

Inconvenientes en la obtención, preservación y presentación de la prueba electrónica

Sergio Appendino¹, Beatriz Parra de Gallo¹, Fredi René Aprile¹

Resumen

Las tareas relacionadas con la obtención, preservación y presentación de la prueba digital en una causa judicial parecen no ser tan simples. El artículo que se presenta a continuación refleja los inconvenientes desde su definición, mención en la legislación vigente, tratamiento en el proceso judicial y su implicancia en el campo pericial informático.

Palabras clave: pericia informática - prueba digital - legislación - proceso pericial - prueba electrónica

Introducción

El presente ensayo se basa en el trabajo sobre «Medios de Prueba Electrónicos: Estado de Avance en la Legislación Argentina» (Rivolta, 2007). Se tomó este trabajo como marco referencial para analizar la prueba electrónica, desde el punto de vista del Derecho y realizar aportes desde el punto de vista de la actividad pericial informática. Si bien muchos de los aspectos técnicos involucrados en las descripciones que siguen caen en el ámbito de otras disciplinas técnicas (telecomunicaciones y electrónica entre otras), se obvian estas diferencias para intentar hacer de este análisis un documento claro para el lector lego en esa materia.

Estado de la legislación procesal en materia de evidencia digital

Sin entrar en el detalle de la descripción geográfica expuesta por la Dra. Rivolta, vale recuperar los siguientes párrafos:

- La Argentina no dispone de normas específicas en materia de procedimiento judicial digital.
- Se admite para algunas medidas probatorias el uso de medios electrónicos (reconocimiento de voz, de imágenes, testimonial filmada)
- En algunas provincias¹ la totalidad de los juicios se instrumentan en formato digital, así

¹ Facultad de Ingeniería e Informática, UCaSal.

¹ Si bien la autora señala la Ciudad de Buenos Aires, Chubut y Río Negro, también la provincia de Salta utiliza este sistema para las notificaciones a las comisarías y existe un proyecto para extender la certificación a los abogados del fuero laboral.

como la comunicación del expediente electrónico y las notificaciones con firma digital.

- Está bastante generalizada la opinión de considerar equiparables los documentos electrónicos con la prueba documental que dichos Códigos admiten.
- Sin embargo, la duda surge en relación con la presentación de los medios probatorios en formato digital. Al no existir normas específicas, sumado al hecho de que los procedimientos se tramitan en soporte papel, en expedientes tradicionales, el método que se aplique para la presentación de la prueba electrónica será crucial a la hora de analizar su valor probatorio. Aunque la evidencia digital sea admitida como tal, el Juez tiene toda la libertad de analizar y decidir sobre su validez como medio de prueba.

He aquí uno de los primeros problemas que debe sortear el perito al momento de presentar la prueba electrónica: ¿Qué se presenta? ¿El propio objeto o su representación en un modo visual para el juez? ¿No sería como presentar «una foto del arma homicida» en vez del arma homicida? Por ello es sumamente importante presentar ambas cosas: el elemento electrónico (en soporte digital) y su representación en papel, ya que la sola presentación de un impreso no es suficiente para «certificar» que tal prueba existe.

Concepto de evidencia digital: como objeto y como representación

Con toda claridad la autora establece el concepto de «evidencia digital como objeto», resultante de delinquir mediante el uso de las TIC's², y el de «evidencia digital como representación» cuando se trata de elementos que ayudan a probar otros hechos delictivos externos a la evidencia digital.

De nuestra experiencia como Peritos Informáticos de la Corte de Justicia de la Provincia de Salta, las más de las veces nos ha tocado «certificar» una evidencia digital, es decir, verificar la validez de un documento electrónico (mail, planilla de cálculo, fotografías, llamadas telefónicas de/a celulares, mensajes de texto, etc.), en otras ocasiones participamos en pericias relacionadas con delitos informáticos que son fácilmente reconocibles (pornografía infantil por citar un ejemplo); pero en menor medida se nos ha convocado en pericias de delitos no tan reconocibles, como ser el «acceso indebido a datos»³ o «alteración del normal funcionamiento de un sistema informático o transmisión de datos»⁴. Consideramos que esta ausencia de tipificación, por parte de los profesionales del derecho en su parte actora o demandada, conforma lo que se puede denominar como «ausencia del Derecho Informático». Muchos delitos meramente informáticos son tratados por analogía como parte de los delitos civiles y penales. El Dr. Nicolás Tato en su

² TIC's: Tecnologías de la Información y las Comunicaciones. Algunos autores hablan ya de las NTIC's, las Nuevas TIC's para sumar la telefonía celular y *cloud computing* (es un nuevo modelo de prestación de servicios de negocio y tecnología, que permite al usuario acceder a un catálogo de servicios estandarizados y responder a las necesidades de su negocio, de forma flexible y adaptativa, en caso de demandas no previsibles o de picos de trabajo, pagando únicamente por el consumo efectuado).

