

XXX CONGRESO NACIONAL DE DERECHO PROCESAL
-SAN JUAN -

Derecho Procesal Penal, Comisión 1:

“Prueba digital y reglas de la litigación adversarial”

Título: Notas sobre la Prueba Digital

Nombre del autor: Yurec Martín Miguel

Dirección postal: 5 N°435, La Plata, Bs.As., Argentina, Código Postal: 1900.

Teléfono: 0221 15 6080005

Email: martinyurec@gmail.com

Breve síntesis de la propuesta: En el presente trabajo enunciaremos las principales características de la prueba digital, su incidencia en los procesos penales en la actualidad y en particular haremos especial referencia al trabajo de los peritos informáticos, sus labores, los reglamentos, protocolos y guías internacionales y principios que regulan el peritaje informático. Hemos abrevado de fuentes tanto nacionales como internacionales para observar esta nueva profesión que influye cada vez en más procesos.

Postulación: Al Premio de la Asociación Argentina de Derecho Procesal o “el Dial.com”.

Notas sobre la Prueba Digital

Sumario: Introducción. Sobre la prueba y la prueba digital. De la pericia informática. Conclusiones.

Introducción

La tecnología envuelve casi todos los aspectos de la vida moderna, sea desde cómo nos conocemos y relacionamos, dónde y cómo llevamos nuestras finanzas y así influye directamente sobre los procesos judiciales.

A partir de este trabajo analizaremos algunas características de la prueba digital, distinta a los medios de prueba tradicionales, ya que los datos informáticos tienen la particularidad de ser “ceros y unos” que requerirán tanto métodos de recolección como conocimientos técnicos muy precisos.

Sobre la prueba y la prueba digital.

El maestro Lino Palacios definió la prueba como *“el conjunto de actos procesales, cumplidos con el auxilio de los medios previstos o implícitamente autorizados por la ley, y encaminados a generar la convicción judicial acerca de la existencia o inexistencia, la veracidad o la falsedad, de los hechos sobre los cuales versa la imputación.”* Hablamos de lo que confirma o desvirtúa sea una hipótesis o afirmación, en la búsqueda de la verdad de los hechos en una hipótesis acusatoria la prueba será el medio para lograr la reconstrucción de los hechos, siempre respetando el presupuesto indispensable de su legalidad, refiriéndonos a su obtención e incorporación al proceso.

Los sujetos que aportan la prueba, son el intermediario entre la prueba y el juez, el dato conviccional transmitido puede ser obtenido accidentalmente como en el caso de los testigos o puede ser por encargo como los peritos mientras las actuaciones estén dentro de lo regulado por la ley. Como así dentro del principio de libertad probatoria dentro de un proceso penal conforme lo dispuesto por el Art. 127 del Código Procesal Penal de la Nación, comprendiendo que los hechos y circunstancias de interés para la solución del caso se podrá realizar por cualquier medio de

prueba, salvo que estén expresamente prohibidos por ley y como así se podrán utilizar otros medios de prueba además de los comprendidos en el código mientras que no vulneren derechos o garantías constitucionales u obstaculicen el control de la prueba por los demás intervinientes.

Al clasificar la prueba digital estamos refiriéndonos a un medio de prueba ya que *“es el procedimiento establecido por la ley tendiente a lograr el ingreso del elemento de prueba en el proceso”* y más específicamente nos referiremos al sistema de peritos por el cual se produce la prueba misma se obtiene o valora mediante elementos científicos. Su valoración se realizará como por los intervinientes como por los jueces –o jurado- de conformidad con la sana crítica racional, pero con un rasgo especial, la valoración de la prueba depende íntimamente con la idoneidad, experiencia y experticia de los peritos que realizan el dictamen con lo que a fin de debatir la credibilidad del informe o existieran discrepancias entre informes lo indispensable será el conocimiento y la experiencia agregando a lo dicho por el doctor Maier al respecto que no sólo de la experiencia del perito informático en este caso, sino bien a la experiencia de miles de casos por los cuales mediante tratados sobre el tema demuestran científicamente resultados inexorables.

De la pericia informática.

