

**SUPLEMENTO
ESPECIAL**

DERECHO PROCESAL ELECTRÓNICO

**Aspectos esenciales de los cambios
introducidos por la tecnología
en el proceso judicial**

AÑO 2018

**Nuevas tecnologías en el proceso civil y comercial |
Garantías constitucionales en el proceso digital | Prueba informática |
Firma digital y redargución de falsedad | Valor probatorio del correo electrónico |
Carga de la prueba | Las TIC y el proceso de familia |
Legalización de partidas con firma digital | Cadena de custodia |
Prueba electrónica en el proceso penal**

PRUEBA ELECTRÓNICA EN EL PROCESO PENAL

UN CASO TESTIGO: FRUTO DE EVIDENCIA DIGITAL ENVENENADA

Federico A. Borzi Cirilli*

I - NUEVOS DESAFÍOS

El presente trabajo tendrá por objetivo analizar la prueba digital en el marco del proceso penal y, particularmente, abordar la teoría del fruto del árbol venenoso con referencia a estos especiales elementos probatorios. En esta iniciativa veremos cómo se inscriben las evidencias digitales dentro de los tradicionales medios de prueba que suelen establecer los Códigos de Procedimiento en Materia Penal, aunque también analizaremos cómo pueden verse vulneradas determinadas garantías constitucionales a través de ellas.

No cabe duda de que a esta altura del desarrollo tecnológico la prueba electrónica impone una serie de retos al operador jurídico, sin importar de qué lado del mostrador se encuentre, a saber: cómo recogerlas, cómo custodiarlas debidamente, cómo llevar a cabo su incorporación al proceso penal, cómo sostener su validez probatoria; y, llegado el caso, cómo controvertirlas cuando puedan perjudicar los intereses del cliente. Como ya advertimos, el proceso de seguimiento de la prueba electrónica puede -y suele- tener directa incidencia en la protección de las garantías constitucionales de las partes en el

(*) Abogado (UBA). Especialista en Derecho Penal (UBA/CASI). En ejercicio independiente de la profesión en el Fuero Penal Ordinario Nacional, Provincial y Federal. Autor de numerosas publicaciones en temas de Derecho Penal y Procesal Penal

proceso; en consecuencia, todos los operadores jurídicos debemos velar por que no sean fuente de afectación so pretexto de constituir novedades tecnológicas. Precisamente allí es donde podrá entrar en juego la regla de exclusión probatoria y su consecuente doctrina del fruto del árbol venenoso. A modo de ejemplo, podemos citar el caso de España, donde, mediante una reforma de octubre del año 2015, se abordó justamente esta problemática en pos del fortalecimiento de las garantías procesales y la debida regulación de las medidas de investigación tecnológica.

Su premisa básica radica en la necesidad de autorización judicial y en la consagración de los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de cada medida. Esto, como veremos en el punto siguiente, tiene que ver con medios de prueba tales como interceptaciones de comunicaciones telefónicas y telemáticas, captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, utilización de dispositivos técnicos de seguimiento, localización y captación de imagen, registro de dispositivos de almacenamiento masivo de información o registros remotos sobre equipos informáticos.

II - PRUEBA ELECTRÓNICA Y MEDIOS DE PRUEBA EN EL PROCESO PENAL

Como es natural, este tipo de evidencias tienen una inevitable conexión con las nuevas tecnologías de información y comunicación (TIC). Así, se las ha caracterizado, con apoyo en el diccionario de la Real Academia Española, como aquellas compuestas por dos elementos: uno material, que depende de un *hardware*, la parte física y visible de la prueba para cualquier usuario de a pie, por ejemplo, la carcasa de un *smartphone* o una memoria USB; y, por otro lado, un elemento intangible, que es representado por un *software*, consistente en los metadatos y archivos electrónicos modulados a través de unas interfaces informáticas.

También hemos tenido oportunidad de definir a la evidencia digital en otro trabajo⁽¹⁾ como *"Toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión ... el documento electrónico en sentido amplio es el ... gestado con intervención de una computadora a través de sus propios órganos de salida (monitor, impresora, etc.), cuya característica es que son perceptibles y con textos alfanuméricos legibles directamente por el hombre sin necesidad de intervenciones por parte de máquinas traductoras, mientras que, en sentido estricto, es el documento elaborado por el propio hardware, conforme al sistema utilizado y programa establecido, que desde su creación hasta su archivo permanece sin haber salido del contexto de su origen..."*.

