EL PERITAJE INFORMÁTICO Y LA EVIDENCIA DIGITAL EN COLOMBIA

CONCEPTOS, RETOS Y PROPUESTAS

Jeimy José Cano Martínez
(Coord.)
GECTI

UNIVERSIDAD DE LOS ANDES • FACULTAD DE DERECHO
EDICIONES UNIANDES

JEIMY JOSÉ CANO MARTÍNEZ

Ph. D., CFE. Miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI), Facultad de Derecho, Universidad de los Andes, Colombia. Ingeniero de Sistemas y Computación, Universidad de los Andes. Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Ph. D. en Business Administration, Newport University. Diplomado en Sistema Penal Acusatorio, Universidad Militar Nueva Granada, Colombia. Profesional certificado en Computer Forensic Analysis (CFA) del World Institute for Security Enhancement, Estados Unidos. Profesional acreditado como Certified Fraud Examiner (CFE) por la Association of Certified Fraud Examiners.

Monterrey, octubre 26 de 20

Muy apreciada y respetada Marilina:

Esta obra es producto de la mas reciente
investigacion del GECTI. Esperamos
que resulte de su interés y agradecemos
sus muy valiosos y bienvenidos
comentarios.

Un abrazo,

Nelson Remolina Angarita
Director del GECTI
Universidad de los Andes

EL PERITAJE INFORMÁTICO Y LA EVIDENCIA DIGITAL EN COLOMBIA

JEIMY JOSÉ CANO MARTÍNEZ
(COORDINADOR)

EL PERITAJE INFORMÁTICO Y LA EVIDENCIA DIGITAL EN COLOMBIA. CONCEPTOS, RETOS Y PROPUESTAS

GECTI

UNIVERSIDAD DE LOS ANDES – FACULTAD DE DERECHO
EDICIONES UNIANDES
BOGOTÁ, 2010

El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas / Jeimy José Cano Martínez, coordinador.-- Bogotá: Universidad de los Andes, Facultad de Derecho, Ediciones Uniandes, 2010.
372 p. ; 16 x 23 cm (Colección Biblioteca Jurídica Uniandina)

ISBN 978-958-695-492-1

1. Prueba (Derecho) – Investigaciones – Colombia 2. Derecho informático - Colombia 3. Delitos por computador – Legislación – Investigaciones - Colombia I. Cano Martínez, Jeimy José II. Universidad de los Andes (Colombia). Facultad de Derecho. Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática III. Universidad de los Andes (Colombia). Facultad de Derecho IV. Tít.

CDD 347.064 SBUA

Primera edición: mayo de 2010

Ediciones Uniandes
Carrera 1ª No. 19-27, edificio AU 6, piso 2
Bogotá, D. C., Colombia
Teléfono: 339 49 49 - 339 49 99, ext. 2133
http//:ediciones.uniandes.edu.co
Correo: infeduni@uniandes.edu.co

ISBN: 978-958-695-492-1

Diseño de la colección: Magda Salazar
Diagramación: Leonardo Cuéllar V.
Corrección de estilo: Julio Eduardo Mateus

Impresión y acabados: Editorial Kimpres Ltda.
Calle 19 sur No. 69 C-17, Bogotá, D. C.
Pbx: 413 6884 - Fax: 290 7539
info@kimpres.com
Bogotá, D. C., Colombia

Impreso en Colombia - Printed in Colombia

PRÓLOGO

El peritaje informático y la evidencia digital en Colombia. Conceptos, retos y propuestas es el quinto libro publicado por el Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes. Se trata de una obra, dirigida por el profesor Jeimy Cano Martínez, que reúne un conjunto de investigaciones especializadas sobre el peritaje informático y la evidencia digital.

El GECTI se ha propuesto aunar esfuerzos, compartir y difundir conocimientos para poner en marcha una articulación valiosa entre expertos de distintas disciplinas que le permita fomentar un trabajo multidisciplinario y establecer un puente entre la universidad y la sociedad con el fin de promover reflexiones y acciones en materia de Internet, la sociedad de la información, las telecomunicaciones y temas convergentes. En desarrollo de dicho objetivo, el profesor Cano se encargó de la definición temática y metodológica de los capítulos.

En el libro se analizan los conceptos fundamentales de la ley 527 de 1999 que son relevantes en materia de peritaje informático y evidencia digital. Posteriormente, se aborda el estudio nacional e internacional de

los aspectos que se deben tener en cuenta para valorar el precitado tipo de evidencia. A continuación, se realiza una revisión de las principales consideraciones sobre el estado actual del peritaje informático y los estándares de manipulación de pruebas electrónicas, así como del contexto de la formación del perito informático en el escenario internacional y su realidad en Colombia.