Como prueba pericial podemos comprender el procedimiento regulado para obtener en el proceso conclusiones probatorias a través de peritos, nos referimos a una actividad compleja que determina los puntos a considerar y el dictamen que se obtiene de ellos, es la manera de introducir al proceso un juicio técnico o científico a fin de comprender los hechos. El órgano de la peritación será el perito que realizando un peritaje introducirá sus conclusiones técnicas en el proceso, siendo él un experto en un arte, oficio, ciencia o técnica debiendo ser nombrado a que dictamine a fines de probar, debiendo ser imparcial aun cuando su nombramiento provenga de una de las partes. Como bien indica Maier será requisito básico de los peritos ser idóneos, deben ser aptos respecto a los conocimientos especiales en la materia y pueden requerirse más de uno ya que particularmente la ciencia informática se encuentra ramificada tanto –o más- que las ciencias médicas

y dependiendo los puntos de pericias a contestar un solo profesional no pueda dar una contestación acabada al respecto. A su vez como en otras materias habrá peritos oficiales como peritos de parte, con la particularidad que en materia informática el peritaje muchas veces es llevado adelante por parte de la Policía Judicial y en algunos casos por la misma subsecretaría de informática del poder judicial –como en caso de la Provincia de Buenos Aires-

Eoghan Casey remarca la aproximación de la prueba digital a la pericia científica, más hace hincapié en que la admisibilidad de la prueba digital dependerá como en toda ciencia a las herramientas y técnicas, generando un proceso científico que genere un informe serio y convincente. De hecho en muchos estados de EE.UU. la prueba digital es tomada como “nueva evidencia científica” y su valoración se toma a partir de cuatro criterios de calidad desarrollados en el caso “Daubert v. Merrell Dow Pharmaceuticals, Inc.” (1993): 1-Si la teoría o técnica puede ser o ha sido testeada. 2- Si hay un margen de error conocido y la existencia de estándares de control en la técnica de operación. 3- Si la teoría o técnica ha sido sujeta a revisiones y publicaciones. 4-Si la teoría o técnica tomó aceptación general dentro de la comunidad científica. Casey toma la presentación de un reporte de un experto. Bajo estos mismos criterios el doctor Leopoldo Sebastián Gómez, abogado y Licenciado en Ciencias de la Computación, ha redactado un protocolo de actuación en pericias informáticas para el poder judicial de la Provincia del Neuquén en el que detalla las modalidades de trabajo interno en el envío de material tecnológico al laboratorio pericial, a fin de comprender las técnicas realizadas por los especialistas y la importancia de la cadena de custodia.

En un proceso penal a fin de investigar la evidencia se habla de dos grandes etapas la primera de incautación de la prueba y mantenimiento de la “Cadena de Custodia”, y la segunda se basa en el análisis de la información y redacción del informe pericial. La primera debe ser llevada a cabo por personal policial junto al Fiscal responsable y la segunda efectuada en un laboratorio por un perito, manteniendo en todo momento los estándares de la ciencia forense específica, en función a los puntos de pericia especificados por los operadores judiciales. Tanto en la primer etapa como en la segunda cuidando celosamente la cadena de custodia ya que comienza desde que es

identificado el material tecnológico sobre el que se deberá trabajar en adelante -con particular cuidado en la colocación de precintos de seguridad al momento del secuestro a fin de garantizar la autenticidad e integridad de la evidencia- hasta la redacción del informe por el perito profesional.

Tanto Casey como Gómez, recalcan la importancia del secuestro del material y el trabajo en un área controlada o laboratorio, ya que el material a utilizar deben ser los “originales” atento que revisten caracteres únicos sobre los cuales debe hacerse la pericia como así las tareas a desarrollarse se tornan dificultosas para ser ejecutadas en el lugar de los hechos.

Una vez que los peritos obtienen el material sobre el cual peritar -con el oficio pertinente las cintas de seguridad con sus números de serie intactos que fueran detalladas en el acta de allanamiento- deberían realizar una “imagen forense” no así un backup ya que la “imagen forense” es una copia bit a bit de la evidencia en un formato particular utilizado por los software determinados al análisis forense, mientras el backup en sí es un procedimiento invasivo que altera la evidencia y no conserva la información oculta o remanente de particular importancia a la hora de realizar el peritaje.

Según Piccirilli en su tesis doctoral en Ciencias Informáticas “Protocolos a aplicar en la forensiainformática en el marcode las nuevas tecnologías(pericia – forensia y cibercrimen)” manifiesta la importancia que estén bien solicitados los puntos de pericia atento que el perito deberá estudiar qué, cómo responder y qué herramientas y métodos aplicará en el proceso. Es ineludible conocer punto por punto lo que el Juez requiere atento a dar acabada y precisa respuesta, tanto en cuanto un perito no debe apartarse de lo requerido. Sin embargo es común que uno de los puntos de pericia sea algo tal como *“todo aquello que el perito pueda aportar que arroje luz sobre la causa”*.

