIO DEL PINO, Santiago: *Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0* [fecha de consulta 16 de septiembre de 2013] Disponible en: http://www.oas.org/juridico/english/cyb_pan_manual.pdf. DEPARTAMENTO DE JUSTICIA DE LOS ESTADOS UNIDOS: INSTITUTO NACIONAL DE JUSTICIA: *Examen forense digital: una guía para la aplicación de la ley (Forensic Examination of Digital evidence: A Guide Law Enforcement)* (2004) [fecha de consulta 16 de septiembre de 2013] Disponible en: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf. GRANCE, Timothy; CHEVALIER, Susanne, et al: *Guía para la integración de técnicas forenses sobre el incidente de respuesta: Recomendaciones del Instituto Nacional de Estándares y Tecnología (Guide to Integrating Forensic Techniques into Incident Response: Recommendations of the National Institute of Standards and Technology)* (2006) [fecha de consulta 14 de septiembre de 2013] Disponible en: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=50875.

dispositivos; así como también etiquetar las entradas a los dispositivos a los que estén conectados los cables, además de etiquetar estos últimos; dibujar las conexiones de los cables con las entradas a las que estén conectados, de manera de poder reconstruir la escena a futuro, tomar nota de la actividad registrada en el monitor antes de realizar cualquier acción, fotografiar o filmar la pantalla; identificar y recoger evidencia física que esté asociada a la electrónica, como manuales u otros documentos que contengan información de interés para la investigación: contraseñas, direcciones de correo electrónico u otras de relevancia.

Al momento de proceder a levantar la evidencia se deben registrar todas las acciones llevadas a cabo y cualquier cambio que se produzca en el monitor, computador, impresora o cualquier otro dispositivo, que haya sido resultado de estas acciones. La forma de proceder dependerá de si el monitor está encendido, apagado o en suspensión. En el primer caso es recomendable fotografiar la pantalla y registrar la información que se muestra en ella; si la pantalla está en modo de suspensión o se ve un protector de pantalla, se sugiere desplazar el mouse, a partir de lo cual la pantalla debería mostrar actividad o pedir una contraseña, momento en que se debe fotografiar la pantalla y registrar la información que se muestra en ella. Finalmente, si el monitor está apagado, se deberá registrar esta circunstancia, prender el monitor y determinar si existe actividad, procediendo del modo antes indicado.

Enseguida, y sin importar el estado de encendido del computador, desconectar el cable de energía de la salida del computador; o en caso de ser un computador portátil, remover la batería. Verificar si existe algún tipo de conectividad, como módem telefónico o mediante cable de red. En caso de conexión telefónica, tratar de identificar el número telefónico. Poner cinta en todos los conectores de entrada del gabinete y sobre la entrada del cable de energía. Registrar números de fabricación, de modelo y de serie. Fotografiar y dibujar las conexiones del computador y los correspondientes cables. Etiquetar todos los conectores y finales de cable para poder reconectar el equipo de forma exacta en alguna ocasión posterior. De similar forma, etiquetar los conectores de entrada sin usar como tales. Finalmente, confeccionar el correspondiente formulario de cadena de custodia.

Atendida la naturaleza de las especies, el almacenamiento de estas debe ser efectuado en envoltorios que protejan los medios magnéticos de la electricidad estática; se debe evitar doblar o rayar medios computacionales como disquetes o discos compactos.

Al momento del traslado deberá mantenerse la evidencia informática alejada de fuentes magnéticas. Radiotransmisores, parlantes magnéticos y asientos calientes son ejemplos de cosas que pueden dañar dicha evidencia. Tampoco

debe exponérseles a condiciones de calor, frío o humedad extremos, ya que pueden dañar la evidencia informática, lo mismo que golpes o vibración excesiva producto, por ejemplo, de un traslado prolongado a bordo de un vehículo motorizado.

Posteriormente, y una vez resguardadas las especies en el lugar de almacenamiento, este debe mantener las mismas condiciones antes señaladas.

En forma previa al análisis pericial destinado a la obtención de información contenida en los soportes informáticos y a objeto de preservar la evidencia contra daños accidentales o intencionales, usualmente se realiza una copia o imagen "espejo" exacta del medio analizado. Estas copias duplicadas deben ser escritas en otro disco rígido o CD-ROM, debiendo documentarse todo el proceso de la generación de imágenes.

