04.
Trabajos científicos de cursantes y egresados de la Escuela Judicial

La prueba documental informática y la intervención del perito informático en la investigación criminal.

Revista Escuela Judicial: ISSN en trámite
Año: 01/N°1 - Noviembre 2021
Recibido: 14/09/2021
Aprobado: 01/10/2021

La prueba documental informática y la intervención del perito informático en la investigación criminal

The computerized documentary evidence and the intervention of the computer expert in the criminal investigation

Por Paola Vanesa Sifre[1]
Universidad Nacional de La Plata, Argentina

Resumen: En este trabajo se exponen algunos de los temas que encontramos al momento de investigar un delito, como la prueba documental informática, la forma de su resguardo y sus particularidades, la relación con la informática forense y sus idóneos y con las ciencias criminalísticas. Todo ello, relacionado con una investigación penal durante sus distintas etapas procesales, y visualizando preguntas y debates de un futuro más que cercano.

Palabras clave: Prueba documental – Informática forense – Cadena de custodia – Normativa.

1. Abogada (Universidad Nacional de La Plata). Técnica universitaria en Criminalística (Universidad Católica de La Plata). Instructora judicial de la Ayudantía de delitos acaecidos en unidades penitenciarias del Departamento Judicial de La Plata. Egresada de la escuela Judicial del Consejo de la Magistratura en Derecho Público y Derecho Privado.

Abstract: *Here in this work some of the issues that we encounter today when investigating a crime are exposed, such as computerized documentary evidence, the forms of its protection and its particularities, the relationship with forensic information technology and its experts and this with the crime sciences. All this related to a criminal investigation during its different procedural stages and visualizing the questions to be asked and debated by lawyers, magistrates and legal professionals in the near future.*

Keywords: *Documentary evidence – Computer forensics – Chain of custody.*

La informática forense se encuentra dentro del vasto campo de las ciencias de la criminalística.[2] En ella, la evidencia o los indicios carecen de forma física, ya que la información está dada por secuencias de bits o permutaciones de unos y ceros que, a través de un traductor, pueden ser interpretadas por el usuario en uno u otro extremo de los terminales computarizados. Por ello es que, a la par de la evolución de la diversidad de funciones y operaciones monetarias, comerciales, políticas que se realizan a través de internet, también evoluciona el delito informático con el que se vulneran estas operaciones, por lo que es forzosamente necesaria la implementación de nuevas técnicas de protección para brindar seguridad a los usuarios; y, si aun así se produjera un ilícito, tener las herramientas para obtener la información adulterada y el posterior transporte y resguardo de la misma para futuras pericias.

Según Darahuge y Arellano González (2011), la informática forense "es el conjunto multidisciplinario de teorías, técnicas y métodos de análisis que brindan soporte conceptual y procedimental a la investigación de la prueba indiciaria informática" (p. 9). Otra definición brindada en el mismo manual dice: "La informática forense es un método probatorio consistente en la revisión científica, tecnológica y técnica con fines periciales de una colección de evidencias digitalizadas para fines de investigación o legales" (id.).

Esta disciplina ha ido creciendo a la velocidad de los avances tecnológicos, como así también las herramientas y los soportes

2. Para la confección de este artículo se recurrió al *Manual de Informática Forense*, de María Elena Darahuge y Luis Enrique Arellano González (2011), que, si bien no es el más actualizado, es el que consideramos que ofrece la mayor claridad y sencillez en los conceptos. Por otro lado, este trabajo intenta describir el manejo de la evidencia forense digital y no tanto de actualidad informática.

digitales que forman parte de nuestra vida, y las conductas delictivas en general, aunque muchas de estas no sean específicamente un delito informático, ya que en la mayoría de los delitos cometidos en nuestra sociedad (como en las correspondientes investigaciones que intentan dilucidarlos y probarlos) se involucra al menos un dispositivo tecnológico.

Hoy, muchas de las acciones que llevamos a cabo diariamente –y más en el contexto que nos toca atravesar por la aparición del virus de la covid-19– son a través de computadoras o celulares, quedando reservados datos como las direcciones de IP[3], las localizaciones geográficas y los historiales de navegación de las páginas de internet o las aplicaciones de celular (a través del IMEI)[4] del pago de servicios o compras en tiendas virtuales, el envío de correos electrónicos, entre otras actividades que realizamos.

Con el avance de una investigación criminal llevada a cabo por un fiscal de Instrucción, y dados los distintos hechos que se investigan, la prueba documental informática se presenta como una prueba más de todo el plexo convictivo.