³ Art. 5 de la Ley 26.388 de Delitos Informáticos

⁴ Art. 9 de la Ley 26.388 de Delitos Informáticos

página web⁵ describe esta problemática explicando la dificultad del derecho penal o civil para manejar adecuadamente estos delitos con sus categorías estáticas o analogía limitada.

Medios de prueba electrónica. Proceso civil. Proceso penal

Para analizar este apartado se toman como base los códigos procesales vigentes en la provincia de Salta.

Proceso civil

El Código Procesal Civil y Comercial de la Provincia de Salta⁶ fija en su Sección 6 todas las disposiciones respecto de «Prueba de Peritos» en 20 artículos que regulan la actividad pericial. De allí se pueden destacar como de interés para el actual análisis los siguientes artículos:

Artículo 473º: Planos. Exámenes científicos y reconstrucción de los hechos. De oficio o a pedido de parte, el secretario podrá ordenar:

- 1) Ejecución de planos, relevamientos, reproducciones fotográficas, cinematográficas o de otra especie de objetos, documentos o lugares, con empleo de medio o instrumentos mecánicos;
- 2) Exámenes científicos necesarios para el mejor esclarecimiento de los hechos controvertidos;
- 3) Reconstrucción de hechos, para comprobar si se han producido o pudieron realizarse de una manera determinada.

A estos efectos podrá disponer que comparez-

can los peritos y testigos.

Artículo 474º: Forma de presentación del dictamen. El dictamen se presentará por escrito con copias para las partes. Contendrá la explicación detallada de las operaciones técnicas y de los principios científicos en que los peritos funden su opinión.

Los que concordaren, los presentarán en un único texto firmado por todos. Los disidentes lo harán por separado, salvo que por circunstancias especiales ello no fuere posible.

Se coincide con la Dra. Rivolta respecto de que:

La Argentina no dispone aún de Guías o Manuales de Admisibilidad de Evidencia Digital o Manejo de la prueba, dejándose en cada caso librado al criterio de los peritos, de las partes o del juez, el procedimiento a seguir para asegurar que la obtención de la prueba respete los requisitos mínimos de seguridad, autenticidad, integridad y confidencialidad.

Aunque esto, en la práctica, no impide que la actividad pericial informática se desarrolle en el marco de metodologías y estándares técnicos que le otorgan rigor científico a la actividad pericial. Tal como la aplicación de las Normas ISO 27000⁷ sobre Seguridad Informática, las Normas de Auditoría Informática⁸ o normas internacionales de forensia tales como: RFC 3227 (Guidelines for Evidence Collection

⁵ Tato N., El derecho informático como una nueva rama del derecho, www.nicolastato.com.ar [22/06/2011].

⁶ Aprobado por Ley 5.233, de 1978. El texto completo puede leerse en: <http://www.camdipsalta.gov.ar/LEYES/leyes7379/5233Codigo%20Procesal%20Civil.htm> [07/06/2011].

⁷ <http://www.iso27000.es/> página veinte al 17/06/2011.

⁸ <http://auditoriasistemas.com/auditoria-de-sistemas-informaticos/> [07/06/2011].

and Archiving)⁹, IOCE¹⁰ (Guía para las mejores prácticas en el examen forense de tecnología digital), o CP4DF (Códigos de prácticas para digital forensics)¹¹.

Debe destacarse también la disposición sobre valor de la prueba pericial, que deja a criterio del juez la admisibilidad de la misma:

Artículo 476º: Fuerza probatoria del dictamen pericial. La fuerza probatoria del dictamen pericial será estimada por el juez teniendo en consideración la competencia de los peritos, la uniformidad o disconformidad de sus opiniones, los principios científicos en que se funden, la concordancia de su aplicación con las reglas de la sana crítica y demás pruebas y elementos de convicción que la causa ofrezca.

Procesos penales

El Código Procesal Penal¹² vigente en Salta, incluye en el Capítulo V, denominado «Peritos», todas las disposiciones que regulan la actividad pericial en 17 artículos, de los que vale mencionar el siguiente:

Art. 252. El dictamen pericial podrá expedirse por informe escrito o hacerse constar en acta, y comprenderá en cuanto fuere posible:

1. La descripción de las personas, lugares, cosas o hechos examinados, en las condiciones que hubieren sido hallados.
2. Una relación detallada de todas las operaciones practicadas y sus resultados.
3. Las conclusiones que formulen los peritos,

conforme a los principios de su ciencia, arte o técnica.

4. Lugar y fecha en que se practicaron las operaciones.

El juez valorará la pericia de acuerdo con las reglas de la sana crítica.