Existen herramientas técnicas que permiten acreditar la identidad de la evidencia con la copia obtenida sobre la cual se efectuará el análisis pericial, mediante la generación de códigos alfanuméricos que surgen al momento de generarse los clones de la información contenida en algún dispositivo de almacenamiento resguardando de esta forma la integridad de los datos.

El uso de esta copia para efectos del análisis pericial no solo resguarda la integridad de la evidencia, sino que también permite mantener un respaldo para reconstruir una nueva copia si fuese necesario.

Finalmente, y en relación al registro documental, la información de la documentación y reportes debe completarse durante todo el proceso de levantamiento de las evidencias informáticas, de modo tal que las notas sean lo suficientemente detalladas para permitir una réplica exacta de las acciones adoptadas, documentando de igual manera cualquier irregularidad y toda acción tomada con respecto a aquellas irregularidades por parte del personal examinador de manera de adelantar posibles objeciones al tratamiento que se ha dado a la evidencia. Estos registros serán el respaldo con que contará el personal experto al momento de exponer su trabajo en el juicio oral y explicar las operaciones realizadas para capturar la información contenida en la evidencia.

Efectos de un eventual incumplimiento de los protocolos y recomendaciones en el manejo de la evidencia informática.

Las recomendaciones y "buenas prácticas" que diversos instrumentos señalan para el adecuado resguardo de la evidencia contenida en soportes informáticos no son vinculantes para los organismos técnicos encargados de la práctica de

estas diligencias[11]; es decir, no hay una obligación legal para proceder de una determinada manera en el manejo de esta evidencia, y consecuentemente no hay tampoco una sanción expresa al incumplimiento de los protocolos antes mencionados.

Desde ya, es posible descartar que el incumplimiento de estos protocolos derive en una exclusión probatoria de la evidencia en la audiencia preparatoria del juicio oral. En efecto, conforme dispone el artículo 276 del Código Procesal Penal, las causales de exclusión probatoria son la impertinencia, la sobreabundancia y la vulneración de garantías constitucionales[12], ninguna de las cuales se configuraría por el incumplimiento a las recomendaciones sobre el resguardo de esta evidencia.

Los problemas en el adecuado manejo de la evidencia, y consecuentemente el tratamiento de la cadena de custodia, afectan el valor probatorio de la especie presentada a juicio, y como tal las objeciones a las medidas de custodia y conservación serán materia del debate de fondo en el juicio oral para deslegitimar la autenticidad o integridad de la especie presentada en el proceso.

La jurisprudencia del proceso penal ha fallado en este sentido descartando la exclusión por inobservancia de garantías a propósito de un inadecuado manejo de la cadena de custodia, permitiendo incluso suplir, mediante distintos medios, la cadena de custodia original[13].

---

[11] Las propias guías se encargan de señalar en forma expresa el carácter de recomendaciones de sus contenidos sujetos a las prácticas y disposiciones de cada ordenamiento: *Debido a que diferentes organizaciones están sujetas a diferentes leyes y reglamentos, esta publicación no debe ser utilizada como una guía para la ejecución de una investigación forense digital, interpretarse como asesoramiento legal, o ser utilizada como la base para las investigaciones de la actividad criminal. En cambio, las organizaciones deberían utilizar esta guía como punto de partida para el desarrollo de una capacidad forense en relación con una amplia orientación proporcionada por los asesores legales, los funcionarios encargados de hacer cumplir la ley, y la gestión* ("*Because different organizations are subject to different laws and regulations, this publication should not be used as a guide to executing a digital forensic investigation, construed as legal advic, or used as the basis for investigations of criminal activity. Instead, organizations should use this guide as a starting point for developing a forensic capability in conjunction with extensive guidance provided by legal advisors, law enforcement officials, and management").* GRANCE y CHEVALIER (2010) p. 7.

[12] Artículo 276 Código Procesal Penal.- Exclusión de pruebas para el juicio oral. El juez de garantía, luego de examinar las pruebas ofrecidas y escuchar a los intervinientes que hubieren comparecido a la audiencia, ordenará fundadamente que se excluyan de ser rendidas en el juicio oral aquellas que fueren manifiestamente impertinentes y las que tuvieren por objeto acreditar hechos públicos y notorios.

