Evidencia digital
Su importancia en la investigación

Por María Elisa Sosa[1]

Resumen:*Las tecnologías de la información y las comunicaciones están cambiando las sociedades en todo el mundo al mejorar la productividad en las industrias tradicionales, revolucionar los procesos laborales y modificar la velocidad y el flujo de capitales. Sin embargo, este crecimiento rápido también ha desencadenado nuevas formas de delincuencia informática. La investigación de la delincuencia en este ámbito no es una tarea fácil, ya que la mayoría de los datos probatorios son intangibles y transitorios. Los investigadores de delitos cibernéticos buscan vestigios digitales, que suelen ser volátiles y de vida corta. Y aquí surge la importancia de la obtención, tratamiento y resguardo de la evidencia digital. Abordaré el tema haciendo una breve explicación del concepto de la evidencia digital, sus características, los principios por los que es gobernada y los principios básicos en materia de evidencia digital*

Palabras clave: ciberdelitos – evidencia digital- prueba – investigación.

Evidencia digital concepto

Puede definirse la evidencia digital como el conjunto de datos e información, relevantes para una investigación, que se encuentra almacenada en o es transmitida por una computadora o dispositivo electrónico.[2]

Características

La evidencia digital contiene algunas características propias que la distinguen de cualquier otra evidencia tradicional. Entre otras, contiene las siguientes particularidades:

- **Volátil:** Puede perderse si no se recolecta en tiempo y forma.
- **Duplicable:** Pueden realizarse diversas copias sin poder reconocer el original.
- **Alterable:** Factible de su modificación y/o borrado y sin el registro de esas acciones.
- **Anónima**: En algunos casos no se pueden determinar el autor de las mismas.

Posee datos adicionales no visibles por las herramientas tradicionales usadas por el usuario: Último acceso, modelos de cámara usados en una fotografía, coordenadas de geo posicionamiento, autor, última impresión, secuencia de recorrido de un correo electrónico, etc.). Su recolección, preservación y presentación involucra una serie de procedimientos a cumplir en tiempo y forma, a fin de mantener la integridad, autenticidad, confiablidad y validez legal de la misma.[3]

Principios de tratamiento de la evidencia digital

Varios documentos han abordado esta temática, entre ellos se destaca la norma ISO/IEC 27037:2012[4] que brinda

[1] Abogada – Universidad Nacional del Nordeste (UNNE), Especializada en Cibercrimen UNQ.

[2] Guía para la obtención, preservación y tratamiento de evidencia digital recuperado de https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf

[3] Guía de Ciberdelitos Poder Judicial de Salta recuperado de file:///C:/Users/veronica/Downloads/ciberdelitos_web_v020518.pdf

[4] **La ISO** (International StandarizationOrganization) es la entidad internacional encargada de favorecer

lineamientos para la identificación, recolección, obtención y preservación de la evidencia digital de forma tal de poder ser utilizada como evidencia útil. Para algunos autores, la regla indica que la evidencia digital es gobernada por tres principios fundamentales: la relevancia, la confiabilidad y la suficiencia. Estos tres elementos definen la formalidad de cualquier investigación basada en evidencia digital. La relevancia es una condición técnicamente jurídica, que habla sobre aquellos elementos que son pertinentes a la situación que se analiza o investiga, con el fin de probar o no una hipótesis que se ha planteado alrededor de los hechos. Todo aquello que no cumpla con este requisito será irrelevante y excluido del material probatorio recabado para efectos del caso bajo estudio. La confiabilidad es otra característica fundamental, que busca validar la repetibilidad y auditabilidad de un proceso aplicado para obtener una evidencia digital. Es decir, que la evidencia que se extraiga u obtenga sea lo que deba ser; y que si un tercero sigue el mismo proceso, deberá obtener resultados similares, verificables y comprobables. Finalmente, el principio de suficiencia, se relaciona con la completitud de pruebas informáticas. En otras palabras, significa que con las evidencias recolectadas y analizadas tenemos elementos suficientes para sustentar los hallazgos y verificar las afirmaciones efectuadas sobre la situación investigada. Este elemento está sujeto a la experiencia y formalidad del perito informático en el desarrollo de sus procedimientos y priorización de esfuerzos.[5]

Si bien puede haber otros elementos que ayuden en el gobierno de la evidencia digital, ISO ha determinado que estos tres establecen las condiciones necesarias y suficientes para que los expertos en informática forense recaben, aseguren y preserven elementos materiales probatorios sobre medios digitales, los cuales podrán ser revisados y analizados por terceros interesados y sometidos a contradicción según el ordenamiento jurídico donde se encuentren.

Otros documentos hablan de principios básicos en materia de evidencia digital que deben tenerse en cuenta a lo largo de todo el procesamiento de este tipo de prueba.