Definido el elemento, y previo adentrarme en su inclusión dentro de los denominados medios de prueba penal, debemos aclarar que desde el ámbito legislativo hasta el momento no se ha producido en nuestro país una normativa que establezca un procedimiento especial para recoger, conservar y en última instancia valorar la prueba

(1) Borzi Cirilli, Federico A.: "Ciberdelitos y evidencia digital: problemática probatoria. Los nuevos tipos penales en la era de internet" - ERREIUS - Sup. Esp.: "Ciberdelitos y delitos informáticos" - agosto/2018 - Cita digital IUSDC285986A

electrónica. Existen posturas que entienden que no sería necesaria una regulación tal, sosteniendo que la única diferencia con la prueba tradicional radica en el diferente soporte. Pese a ello, debemos destacar que estas evidencias digitales provenientes de tecnologías en constante evolución -por tanto, de carácter efímero- poseen características muy particulares y muchas veces resultan manipulables, aun en mayor medida que las pruebas tradicionales. Esta circunstancia me persuade en relación con afirmar, contrariamente a lo sostenido, que sí resultaría necesaria una regulación específica de ellas con la finalidad de propender a una utilización más uniforme y previsible -por lo tanto, dotada de mayor grado de seguridad jurídica- de este tipo de pruebas.

Sin perjuicio de lo dicho, hasta tanto se promueva una regulación especial, resultan de aplicación las normas referidas a los llamados medios probatorios análogos, ello además de las reglas procesales referidas a los medios audiovisuales cuando estos sean electrónicos, es decir, medios de prueba que permitan la reproducción ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación y otros semejantes.

En este sentido, y todo enmarcado en el principio de libertad probatoria -que a continuación abordaremos-, rigen los siguientes artículos: 216 (inspección judicial y reconstrucción del hecho); 224 (registro domiciliario y requisita personal); 231 (secuestro); 239 (testigos); 253 (peritos); 268 (intérpretes); 270 (reconocimientos); 276 (careos), todos del Código Procesal Penal de la Nación. Similar resulta la situación en el ámbito de la Provincia de Buenos Aires, donde rigen, en lo pertinente, los artículos 212 (inspección y reconstrucción del hecho); 219 (registro domiciliario y requisita personal); 226 (secuestro); 232 (testigos); 244 (peritos); 255 (intérpretes); 257 (reconocimientos); 263 (careos); 265 bis (filmaciones y grabaciones), todos del Código Procesal Penal de la Provincia de Buenos Aires.

Especial atención nos merece este último artículo, introducido a la ley procesal bonaerense en el año 2010 mediante la ley 14172, motivo por el cual lo transcribiremos: *“El fiscal deberá requerir a organismos públicos y/o privados las filmaciones obtenidas mediante sistema de monitoreo, y las grabaciones de llamadas a los teléfonos del sistema de emergencias. La totalidad del material obtenido será entregado al fiscal en su soporte original sin editar, o de no ser posible, en copia equivalente certificada en soporte magnético y/o digital. El fiscal conservará el material asegurando su inalterabilidad, pondrá a disposición de las partes copia certificada, debiendo facilitar las copias que le solicitaren. Las reglas precedentes serán aplicables a las filmaciones obtenidas por particulares mediante sistema de monitoreo en lugares públicos o de acceso público”*.

III - GARANTÍAS CONSTITUCIONALES INVOLUCRADAS

Ya observamos que estas pruebas electrónicas se insertan al proceso penal a través de los medios de prueba tradicionales aplicados analógicamente, siempre dentro del amplio margen que concede el principio de libertad probatoria. Recordemos que este principio, imperante en nuestro proceso penal tras la derogación de las pruebas legales o tasadas, establece que los hechos bajo investigación en el proceso penal podrán acreditarse

por cualquier prueba, siempre y cuando no se vulneren garantías constitucionales mediante su producción. Esto tiene su correlato en el sistema de la sana crítica racional, según el cual el juez, para formar su juicio de convicción acerca de la ocurrencia de un hecho delictivo y su autoría, cuenta con libertad en la elección y valoración de las pruebas, por supuesto siempre respetando los principios de la filosofía, la lógica y la experiencia generales.

