Revista de Derecho
Comunicaciones y
Nuevas Tecnologías

Consideraciones Sobre el Estado del Arte del Peritaje Informático y los estándares de manipulación de pruebas electrónicas en el mundo

Javier Pimentel Calderón

Jeimy José Cano

Contenido

"Tanto en los asuntos de índole civil, en sentido amplio (que abarcan también lo comercial, laboral, etc.), como en los penales, se presenta como cuestión decisiva la de la prueba. No basta tener derecho sino que se requiere poder exigirlo, Y para esto, tener aptitud de probarlo.
*Juan Larrea Holguín**

CONSIDERACIONES SOBRE EL ESTADO DEL ARTE DEL PERITAJE INFORMÁTICO Y LOS ESTÁNDARES DE MANIPULACIÓN DE PRUEBAS ELECTRÓNICAS EN EL MUNDO

*Javier Pimentel Calderón***
*Jeimy José Cano****

RESUMEN

Las nuevas tecnologías se hacen cada día más importantes; la gente usa el internet para comprar, las grandes corporaciones se valen del correo electrónico para funcionar de forma más eficiente y los delincuentes se hacen diestros en la utilización de los avances tecnológicos como herramienta para delinquir. La prueba documental y el arma homicida están perdiendo vigencia con rapidez. Este artículo aborda el tema de la prueba electrónica, de la manipulación de la misma y de los retos que esta tarea conlleva, dándole un vistazo a las diferentes directrices de manipulación de pruebas electrónicas y de evidencia digital que los países más avezados en estos temas han planteado como solución a los problemas de admisibilidad y a otros retos que usualmente se le presentan a un operador jurídico que pretende usar información almacenada en medios electrónicos como prueba.

ABSTRACT

New Technologies are gaining importance as time passes. People use internet for shopping, big corporations see in email a powerful tool for increasing efficiency and criminals try to develop computer skills in order to use technology as a tool in their misdeeds. This article addresses the topic of electronic evidence and the most common problems that the management and exhibition of this type of evidence arise, examining some of the standards set by the countries with more experience regarding these issues.

Keywords: Computer Expert Witness, Electronic Evidence, Computer Crime, Computer Forensics, Perito Informático, Directrices de manipulación de Evidencia Digital, Evidencia Electrónica, Prueba Electrónica, Derecho Informático, Principio de Neutralidad Tecnológica, Peritaje Informático.

* Holguín Larrea, Juan. En: La Prueba Electrónica (Prólogo). Editorial Temis. 2004.

** Estudiante de la Facultad de Derecho de la Universidad de los Andes, j-piment@uniandes.edu,co.

*** Ingeniero de Sistemas y Computación de la Universidad de los Andes, graduado del Magíster en Ingeniería de Sistemas y Computación de la misma universidad y Doctor en Filosofía de la Administración de Empresas de Newport University, California en los Estados Unidos. Se ha desempeñado como profesor de cátedra en la Facultad de Ingeniería de la Universidad de los Andes en el área de la seguridad informática y la computación forense, así como de la Facultad de Derecho de la misma universidad, donde hace parte del GECTI. Es actualmente miembro de la Red Iberoamericana de Criptología y Seguridad de la Información – CriptoRED http: //www.alfa-redi.org. Correo electrónico: jcano@uniandes.edu.co

INTRODUCCIÓN

En un mundo globalizado en el que las personas celebran contratos mediante el simple intercambio de mensajes de datos y en el que los criminales han encontrado en la informática y en las redes de datos herramientas para delinquir impunemente, se hace cada vez más necesario que los aparatos judiciales tengan a su disposición funcionarios y colaboradores que posean los conocimientos informáticos, técnicos y jurídicos necesarios para ofrecer certeza sobre la integridad de la evidencia obtenida en entornos digitales.

El presente trabajo hace parte de una serie de tres investigaciones conjuntas orientadas a resolver el siguiente problema jurídico: ¿Las prácticas de peritaje informático y la formación de peritos informáticos en Colombia se ciñen a los estándares internacionales y cumplen con los requisitos y consideraciones especiales que exige la manipulación de evidencia digital?. En este primer trabajo se pretende dar un vistazo a los estándares y prácticas internacionales más importantes en materia de peritaje informático, siempre con el cometido de establecer cuales son los conocimientos informáticos, técnicos, jurídicos y en general cuales son las prácticas que se deben exigir a un experto para que sus dictámenes sean considerados como prueba pericial idónea.

La adecuada manipulación de la evidencia digital se erige como un reto incluso para los aparatos judiciales de los países más avezados en las prácticas de seguridad informática y es por eso que los autores de este trabajo consideramos relevante tener en cuenta las respuestas que esos países le han dado al reto antes de crear nuestros propios estándares y procedimientos en materia de peritaje informático.

En los primeros capítulos de este trabajo se realizará una breve contextualización en el tema del peritaje considerado en abstracto para luego ahondar en la definición de peritaje informático y así realizar un análisis de algunos de los estándares y prácticas internacionales que rigen actualmente dicha materia. La meta que nos hemos impuesto es llevar a cabo una evaluación del estado del arte del peritaje informático en Colombia y realizar una propuesta sobre los conocimientos y destrezas mínimas que se deben afianzar en aquellas personas que se desempeñaran como peritos informáticos en nuestro país. Para lograr ese cometido necesariamente debemos realizar un estudio concienzudo que nos permita identificar los rasgos y características esenciales de los estándares internacionales sin el ánimo de realizar juicios *a priori* sobre la conveniencia de transplantarlos a nuestro sistema judicial. Una vez concluida esta primera parte del trabajo tendremos una visión holística sobre la tendencia mundial en materia de peritaje informático y sin el temor de caer en la trampa del etnocentrismo, estaremos en condiciones de realizar una sugerencia informada para ayudar a la implementación de lo que sería el estándar colombiano de buenas prácticas en materia de peritaje informático.

¿QUÉ ES EL PERITAJE?

En ciertas ocasiones los conocimientos del Juez y de los funcionarios de su despacho resultan insuficientes para aclarar ciertas cuestiones sensibles que surgen en un determinado proceso judicial. Por esa razón, se admite la posibilidad de que personas expertas en aquellos temas desconocidos para el juez, rindan dictámenes que brinden certeza sobre el tema de prueba[1] en un litigio o proceso penal.

Es claro entonces, que

1 "El Tema de Prueba está constituido por aquellos hechos que es necesario probar, por ser de los supuestos de las normas jurídicas cuya aplicación se discute en un determinado proceso." PARRA QUIJANO, JAIRO. *Manual De Derecho Probatorio*. Décima Cuarta Edición. Librería Ediciones Del Profesional Ltda. Bogotá 2004. p. 143.

> *"Cuando en sentido general, en el proceso se requieran conocimientos especializados, es decir, de aquellos que escapan a la cultura de las gentes, puede y debe recurrirse a quienes por sus estudios, experiencia, etcétera, los posean; esos conocimientos pueden ser técnicos, científicos o artísticos."*[2]

Así las cosas, se puede afirmar que el peritaje no es otra cosa que un medio de prueba por medio del cual se le confiere a un experto la facultad de rendir un concepto en el tema de su conocimiento, para ayudar al juez en su tarea de forjarse un criterio o una convicción propia sobre unos hechos determinados que son tema de prueba en un proceso judicial. El dictamen pericial es entonces:

> *"un medio de prueba que consiste en la aportación de ciertos elementos técnicos, científicos o artísticos que la persona versada en la materia de que se trate hace para dilucidar la controversia, aporte que requiere de especiales conocimientos."*[3]

En materia de procedimiento penal, la peritación *"es el acto procedimental en el que el técnico o especialista en un arte o ciencia (perito), previo examen de una persona, de una conducta o hecho, o cosa, emite un dictamen conteniendo su parecer y los razonamientos técnicos sobre la materia en la que ha pedido su intervención."*[4]

Así las cosas, es preciso hacer hincapié en la necesidad de que los peritos acrediten que son verdaderos expertos con el fin de que su dictamen revista verdadera importancia y autoridad. En ese orden de ideas, se preferirá necesariamente a aquellas personas que acrediten "una reconocida solvencia profesional, ética y moral"[5], además de una formación idónea y una experiencia adecuada en el área del conocimiento sobre la que versará el dictamen. No obstante, lo anterior no implica necesariamente que se deba acreditar un título profesional para obrar como perito ya que resulta obvio que alguien puede ser un experto en un determinado tema y no poseer un título profesional que acredite tal experticio, como en el caso de las personas que se hacen doctas en ciertos temas técnicos, artísticos o incluso científicos por la simple experiencia. Lo anterior resulta plausible en tanto el dictamen del perito no reemplaza al fallo del juez sino que por el contrario, se allega al proceso con la intención de ayudar al fallador quien deberá valorarlo como a cualquier otro medio probatorio para lograr una providencia que se compadezca con los hechos que se acreditaron en el caso *subjudice*. Será el juez quien decidirá si el dictamen en cuestión le ofrece certeza sobre un determinado hecho y por ende estaría en sus manos el restarle importancia a un dictamen que provenga, a todas luces, de una persona inexperta en los temas sobre los que versa la pericia. En España, por ejemplo, se admite la posibilidad de que una persona entendida en un determinado tópico y no titulada oficialmente pueda obrar como perito:

> *"Así, la LEC, art. 340, en su párrafo primero, al referirse a lasa (SIC) condiciones de los peritos, dispone: los peritos deberán poseer el título oficial que correspondas (SIC) a la materia objeto del dictamen y a la naturaleza de éste; y dice a continuación: si se trata de materias que no estén comprendidas en títulos profesionales oficiales, habrán de ser nombrados entre personas entendidas en aquellas materias"*[6].