La prueba documental, tal como la definían los autores clásicos del derecho procesal, es uno de los medios disponibles para demostrar la veracidad de un hecho que es alegado, por cuanto la información que consta en documentos o escritos puede ser valorada por un

3. El "Internet Protocol" o Protocolo de Internet es una especie de matrícula para identificar cada ordenador cuando este se encuentra conectado a una red de internet. Hay dos tipos de direcciones IP: las públicas y las privadas; las primeras son la matrícula que se asigna para identificar al usuario, y las segundas son las que se utilizan cuando se conecta cada aparato a la red domiciliaria.

4. El International Mobile Station Equipment Identity, es un código de quince dígitos pregrabado por el fabricante para identificar cada equipo móvil a nivel mundial.

juez como una muestra de la autenticidad de un hecho. El maestro Lino Enrique Palacios (2004) dice que "no solo son documentos los que llevan signos de escritura, sino también todos aquellos objetos que como los hitos, planos, marcas, contraseñas, mapas, fotografías, películas cinematográficas, cintas megatofónicas, vídeos, etcétera, poseen la misma aptitud representativa" (p. 424). El autor era un adelantado en su tiempo, abriendo la posibilidad a las nuevas formas de pruebas que se dan en la actualidad.

"La prueba documental informática es una especie de la prueba documental clásica", (Darahuge & Arellano González, 2011, p. 19); la diferencia es el soporte material que la contendrá.

Los formatos en los que se puede presentar la prueba documental recolectada en una investigación pueden ser físicos o digitales. La recolección de este tipo de pruebas se puede dar tanto en el ámbito del fuero penal como en el del fuero civil, laboral o dentro de los procesos de familia.

El Código Procesal Civil de la provincia de Buenos Aires (art. 385 y ss.) regula lo atinente a la prueba documental.[5] Dentro del ámbito penal, la misma se regula por lo establecido en el Código Procesal Penal para la producción de la prueba y siempre que la misma sea obtenida observando las garantías constitucionales que poseen los imputados en tal carácter (arts. 1, 60, 90 y 247).[6]

---

5. Código Procesal Civil y Comercial de la Provincia de Buenos Aires. Decreto-Ley 7425/68, Capítulo V Prueba, Sección 2° Prueba Documental. Arts. 358 a 393.

6. Código Procesal Penal de la Provincia de Buenos Aires. Ley 11.922 sancionada el 18 de diciembre de 1996 y promulgada el 10 de enero de 1997, publicada en el Boletín Oficial el 23 de enero de 1997; modificada por la Ley N° 12.059 sancionada el 11 de diciembre de 1997, promulgada el 19 de diciembre de 1997 y publicada en el Boletín Oficial el 9 de enero de 1998.

En los casos en que se encuentre bajo investigación personal de alguna fuerza de seguridad, la toma de la evidencia informática está a cargo de los peritos informáticos dependientes del Ministerio Publico Fiscal. En nuestra provincia, por ejemplo, se encuentra en funcionamiento dentro de la Policía Judicial el Gabinete Informático, que interviene en cumplimiento de la Resolución 1390/01[7] de la Procuración General de la provincia de Buenos Aires y de la "Guía de investigación en casos de severidades, vejaciones y apremios ilegales ocurridos en ámbitos de encierro" de la Procuración General (Resolución 271).[8]

La prueba documental informática es una prueba documental más y será valorada por los magistrados como otra prueba de cargo, con el resto de los elementos colectados por el director del proceso, en el ámbito de nuestra provincia de Buenos Aires, el agente fiscal de Instrucción.[9] La diferencia radica en la toma o la manipulación de la misma. Será recolectada en el lugar de los hechos por los profesionales del área informática de las fuerzas de seguridad o los peritos dependientes de las Asesorías Periciales Departamentales, según sea el caso bajo investigación de acuerdo con la mencionada Resolución 1390/01.

---

7. Resolución General dictada por el procurador Dr. Matías Eduardo De La Cruz con fecha del 10 de diciembre de 2001, la cual dispone que el Ministerio Público Fiscal provincial deberá brindar especial importancia a hechos delictivos vinculados con torturas, apremios ilegales y delitos económicos.

8. Resolución General dictada por la procuradora Dra. María del Carmen Falbo con fecha del 13 de abril de 2015.

9. "El Agente Fiscal tendrá las siguientes facultades: 1. Dirigirá, practicará y hará practicar la Investigación Penal Preparatoria actuando con la colaboración de la Policía en función judicial, solicitando las medidas que considere necesarias, ante los jueces o ante cualquier otra autoridad" (art. 59 del Código Procesal Penal. Ley 11.922 y sus modificatorias).