El fundamental artículo 18 de la Constitución Nacional resulta proyector de la mayoría de las garantías penales de nuestro ordenamiento, aunque a partir del año 1994 se ha visto complementado por tratados de derechos humanos incorporados a la Constitución; entre los más relevantes: la Convención Americana de Derechos Humanos (CADH) y el Pacto Internacional de Derechos Civiles y Políticos (PIDCP). Puntualmente en lo que tiene que ver con las pruebas electrónicas a producirse, deberá brindarse al acusado la posibilidad de controvertirlas; esto quiere decir que el elemento de convicción que se pretenda utilizar para fundar una condena en su contra deberá haber podido ser controlado y, consecuentemente, habérsele permitido al acusado producir prueba en su contra. Esta circunstancia impone no solo el modo como fue recogida una evidencia digital, sino su debida conservación. En este sentido, el artículo 8.2 de la citada CADH establece: *"Durante el proceso, toda persona tiene derecho, en plena igualdad, a las siguientes garantías mínimas: b) comunicación previa y detallada al inculpado de la acusación formulada; c) concesión al inculpado del tiempo y de los medios adecuados para la preparación de su defensa; f) derecho de la defensa de interrogar a los testigos presentes en el tribunal y de obtener la comparecencia, como testigos o peritos, de otras personas que puedan arrojar luz sobre los hechos..."*.

Otra de las garantías que cobra relevancia en la temática que analizamos es la de inviolabilidad de las comunicaciones privadas y la correspondencia. En este sentido, las formalidades establecidas para la antigua correspondencia postal según el citado artículo 18: *"El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados"*, resultan aplicables a los correos electrónicos, así como a conversaciones de mensajería instantánea. Al respecto, el artículo 17 del PIDCP establece: *"Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques"*.

También deberá establecerse de manera adecuada el sustrato fáctico de acusación, así como su calificación legal, a fin de que pueda respetarse la congruencia procesal necesaria desde la primera fase hasta una eventual condena. Sobre todo cuando tratamos con hechos muchas veces intangibles, como los producidos por vía electrónica, resulta relevante velar por esta garantía, so pena de incurrir en violación al derecho de defensa en juicio del acusado.

Sin ánimo de ser exhaustivo, valen las referencias efectuadas para pasar al punto siguiente y neurálgico del trabajo: ¿qué ocurre cuando las pruebas electrónicas no son seguras o directamente han sido adulteradas?



IV - MANIPULACIÓN DE EVIDENCIA DIGITAL Y DOCTRINA DEL FRUTO DEL ÁRBOL VENENOSO

Llegados a este punto, encontrándonos ya alertados acerca de los nuevos desafíos que plantean las evidencias digitales y habiendo pasado revista a la normativa aplicable, así como a algunas garantías constitucionales que pueden activarse a su respecto, quiero profundizar en determinados casos en los que se plantean inconvenientes en torno a la validez de estas evidencias y cómo puede resolverse el conflicto desde el punto de vista jurídico.

Como explica Araya Vega en su trabajo sobre el tema, la regla de exclusión, o *exclusionary rule*, por su origen norteamericano, establece que no podrá aceptarse como válida para sustentar una posición contraria a la del imputado o acusado la prueba directamente relacionada con elementos de prueba ilícitos. Como consecuencia de esta regla, la doctrina del fruto del árbol venenoso o árbol emponzoñado (*fruit of the poisonous tree doctrine*) establece que cuando el procedimiento inicial es violatorio de garantías constitucionales, esa ilegalidad se va a proyectar a todos los actos que resulten consecuencia de este. Así, se prohíbe valorar todas las pruebas derivadas de la prueba ilícitamente obtenida.

Cabe recordar, sin perjuicio de lo antedicho, que esta doctrina cuenta con tres excepciones: no se aplica cuando existe una vía de investigación independiente que permite obtener las pruebas por un cauce distinto del empleado y considerado ilegal; cuando las circunstancias hubieren llevado al mismo resultado de modo inevitable; o cuando el enlace jurídico entre una prueba y otra no es evidente, es decir, no existe una insoluble conexión fáctica entre ambas pruebas y se debe realizar un juicio de valor para encontrar rastros de dicha conexión. Veamos ahora de qué modo pueden manipularse ciertas pruebas electrónicas.