El artículo 8 de nuestro Código de Procedimiento Civil recoge el criterio mencionado anteriormente al establecer para los auxiliares de la justicia, entre ellos los peritos, los siguientes lineamientos:

2 Ibídem. p. 628.
3 Ibídem.
4 BAILÓN BALDOVINOS, ROSALÍO cita a COLIN SANCHEZ GUILLERMO. *Derecho Procesal Penal*. Editorial Limusa 2002. p. 84.
5 RODRIGUEZ JOUVENCEL, MIGUEL. Manual del Perito Médico. *Fundamentos Técnicos y Jurídicos*. Ediciones Díaz de Santos. Edición 2002. p. 251.
6 Ibídem.

> *"Los cargos de auxiliares de la justicia son oficios públicos que deben ser desempeñados por personas idóneas, de conducta intachable, excelente reputación e incuestionable imparcialidad. Para cada oficio se exigirán versación y experiencia en la respectiva materia y, cuando fuere el caso, título profesional legalmente expedido."*

En cuanto a la actividad de los peritos, es claro que éstos "examinarán conjuntamente las personas o cosas objeto del dictamen y realizarán personalmente los experimentos e investigaciones que consideren necesarios"[7] para culminar con un informe en los términos del numeral 6 del artículo 237 de nuestro C.P.C, que establece lo siguiente:

> *"El dictamen debe ser claro, preciso y detallado; en él se explicarán los exámenes, experimentos e investigaciones efectuados, lo mismo que los fundamentos técnicos, científicos o artísticos de las conclusiones"*

El artículo citado anteriormente reviste la mayor importancia para efectos de este trabajo en tanto permite vislumbrar el primer error en el que podría incurrir un perito al elaborar su dictamen. Como lo expresa el maestro Jairo Parra Quijano, la primera tarea del juez consiste en *"observar si efectivamente existe un dictamen pericial, esto es, analizar cuidadosamente si se cumplieron los requisitos del numeral 6 del artículo 237 del C.P.C"*[8]. En ese orden de ideas, es claro que un experto estaría incurriendo en una falla si elabora su informe sin observar los requisitos esenciales que harán de su declaración un verdadero dictamen pericial. Lo anterior requiere entonces que los peritos, como auxiliares de la justicia, dispongan de ciertas aptitudes jurídicas y dispongan no solo de un conocimiento en la materia sobre la cual versará su informe sino que además, dispongan de nociones básicas de Derecho Procesal.

Entendido lo anterior, es preciso hacer una síntesis de las principales características de la prueba pericial:

1. Supone la concurrencia de un experto con título profesional legalmente expedido cuando fuere el caso. Esto es particularmente importante para nuestro trabajo en tanto el juez podría restarle importancia a un dictamen rendido por una persona inexperta.

2. El experto rinde un informe o una "declaración de carácter técnico, científico o artístico" (PARRA QUIJANO, 2004).

3. El dictamen rendido por el experto no reemplaza al fallo del juez, debe ser valorado y sopesado frente a las demás pruebas allegadas al proceso.

4. Los peritos en Colombia están impedidos y son recusables como los jueces. (Art. 235 del C.P.C).

5. En Colombia, el dictamen debe seguir los lineamientos establecidos en el numeral 6 del artículo 237 del C.P.C.

Dilucidado el concepto de peritaje, es preciso entrar en la materia esencial de este trabajo, a saber, el peritaje informático. Para ello, resulta necesario hacer un análisis de ciertos conceptos que hacen parte de una disciplina denominada Derecho Informático sin los cuales no se podría abordar correctamente una discusión sobre el tema central del presente artículo.

APROXIMACIÓN AL DERECHO INFORMÁTICO

No es un secreto que el mundo está en constante cambio y que la informática[9] juega un papel

7 PARRA QUIJANO, JAIRO. Op. Cit. p. 633

8 PARRA QUIJANO, JAIRO. Op, Cit. p. 636.

9 La Informática es "La disciplina que estudia el fenómeno de la información, y la elaboración, transmisión y utilización de la información principalmente, aunque no

muy importante en la actualidad debido a su convergencia con las telecomunicaciones. Así las cosas, no causa sorpresa que haya nacido una nueva disciplina "que se encarga de poner (SIC) orden las nuevas relaciones que han surgido con la aparición de las Tecnologías de la Información y las Comunicaciones."[10]

Dicha disciplina, denominada Derecho Informático surge "cuando el derecho no es la materia estudiada, sino el punto de vista desde el cual se estudia la informática"[11]. En ese sentido, el Derecho Informático no es más que una disciplina que se encarga de estudiar y regular las nuevas relaciones jurídicas que la Informática y las TICs permiten en el mundo actual. De la misma forma, la experiencia ha enseñado que el Derecho Informático "ha sido una útil herramienta para adaptar aquellas instituciones de Derecho que han sido afectadas por el creciente uso de los medios tecnológicos."[12]

Mucho se ha discutido sobre la posibilidad de considerar al Derecho Informático como una rama autónoma del Derecho. Por mi parte, acojo la idea de que el Derecho informático no es en si mismo una rama del Derecho en tanto su estudio resultaría imposible sin la enseñanza de la dogmática y los conceptos de otras áreas del Derecho. Los delitos informáticos, por ejemplo, son tema de estudio del Derecho Penal y por ende deberían enseñarse como parte de esa disciplina; lo mismo ocurre con los contratos electrónicos, cuya regulación debería ser objeto de estudio en un curso de Contratos.

Con respecto a esta discusión vale la pena transcribir la siguiente reflexión de Juan Carlos Riofrío:

> "Como dijimos, la res informática constituye el objeto material de nuestra ciencia. El objeto formal, el punto de vista bajo el que se estudiará la res informática será el del derecho. Estas dos frases suenan bien y son correctas, pero ayudan poco a delimitar nuestro derecho, pues alrededor de esa res informática observamos que existen normas y principios propios de otras ramas del derecho: sobre cada programa hay un derecho de propiedad intelectual, cada negocio realizado a través de esa res informática se rige bajo la ley mercantil, hay obligaciones tributarias que satisfacer, cada noticia debe ceñirse a unas determinadas normas específicas de la información, se hallan tipificadas una gran cantidad de conductas en la legislación penal... Y lo peor de todo es que si quitamos lo mercantil, lo tributario, lo informativo, lo penal, lo contractual y todo lo que se halle dentro de otra rama del derecho distinta al DI, ¿qué nos quedará? En una palabra: nada."[13]

Entendido lo anterior y en aras de evitar centrarnos en discusiones que no son esenciales para el tema que nos ocupa y así extender excesivamente este trabajo, es preciso omitir algunas otras consideraciones sobre la naturaleza del Derecho Informático. En ese orden de ideas, resulta pertinente realizar algunas consideraciones sobre el concepto de prueba electrónica.

necesariamente, con la ayuda de ordenadores y sistemas de telecomunicación como instrumentos". ALTMARK, DANIEL. Informática y Derecho, Vol 1, Editorial Depalma. Buenos Aires, 1987, p. 6.

10 BENCOMO YARINE, EDEL. *Reseña De La Legislación Informática en Cuba*. En: Alfa Redi, Revista de Derecho Informático. No. 102 Enero de 2007. Disponible en: http://www.alfa-redi.com/rdi-articulo.shtml?x=8408

11 RÍOFRIO MARTINEZ VILLALBA, JUAN. *La pretendida Autonomía del Derecho Informático*. En: Alfa Redi, Revista de Derecho Informático. No. 50 Septiembre de 2002. Disponible en: http://www.alfa-redi.com/rdi-articulo.shtml?x=1448

12 BENCOMO YARINE, EDEL. Op. Cit.

13 RÍOFRIO MARTINEZ VILLALBA, JUAN. La pretendida *Autonomía del Derecho Informático*. En: Alfa Redi, Revista de Derecho Informático. No. 50 Septiembre de 2002. Disponible en: http://www.alfa-redi.com/rdi-articulo.shtml?x=1448

CONSIDERACIONES SOBRE LA PRUEBA ELECTRÓNICA

En la actualidad los documentos electrónicos[14] hacen parte de la vida cotidiana. Las nuevas tecnologías han generado un auge exacerbado del correo electrónico y de los mensajes de datos como género, definidos por nuestra legislación en los siguientes términos:

> *"La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax"*[15].