Si estimare que la aprobación en los mismos términos en que hubieren sido ofrecidas las pruebas testimonial y documental produciría efectos puramente dilatorios en el juicio oral, dispondrá también que el respectivo interviniente reduzca el número de testigos o de documentos, cuando mediante ellos deseare acreditar unos mismos hechos o circunstancias que no guardaren pertinencia sustancial con la materia que se someterá a conocimiento del tribunal de juicio oral en lo penal.

Del mismo modo, el juez excluirá las pruebas que provinieren de actuaciones o diligencias que hubieren sido declaradas nulas y aquellas que hubieren sido obtenidas con inobservancia de garantías fundamentales.

Las demás pruebas que se hubieren ofrecido serán admitidas por el juez de garantía al dictar el auto de apertura del juicio oral.

[13] Así, por ejemplo, a propósito de un recurso de apelación formulado por el Ministerio Público contra la decisión del Juez de Garantía de excluir evidencia por infracción de garantías constitucionales atendido

En nuestro ordenamiento, como se señaló, la custodia y conservación de los objetos y documentos recogidos en el sitio del suceso pertenece al Ministerio Público, y es precisamente el ente persecutor el principal promotor de un adecuado manejo que permita presentar el caso sin que la evidencia sea objetada por falta de autenticidad respecto de aquella obtenida en el lugar de los hechos. Es el propio acusador quien debe formar convicción en el sentenciador "*más allá de toda duda razonable*"[14], de su teoría del caso, y por tanto cualquier manejo indebido puede imponer reparos que menoscaben la credibilidad de la evidencia presentada en juicio[15].

En efecto, el tratamiento inapropiado de la evidencia permitirá que la defensa articule en el Tribunal una duda razonable sobre los resguardos utilizados por la Fiscalía sobre objetos y documentos que son presentados en juicio, de manera de impedir una decisión de condena que esté construida sobre una base precaria bajo una investigación negligente[16].

Conclusiones

1. Los archivos digitales, correos electrónicos y los soportes que los contienen constituyen antecedentes probatorios de relevancia no solo para los delitos informáticos consistentes en atentados a un sistema de información, sino también a una multiplicidad de delitos tradicionales en los cuales el medio de comisión sea realizado por un dispositivo electrónico, o que este contenga antecedentes de relevancia para el esclarecimiento de los hechos.

2. La evidencia electrónica comparte las exigencias del cumplimiento de protocolos de actuación a efectos de su levantamiento, traslado, custodia y análisis con los demás objetos y documentos relevantes para la investigación, que se traducen en el resguardo de la cadena de custodia. Sin embargo, atendida su naturaleza, se han elaborado protocolos adicionales que se

el quebrantamiento de la cadena de custodia, se resolvió: "*Que al momento de alegarse la afectación a la cadena de custodia o el vicio de la prueba, ello se realiza ante la incertidumbre que pudiera generar el tiempo que demoró en remitirse al organismo fiscal correspondiente,* ***situación que corresponde ser analizada en cuanto a su contenido, como también grado de pureza a los jueces del fondo, no afectando de esta manera la sustancia misma, toda vez que lo anterior no tiene su origen en diligencias que han sido declaradas nulas, como tampoco que se hayan obtenido con inobservancia de garantías fundamentales****, lo que se ve reforzado con la diligencia realizada por la Policía y el acta de incautación que se levantó, de manera que no corresponde excluir dicha prueba por la Juez de Garantía.*

Si la Policía se retrasó en el cumplimiento de una obligación, ello no constituye vulneración de garantía s, sino más bien podrá constituir alguna infracción de carácter administrativo, pero no una causal de exclusión de prueba". Corte de Apelaciones de Antofagasta (2010) Rol 369-2010, 30 de noviembre de 2010, considerando sexto, [fecha de consulta 31 de agosto de 2013] Disponible en: www.poderjudicial.cl. Énfasis agregado.

[14] Artículo 341 Código Procesal Penal.

[15] En el sentido propuesto: HORVITZ LENNON, María Inés; LÓPEZ MASLE, Julián (2002): *Derecho Procesal Penal chileno* (Santiago, Editorial Jurídica de Chile) Tomo II.