Pese a la tendencia -aclaro que es solo intuitiva- de que las evidencias digitales son infalibles, no cabe duda -como ya adelantamos- de que, así como sucede con cualquier tipo de prueba, las pruebas electrónicas pueden ser fácilmente manipulables, incluso en mayor medida que las pruebas tradicionales. En este último sentido, no debemos olvidar que la adulteración de elementos de prueba configura delito en los términos del artículo 255 del Código Penal, en cuanto reprime con hasta cuatro años de prisión, y multa para los casos culposos, a todo "el que sustrajere, alterar, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo".

En similar sentido, resulta aplicable, atento a la modificación que se efectuara al artículo 77 del citado cuerpo legal, el tipo penal de falsificación de documentos, en cuanto reprime a "El que hiciere en todo o en parte un documento falso o adultere uno verdadero,

de modo que pueda resultar perjuicio...". Recordemos que mediante la ley 26733 del año 2011 se modificó el Código Penal, estableciendo: "El término 'documento' comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos 'firma' y 'suscripción' comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos 'instrumento privado' y 'certificado' comprenden el documento digital firmado digitalmente".

Eventualmente los autores de dicha adulteración podrán ser sometidos a proceso por esos hechos; ahora bien, veamos en qué pueden consistir esas manipulaciones, con la advertencia de que se deberán tomar los debidos recaudos para establecer si aquellas provienen de actos humanos, y no de actos automáticos de la PC u otros dispositivos similares.

Podemos encontrarnos con casos como la impresión de una imagen, un correo o mensajes enviados por WhatsApp para su posterior aportación al proceso judicial; casos que, en realidad, pueden suponer la omisión de importantes datos de los que puede depender la valoración que finalmente se haga. Cabe observar que, de esa manera, no estaría quedando constancia de la integridad de los medios en que se almacenaba originalmente la información y, en particular, su preservación a los efectos de posteriores comprobaciones e informes. Esto nos introduce en la problemática referente a la transcripción y presentación en papel de las evidencias digitales; es que, si bien legalmente no existen impedimentos al respecto, su uso debe limitarse al de facilitar la lectura y valoración, pero siendo acompañado en todo caso por el documento electrónico correspondiente.

Considero que la intervención de peritos informáticos será cada vez más necesaria para una debida labor probatoria en los que podemos denominar cibercasos. Es que, cuando hablamos de documentos electrónicos, existen herramientas que permiten crear su huella digital o una cadena alfanumérica hexadecimal generada a partir de la aplicación de un algoritmo que identifica de manera inequívoca dicho documento, de manera tal que el menor cambio realizado sobre aquel podría ser rápidamente detectado. Esto además permite realizar duplicados de dichos documentos y probar que se corresponden plenamente con el original.

Como se adelantó, un cambio, como la mera conversión de una imagen a otro formato que ocupe menos espacio o simplemente a uno de los admitidos por el sistema (aunque en la práctica únicamente se compruebe en realidad la extensión), o su reducción, supone una alteración del documento, que entraña dificultades posteriores si no aportamos asimismo el documento electrónico original. Obtenemos en realidad un nuevo documento identificado por un *hash* distinto y que puede haber perdido por el camino multitud de información que nos podría haber resultado útil. Por si no fuera poco, se subestima de manera peligrosa la importancia de aquellos datos no visuales con los que los equipos trabajan, pese a no mostrarlos al usuario.

Esto tiene que ver con los metadatos existentes en otros documentos, como imágenes, también fácilmente modificables en nuestros equipos; ya no se requiere de grandes conocimientos informáticos para realizar esta tarea, al existir aplicaciones de fácil

uso que pueden descargarse. El problema en la práctica es que muchas veces se descubren vulnerabilidades reveladoras de que incluso esta información oculta puede ser modificada de forma sencilla. Los terminales móviles pueden facilitar información de geolocalización falsa a las aplicaciones con las que trabajan, y hay aplicaciones que incluyen la clave privada utilizada para firmar los ficheros como propios dentro de la propia aplicación y accesible para sus usuarios.