No obstante, nuestro ordenamiento jurídico no establece una definición legal de prueba electrónica y por ende resulta necesario acudir a la doctrina nacional e internacional en aras de encontrar y fijar una definición adecuada de prueba electrónica para efectos de este trabajo.

Lo cierto al respecto es que no existe una definición amplia y genérica de prueba electrónica (TORRENTE, D. 2007). La doctrina usa y expone múltiples definiciones entre las cuales podemos resaltar las siguientes:

> *"prueba electrónica es cualquier información obtenida a partir de un dispositivo o medio digital y que sirve para adquirir convencimiento de la certeza de un hecho".*[16]

Cabe resaltar que esta acepción fue establecida como definición inicial operativa de un grupo de trabajo conformado con el objeto de estudiar el concepto de prueba electrónica y su utilidad radicaba en que podía ser usada como punto de referencia y comparación para analizar algunas legislaciones en busca de un concepto análogo. El estudio en comento, concluyó que ninguno de los sistemas jurídicos analizados establece, en estrictos términos jurídicos, una definición legal de prueba electrónica equiparable a aquella planteada como definición inicial por los investigadores[17]. Como se había expresado anteriormente, las legislaciones no abundan en definiciones en lo que respecta al concepto de prueba electrónica; al parecer los legisladores prefieren mantener una cierta prudencia que a mi juicio obedece al temor típico que embarga a los legisladores del mundo en el momento en que se ven apremiados a fijar conceptos en términos jurídicos estrictos, en materias que trascienden el dogma y la teoría del derecho para abarcar otros temas que las nuevas tecnologías ponen de presente. Dicho temor podría ser extensión de todas esas dudas que embargan a los juristas tradicionales al embarcarse en el estudio de la convergencia entre el derecho y la tecnología.

Si bien el concepto de prueba electrónica no es un tema pacífico de discusión, resulta claro que no solo los mensajes de datos y los documentos electrónicos se pueden considerar como prueba electrónica. Aunque la ley 527 de 1999 se limita a concederle aptitud como medio de prueba a los mensajes de datos en los siguientes términos: "Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Códi-

14 "Con Documento Electrónico, básicamente nos referimos a aquellos documentos cuyo soporte se encuentra en medios electrónicos, llámese mensaje de datos, registro contable electrónico o el texto electrónico de un contrato. María Fernanda Guerrero cita un concepto que destaca las características relevantes del documento electrónico: "Cualquier representación en forma electrónica de hechos jurídicamente relevantes. Susceptibles de ser asimilados asimilados en forma humanamente comprensible". REMOLINA ANGARITA, NELSON. *Desmaterialización, documento electrónico y centrales de registro*. En: Comercio Electrónico. GECTI. Editorial Legis. Bogotá, 2005. p. 150.

15 Art. 2. Literal A. L.527/99.

16 TORRENTE, DIEGO. *CONFERENCIA AEEC: EN BUSCA DE UNA DEFINICIÓN PARA 'PRUEBA ELECTRÓNICA'*. En: E-Newsletter de Cybex. No 27. Abril de 2007.

17 "El análisis de las legislaciones y las respuestas de los expertos entrevistados reveló que no existe, en términos jurídicos, un concepto genérico y amplio de'prueba electrónica' equiparable al construido por nosotros" TORRENTE, DIEGO. O.P Cit.

go de Procedimiento Civil."[18], no sería adecuado afirmar que sólo los mensajes de datos pueden obrar como prueba en la medida en que otra información consignada en medios informáticos, que no constituye documento o mensaje de datos alguno, puede ofrecer certeza o convencimiento sobre unos hechos determinados.

Un buen ejemplo serían las huellas que deja un intruso que ha irrumpido abusivamente en un sistema informático. Para un experto en computación forense, los registros de acceso al sistema comprometido y en general las diferentes alteraciones sutiles en el funcionamiento y los datos de un sistema informático, son tan útiles y dicientes como podrían serlo (para un experto en ciencias forenses ajenas a la informática) las huellas que deja un criminal al manipular el cuerpo del delito.

No podríamos pensar que estas huellas criminales que sólo se pueden vislumbrar en un entorno digital constituyen un mensaje datos o un documento electrónico, sin embargo resulta claro que, evaluadas y exhibidas en un proceso judicial por un experto en computación forense, pueden ofrecerle certeza al juez sobre las condiciones en las que se llevó a cabo un determinado *cybercrimen* y por ende, a la luz de la definición operativa expuesta anteriormente, pueden constituir verdaderas pruebas electrónicas.

Por último, con un ánimo meramente enunciativo, sería pertinente señalar algunas de las diferentes formas en las que se puede encontrar la evidencia digital (SOMMER, P. 2005):

- Contenido de un archivo: "Usualmente, las palabras y figuras en un documento o reporte, imágenes, (..) emails, páginas web"[19] entre otros.
- Meta Data: En términos simples, el meta data podría vislumbrarse como información sobre la información. En efecto, éste tipo de evidencia sería muy útil en la medida en que consiste en "datos sobre los datos, que no son inmediatamente visibles pero que indican, por ejemplo, quien creó un archivo, cuantas veces ha sido editado y cuantas veces ha sido impreso." [20]
- Datos de Directorio: "Información sobre un archivo que se guarda en los medios de almacenamiento y contiene detalles de nombre, fechas relevantes y tamaño"[21] entre otros.
- Datos de Configuración: "Archivos y datos de directorio que permiten que un computador o una aplicación se comporte de una forma en particular y que pueden proveer evidencia sobre la forma y el tiempo en el que un computador fue usado"[22].
- Datos de *Logging*: Estos son archivos creados por "programas y sistemas operativos, que registran la actividad en un determinado sistema y pueden ser usados para intentar la reconstrucción de eventos"[23].
- Material forense recuperado: Para la obtención de este material sería preciso contar con una persona diestra en Computación forense en la medida en que se trata de "material obtenido de medios de almacenamiento que no sería normalmente visto, como por ejemplo, archivos que no han sido debidamente eliminados"[24], entre otros.
- Interpretaciones de expertos: Estos podrían constituir pericias electrónicas en los términos del acápite siguiente y pueden versar sobre cualquiera de las formas de evidencia señaladas anteriormente.

18 Art. 10. L.527/99.

19 Sommer, P. (2005). DIRECTORS AND CORPORATE ADVISORS' GUIDE TO DIGITAL INVESTIGATIONS AND EVIDENCE [Versión Electrónica], p. 29. Accesado en Mayo de 2007 en la dirección http://www.iaac.org.uk/Portals/0/Evidence%20of%20Cyber-Crime%20v12-rev.pdf.

20 Ibídem.

21 Ibídem.

22 Ibídem.

23 Ibídem.

24 Ibídem.

CONSIDERACIONES SOBRE PERITAJE INFORMÁTICO

Un dictamen pericial, como se expresó en el primer capítulo, puede tratar temas científicos, técnicos o artísticos. En caso de que un dictamen verse sobre temas atinentes a la informática, se estará en presencia de un peritaje informático. Más aún, cuando la pericia analice o considere una prueba electrónica allegada al proceso, el perito deberá disponer de conocimientos específicos en el área de la informática forense y por ende, su dictamen constituirá también un peritaje informático.

Este perito informático no es más que un experto "en el área de las tecnologías de la información que de acuerdo con el tema requerido puede ser seleccionado según su competencia y experiencia para una labor de análisis"[25].

En ese orden de ideas, podríamos afirmar que el peritaje informático es una disciplina que convierte la información contenida en medios informáticos, aunada al conocimiento que posee una persona sobre tecnologías de la información, en herramientas valiosas para ofrecer certeza o convencimiento al juez sobre unos hechos determinados. Es así que a través del peritaje informático la prueba electrónica obtiene verdadera eficacia.