La evidencia física y la digital comparten el fundamento respecto a minimizar la contaminación, documentar todo lo actuado, utilizar principios y estándares establecidos y abogar por la admisibilidad de la evidencia. Sin perjuicio que la evidencia digital guarde algunos bemoles característicos al nuevo paradigma que escribe. Tiene la particularidad de poderse repetir, que se encuentren múltiples copias o versiones, para ser más específicos surgen tres variables que deben considerarse imperativamente durante las

actividades de los especialistas la temporalidad, el volumen y la ubicuidad. La temporalidad hace referencia a que los datos almacenados en un dispositivo pueden estar por un tiempo breve o bien durante años, el volumen porque pueden ser bits o millones formando terabites y pueden estar en un lugar o bien en lo que hoy en día llamamos una “nube”. Estos elementos son fundamentales y deben tenerse en cuenta todo el tiempo que hablemos de cómo se efectúan las pericias informáticas atento a que sientan las bases al tratamiento dado al material, pero sin embargo la ubicuidad y el volumen son los que destacan la complejidad del asunto siendo que día a día tanto las computadoras como los celulares crecen en cantidad de datos que pueden almacenar o procesos que pueden realizar al mismo tiempo haciendo el trabajo pericial más difícil y requiriendo mayores recursos.

Hoy en día existen múltiples protocolos y guías de buenas prácticas y actuaciones que marcan el trabajo pericial en la materia atento a la brevedad que nos atestiguaremos la guía del año 2002 de la IETF conocida bajo RFC 3227 siendo la misma una guía para la recolección y archivo de evidencia digital, si bien la misma ha quedado un tanto vetusta comenzó a forjar una línea de trabajo e ideó principios acerca de cómo identificar y preservar prueba digital, como así la categorización al orden de volatilidad de la evidencia, determinación de prioridades para la adquisición y la importancia de la cadena de custodia; la ACPO 2004-2012 estableció claves para el manejo de evidencia, 1) Ninguna acción de las fuerzas de seguridad debe alterar los datos informáticos recolectados; 2) La persona que deba acceder a un dato almacenado en una computadora o medio de almacenamiento debe ser competente para esa tarea en particular; 3) Debe crearse y preservarse un registro de autoría sobre toda la evidencia electrónica a fin de que cualquier profesional independiente y capacitado pueda llegar al mismo resultado; 4) La persona a cargo de la investigación debe tener responsabilidad ante la ley de cumplimentar los principios.

Respecto al segundo principio, es decir que la persona que intenta acceder a la información esté capacitada para realizar dicha acción, trae a corolario la regla ISO/IEC 27037:2012 describiendo la misma lineamientos de trabajos para la identificación, recolección, adquisición y preservación de evidencia. Particularmente la norma clasifica los roles de dos tipos de peritos

el DEFR (siglas para Digital Evidence First Responder –primer responsable de evidencia digital-) y el DES (siglas para Digital Evidence Specialist –especialista en evidencia digital-). Las personas que se desempeñan como DEFR son quienes llevan a cabo tareas de campo en procedimientos respecto a la identificación y preservación de evidencia digital, entendiendo a estos como peritos con una capacitación más básica, mientras que los DES son quienes están mayormente capacitados y se encargan de las etapas metodológicas de análisis y presentación de la evidencia trabajando principalmente en laboratorio. En Argentina el trabajo clasificado dentro de la actuación del DEFR es llevada adelante principalmente por personal policial, sin perjuicio de que mayoritariamente el mismo no tenga una capacitación adecuada, mientras que el perfil de DES está conocido estrictamente como perito informático.

En el país cabe destacar el trabajo realizado por Leopoldo S. Gómez en el poder judicial de la Provincia de Neuquén, donde en el 2006 se publicó una guía operativa para el secuestro de tecnología informática utilizado exitosamente por personal policial de dicha provincia, como así el protocolo de actuación para pericias informáticas en el año 2012, la cual tiene carácter obligatorio para operadores judiciales en el poder judicial de la provincia de Neuquén. La guía contiene tanto un apartado con una guía operativa para el secuestro de tecnología informática, enumera principios rectores, guía buenas prácticas y normas que regulan la actividad.

Si bien el protocolo y la guía son de fácil acceso y lectura cabe destacar –o resumir- ciertos aspectos de las mismas. El procedimiento lleva dos etapas a) la incautación de la prueba y mantenimiento de la cadena de custodia. B) análisis de la información disponible y redacción del informe. Como indicáramos anteriormente, la primera etapa de recolección debe ser llevada a cabo por personal policial junto al Fiscal de la causa. La segunda etapa debe ser llevada adelante por un perito informático en un laboratorio siguiendo los estándares de la ciencia forense. Es de suma importancia la utilización de precintos de seguridad desde el momento del secuestro del material, debe elegirse el secuestro de material a otra alternativa a fin de preservar el material digital, se debe comprender que existen características únicas del material original que no se comprobaran de copias.