Así, al interrogante acerca de si puede acreditarse que un documento electrónico ha sido modificado por la parte que lo aporta debe responderse de modo afirmativo, y dependerá de otras circunstancias a ser analizadas caso por caso, teniendo además en cuenta que lo que se da por válido hoy puede sorprender mañana, descubriéndose que no resultaba tan certero como parecía. Esto no debe llevarnos a una falta de esfuerzo en la aportación de estas pruebas o a la falta de impugnación de las de la parte contraria, porque de ello finalmente dependerá la valoración que realice el juez.⁽²⁾

V - UN CASO TESTIGO, ¿CÓMO FUNCIONA EN LA PRÁCTICA?

Resulta pertinente a esta altura del trabajo recurrir a un pronunciamiento de la Sala Penal del Tribunal Supremo Español (Sección 1ª - Nº 16/2014 - 30/1/2014), ya que, no tengo duda alguna, llamará la atención del lector por lo inesperado de su resultado. Se trata de un caso en el que se condenó a un policía, de apellido Fructuoso, que había solicitado dinero a dos narcos, Nazario y Ruperto, a cambio de su colaboración en los hechos.

Veamos el caso con mayor precisión.

Gonzalo Fructuoso, policía nacional, resultó autor penalmente responsable del delito de cohecho, imponiéndosele cuatro años de prisión y una multa de 45.000 euros e inhabilitación especial para empleo o cargo público por nueve años y seis meses por haberse contactado con Domingo Ruperto e Ildefonso Nazario ("El Sordo" y "Chipiron"), ambos acusados por delitos contra la salud pública, mediante SMS enviados desde su teléfono celular e *e-mails* desde su cuenta de correo electrónico, con la finalidad de ofrecerse como colaborador participe de ellos en una operación de tráfico de estupefacientes que estos proyectaban realizar. Para ello, habría exigido amenazadoramente a Ildefonso Nazario una compensación económica -en el caso se habrían entregado en efectivo 30.000 euros- como contravalor de la información que podía proporcionar acerca del estado de las investigaciones policiales sobre su caso, información de la que disponía por razón de su oficio, lo que desconocían los mencionados receptores de la oferta.

Las pruebas que resultaron determinantes para la condena de Fructuoso, en lo que nos interesa, fueron ocho evidencias electrónicas:

1. Cuarenta y cuatro correos electrónicos intercambiados entre Nazario y Fructuoso.
2. Conexión IP desde la que Fructuoso se conectó a internet para remitir los correos.
3. CD remitido por Microsoft conteniendo correos electrónicos y su transcripción.

(2) Ejemplos extraídos del trabajo de León, Oliva y Valero Barceló (Coords.): "La prueba electrónica. Validez y eficacia procesal" - Juristas con Futuro - E-book - setiembre/2016

4. SMS intercambiados entre Domingo Ruperto y Fructuoso.
5. Informe pericial informático que analiza el contenido del CD remitido por Microsoft.
6. Informe pericial informático que analiza los SMS enviados y recibidos desde determinados teléfonos.
7. Informe de Microsoft sobre los datos contenidos en los correos electrónicos que se habrían enviado Fructuoso, Ruperto y Nazario.
8. Informe de Telefónica sobre conexiones IP del correo atribuido a Fructuoso.

De esa manera, para arribar a la condena, la policía había identificado la dirección IP desde la cual Fructuoso se conectaba para enviar los correos (un cibercafé ubicado en Pontevedra) a través de una cuenta de e-mail de nombre ficticio, denominada "Hugo Fructuoso". Hasta ahí cualquiera podría afirmar que el cuadro probatorio colectado en contra del policía parecía no solo abundante sino sólido y conectado.

Sin embargo, la causa terminó anulándose tras haber entrado en juego la doctrina del fruto del árbol venenoso, en tanto el Supremo Español determinó que fue *"nula e irregular (la) obtención de mandamientos e intervención de correos electrónicos y datos asociados de Telefónica a raíz de las mismas..."*. A continuación transcribiré y clasificaré una serie de párrafos de la sentencia por la potencial utilidad, no solo académica sino práctica, que podrá tener para el lector:

a) No fueron judicialmente autorizadas las intervenciones de correos electrónicos