Si bien enuncia un contenido general para el informe pericial, tampoco se hace mención acerca de las reglas o guías para realización de la pericia. En el párrafo último se deja a consideración del juez la admisibilidad de la prueba.

Valor legal del documento electrónico

A lo dispuesto por la Ley 25506 de Firma Digital, la Dra. Rivolta le suma una interesante discusión sobre la participación de los escribanos en la certificación de la prueba (tanto impresa como electrónica), así como la diferencia entre «firma electrónica» y «firma digital».

Para la legislación argentina los términos «firma digital» y «firma electrónica» no poseen el mismo significado. La diferencia radica en el valor probatorio atribuido a cada uno de ellos, dado que en el caso de la «firma digital» existe una presunción *iuris tantum* en su favor; esto significa que si un documento firmado digitalmente es verificado correctamente, se presume salvo prueba en contrario que proviene del suscriptor del certificado asociado y que no fue modificado. Por el contrario, en el caso de la firma electrónica, en caso de ser desco-

⁹ <http://www.faq.s.org/rfcs/rfc3227.html> [07/06/2011].

¹⁰ http://www.ioce.org/fileadmin/user_upload/2002/Guidelines%20for%20Best%20Practices%20in%20Examination%20of%20Digital%20Evid.pdf [07/06/2011].

¹¹ http://www.cftt.nist.gov/Methodology_Overview.htm [07/06/2011].

¹² Promulgado en 1985, puede encontrarse en <http://www.mpfsalta.gov.ar/Files/FileManager/C%C3%B3digo%20Procesal%20Penal%20de%20Salta%20.pdf> [07/06/2011].

nocida la firma por su titular corresponde a quien la invoca acreditar su validez.

Y aunque se reconoce plena validez a la firma digital y a la firma electrónica, se destaca en este apartado el vacío jurídico respecto de la «... conservación del documento, ni de la metodología para la obtención de la prueba, ni del procedimiento para su presentación en el expediente judicial que por ahora tramita en soporte papel...»

Permítasenos profundizar este punto: «conservación del documento». Cuando la prueba digital se encuentra en una computadora personal—más precisamente en el disco rígido— o en otros dispositivos de almacenamiento como DVD, CD, pen drive; para conservar la prueba sólo es suficiente retener el dispositivo en el juzgado. Pero cuando la prueba se encuentra en Internet (correos electrónicos vía web mail, páginas web, bases de datos web, etc.) no es tan sencillo conservarla debido a que el trámite de acceso y/o secuestro del servidor en donde se encuentra tal información se ve entorpecido por la ubicación física y geográfica de estos equipos; a esto se suma la falta de regulación de Internet, en donde no todos los servidores tienen una identificación de propiedad legalmente aceptada y autorizada.

Admisibilidad de la evidencia digital

La Dra. Rivolta plantea los casos de admisibilidad de otro tipo de prueba digital, i.e., pruebas digitales de voz y videos. Y si bien existe preocupación por la inalterabilidad de la prueba y las condiciones de seguridad y fiabilidad con que se obtienen, no se hace ninguna mención respecto de cómo debe presentarse tal prueba. Y aquí nos ocupamos de otra cuestión de sumo interés práctico: la presentación de la prueba digital, que se podría tipificar según como se presenta:

- Cuando la prueba digital original no se puede presentar directamente (correo electrónico de una cuenta dominio Hotmail por ejemplo), se presenta una «copia» de la misma con el agregado de todos los atributos técnicos que certifiquen la existencia del original cuya copia se presenta (los encabezados del correo electrónico que marcan las IPs de recorrido por ejemplo). En estos casos se suele presentar un CD/DVD con la copia de la prueba digital y un impreso del mismo.
- Respecto de la «certificación de la copia de una prueba digital», hay opiniones encontradas acerca de si se requiere de la certificación de un escribano o es suficiente con el rigor metodológico utilizado y la solvencia técnica del perito para certificar la copia. En casos de «prueba anticipada» se entiende que los actuantes (oficial de justicia y perito) certifica *per se* la copia que se obtenga de una prueba electrónica.
- Cuando la prueba digital no es legible directamente desde la copia digital porque se requieren programas especializados. Se debe presentar el documento digital más el software necesario para su visualización y se advierte al Juez que tales elementos se requieren para poder ver la prueba digital. En estos casos no se acompaña un impreso de la prueba digital. Y aquí se agrega un componente «extra» cuando se requiere un software propietario, ya que esto implicaría que el juzgado (o los abogados o quienes quieran acceder a la prueba digital) deban pagar para adquirir el software correspondiente. Idénticas consideraciones pueden hacerse cuando se requiere un «hardware» específico para acceder a la prueba digital (celulares, ipod, etc.).
- Cuando la magnitud de la prueba digital hace impráctica la presentación impresa (un archivo con 1200 registros por ejemplo), usualmente se entrega la prueba digital con una impresión de muestra.