El trabajo del perito informático es entonces ofrecer un "dictamen técnico y científico sobre el objeto de análisis en el cual cuenta con la experiencia y conocimiento requerido, con el fin de que a través de fuentes de información y análisis exhaustivo llegue a conclusiones que pueda sustentar"[26]. Así las cosas, no sólo deberá poseer los respectivos conocimientos técnicos en informática sino que además deberá poseer ciertos conocimientos jurídicos y ciertas destrezas criminalísticas y forenses. En los capítulos siguientes, analizaremos los estándares que deben cumplir los peritos informáticos en el mundo para garantizar la idoneidad de sus dictámenes y para darle verdadero peso a sus afirmaciones como medio de prueba en un proceso. Dichos estándares reflejan la postura de cada país en cuanto a los conocimientos técnicos, jurídicos, criminalísticos y forenses que debe poseer un perito informático, así como las exigencias que se hacen en diferentes países en cuanto a las destrezas y consideraciones que debe observar cualquier persona que aspire a llevar a cabo un verdadero peritaje informático.

¿POR QUÉ ES NECESARIO UN PERITO INFORMÁTICO?

Este es el siglo XXI, el auge de los documentos electrónicos es tal que "cada año se envían en todo el mundo más de 2,8 trillones de correos electrónicos y, en la actualidad, más del 90% de los documentos que se crean en la organización son ya electrónicos, de los cuales menos del 30% llegan a imprimirse en papel."[27]

Las legislaciones y los modelos que dictan pautas para crear leyes (la ley modelo de UNCITRAL es un buen ejemplo) tienden a permitir el perfeccionamiento de contratos y negocios jurídicos mediante un simple intercambio de mensajes de datos.

Los criminales, por su parte, ven en el internet y en las tecnologías informáticas verdaderas herramientas para delinquir impunemente y en muchas ocasiones se hacen diestros en el uso de nuevas tecnologías para cometer sus crímenes. No es un secreto que el Internet ha sido determinante en algunos fraudes bancarios millonarios y que los hackers maliciosos, los crackers y en general los cybercriminales, se sienten más seguros

25 CANO, Jeimy. *Estado del arte del Peritaje Informático en Latinoamérica*. En: Revista Alfa-Redi disponible en www.alfa-redi.org p. 8.

26 Ibídem.

27 DE LA TORRE, Juan. AGUD ANDREU, Sergio. Pruebas Electrónicas: *Una Nueva Realidad*. En: E-Newsletter de Cybex. No 27. Abril de 2007

al saber que son algo menos vulnerables que un criminal común, sentados frente a una pantalla de computador a una distancia considerable del lugar en el que su crimen producirá efectos.

Los delitos informáticos se encuentran en su apogeo. Según cifras oficiales, de enero a mayo de 2007 en Colombia "se han denunciado casi 180 casos de fraude electrónico, que en total han costado más de 349.000 millones de pesos a personas naturales y cerca de 6.6 billones de pesos a empresas."[28] Así las cosas, el nuevo panorama nos obliga a hacernos, entre otras, las siguientes preguntas:

- Dado un litigio en el que se plantea la inexistencia o nulidad de un determinado contrato de compraventa celebrado mediante el intercambio de mensajes de datos ¿Quien estaría en capacidad de ofrecer certeza al juez sobre la procedencia de un mensaje de datos en el que se aceptó la oferta para contratar?

- Verificado el acceso abusivo a un sistema informático y la vulneración de los datos en él contenidos ¿quien podría asistir a un fiscal en el manejo y discernimiento de las huellas que el intruso ha dejado en el sistema comprometido? ¿Quién podría brindarle certeza al juez sobre el modus operandi del intruso y quién podría extraer verdaderas conclusiones que permitan la condena del responsable?

La lista de preguntas de ese tipo sería interminable y teniendo en cuenta las consideraciones realizadas anteriormente sobre peritaje informático y las características especiales de la evidencia digital, la respuesta a todas es obvia: La persona idónea para llevar a cabo esas tareas es un perito Informático.

Lo anterior resulta aún más importante si se tiene en cuenta que la manipulación y el examen de pruebas electrónicas es una tarea que requiere particular cuidado en consideración a las características especiales de la evidencia digital, a saber:

- La evidencia digital se puede reproducir y alterar muy fácilmente: "Es una característica que la hace maleable, lo cual, por un lado puede ayudar a la duplicación requerida para su análisis posterior, pero por otra parte, la hace vulnerable y fácilmente modificable"[29].

- "La Evidencia digital es anónima"[30]: En muchas ocasiones, establecer la verdadera procedencia de un mensaje de datos no firmado digitalmente (por ejemplo) es muy difícil para alguien sin el debido entrenamiento.

- "La forma de la evidencia digital es tan importante como su contenido. Es importante revisar el contenido del documento pero al mismo tiempo los medios a través de los cuales se crearon, enviaron o enrutaron los contenidos hacia su destino"[31].

- "La evidencia digital tiene dificultades para ser llevada a la corte"[32].

- La recopilación, búsqueda, acceso, almacenamiento y transferencia de evidencia digital son tareas que exigen consideraciones y cuidados especiales para garantizar la integridad de la misma y la observancia de la cadena de custodia.

En ese orden de ideas, es claro que no se podría confiar la manipulación de ese tipo de evidencia a una persona inexperta en los temas técnicos y jurídicos a los que se hizo referencia en acápites

28 Los delitos informáticos, en aumento. (Lunes 7 de Mayo de 2007). El Tiempo, pp. 2-2.

29 CANO, Jeimy. *Evidencia Digital: Conceptos y Retos*. En: Comercio Electrónico. GECTI. Editorial Legis. Bogotá, 2005. p. 185.

30 Ibídem.

31 Ibídem. p. 186.

32 Ibídem.

anteriores y que se especificaran en los capítulos siguientes, máxime si se tiene en cuenta que en tratándose de pericias informáticas y en casos en los que las pruebas allegadas al proceso sólo sean electrónicas, el fallo del juez, aunque no se vería reemplazado por el dictamen del perito, sí estaría altamente influenciado y motivado por el dictamen del experto en cuestión. En esos casos, las consecuencias de escoger a una persona inexperta para rendir dictamen serían funestas toda vez que la decisión del juez se vería distorsionada por el análisis y las conclusiones equivocadas que se hicieron de las pruebas electrónicas allegadas al proceso.

Justificado el presente trabajo y dilucidados algunos conceptos claves, es preciso seguir adelante con el análisis de los principales estándares que deben observar los peritos informáticos alrededor del mundo para evitar problemas como el descrito en el párrafo anterior, y para evitar que sus dictámenes y las pruebas electrónicas en ellos analizadas sean descartadas por los jueces o puestas en duda por las partes interesadas en un litigio.

PERITAJE INFORMÁTICO Y MANIPULACIÓN DE EVIDENCIA DIGITAL EN EUROPA

La forma disímil en la que estos temas son tratados en los diferentes países Europeos nos obligaría a dar un vistazo a la legislación y doctrina de cada país en ausencia de una investigación seria, como la realizada por el grupo de investigación de cybex[33] sobre la admisibilidad de la evidencia digital en las cortes Europeas. Para efectos de este trabajo, nos apoyaremos en dicha investigación en aras de evitar extendernos excesivamente.

En primer lugar, es preciso resaltar que un grupo de países Europeos " tiene en común que su tradición jurídica establece unos criterios muy amplios de admisibilidad de la prueba. Se basan en la libre consideración del juez a la hora de admitir o no la prueba electrónica"[34]. Estos países son Austria, Dinamarca, Suecia y Finlandia.

Otro grupo de países, como se expresa en la investigación de Cybex, regula de manera más restrictiva la admisibilidad de la prueba erigiendo ciertos requisitos de orden legal.

No obstante, la mayoría de juristas europeos entrevistados señaló que "la persona encargada de la obtención de la prueba electrónica es el factor que más influye en el valor probatorio que se le pueda atribuir"[35]. Esta afirmación resulta muy importante en la medida en que resalta la importancia de que la manipulación de la prueba electrónica se lleve a cabo por expertos. Entendido lo anterior, causa sorpresa que en Europa no exista una regulación vigente que fije los requisitos y características que deben reunir quienes pretendan ostentar el título de expertos en informática forense. Sobre este tema en específico, la posición de los juristas Europeos es una tendencia a preferir a los fiscales y policías como los expertos en informática forense por excelencia, otorgándoles a éstos la responsabilidad de obtener la prueba electrónica y de manipularla adecuadamente.

En cuanto al proceso de recolección de evidencia, en el reino unido se han tenido en cuenta los diferentes problemas que plantea la manipulación de las pruebas electrónicas y por ende, la asociación de jefes de policía (*Association of Chief Police Officers*) sugiere ceñirse a un procedimiento forense estandarizado que normalmente consta de cuatro etapas:

33 Cybex es una empresa española líder en la investigación del fraude empresarial y económico en entornos virtuales. Véase: http://www.cybex.es..

34 Cybex. (2006). *La Admisibilidad de las Pruebas Electrónicas Ante Los Tribunales*. Revisado el 7 de mayo de 2007, disponible en: http://www.cybex.es/agis2005/docs/libro_aeec_sp.pdf.