"El motivo insiste, por ello, en que la solicitud y obtención por la policía de las autorizaciones judiciales de intervención de las cuentas de correo electrónicas y datos asociados a las mismas -que constituyen el único elemento 'corroborador' del contenido de las conversaciones entre Ildelfonso Nazario (Sordo y el Chipiron)- debe apreciarse la falta de regularidad y licitud de las mismas..."

b) El oficio a Microsoft que consta es de la misma fecha de respuesta de esta

"...Si bien la actuación policial hasta el momento de la obtención del IP no puede tacharse de vulneradora del derecho al secreto de las comunicaciones, no le falta razón al recurrente cuando afirma la ilicitud y no regularidad en la obtención de los demás datos relacionados con la cuenta atribuida al 'Chipiron' y sus conexiones desde dicho IP. En efecto la información que en el oficio policial de 30/7/2008, dirigido al Juzgado para que, a su vez, solicite información telefónica sobre los datos relativos a las conexiones IPs -se dice facilitada el día 28/7/2008- por Microsoft identificando el IP de la supuesta cuenta del 'Chipiron', DIRECCION000, como la correspondiente de NUM009 a nombre de un tal Hugo Fructuoso, y que todas las conexiones respecto de dicha cuenta se realizan y producen desde dicha IP, no está documentada en la causa y no resulta posible que Greco Galicia hubiese recibido dicha información vía judicial de las IPs el 28 de julio por cuanto la providencia autorizando tal petición y los mandamientos con tal finalidad dirigidos a Microsoft, son precisamente de esa misma fecha y tales datos no se remitieron por Microsoft sino por oficio y CDE con escrito de 5 agosto".



c) No consta la respuesta de Telefónica

"...En relación a la información que en el mismo oficio de 30/7, se dice remitida por Telefónica, sobre que dicho IP estaría ubicada en su cibercafé llamado Ciberpcr sito en la calle José Casal de Pontevedra y que en alguna ocasión había frecuentado el hoy recurrente, tal información tampoco consta documentada en la causa. Por el contrario la solicitud policial es de fecha 30 julio y la providencia del juez accediendo a la petición de los datos es de 6 agosto (folio 4185), sin que conste respuesta ni información alguna de Telefónica remitida al Juzgado".

d) No hubo control de pruebas de cargo por la defensa

"Pues bien respecto al contenido del CD la sentencia recurrida continúa sin hacer un análisis de la pericial informática, ni referencia a la diligencia de volcado en presencia del secretario judicial del contenido CD cuyo resultado se refleja en aquel informe aportado por la defensa que contradice el texto de los mensajes electrónicos aportados policialmente fuera del control judicial y sin contradicción por las partes y desvirtúa la realidad de su emisión".

e) El listado de correos intercambiados no surge del CD aportado y no se sabe de dónde proviene

"...En efecto el informe pericial realizado por los peritos informáticos Sres. Belarmino Segundo e Ignacio Alexander el 30/8/2010, ratificado en el plenario, explica que en el CD remitido por Microsoft con escrito de 5/8/2008 (folio 4201) los datos que contiene son relativos al registro y numero de conexión IP de las cuentas atribuidas a Sordo y al 'Chipiron', destacando que debe accederse al mismo mediante contraseña 'asdfsdt', que no fue facilitada hasta el 16/2/2010 (folio 6734), sin que en ningún momento en dicho CD se hubieran incluido los mensajes que en las referidas direcciones de correo electrónico se pudieran encontrar salvaguardadas, y analizado el contenido del CD comprueban que no contiene ninguna clase de listado o relación de los posibles mensajes intercambiados, entre ambas direcciones de correos electrónicos, y sin que conste en las actuaciones vía alguna de la posible aportación de fuente oficial del listado de correos obrantes en las actuaciones".

f) Conclusión Judicial

"...Por todo ello los peritos en el plenario concluyeron que el listado de correos aportado en las actuaciones comprensivo de las supuestas comunicaciones intercambiadas entre 'Sordo' y el 'Chipiron' resulta absolutamente inviable e incompatible con las conexiones IPs remitidas por Microsoft, lo que supone, por tanto, que dichos mensajes no se han podido crear ni emitir desde dichas cuentas ni corresponderse tampoco con la IP que se asigna; y por otro lado, que tampoco se constata ni en los autos ni en ninguno de los CDs examinados la información que permita establecer o determinar la correspondencia de la IP atribuida al 'Chipiron' con una línea telefónica correspondiente a la empresa domiciliada en la calle José Casal Nº 8, Pontevedra, que se correspondería con el locutorio del cibercafé" (ponente: Juan R. Berdugo Gómez de la Torre).