- Cuando la prueba digital está en un dispositivo secuestrado, se extrae una copia para su manipulación o procesamiento, que es entregada en soporte digital y en forma impresa si el Juez lo amerita.

Hasta aquí algunos ejemplos sobre la presentación de la prueba.

Peritos informáticos

Respecto de este tema el documento concluye que:

Respecto de los expertos informáticos, dado que el tema no está expresamente regulado en las normas de procedimiento, no existen criterios, políticas ni manuales para la obtención, producción, conservación y presentación de pruebas electrónicas. Tampoco reglas y obligaciones específicas para dichos peritos. Se aplican las generales de la ley respecto de estos colaboradores de la Justicia.

Y aquí encontramos el meollo del asunto. Para las pericias informáticas se aplican las generales de la ley, que tratan siempre de «pruebas materiales», mientras que la prueba digital es «intangible». Esta intangibilidad hace que la prueba digital sea difícil de admitir (por su volatilidad, alterabilidad, duplicidad, etc.) y que además se requiera extremar los recaudos en el proceso de obtención, preservación y presentación de la prueba.

Conclusiones

El documento sobre «Medios de prueba electrónicos: Estado de avance en la legislación argentina» resultó de sumo interés para conocer el marco legal de la prueba electrónica en nuestro país y se ha intentado aportar la visión del experto informático.

Si bien quedan muchas cosas por profundizar, permítasenos elaborar algunas conclusiones con lo dicho hasta aquí:

-Es imperioso que los informáticos generemos guías o manuales de trabajo para la obtención, preservación y presentación de la prueba digital. Quién más que nosotros podremos decir cuáles son los criterios o estándares que le darán rigor científico a la tarea. Pero eso sería solo el principio de un extenso camino para llegar a definir una metodología *legalmente aceptada* para el tratamiento de la prueba electrónica. La intención final debería ser que las normas propuestas sean aceptadas por la comunidad científica, por los propios actores informáticos y por el ámbito judicial.

-Es indiscutible que la tecnología no se puede separar del acto delictivo, siendo cada vez más fuerte la dependencia tecnológica que cada día avanza más y más hacia las redes convergentes (datos, voz y video montada sobre *cloud computing*), migrando de la «pc hogareña» al «espacio en la red».

-Se debe reconocer que la «prueba digital» no puede ser íntegramente tratada por un profesional informático, en muchas oportunidades se requiere de otros profesionales técnicos para su interpretación y manipulación adecuadas, tales como expertos en telefonía celular, en telecomunicaciones, en video filmaciones, entre otros.

Referencias bibliográficas

Parra de Gallo, Herminia Beatriz. «La prueba electrónica: inconvenientes sobre la obtención, preservación y presentación, un enfoque desde el perito informático». Trabajo presentado en el curso «Informática Forense: Problemática Jurídica de la Prueba Electrónica», mayo 2011.

Rivolta, Mercedes. Medios de prueba electrónicos: Estado de avance en la legislación argentina. VI Congreso Argentino de la

- Administración Pública, 2007.
- Ley 26.388 de Delitos Informáticos, <http://www.infoleg.gov.ar/infolegInternet/anejos/140000-144999/141790/norma.htm> [07-06-2011].
- Código Procesal Civil y Comercial de la Provincia de Salta, <http://www.camdipsalta.gov.ar/LEYES/leyes7379/5233Codigo%20Procesal%20Civil.htm> [07-06-2011].
- Normas ISO 27000 sobre Seguridad Informática, <http://www.iso27000.es/> [06-06-2011].
- Normas de Auditoría Informática, <http://auditoriasistemas.com/auditoria-de-sistemas-informaticos/> [06-06-2011].
- Código Procesal Penal de la Provincia de Salta, <http://www.mpfsalta.gov.ar/Files/FileManager/C%C3%B3digo%20Procesal%20Penal%20de%20Salta%20.pdf> [06-06-2011].
- Tato, N. El derecho informático como una nueva rama del derecho. www.nicolastato.com.ar [22-06-2011].
- RFC 3227 Guidelines for Evidence Collection and Archiving, <http://www.faqs.org/rfcs/rfc3227.html> [22-06-2011].
- IOCE Guía para las mejores prácticas en el examen forense de tecnología digital, http://www.ioce.org/fileadmin/user_upload/2002/Guidelines%20for%20Best%20Practices%20in%20Examination%20of%20Digital%20Evid.pdf, [22-06-2011].
- CP4DF Códigos de prácticas para digital forensics, http://www.cftt.nist.gov/Methodology_Overview.htm, [22-06-2011].