A partir de lo anterior, se plantean reflexiones sobre la formación de los jueces en temas de delito informático y la evidencia digital en el campo internacional y sus implicaciones en la administración de justicia colombiana, destacando la necesidad de una justicia especializada en la materia, para lo cual se ha presentado una propuesta dirigida a dicha formación.

Finalmente, los autores hacen una revisión de los delitos informáticos en Colombia, con particular énfasis en la ley 1273 de 2009, y analizan la noción de almacenamiento electrónico de la información, destacando los principales conceptos y técnicas de las investigaciones forenses en informática.

Eduardo Cifuentes Muñoz
Decano de la Facultad de Derecho
Universidad de los Andes

TABLA DE CONTENIDO

capítulo ii

valoración de la evidencia digital: análisis y propuesta en el contexto de la administración de justicia en colombia

capítulo iii

consideraciones sobre el estado actual del peritaje informático y los estándares de manipulación de pruebas electrónicas en el mundo

capítulo iv

contexto actual de la formación del perito informático en el escenario internacional y su realidad en colombia

CAPÍTULO V

LA FORMACIÓN DE LOS JUECES EN TEMAS DE DELITO INFORMÁTICO Y LA EVIDENCIA DIGITAL EN EL CONTEXTO INTERNACIONAL Y SUS IMPLICACIONES EN LA ADMINISTRACIÓN DE JUSTICIA EN COLOMBIA

capítulo vi

anotaciones sobre la ley 1273 de 2009

CAPÍTULO VII

EL CONCEPTO DE LA INFORMACIÓN ELECTRÓNICAMENTE ALMACENADA EN EL ORDENAMIENTO JURÍDICO COLOMBIANO: ANÁLISIS Y PROPUESTA PARA COLOMBIA

CAPÍTULO VIII

ESTRATEGIAS ANTIFORENSES EN INFORMÁTICA: RETOS Y REFLEXIONES

AGRADECIMIENTOS

El poeta y novelista James Joyce, citado por John Maxwell en su libro *Líder de 360 grados*, dice: "Su mente le devolverá lo que usted pone en ella", una frase ajustada exactamente a lo ocurrido con esta obra que usted tiene en sus manos.

Cuando iniciamos este proyecto de investigación en 2007 éramos conscientes de estar ante un reto importante, dada la realidad desbordante de unos hechos y frente al desafío de navegar en medio de lo desconocido. Gracias a la confianza del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) y de la Facultad de Derecho de la Universidad de los Andes, es posible entregar el resultado de muchas horas de trabajo y revisión, de numerosas reflexiones y debates, de considerables lecturas y modificaciones, el cual no busca otra cosa que tratar de mirar al futuro y ver cómo hacemos de la práctica del derecho y la tecnología un espacio conjunto para crear y construir.

Damos las gracias a todos los que creyeron en esta empresa académica; a la dedicación y entrega de cada uno de los estudiantes, hoy destacados abogados: Javier Pimentel, Andrea Rueda, Ángela Ramírez,

Martha Segrera y Luis Andrés Iregui, quienes se lanzaron a descubrir nuevas posibilidades y distinciones para el derecho moderno, sabiendo que, a pesar de la neblina densa que se presentaba, era posible llegar al destino trazado. Igualmente, muchas gracias al profesor Nelson Remolina Angarita, quien como integrante del equipo académico contribuyó con la redacción de algunos capítulos de la obra.

También nuestros agradecimientos a la Facultad de Derecho y en su nombre al decano, doctor Eduardo Cifuentes Muñoz, por la oportunidad para plasmar en este libro el resultado de nuestras inquietudes académicas, nuestras "locuras" conceptuales, fruto de ese deseo constante para ver más allá de la realidad y materializar de manera concreta y real lo expuesto en la misión de la Facultad: "promover estudiantes y profesionales competentes, críticos y comprometidos con la sociedad" y su entorno nacional e internacional. De la misma forma, expresamos nuestra gratitud a la doctora Tatiana González Abaunza, quien desde la Facultad de Derecho nos brindó apoyo incondicional y profesional para que la obra fuese publicada.

Jeimy J. Cano, Ph.D, cfe
Profesor distinguido
Miembro investigador del gecti
Facultad de Derecho
Universidad de los Andes
Bogotá, D. C.
Colombia

LOS AUTORES

JEIMY JOSÉ CANO MARTÍNEZ. Ph. D., CFE. Miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI), Facultad de Derecho, Universidad de los Andes, Colombia. Ingeniero de Sistemas y Computación, Universidad de los Andes. Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Ph. D. en Business Administration, Newport University. Diplomado en Sistema Penal Acusatorio, Universidad Militar Nueva Granada, Colombia. Profesional certificado en Computer Forensic Analysis (CFA) del World Institute for Security Enhancement, Estados Unidos. Profesional acreditado como Certified Fraud Examiner (CFE) por la Association of Certified Fraud Examiners. Contacto: jjcano@yahoo.com.