VI - CONCLUSIONES

Es probable que este trabajo haya generado inquietud en el lector, y debo admitir que -de haber sido ese el caso- no resulta errado. Es que las pruebas electrónicas, máxime en el proceso penal, en el que más fuertemente se despliegan las garantías constitucionales, poseen menos certezas que las que quizás alguna vez creímos. Digna prueba de ello resulta el pronunciamiento del Supremo Español, que a simple vista parecía contar con un considerable cúmulo de evidencias para confirmar la condena impuesta al policía; sin embargo, como se observó, esas ocho pruebas electrónicas que lucían indestructibles se resquebrajaron al punto de coadyuvar a la absolución del acusado. En ese juego de interrelación entre las pruebas electrónicas, las garantías constitucionales, la regla de exclusión probatoria y la doctrina del fruto del árbol venenoso, esta vez primaron las últimas.

Esto no debe hacer más que alentarnos a una continua capacitación en derecho procesal electrónico a fin de que, en caso de que nos encontremos a cargo de la acusación de un ciberdelito, podamos sostenerla y lograr una condena en base a las evidencias digitales colectadas; y para el caso de que nos encontremos en la vereda de enfrente, podamos controvertir adecuadamente la prueba digital de cargo y, en su caso, propiciar la desvinculación de nuestro cliente.

Quizás una de las herramientas para obtener cierta seguridad en la obtención de prueba electrónica pueden ser los escribanos, de modo que el acceso a la información se haga directamente por el notario y desde un equipo del profesional, ello con miras a eliminar o reducir posibilidades de alteración. De esta manera se lograría cierto grado de objetividad en la obtención de la prueba, ello por supuesto más allá de la valoración que luego efectúe la justicia. Esta afirmación incluye no solo la "clásica" prueba electrónica, como son los documentos digitales, sino también lo que puede denominarse "constatación de hechos digitales", es decir, todos aquellos medios de prueba en formato electrónico, de hechos, actos o situaciones que no pueden ser amparados bajo el concepto de documento electrónico con firma electrónica reconocida, pero que pueden ser opuestos a otras personas o presentados en juicio.

En la misma línea demarcada, interesante resulta recurrir a la norma ISO/IEC 27037:2012, que brinda lineamientos relativos a la adquisición y preservación de las evidencias digitales a fin de aprovechar al máximo su caudal probatorio. Según esta normativa de carácter internacional, la prueba digital debe ser adquirida del modo menos intrusivo posible, tras un proceso que sea trazable y auditable, tratando de preservar la utilidad y originalidad de la prueba. Ese proceso debe ser reproducible, comprensible y verificable, y para ello las herramientas utilizadas deben ser contrastadas.

Pues bien, después de haber abordado temas como la manipulación de evidencias electrónicas, la violación de garantías constitucionales en su derrotero hacia el proceso, y a partir del caso testigo que analizamos, considero que el lector comprende -ahora quizás en un grado mayor- el valor de normativas como la recién vista. Sin lugar a dudas, el magistrado que intervenga en un ciber caso siempre tendrá la posibilidad de recurrir a un perito informático, de requerirlo -y debo acotar que generalmente lo requerirá-, para de esa manera tener mayor fiabilidad sobre la prueba electrónica. Pero también es cierto que, muchas veces, hasta que se alcance ese estadio procesal transcurrirá tiempo y es en ese lapso precisamente en el que corren peligro las evidencias digitales.



**SUPLEMENTO
ESPECIAL**

DERECHO PROCESAL ELECTRÓNICO

**Aspectos esenciales de los cambios
introducidos por la tecnología
en el proceso judicial**

AÑO 2018

**Nuevas tecnologías en el proceso civil y comercial |
Garantías constitucionales en el proceso digital | Prueba informática |
Firma digital y redargución de falsedad | Valor probatorio del correo electrónico |
Carga de la prueba | Las TIC y el proceso de familia |
Legalización de partidas con firma digital | Cadena de custodia |
Prueba electrónica en el proceso penal**