La recolección de la prueba indiciaria de carácter físico en un delito informático debe llevarse a cabo como cualquier toma de evidencias en el lugar de los hechos, en presencia de testigos que deben dar fe de las tareas realizadas por el perito, dando cuenta de las operaciones realizadas mediante las actas de procedimiento, siempre cumpliendo estrictamente el contenido de los artículos 117[10] y 118[11] del Código Procesal Penal de la provincia (Ley 11.922). Los peritos deben cumplir con la confección de la correspondiente cadena de custodia, "el registro cronológico y minucioso de la manipulación adecuada de los elementos, rastros e indicios hallados en el lugar del hecho, durante todo el proceso judicial" (MJDH, 2017, p. 47). Estas actas seguirán al efecto secuestrado y expondrán por qué manos pasó desde el inicio de la cadena hasta su llegada al laboratorio. También será tarea del perito proceder a cerrar los puertos de ingreso a CPU, notebook o discos rígidos, entre otros, con las fajas de seguridad firmadas por los actuantes, en garantía de ley y a los

---

10. "Regla General. Cuando el funcionario público que intervenga en el proceso deba dar fe de los actos realizados por él o cumplidos en su presencia, redactará un acta en la forma prescripta por las disposiciones de este capítulo. A tal efecto, el Juez o Tribunal serán asistidos por un Secretario, mientras que el Agente Fiscal lo será, en la medida que sea posible, por un Secretario, un ayudante Fiscal o un Oficial de la Policía Judicial o Administrativa; el Juez de Paz y los Oficiales o Auxiliares de Policía, por un testigo que, si es factible, sea extraño a la repartición policial. Los testigos deberán estar presentes durante todo el trámite del acto. La imposibilidad de asistencia por un funcionario o testigo deberá ser expresamente señalada, al igual que sus causas determinantes" (Capítulo IV. ACTAS. Art. 117 del Código Procesal Penal. Ley 11.922 y sus modificatorias).

11. "Contenidos y formalidades. Las actas deberán contener el lugar, la fecha, el nombre y apellido de las personas que intervienen; el motivo que haya impedido, en su caso, la intervención de las personas obligadas a asistir, la indicación de las diligencias realizadas y su resultado, las declaraciones recibidas, si éstas fueron hechas espontáneamente o a requerimiento y si las dictaron los declarantes. Concluida o suspendida la diligencia, el acta será firmada, previa lectura, por todos los intervinientes que deban hacerlo. Cuando alguno no pudiere o no quisiere firmar, se hará mención de ello. Si tuviere que firmar una persona ciega o una analfabeta, se les informará que el acta puede ser leída y en su caso suscripta por una persona de su confianza, lo que se hará constar" (Capítulo IV. ACTAS. Art. 118 del Código Procesal Penal. Ley 11.922 y sus modificatorias).

efectos de no provocar nulidades en los momentos posteriores de la investigación criminal.

Pero ¿qué sucede cuando se produce un hecho delictivo a través de internet? En este caso, los elementos de prueba están compuestos por bits, bytes, megabytes, dependiendo de la cantidad de información que haya sido necesaria para la producción del hecho, o la cantidad de datos que hayan sido sustraídos.

Pero Darahuge y Arellano González (2011) mencionan que "un bit no es similar sino idéntico a otro bit" (p. 65), variando únicamente según la ubicación que adopte en un conjunto mayor, por lo que surge el inconveniente al momento de proceder al "secuestro" de la prueba documental necesaria para efectuar la investigación, y, como consecuencia, la necesidad de un manto de legalidad que legitime la autenticidad de esos datos que van a ser trasladados y peritados. Si habitualmente se utiliza la cadena de custodia para señalar y mantener un control del derrotero de un indicio o evidencia física relevada en la escena de un hecho, y de las personas que tuvieron acceso a los mismos, aunque más no sea para su transporte, para los delitos informáticos existe su homóloga cadena de custodia digital.

La característica de seguridad e inviolabilidad de la cadena de custodia informática forense o digital radica en la capacidad de añadir información extra que contenga los datos propios de la información que protege mediante lo que se conoce como "hash"[12].

12. "Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada [...] una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado". Disponible en: https://www.genbeta.com/desarrollo/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales

Como las herramientas tecnológicas están presentes en todo tipo de delitos, la legislación ha ido acompañando la evolución de la tecnología que es utilizada con fines delictuales, dando lugar a la incorporación en el Código Penal del delito de *grooming*, descrito como la captación de un menor de edad por medio de dispositivos electrónicos con el fin de menoscabar su integridad sexual.[13]