Si bien no es una pericia informática sí es prueba informática el pedido de informe a servidores, los servidores de internet son los prestadores del servicio por el cual un usuario se conecta a la red mundial. Esta conexión se establece mediante una dirección de "IP" compuesta por cuatro números de tres caracteres cada uno, por el cual un dispositivo se conecta a dicho servidor, es un protocolo de transmisión con la tarea elemental de establecer la comunicación entre dos puntos remotos, mediante esta identificación los servidores pueden informar la navegación o transmisión de datos de un usuario.

Cabe recalcar la importancia y la asiduidad con la que se realizan hoy en día pericias informáticas sobre tecnologías móviles, entendiendo tanto teléfonos celulares, tabletas y dispositivos similares, alcanzando en la actualidad el 60% de las pericias que se realizan y requiriendo de componentes de software y hardware particulares para el desarrollo pericial. A nivel internacional se han redactado múltiples trabajo respecto a la importancia actual del trabajo y particular manejo con la evidencia digital y los dispositivos móviles, como ya dijéramos el trabajo debe realizarse siguiendo un método y lineamientos procedimentales a fin de no peligrar la integridad de la evidencia recolectada, todos ellos recalcando la importancia de a la hora de manipular el dispositivo móvil "aislar" el mismo de todo tipo de conexión. Hoy en día los celulares tienen múltiples maneras de conectarse sea por la red telefónica, radio, bluetooth, infrarojo, NFC o Wifi, por esto es que el aislamiento de todas estas vías de comunicación son necesarias previas a la examinación previniendo que más datos sean escritos dentro del dispositivo o bien la destrucción de datos de manera remota. Como bien podemos observar la actuación tanto en computadoras como dispositivos móviles requiere hoy en día de la incautación de las unidades a fin de trabajar en laboratorio con los mismos, pero en los teléfonos celulares cabe recalcar la importancia de mantenerlo aislado y en la práctica el apagado es la solución más sencilla más allá de las dificultades a la hora de encenderlo.

Más allá de las técnicas periciales más adecuadas y de los protocolos realizados, hay una realidad que debemos enfrentar que al realizar las pericias informáticas hasta aquí nos hemos referido principalmente al "debe

ser” ya que los equipos requeridos –hardwares- o los programas informáticos necesarios –softwares- para realizar pericias como se realizan en países pioneros en la materia de recolección de evidencia digital no se consiguen en el país principalmente por entidades públicas. Sea por la policía judicial, por gendarmería nacional o por el poder judicial mismo no se tiene el presupuesto –o bien no se destina- para conseguir equipos avanzados que puedan realizar el trabajo en el mejor de los ámbitos. Por ejemplo en la provincia de Buenos Aires cada departamento judicial tiene su delegación de informática la cual asiduamente le llegan requerimientos de pericias informáticas debido a que no dan abasto los peritos de la policía judicial de la provincia, dichos requerimientos de pericias a su vez son comunicados por las delegaciones a la Subsecretaría de Informática de la Suprema Corte de Justicia quien indica a la delegación si puede llevar adelante la pericia, si requiere de colaboración de una delegación cercana o bien si ella asume la misma. Si bien la mayor parte de las pericias en materia penal son realizadas por la fuerza policial la Subsecretaria del más alto tribunal de la provincia realiza un gran número de ellas anualmente y los materiales al alcance no son los recomendados por los protocolos internacionales, de hecho la subsecretaría ha solicitado los últimos tres años hardware específico para la realización de pericias y no han podido adquirir el mismo. Conforme hemos esbozado sin el hardware específico los peritos no pueden realizar lo que hemos enunciado como “imágenes periciales” o bien con hardware que impida la escritura al manipular los dispositivos los peritos pueden dejar rastros de haber realizado la pericia haciendo el trabajo mucho más dificultoso.

Conclusiones.