Estos son:

1. Al llegar a la escena donde se va a obtener evidencia digital, lo primero que debe hacerse es evitar su contaminación, retirando del lugar a toda persona ajena al procedimiento que se está llevando a cabo;
2. En segundo lugar, ninguna acción de las fuerzas de seguridad o de sus agentes debe alterar los datos contenidos las computadoras o dispositivos de almacenamiento informático que luego serán utilizados como elementos de prueba;
3. Si las circunstancias del caso hacen necesario que se deba acceder a los datos o información

normas de fabricación, comercio y comunicación en todo el mundo, brindando estándares internacionales. La regla citada puede adquirirse en http://www.iso.org/iso/cataloauedetail?csnumber 4438\

[5] Guía para la obtención, preservación y tratamiento de evidencia digital recuperado de https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf

contenida en las computadoras o dispositivos de almacenamiento informático, la persona que efectúe dicha tarea debe ser idónea, es decir, contar con los conocimientos técnicos informáticos que la situación merece y, a su vez, capaz de explicar el motivo por el cual debió interactuar con la evidencia digital -por lo general, la urgencia del caso-, y los pasos llevados a cabo;

4. Finalmente, se debe auditar y registrar fehacientemente todo el proceso relativo a la manipulación de la evidencia digital, precisando detalladamente las medidas y acciones llevadas a cabo, teniendo como eje central, la preservación de la cadena de custodia[6]

Su importancia en la investigación

La evidencia digital es una prueba de fácil adulteración por sus especiales características, por tanto, su manipulación debe resguardar ciertos protocolos de seguridad. Así también lo debe hacer, el proceso de secuestro de su continente como el proceso extracción de datos, ya que la prueba digital, en su estado natural, no permite entrever qué información es la que contiene en su interior, por lo que resulta para ello ineludible, examinar a través de instrumentos y procesos forenses específicos.

Por su naturaleza volátil y modificable, por la facilidad para copiarla y eliminarla, la evidencia digital requiere de un gran cuidado en cuanto a su conservación y de gran especialización en los peritos que la manipulan, a fin de no alterarla y conservarla a los fines de la presentación en un eventual juicio.

Algunos autores señalan que el Registro de la cadena de custodia sólo es útil a los fines del aseguramiento de los continentes de los datos informáticos, pero no de los datos en sí mismos. Ya que el resguardo físico de los dispositivos no aseguraría al cien por cien la conservación de su contenido. En la actualidad una manera de sortear esta dificultad y garantizar la integridad de la evidencia es a través de la aplicación de algoritmos matemáticos que calculan un número único basado en el contenido del mensaje de datos, conocido como función HASH». Así si el documento sufriese alguna alteración el Hash se modificaría también y dejaría al descubierto la alteración de la evidencia.[7]

Otro aspecto a tener en cuenta es la llamada cadena de custodia de los elementos de prueba, entendida como el control que se efectúa tanto de las personas que recogen la evidencia como de cada persona o entidad que posteriormente tiene la custodia de la misma. La cadena de custodia debe contener un identificador unívoco de la evidencia, de las fechas en las que los artículos fueron recogidos o transferidos, datos sobre el responsable que realizó la recolección, datos sobre la persona que recibe la evidencia y los datos de las personas que acceden, el momento y la ubicación física, número del

[6] Guía para la obtención, tratamiento y preservación de evidencia digital recuperado de https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf

[7] Las garantías procesales en la obtención de evidencia digital recuperado de https://aldiaargentina.microjuris.com/2021/04/27/doctrina-las-garantias-procesales-en-la-obtencion-de-evidencia-digital/

caso, y una breve descripción de cada elemento. El pasaje de la evidencia de un sitio a otro y las tareas realizadas, cualquier cambio inevitable potencial en evidencia digital será registrado con el nombre del responsable y la justificación de sus acciones. El objetivo de la cadena de custodia es garantizar la autenticidad de la evidencia que se utilizará como prueba dentro del proceso.[8]

Conclusión

Los delitos informáticos, presentan nuevos y grandes desafíos a la ciencia jurídica ya que esta debe actualizarse constantemente, conforme avanza la tecnología, La gran creciente de casos de ciberdelitos según un informe de la (UFECI) 9 ha aumentado en un 3000% a raíz de la pandemia, este crecimiento exponencial hace necesaria la capacitación de peritos informáticos y agentes policiales como así también de abogados de los protocolos de actuación nacionales en materia de evidencia digital ya que es muy importante para el éxito de la investigación de estos delitos su obtención, preservación y tratamiento. La prueba digital es fundamental para la investigación por la información y datos de valor que pueden extraerse de los distintos dispositivos electrónicos, tanto aquellos aportados por el denunciante como los que se encuentren en el lugar de allanamiento. Dicha prueba puede ser en ciertos delitos de extrema preponderancia y en algunos casos, la única evidencia que se puede obtener para el esclarecimiento del delito investigado.

Referencias bibliográficas

- Guía de obtención, preservación y tratamiento de evidencia digital. Ministerio público fiscal de la república argentina r. (PGN 756/2016) recuperado dehttps://www.fiscales.gob.ar/wp-content/uploads/2016/04/pgn-0756-2016-001.pdf
- Guia de ciberdelitos - poder judicial de salta recuperado de file:///c:/users/veronica/downloads/ciberdelitos_web_v020518.pdf
- Las garantías procesales en la obtención de evidencia digital recuperado **de** https://aldiaargentina.microjuris.com/2021/04/27/doctrina-las-garantias-procesales-en-la-obtencion-de-evidencia-digital/
- Protocolo general de actuación para las fuerzas policiales y de seguridad en la investigación y proceso de recolección de pruebas en ciberdelitos. Ministerio de seguridad - Resolución 234/2016 recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/262787/norma.htm

[8] Protocolo general de actuación para las fuerzas policiales y de seguridad en la investigación y proceso de recolección de pruebas en ciberdelitos. **MINISTERIO DE SEGURIDAD - Resolución 234/2016** recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/262787/norma.htm

[9] Unidad Fiscal Especializada En Ciberdelincuencia.