[16] Sobre el estándar de convicción y duda razonable: DUCE JULIO, Mauricio; RIEGO RAMIREZ, Cristián (2007): *Proceso Penal* (Santiago, Editorial Jurídica de Chile).

sugiere respetar a efectos de mantener la integridad e inalterabilidad de la información contenida en soportes informáticos.

3. Estos protocolos no son reglas legales, sino recomendaciones forenses para un adecuado tratamiento de la evidencia digital. Su cumplimiento permite al sentenciador apreciar su valor probatorio exento de los cuestionamientos que podrían surgir por un incorrecto manejo forense de los soportes digitales y su contenido, afectando la credibilidad de la prueba y la ponderación que en la sentencia harán los jueces sobre la evidencia rendida.

Bibliografía

1.- ACURIO DEL PINO, Santiago: *Manual de Manejo de Evidencias Digitales y Entornos Informáticos*. Versión 2.0 [fecha de consulta 16 de septiembre de 2013] Disponible en: http://www.oas.org/juridico/english/cyb_pan_manual.pdf.

2.- DEPARTAMENTO DE JUSTICIA DE LOS ESTADOS UNIDOS: INSTITUTO NACIONAL DE JUSTICIA: Examen forense digital: una guía para la aplicación de la ley (Forensic Examination of Digital evidence: A Guide Law Enforcement) (2004) [fecha de consulta 16 de septiembre de 2013] Disponible en: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf.

3.- DUCE JULIO, Mauricio; RIEGO RAMIREZ, Cristián (2007): *Proceso Penal* (Santiago, Editorial Jurídica de Chile).

4.- GRANCE, Timothy; CHEVALIER, Susanne, et al: *Guía para la integración de técnicas forenses sobre el incidente de respuesta: Recomendaciones del Instituto Nacional de Estándares y Tecnología* (Guide to Integrating Forensic Techniques into Incident Response: Recommendations of the National Institute of Standards and Technology) (2006) [fecha de consulta 14 de septiembre de 2013] Disponible en: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=50875.

5.- HERRERA BRAVO, Rodolfo (1998): "Reflexiones sobre los delitos informáticos motivadas por los desaciertos de la ley chilena Nº 19.223", en *REDI Revista Electrónica de Derecho Informático*, N° 5, [fecha de consulta 13 de septiembre de 2013] Disponible en: http://vlex.com/vid/informaticos-motivadas-desaciertos-chilena-223-107005.

6. HORVITZ LENNON, María Inés; LÓPEZ MASLE, Julián (2002): *Derecho Procesal Penal chileno* (Santiago, Editorial Jurídica de Chile) Tomo II.

7.- Instructivo N° 19. Respecto de las funciones de la policía previstas en los artículos 83 y 90 del Código Procesal Penal, en MINISTERIO PÚBLICO, FISCALÍA NACIONAL (2001) Reforma Procesal Penal. Instrucciones Generales N°s 1 a 25 (Santiago, Editorial Jurídica de Chile).

8.- Instructivo N° 44. Sobre los objetos y las evidencias del delito en relación al nuevo proceso penal, en MINISTERIO PÚBLICO, FISCALÍA NACIONAL (2001) Reforma Procesal Penal. Instrucciones Generales N°s 26 a 50 (Santiago, Editorial Jurídica de Chile).

9.- LLOBET RODRÍGUEZ, Javier (1998): *Proceso penal comentado* (San José, UCI).

Normas

1.- Ley N° 19.223, Tipifica figuras penales relativas a la informática, Diario Oficial, 07 de Junio de 1993.

2.- Ley N° 19.696, Establece Código Procesal Penal, Diario Oficial, 12 de octubre de 2000.

Jurisprudencia

1.- Corte Suprema (2010): Rol 3657-10, 23 de agosto de 2010, considerando sexto, [fecha de consulta 31 de agosto de 2013] Disponible en: www.poderjudicial.cl.

2.- Corte de Apelaciones de Antofagasta (2010) Rol 369-2010, 30 de noviembre de 2010, considerando sexto, [fecha de consulta 31 de agosto de 2013] Disponible en: www.poderjudicial.cl.