Las dificultades a las que se enfrenta la prueba digital en la actualidad son las grandes falencias que existen en la cadena de custodia de la evidencia recolectada. La misma está pensada en mantener un registro de toda operación que se realiza y lamentablemente son múltiples los casos en que por una mala manipulación de la evidencia digital o actos no informados se modifica la información original o es alterada y pierde su valor probatorio. Como múltiples guías de recolección de evidencia digital indican, y hemos

expuesto, la sustracción de material informático es la manera más simple y efectiva para recolectar la prueba digital pero esta cumplirá sus fines sólo cuando es llevada a cabo por personal idóneo, en la práctica se encuentran situaciones de recolección de evidencia altamente volátil -como la que se encuentra en una memoria RAM-y al momento de generar una clonación o una imagen forense aún persiste el riesgo de generar una nueva pericia sobre el mismo material.

Si bien el secuestro de dispositivos electrónicos es una de las medidas más comunes a la hora de recolectar evidencia digital las pericias informáticas se realizan cada vez de mayores maneras, desde pedidos de informes a servidores –los cuales atento a la cantidad de pedidos de informes sólo responden los de mayor gravedad- a peritajes sobre dispositivos de geo locación, peritajes de imágenes digitales o bien informar en actuaciones de control disciplinario respecto al uso de una computadora de un funcionario, si usó o no la misma mientras debía estar haciéndolo o si ingresó en sitios web no homologados por la Corte en la que se desempeña.

Actualmente en el país encontramos peritos profesionales que se desarrollan como el típico “perito de lista” que puede ser desinsaculado para realizar una pericia y cobra sus honorarios a la vez que también hay profesionales informáticos con títulos de universidades nacionales que desarrollan su trabajo en entidades públicas que no reciben un pago por bloqueo de título. Así mismo encontramos en todos ellos un mismo reclamo “mayor precisión en los puntos de pericia”, tanto peritos de lista como los que se desempeñan dentro del poder judicial –como textos publicados- refieren que un problema mayúsculo a la hora de realizar las pericias es la poca claridad con la que están redactados los oficios y solicitan qué peritar, como así no comprenden de qué manera funciona básicamente la informática demostrando que es cuasi urgente la necesidad de mayor capacitación por parte de los agentes judiciales en materia informática.

En la región del continente el país que más se ha desarrollado últimamente en materia de la prueba informática es Brasil quien mediante su Corte Federal ha compuesto un cuerpo de peritos informáticos, los cuales requieren ser egresados de una universidad pública y ganan un aproximado de once mil reales –para un ingresante- al mes haciendo muy tentador la

oferta para los jóvenes profesionales, empero han puesto un estándar alto de calidad con exámenes rigurosos para el ingreso. Desde este humilde escaño vemos necesario seguir los pasos del país vecino, buscar un mayor aporte presupuestario por parte de los organismos públicos para la profesionalización y capacitación de agentes dedicados a la realización de tareas comunes a la materia como así un esfuerzo por parte de los agentes judiciales como profesionales en general de comprender el funcionamiento y capacidades de la informática.

Referencias

- Eoghan Casey - "Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet" 2011.
- Maier, Julio B. J. "Derecho Procesal Penal" Tomo III, Parte General Actos Procesales", Ed. AdHoc 2015, Argentina.
- Palacios Lino – La prueba en el proceso penal. Abeledo Perrot, Argentina.
- Cafferata Nores y otros – Manual de Derecho Procesal Penal, Ed. Ciencia, Derecho y Sociedad, Córdoba, Argentina.
- Claría Olmedo Jorge – Derecho Procesal Penal Tomo II. Rubinzal – Culzoni Editores, Buenos Aires, Argentina.
- ACPO (2004). Good Practice Guide for Computer-Based Electronic Evidence. Association of Chief Police Officers.
- Gómez, L. (2006). Guía Operativa para Procedimientos Judiciales con Secuestro de Tecnología Informática. Revista de Derecho Informático, ISSN 1681-5726
- Gómez, L. (2012). Protocolo de Actuación para Pericias Informáticas (2012), aprobado por Acuerdo N° 4908, protocolizado y publicado en el Boletín Oficial de la Provincia del Neuquén, Argentina.
- ISO (2012). ISO/IEC 27037:2012., International Organization for Standardization, Geneva.
- Piccirilli Darío A. "Protocolos a aplicar en la forensia informática en el marco de las nuevas tecnologías" UNLP, La Plata 2015. Disponible a través de <http://sedici.unlp.edu.ar/handle/10915/52212> Último ingreso el 30/04/2019
- Lessig Lawrence, El Código 2.0, Cambridge, Basic Books, 2006.

- Brothers, S. (2009). How Cell Phone "Forensic" Tools Actually Work - Proposed Leveling System. Mobile Forensics World 2009. Chicago, Illinois. Disponible através de <https://tools.ietf.org/html/rfc3227>