35 Ibídem.

1. Etapa De Recolección: Implica la búsqueda, reconocimiento, recolección y documentación de la evidencia electrónica[36].

2. Proceso de Examen de la evidencia: Este proceso, como lo explica la ACPO, ayuda a hacer visible la evidencia y explica su origen y su alcance. En él se deben efectuar algunas tareas como: —Documentar el contenido y el estado de la evidencia en su totalidad.— Separar la evidencia útil de la demás información que coexista en el medio electrónico.

3. La Fase de Análisis: En esta etapa se inspecciona la evidencia útil obtenida del proceso de examen indagando por su valor probatorio y relevancia.

4. El reporte o declaración: Según la ACPO, el reporte debe dilucidar el proceso de examen, la información pertinente obtenida mediante dicho proceso y debe contener un análisis del investigador enfocado en esos dos aspectos. En esta etapa, la asociación en comento hace hincapié en que las notas que tome el examinador deben ser preservadas para efectos testimoniales, siempre teniéndose en cuenta que el investigador podrá verse abocado a testificar también sobre la validez del procedimiento de examen de la evidencia digital y sobre sus calificaciones para conducirlo a cabalidad. Otra tarea que resulta muy importante en este proceso de recolección de pruebas digitales es la obtención de una copia fidedigna de los datos contenidos en los medios electrónicos objeto de la investigación. En ese orden de ideas, la ACPO le hace un llamado a la cautela a los investigadores en cuanto a la elección del software y el hardware que usaran en sus investigaciones, para asegurar que la información original no resulte comprometida.

36 England, Wales and North Ireland Association of Chief Police Officers. Good Practice Guide for Computer based Electronic Evidence.

De la bibliografía revisada, se puede extraer que además de las consideraciones específicas que cada legislación impone sobre la manipulación de pruebas electrónicas, éstas también están sujetas a las reglas de exclusión propias de las pruebas tradicionales. Así las cosas, la observancia de la cadena de custodia, de los parámetros de legalidad de la prueba, entre otros, son directrices obligatorias para un perito informático que no quiera poner en duda en un estrado judicial la admisibilidad de las pruebas recolectadas. En ese orden de ideas, es preciso señalar que toda manipulación de pruebas electrónicas requiere un nivel de diligencia y destreza superiores a aquellos exigidos para las pruebas tradicionales en la medida en que su admisibilidad puede cuestionarse por muchas más razones de índole técnica. Nuevamente, la necesidad de que el perito informático (bien sea un agente del estado o un perito de parte) cuente con la formación adecuada para recolectar y manipular pruebas electrónicas se hace latente. De ahí que en el reino unido, la ACPO se haya pronunciado sobre las calidades a exigir de un perito externo o de parte, instando a los encargados de selección a tener en cuenta ciertos aspectos[37] que resultan intuitivos, a saber:

1. El experticio del especialista a seleccionar.

2. Su experiencia en el tipo de trabajo que se le encomendará.

3. Su nivel de entendimiento de la naturaleza de las investigaciones en Gales y el Reino Unido en aspectos específicos cómo el ritmo en el que éstas se realizan y su confidencialidad.

37 Sin embargo, es preciso resaltar que "*en Europa hay una ausencia de normas que determinen las características que tiene que reunir un experto en informática forense. Careciendo de preceptos legales, lo que más valoran, tanto juristas como técnicos es la experiencia específica*".

Cybex. (2006). *La Admisibilidad de las Pruebas Electrónicas Ante Los Tribunales*. Revisado el 7 de mayo de 2007, disponible en: http://www.cybex.es/agis2005/docs/libro_aeec_sp.pdf.

4. El conocimiento contextual del sujeto, que implica primordialmente el entendimiento de las diferencias entre prueba científica y prueba legal.

5. El conocimiento legal o jurídico del sujeto a seleccionar, requisito que implica constatar su entendimiento de los procesos judiciales y del rol que debe desempeñar un perito.

6. Las habilidades comunicativas del sujeto a seleccionar.

Es preciso reiterar, como lo hemos hecho a lo largo de este trabajo, que la admisibilidad de la prueba electrónica en los tribunales está ampliamente supeditada a las calidades y buenas prácticas de las personas que efectuaron el trabajo de recolección, custodia, análisis y exhibición de las pruebas. Un perito informático diligente y cuidadoso al realizar esas tres tareas será un valioso colaborador de la rama judicial.

A manera de conclusión, es pertinente citar el siguiente aparte de la investigación sobre admisibilidad de pruebas electrónicas en Europa, que da muchas luces sobre el estado del arte del peritaje informático en el viejo continente:

> *"LA ADMISIBILIDAD DE LAS PRUEBAS ELECTRÓNICAS EN LOS TRIBUNALES EUROPEOS ESTÁ REGULADA A TRAVÉS DE LAS DISPOSICIONES GENERALES DE LA PRUEBA TRADICIONAL EN EL*
>
> *CONJUNTO DE PAÍSES EUROPEOS, SIN QUE HASTA EL MOMENTO SE HAYA DESARROLLADO NINGUNA REGULACIÓN NACIONAL ESPECÍFICA EN EUROPA."*[38]

PERITAJE INFORMÁTICO Y MANIPULACIÓN DE EVIDENCIA DIGITAL EN ESTADOS UNIDOS

Sin duda alguna, Estados Unidos es uno de los países en los que se ha producido más literatura sobre aspectos concernientes a la manipulación de pruebas electrónicas y en general sobre la pericia informática. El caso Estadounidense, sin embargo, resulta particularmente importante para ilustrar la relevancia de los Derechos Fundamentales en el proceso de búsqueda y recolección de pruebas contenidas en soportes electrónicos.

En efecto, la cuarta enmienda a la constitución americana, estableció ciertos límites para la búsqueda y recolección de evidencia al establecer que las personas gozan de un derecho a no ser objeto de búsquedas o apoderamientos arbitrarios o irracionales en sus personas, casas, papeles y efectos personales.

Las cortes Americanas han desarrollado y delimitado tal derecho en lo que respecta a la expectativa razonable de privacidad en casos que involucren computadores o evidencia digital, asimilando el computador o medio electrónico a un contenedor o compartimiento cerrado tal como un portafolio o un archivador. En ese orden de ideas, las cortes han considerado (véase United States v. Barth, 26 F. Supp. 2d 929, 936-37) que el dueño de un computador, por ejemplo, tiene una expectativa razonable de privacidad sobre la información almacenada en el disco duro de dicho computador, tal como el dueño de un portafolios tiene una expectativa razonable de privacidad sobre los documentos en él contenidos. Comprobada la expectativa razonable de privacidad, el precedente establece que el investigador o quien pretenda conducir una búsqueda o apoderamiento de material probatorio contenido en el medio electrónico en cuestión, deberá obtener una autorización judicial en la que expresamente se le encomiende dicha tarea.

38 Ibidem.

Una de las principales preocupaciones de los americanos es entonces la protección del derecho consagrado por la cuarta enmienda. Este aspecto resulta tan delicado que el departamento de defensa, en el manual para la búsqueda y obtención de evidencia electrónica en investigaciones criminales, hace alusión en primera medida a la forma en que se debe interpretar la cuarta enmienda en los casos que involucren pruebas electrónicas.

Además de la analogía mencionada anteriormente, las cortes americanas han establecido otra subregla importante que establece una excepción a la protección de la cuarta enmienda en la medida en que el investigado pierda el control sobre los archivos o información almacenada en medios electrónicos que le pertenecen. En caso de que se ceda el control de la información a un tercero, como cuando se le envía un disco compacto por correo a un amigo, se debe establecer si el remitente dueño de la información tiene la intención de retener cierto control sobre la información contenida en el disco. En caso de que la intención del remitente no sea retener control alguno sobre la información enviada, se entiende que se extingue también su expectativa razonable de privacidad en lo que respecta al disco compacto y por ende que, bajo los lineamientos de la cuarta enmienda, un agente estatal podría apoderarse o llevar a cabo búsquedas en la información contenida en dicho disco sin una autorización judicial.

Por último, el citado documento del departamento de justicia de los Estados Unidos[39] hace una alusión a las investigaciones privadas, excluyéndolas de la órbita de protección de la cuarta enmienda. Entendido lo anterior, el documento en cuestión resalta que "no hay una violación de la cuarta enmienda cuando un individuo obrando por iniciativa y voluntad propia lleva a cabo una búsqueda de evidencia y expone los resultados de la misma a un agente del estado"[40]. Un precedente que se considera pertinente para ilustrar un caso en el que las cortes típicamente aplicarían la excepción en comento es United States v. Hall (142 F.3d 988), en el que un individuo llevó su computadora a reparación a donde un especialista, quien decidió llevar a cabo una investigación al encontrar indicios de que en el disco duro que revisaba se almacenaba pornografía infantil. La búsqueda del especialista culminó con una denuncia a la policía. Finalmente, los jueces descartaron la vulneración a la cuarta enmienda bajo el argumento de que el estado no había participado en la búsqueda y que, después de la denuncia, la policía había obtenido la debida autorización judicial para llevar a cabo nuevas indagaciones.