Asimismo y más aún se ha ido avanzando con la legislación que incorpora la tecnología y su uso, o, mejor dicho, su uso en diferentes formas delictuales. Ya existe un proyecto de ley de reforma al Código Penal que realiza un capítulo completo y específico para la temática de los delitos informáticos, como ser penas a los que dañen plataformas, archivos, envíos indebidos de correspondencia electrónica, fraudes informáticos, todo tipo de daños informáticos, penando también conductas nuevas como ser el sexting (la difusión de imágenes o videos privados con contenido sexual), todo ello con base en lo establecido en la convención celebrada en Budapest sobre ciberdelincuencia y delitos informáticos en el año 2001, ratificado por nuestra nación en 2017.[14]

El perito, al momento de recabar la prueba documental informática, debe tener en cuenta lo normado por los códigos de procedimiento y lo que la legislación establece para la materia en la que actúa, sobre todo teniendo en cuenta las garantías constitucionales;

---

13. "Sera penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma" (art. 131, incorporado según Ley 26.904, sancionada el 13 de noviembre de 2013 y promulgada el 4 de diciembre de 2013).

14. El Convenio sobre la Ciberdelincuencia contiene 48 artículos, a los que la República Argentina adhirió mediante la Ley 27.411. Resolución 1.291/2019, Ministerio de Justicia y Derechos Humanos.

cumplir con la cadena de custodia y las actas de procedimiento para la recolección del material informático; realizar la aceptación del cargo[15] en caso de que intervenga como profesional de parte en el proceso; y cuando actúe en su rol de perito de oficio, indicar a los magistrados actuantes las medidas a seguir en cuanto a los elementos informáticos, a fin de acreditar el ilícito bajo investigación, realizar el informe pericial correspondiente a la pericia encomendada y presentarse una vez que la causa ha sido elevada a juicio a dar su testimonio de las tareas que realizó ante las audiencias de debate, ya que es un testigo calificado dentro del proceso.

Para ir concluyendo, expondremos someramente sobre la utilización del sistema de almacenamiento de datos virtual conocido como "nube" y su importancia en los casos en que los delitos informáticos poseen grandes cantidades de datos que exceden los límites de los dispositivos de almacenamiento físico de hoy (discos rígidos, tarjetas de memoria o los casi extintos CD y DVD), herramienta que ya es utilizada por grandes empresas para resguardo de la información a cambio de un canon monetario.

Dejaremos planteada una serie de cuestiones para la cuales aún no tenemos una respuesta certera, pero que confiamos que sucesivos trabajos de investigación tendrán la oportunidad de hacer un aporte más claro.

Por un lado, la utilización de la nube como resguardo de evidencia o material de cargo en los procesos judiciales, simplificando la

15. "Obligatoriedad del cargo. El designado como perito tendrá el deber de aceptar y desempeñar fielmente el cargo, salvo que tuviere un grave impedimento" (art. 246 del Código Procesal Penal).

búsqueda de los efectos que contengan información digital, abandonando la práctica del uso de muebles de escritorio o archiveros en las dependencias judiciales, que ocupan espacios cada vez más escasos; o la confección de backups de esa misma información a fin de evitar su pérdida por el deterioro de estos soportes, dados los plazos judiciales y el movimiento de los expedientes que muchas veces acarrean consigo el efecto adjunto a una de sus fojas. Por otro lado, la agilidad en la transmisión de esta información a través de las distintas dependencias de las fuerzas de seguridad o de Asesorías Periciales a los fines de su evaluación técnica en busca de datos útiles a la investigación. Por último, las preguntas: ¿planteará la defensa técnica de las partes la nulidad de datos resguardados en un espacio virtual que no puede ser percibido con los sentidos?, ¿se debatirá la autenticidad de la cadena de custodias digital?, ¿qué sucederá en los debates, cuando un perito citado al efecto comience a digitar comandos en un dispositivo tecnológico y descargue archivos del espacio virtual para ser exhibidos y puestos a discusión ante el tribunal en tiempo real y valorar su carga probatoria para argumentar en beneficio o perjuicio de los ajusticiados?

Debemos recordar que la tecnología ha llegado para quedarse, y cada vez más es parte de nuestras vidas. Por ello debemos tenerla en cuenta al investigar los delitos, pues siempre habrá algo de ella.

Bibliografía

DARAHUGE, M. E. & ARELLANO GONZÁLEZ, L. E. (2011). *Manual de Informática Forense - Prueba indiciaria, informático forense*, 2 tomos. Buenos Aires: Errepar.

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS DE LA NACIÓN (MJDH) (2017). *Manual de actuación en el lugar del hecho y/o escena del delito*. Ciudad Autónoma de Buenos Aires: Ediciones S.A.I.J. Disponible en: http://www.saij.gob.ar/docs-f/ediciones/libros/Manual_actuacion_lugar_hecho_escena_delito.pdf

PALACIO, L. E. (2004). *Manual de Derecho Procesal Civil*. 18ª ed. actualizada. Buenos Aires: Lexis Nexis - Abeledo Perrot.