Esbozada a grandes rasgos la óptica garantista desde la cual se contempla el procedimiento de búsqueda y obtención de pruebas electrónicas en Estados Unidos, es preciso enfocarnos entonces en ciertos estándares de buenas prácticas que se observan reiteradamente en las investigaciones criminales y en procesos de indagación que impliquen la manipulación de pruebas electrónicas en Estados Unidos. En ese respecto, el citado manual del departamento de justicia reconoce que aunque el marco legal para la conducción de búsquedas y recolección de evidencia en casos que comprometan pruebas electrónicas es el mismo que rige para las investigaciones convencionales, "las tecnologías informáticas frecuentemente obligan a los agentes a ejecutar búsquedas en formas no convencionales"[41]. La poca ortodoxia de las investigaciones que comprometen evidencia digital se debe entre otras cosas a los retos que ofrece la

39 Computer Crime and Intellectual Property Section. Criminal Division. United States Department of Justice. (2002) S*earching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. Disponible en: http://www.cybercrime.gov/s&smanual2002.htm#_IB3_

40 Ibídem.

41 Computer technologies frequently force agents to execute computer searches in nontraditional way. Ibídem.

manipulación de pruebas electrónicas enunciados en el acápite 2.4 del presente trabajo, a la volatilidad de los archivos de computadora y a la posibilidad de que el investigado haya tomado medidas para impedir el acceso o para esconder información sensible. En ese orden de ideas, una vez obtenida la autorización judicial, "los agentes e investigadores han encontrado que pueden maximizar la probabilidad de éxito de la búsqueda y asimiento de material probatorio siguiendo los siguientes cuatro pasos"[42]:

1. Conformar un equipo integrado por el agente investigador a cargo del caso, el fiscal o el funcionario a quien corresponda la acusación y un especialista técnico preferiblemente con conocimientos de informática forense.[43]

2. Recopilar la mayor información posible sobre el sistema informático que será objeto de investigación antes de trazar una estrategia de búsqueda o redactar un borrador de la solicitud de autorización que será dirigida al juez competente. Este paso es particularmente sensible en la medida en que ayuda al investigador a hacerse una idea sobre las condiciones en las que se encontrará la información a revisar en el sistema informático. De acuerdo al manual en cuestión, en esta etapa es preciso establecer qué tipo de hardware, software, sistemas operativos y configuraciones de red usa el investigado en aras de vislumbrar en donde puede estar localizada la información que se busca y cómo se podría acceder eventualmente a ella. En esta etapa también resulta particularmente importante tratar de establecer si la búsqueda se realizará en una red computacional complicada o simplemente en un computador aislado.

3. Formular una estrategia para conducir la búsqueda, teniendo en cuenta la información obtenida sobre el sistema computacional a inspeccionar. En este paso, se debe formular un plan de trabajo principal y uno de respaldo que contemplen por lo menos lo siguiente: Si la busqueda se realizará en el sitio en el que se encuentra el sistema a revisar o si por el contrario se removerá el hardware para inspeccionarlo en un laboratorio o en alguna locación diferente; si se realizarán copias de los discos duros o de archivos individuales y en general cual sería la estrategia a seguir si el hardware o el software inspeccionados resultan significativamente diferentes con respecto a las expectativas surgidas a partir de la información recopilada en la etapa anterior.

4. Como último paso para adelantar este tipo de búsquedas e inspecciones, el departamento de justicia de los Estados Unidos recomienda solicitar la autorización judicial consultando la estrategia trazada por el equipo y la información recopilada sobre el sistema a inspeccionar, de forma tal que se le indiquen al juez los procedimientos que se pretenden seguir para la recolección y asimiento del material probatorio. Estas consideraciones resultan muy importantes para los investigadores estadounidenses en la medida en que ellos deben redactar el borrador del *warrant*[44] o de la autorización judicial antes de acudir al juez. Para el caso

42 Ibidem.
43 Ibidem.

44 Un *warrant* en el common law es en un sentido amplio, un escrito o precepto expedido por una autoridad competente y de conformidad con la ley, en el que se encomienda la realización de un acto a un oficial o persona competente para realizarlo, dispensándolo de la responsabilidad por los daños que la realización de tal acto pudiere causar. "*A writ or precept from a competente authority in pursuance of law, directing the doing of an act, and adressed to an officer or person competent to do the act, and affording him protection from damage, if he does it*". Black, H. C. (1891). Dictionary of Law Containing Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern (p. 1234). Disponible en la base de datos Hein Online en la colección Legal Classics.

Colombiano, sería preciso traducir la anterior recomendación haciendo hincapié en el nivel de detalle que debe tener la solicitud de autorización para la recolección de evidencia que será puesta a consideración de la autoridad competente. En efecto, dada la complejidad de los procesos investigativos que recaen sobre soportes electrónicos, sería preciso obtener una autorización que permita llevar a cabo todos los procedimientos necesarios a la luz de la estrategia trazada anteriormente.

Además de las recomendaciones anteriores, el departamento de justicia hace ciertas alusiones a las objeciones y argumentos típicos que esgrimen las partes en los procesos que comprometen pruebas electrónicas. Estos argumentos, como veremos a continuación, son posibles nuevamente debido a las características de las pruebas electrónicas y por ende podrían ser ventilados también ante la jurisdicción Colombiana. Los autores de este trabajo consideramos que sería una valiosa herramienta para el investigador Colombiano contemplar este tipo de argucias con anticipación, en aras de blindar sus procedimientos de búsqueda y asimiento de material probatorio de los posibles ataques de las partes procesales. El manual del departamento de defensa clasifica los argumentos más comunes en tres tipos:

1. Los que cuestionan la integridad de las pruebas, arguyendo la posibilidad de que el material probatorio generado o consignado en medios electrónicos haya sido alterado, manipulado o dañado después de su creación. Este tipo de argumentos atacan la autenticidad e integridad del material probatorio fundándose en que los archivos de computadora pueden ser alterados fácilmente. Para evitar este tipo de cuestionamientos, el investigador puede hacer uso de medios estériles que permitan realizar imágenes o copias fidedignas de información o discos duros. Este tipo de medios estériles se conocen en inglés como *imaging tools* y usualmente son programas de computadora que pueden "copiar toda la información de un disco y hacerla susceptible de análisis forense"[45] sin alterarla.

2. Los que cuestionan la autenticidad de las pruebas, aduciendo dudas sobre la confiabilidad del programa de computadoras que generó los documentos o archivos obtenidos.

3. Los que se valen del anónimato propio de las pruebas electrónicas para poner en duda la identidad de su autor. Para enfrentar este tipo de argumentos, el investigador debe tomar todas las medidas posibles para superar el anonimáto de la prueba, valiéndose primordialmente de su experticio en computación.

Este documento de iniciativa gubernamental resulta particularmente importante para ilustrar la fuerte preocupación por parte del departamento de justicia y las agencias americanas en superar los retos propios de la evidencia digital. La tendencia en Estados Unidos es acordar procedimientos estándar que permitan mantener la evidencia incólume y que ofrezcan certeza sobre su "autenticidad, confiabilidad, completitud o suficiencia y conformidad con las leyes y reglas del poder judicial "(CANO, J. 2005).

Como se expresó anteriormente, existen muchas iniciativas tendientes a fijar estándares de buenas prácticas en materia de manipulación de evidencia digital en Estados Unidos[46]. No obstante, además de que escapa al alcance de este trabajo el tratar de hacer una recopilación o resumen de todas ellas, dicha tarea resultaría infructuosa

45 Mohd, M. (2000). An Overview Of Disk Imaging Tool In Computer Forensics. [Versión Electrónica], Pág, 3. Accesado en mayo de 2007 de http://www.niser.org.my/resources/disk_imaging.pdf.

46 Para más información sobre buenas prácticas en los Estados Unidos, se puede acceder a la página del grupo de trabajo científico sobre evidencia digital: http://ncfs.org/swgde/documents-.

en la medida en que la mayoría de esos procedimientos tienden a ser muy específicos en aras de sortear los retos a los que se puede enfrentar el investigador en el momento de recolectar o allegar pruebas a un determinado proceso en los tribunales americanos. Lo que se pretende en este trabajo es, por el contrario, dar luces sobre los principios básicos que rigen dichos procedimientos con el fin de que el investigador Colombiano entienda qué cuidados mínimos debe tener en el momento de buscar, recolectar o exponer pruebas electrónicas. En efecto, si se asume la responsabilidad de crear un estándar Colombiano, éste debería elaborarse consultando nuestra legislación en lo atinente a nuestras reglas de exclusión de la prueba, el régimen de la ilicitud e inconstitucionalidad de las mismas y previendo las formas en las que los operadores jurídicos explotaran las características de la prueba electrónica para restarle importancia en los tribunales Colombianos. El documento revisado es, a todas luces, un valioso esfuerzo por parte del gobierno americano en aras de dictar directrices a sus investigadores y agentes policiales, sobre las prácticas y consideraciones a seguir con el ánimo de que las pruebas electrónicas allegadas a procesos judiciales no sean descartadas tan fácilmente. Es una tarea imperiosa de nuestros organismos de investigación, estandarizar sus procedimientos y encauzar sus investigaciones de forma tal que las valiosas pruebas que se puedan hallar en soportes electrónicos no sean tachadas de falsas o excluidas de la valoración de los jueces.

En cuanto a la formación de los peritos y expertos, es claro en la literatura revisada que en Estados Unidos el entrenamiento de los mismos en tanto agentes del estado recae en las agencias denominadas "de justicia criminal". En efecto, "se han establecido unidades investigativas de criminalidad de alta tecnología en agencias como el *Federal Bureau of Investigation (FBI), Internal revenue Service (IRS),* en el Servicio secreto de los Estados Unidos y en la Oficina de investigaciones especiales de la fuerza aérea estadounidense"[47].

A manera de conclusión, podemos señalar algunos principios básicos y generales que se siguen en Estados Unidos en el momento de llevar a cabo procedimientos investigativos que impliquen la manipulación de evidencia digital. Dichos principios y pautas se reiteran en la mayoría de los estándares y directrices revisados:

1. Revisar las restricciones que aplican a la búsqueda y recolección de determinada evidencia, obteniendo las autorizaciones respectivas de autoridades competentes. (Véase SWGDE Best Practices for Computer Forensics Version 2.1, July 2006).

2. Antes de iniciar un determinado procedimiento que implique la manipulación u obtención de pruebas electrónicas debe consultarse a un especialista en computación forense[48].

3. "Los datos que se submitan para examen deben ser mantenidos de forma tal que se conserve su integridad".[49]

PERITAJE INFORMÁTICO Y MANIPULACIÓN DE EVIDENCIA DIGITAL EN AUSTRALIA

En una reunión del grupo de trabajo en telecomunicaciones e información de la colaboración económica asiático-pacífica, se dio a conocer un documento aportado por Australia en el que se presentaba el estándar Australiano de directri-

47 Myers, L. J. (2000). High Technology Crime Investigation: A Curricular Needs Assessment of the Largest Criminal Justice And Criminology Programs In The United States. Tesis Doctoral, Texas A&M University. p. 45.

48 Scientific Working Group on Digital Evidence. (2006). Best Practices For Computer Forensics [Versión Electrónica]. Accesado en Mayo de 2007 en la dirección http://ncfs.org/swgde/documents/swgde2006/Best_Practices_for_Computer_Forensics%20July06.pdf.

49 Ibídem.

ces y pautas para la manipulación de evidencia electrónica. En este acápite, revisaremos el estándar de manipulación de evidencia digital a la luz de dicho documento, que puede dar luces sobre el avance de la cooperación asiático pacífica (APEC) en los temas que nos ocupan.

Para efectos de este artículo, es preciso comenzar nuestra revisión de las directrices haciendo hincapié en ciertos principios que el documento aportado por Australia resalta como fundamentales para la administración de evidencia digital:

1. Asegurarse de que los procedimientos a seguir son idóneos para dar certeza sobre la autenticidad y no alteración de la evidencia, sobre la confiabilidad de los programas de computadora que generaron tales registros de evidencia, sobre la fecha y hora de la creación de los mismos, sobre la identidad de su autor y por último sobre la fiabilidad del procedimiento para su custodia y manipulación[50]. (AJOY, G. 2004).

2. "Recolectar información de forma adecuada desde una perspectiva forense"[51].

3. "Establecer procedimientos para la custodia y retención seguras de la información obtenida"[52]. Esto podría lograrse llevando registros de acceso y manipulación realizada a la información que se pretende usar como prueba (AJOY, G. 2004).

4. Determinar si se está manipulando registros originales o copias de los mismos. Así mismo, sería pertinente documentar apropiadamente cualquier tipo de acción tomada sobre los registros de evidencia. En este aspecto, el *paper* Australiano hace hincapié en que la evidencia original debe permanecer inalterada y que en el evento en que su alteración sea inevitable, se debe documentar dicha alteración adecuadamente.

5. Por último, se hace hincapié en que el personal comprometido en los procesos de producción, recolección, análisis y exposición de la evidencia "debe tener un entrenamiento apropiado, experiencia y calificaciones para cumplir sus roles".[53]

En cuanto al uso de imágenes de discos para el examen forense, tal como ocurre en USA, el artículo australiano resalta la importancia de realizar este tipo de procedimientos. En efecto, en él se cita una decisión judicial que fue significativamente influenciada por el hecho de que el demandante omitió realizar una imagen de disco y por el contrario, usó software que eliminó aleatoriamente siete u ocho por ciento de la información contenida en dicho dispositivo. (AJOY, G. 2004). Al final, la corte determinó que lo correcto habría sido "realizar una imagen del disco duro que recolectara cada pieza de información almacenada en el mismo"[54].

Así mismo, en materia de recolección de evidencia, el documento hace alusión (entre otros) a los siguientes estándares que son de particular importancia para nuestra investigación:

1. Los individuos involucrados en procesos de recolección de evidencia digital, deben tomar nota de sus procedimientos, de forma tal que puedan establecer en una corte, incluso años después de la recolección, qué acciones específicas se llevaron a cabo sobre los registros de evidencia. (AJOY, G. 2004)

2. Los individuos involucrados en procesos de recolección de evidencia digital deben ser capaces de discernir entre los datos de un

50 GHOSH, AJOY. *Guidelines for the Management of IT Evidence*. APEC Telecommunications and Information Working Group 29th Meeting. (21-26 March, 2004) Hong Kong, China. p. 12.
51 Ibídem.
52 Ibídem.
53 Ibídem.
54 Ibídem. p. 21. La decisión judicial citada por Ajoy es: *Gates Rubber Company v Bando Chemical Industries Ltd.* 167 FRD 90 (D. Colorado) at 90 and 112.

sistema que pueden ser útiles y aquellos que no lo son.

3. Cuando se recolecta evidencia digital, se debe intentar descubrir información de difícil visibilidad, en aras de obtener material forense recuperado[55] y se debe ser cuidadoso para no alterar este tipo de información de difícil acceso.

Entendidas las anteriores consideraciones, es preciso concluir nuevamente que la principal preocupación del artículo es la posibilidad de que, dadas las características de la prueba electrónica y de la evidencia digital, se le reste eficacia en las cortes. Por tal razón, se hace necesaria la creación de estándares y de directrices que permitan superar los retos típicos a los que se verá enfrentado un acervo probatorio constituido principalmente por pruebas electrónicas. Así mismo, en múltiples ocasiones el documento da cuenta de la importancia de la preparación y formación de expertos que sean capaces de manipular este tipo de pruebas de una manera adecuada.

EL CASO SINGAPUR

Aunque este artículo se ha centrado en la revisión de estándares y buenas prácticas, los autores consideramos pertinente resaltar una propuesta de la Academia de Leyes de Singapur[56] en cuanto a la aproximación legislativa a la regulación de los archivos de computadora como evidencia.

En primer lugar, la academia sugiere que cualquier regulación sobre este tema debe respetar el principio de neutralidad tecnológica que implica necesariamente la adopción de una postura prudente que reconozca la rapidez con la que cambia la tecnología. En ese sentido, el legislador debería evitar cualquier tipo de preferencia o inclinación hacia una tecnología en particular en aras de evitar que la legislación no contemple una tecnología ya existente o quede obsoleta muy rápidamente debido al veloz devenir de la tecnología.

La propuesta específica de la Academia de leyes de Singapur consistía en regular el tema sin sesgar la legislación únicamente hacia los computadores, con el fin de otorgarle a los registros electrónicos en general verdadera admisibilidad como prueba o evidencia. No obstante, se sugería incluir una lista enunciativa que le otorgara admisibilidad a ciertos tipos de evidencia electrónica en específico.

El caso Singapur ilustra claramente las dificultades con las que se enfrenta el legislador en el momento de regular este tipo de temas y su análisis puede ser de gran utilidad para el legislador Colombiano que ha sido particularmente renuente a abordar el tema de las pruebas electrónicas en específico. En efecto, en Colombia el tema se circunscribe a la equivalencia funcional de los documentos electrónicos, del original y de la firma. El principio del equivalente funcional, introducido por la ley 527 de 1999 "tiene como finalidad adaptar y darle la misma fuerza probatoria de los documentos consignados en papel a los documentos en formato de mensajes de datos, firmas electrónicas y demás conceptos tecnológicos"[57]. En virtud de dicho principio, un documento electrónico es un equivalente funcional de un documento consignado en papel y por ende debe ser aceptado como prueba documental en un proceso, sin consideración al medio en el que éste se encuentre almacenado.

55 Véase el acápite 2.2 del presente artículo.

56 SENG DANIEL. CHAKRAVARTHI, SRIRAM. *Computer Output as Evidence Final Report.* Singapure Academy Of Law. Disponible en: http://www.agc.gov.sg/publications/docs/Computer_Output_As_Evidence_Final_Dec_2004.pdf. Revisado en mayo de 2007.

57 PLAZAS RUEDA, Andrea y CANO, Jeimy. *Valoración de La Evidencia Digital: Análisis y Propuesta en el contexto de la administración de justicia en Colombia.* Revista de Derecho Comunicaciones y Nuevas Tecnologías. Volumen 1, Septiembre de 2006. p. 103.

Mucho se ha discutido sobre el sesgo tecnológico de la ley 527 de 1999 en cuanto a la preferencia de la firma digital, sin embargo, después de una revisión de la propuesta de la academia de leyes de Singapur, considero que una de las principales falencias de la ley 527 de 1999 y de nuestra legislación en general, es la ausencia de una disposición que permita dar certeza sobre qué tipos de evidencia electrónica son admisibles en una corte. En ese aspecto, la Academia Singapurense es muy acertada al proponer la inclusión de ciertas "presunciones" a manera de lista enunciativa (no taxativa) que permitan darle luces al juez sobre ciertos tipos de evidencia electrónica en específico que deben ser admitidos como prueba en una corte o tribunal. No obstante, la lista en cuestión no sería óbice para que otros tipos de evidencia digital sean admitidos en los estrados judiciales.

CONCLUSIONES

Sin perjuicio de las conclusiones realizadas a lo largo de este artículo, resulta pertinente hacer hincapié en que la mayoría de los estándares revisados buscan dictar ciertas pautas a los investigadores y peritos para que logren máximizar la posibilidad de éxito de sus búsquedas y para que logren la admisibilidad del material probatorio recolectado. En ese orden de ideas, algunos países han optado por estándarizar los procesos de búsqueda y recolección de evidencia digital como una forma de evitar la improvización y de guiar a sus funcionarios en aras de que puedan defender la idoneidad de sus procedimientos en un proceso judicial. Si se certifica el estricto cumplimiento de un estándar se evitaría exponer el fruto de una ardua investigación a las argucias típicas que se esgrimen en contra de las pruebas electrónicas. Dichas argucias, como sabemos, se valen de la mencionada volatilidad y facil alteración de la evidencia digital para poner en duda su vocación de ofrecer verdadera certeza sobre un determinado hecho.

El caso Estadounidense resulta pertinente para dar un vistazo a la forma en la que se deben vislumbrar las reglas de exclusión de la prueba teniendo en cuenta las características especiales de los procesos de recolección y asimiento de pruebas electrónicas. Los estándares Europeos, por su parte, nos enseñan la importancia de observar ciertos protocolos para la recolección de evidencia digital y la necesidad de que este tipo de procesos se conduzcan siempre con ayuda o supervisión de un perito en informática.

El estándar Australiano hace hincapié en la importancia de que las organizaciones administren correctamente sus registros electrónicos para dotarlos de verdadera eficacia probatoria y nos dicta ciertas pautas para llevar a cabo una exitosa recolección de evidencia.

Por último, una revisión de la propuesta de la academia de leyes de Singapur nos informa sobre la importancia de que el legislador aborde el tema de las pruebas electrónicas teniendo una clara perspectiva del rápido devenir de la tecnología y de la necesidad de ofrecer certeza sobre los tipos de evidencia electrónica que pueden ser admitidos como prueba en un tribunal.

BIBLIOGRAFÍA

ALTMARK, Daniel. *Informática y Derecho, Vol 1, Editorial Depalma. Buenos Aires, 1987, p. 6.*

BENCOMO YARINE, Edel. *Reseña De La Legislación Informática en Cuba. En: Alfa Redi, Revista de Derecho Informático. No. 102 Enero de 2007. Disponible en: http://www.alfa-redi.com/rdi-articulo.shtml?x=8408.*

BLACK, H. C. *(1891). Dictionary of Law Containing Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern (p. 1234). Disponible en la base de datos Hein Online en la colección Legal Classics.*

CANO, Jeimy. *Estado del arte del Peritaje Informático en Latinoamérica. En: Revista Alfa-Redi disponible en www.alfa-redi.org p. 8.*

CANO, Jeimy. *Evidencia Digital: Conceptos y Retos. En: Comercio Electrónico. GECTI. Editorial Legis. Bogotá, 2005. p. 185.*

CYBEX. *(2006). La Admisibilidad de las Pruebas Electrónicas Ante Los Tribunales. Revisado el 7 de mayo de 2007, disponible en: http://www.cybex.es/agis2005/docs/libro_aeec_sp.pdf.*

DE LA TORRE, juan y AGUD ANDREU sergio. *Pruebas Electrónicas: Una Nueva Realidad. En: E-Newsletter de Cybex. No 27. Abril de 2007.*

GHOSH, Ajoy. *Guidelines for the Management of IT Evidence. APEC Telecommunications and Information Working Group 29th Meeting. (21-26 March, 2004) Hong Kong, China. p. 12.*

MOHD, M. (2000). An Overview Of Disk Imaging Tool In Computer Forensics. [Versión Electrónica], p. 3. Accesado en mayo de 2007 de http://www.niser.org.my/resources/disk_imaging.pdf.

MYERS, L. J. (2000). High Technology Crime Investigation: A Curricular Needs Assessment of the Largest Criminal Justice And Criminology Programs In The United States. Tesis Doctoral, Texas A&M University. p. 45.

PARRA QUIJANO, JAIRO. *Manual De Derecho Probatorio. Décima Cuarta Edición. Librería Ediciones Del Profesional Ltda. Bogotá 2004. p. 43.*

PLAZAS RUEDA, Andrea y CANO, Jeimy. *Valoración de La Evidencia Digital: Análisis y Propuesta en el contexto de la administración de justicia en Colombia. Revista De Derecho Comunicaciones y Nuevas Tecnologías. Volumen 1, Septiembre de 2006. p. 103.*

REMOLINA ANGARITA, Nelson. *Desmaterialización, documento electrónico y centrales de registro.* En: Comercio Electrónico. GECTI. Editorial Legis. Bogotá, 2005. p. 150.

RÍOFRIO MARTINEZ VILLALBA, Juan. *La pretendida Autonomía del Derecho Informático.* En: Alfa Redi, Revista de Derecho Informático. No. 50 Septiembre de 2002. Disponible en: http://www.alfa-redi.com/rdi-articulo.shtml?x=1448.

RODRIGUEZ JOUVENCEL, MIGUEL. *Manual del Perito Médico. Fundamentos Técnicos y Jurídicos. Ediciones Díaz de Santos. Edición 2002. p. 251.*

SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE. *(2006). Best Practices For Computer Forensics [Versión Electrónica]. Accedido en Mayo de 2007 en la dirección http://ncfs.org/swgde/documents/swgde2006/Best_Practices_for_Computer_Forensics%20July06.pdf.*

SENG DANIEL. CHAKRAVARTHI, SRIRAM. *Computer Output as Evidence Final Report.* Singapure Academy Of Law. Disponible en: http://www.agc.gov.sg/publications/docs/Computer_Output_As_Evidence_Final_Dec_2004.pdf Revisado en mayo de 2007.

SOMMER, P. *(2005). DIRECTORS AND CORPORATE ADVISORS' GUIDE TO DIGITAL INVESTIGATIONS AND EVIDENCE [Versión Electrónica], Pág, 29. Accedido en Mayo de 2007 en la dirección http://www.iaac.org.uk/Portals/0/Evidence%20of%20Cyber-Crime%20v12-rev.pdf.*

TORRENTE, Diego. *CONFERENCIA AEEC: EN BUSCA DE UNA DEFINICIÓN PARA 'PRUEBA ELECTRÓNICA'. En: E-Newsletter de Cybex. No 27. Abril de 2007.*

United States Department of Justice. Computer Crime and Intellectual Property Section. Criminal Division. (2002) *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* Disponible en: http://www.cybercrime.gov/s&tsmanual2002.htm#_IB3_.