NELSON REMOLINA ANGARITA. Abogado y especialista en Derecho Comercial, Universidad de los Andes. Master of Laws, London School of Economics and Political Sciences. Doctorando en Ciencias Jurídicas, Pontificia Universidad Javeriana. Profesor asociado, Facultad de Derecho de la Universidad de los Andes. Fundador y director del Grupo

de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) [http://gecti.uniandes.edu.co/], Facultad de Derecho de la Universidad de los Andes. Director de la Especialización en Derecho Comercial, Facultad de Derecho de la Universidad de los Andes. Contacto: nremolin@uniandes.edu.co.

ANDREA RUEDA. Abogada, Universidad de los Andes.

JAVIER PIMENTEL. Abogado, Universidad de los Andes.

ÁNGELA RAMÍREZ. Abogada, Universidad de los Andes.

MARTHA SEGRERA. Abogada, Universidad de los Andes.

LUIS ANDRÉS IREGUI. Abogado, Universidad de los Andes.

INTRODUCCIÓN

Afirma Russell Ackoff en su libro *Cápsulas de Ackoff* que la creatividad es "la habilidad para identificar restricciones autoimpuestas, removerlas y explorar las consecuencias de la remoción". En ese contexto, este libro trata de confrontar las restricciones propias de dos disciplinas, las tecnologías de la información y la comunicación (TIC) y el derecho, como una forma de cuestionarnos sobre las posibilidades que se pueden abrir cuando removemos los límites de cada una de ellas y experimentamos la novedad de su complementariedad y la exigente ruta para construir posibilidades donde otros no las ven.

En tal sentido, el Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI), de la Facultad de Derecho de la Universidad de los Andes, busca constantemente abrir reflexiones interdisciplinarias y multidisciplinarias que procuren propuestas aplicadas a la realidad colombiana y latinoamericana de tal forma que se establezcan puntos de encuentro de diversas perspectivas que promuevan avances efectivos entre las TIC y las ciencias jurídicas.

Confrontando la realidad actual del incremento de la cibercriminalidad, de la evolución de los ataques informáticos de los intrusos, el avance de una delincuencia organizada y tecnificada, así como la realidad concreta de un mundo de transacciones digitales y electrónicas, se hace necesario revisar las consecuencias prácticas para el derecho y su relación con una

sociedad de la información y del conocimiento. Por lo tanto, el estudio de las mejores prácticas para el manejo de la evidencia digital, la formación de los peritos informáticos, la actualización de los jueces en temas como el delito informático y la evidencia digital, así como la revisión de las técnicas antiforenses, se hacen temáticas fundamentales para entender cómo el derecho y las tecnologías de la información comparten escenario con el fin de avanzar en el entendimiento de las nuevas condiciones de la delincuencia ahora en medios digitales.

Dado lo anterior, los autores de este libro estamos decididos a evitar la zona de confort y lanzarnos a proponer un análisis sobre esta nueva realidad, decirle a los "malos" que avanzamos tan rápido como ellos —*aunque no sabemos si suficientemente*— para comprender sus estrategias y ofrecerle una nueva excusa a la comunidad científica para repensar lo que conocemos y sugerir los cambios que sean requeridos con el objetivo de vigorizar el discurso jurídico en Internet y los avances tecnológicos frente al reto permanente de la evolución de la sociedad y las TIC.

Fieles a la tradición de innovación y visión de futuro de la Facultad de Derecho de la Universidad de los Andes, se presenta esta obra que busca anticipar nuevas preguntas y oportunidades para crear un nuevo *momentum* en la disciplina jurídica latinoamericana que nos permita avanzar en la predicción del mañana, lo cual no es otra cosa que lanzarnos a identificar nuevas propuestas, opciones novedosas y combinaciones de ideas y conceptos no convencionales para continuar aprendiendo de ese derecho emergente denominado derecho informático.

Jeimy J. Cano, Ph.D, CFE
Profesor distinguido
Miembro investigador del GECTI
Facultad de Derecho
Universidad de los Andes
Bogotá, D. C.
Colombia

CAPÍTULO I

CONCEPTOS FUNDAMENTALES DE LA LEY 527 DE 1999

Nelson REMOLINA ANGARITA*

La firma digital no es mala;
lo malo es imponerla por ley,
*a la fuerza, a las malas***

I. INTRODUCCIÓN

La regulación colombiana evidencia que la ley 527 de 1999 no fue la primera norma que trató lo concerniente a derecho y tecnología.[1] Una labor de "arqueología jurídica" podría concluir que fue la ley 8ª de 1970 la pionera en la materia al autorizar en el artículo 7° al presidente de la república para, entre otras, "adoptar las medidas necesarias para generalizar el *uso del computador electrónico* en los trámites administrativos

* El autor agradece los aportes y comentarios del doctor Rafael Hernando Gamboa Bernate a gran parte de este texto.

** Remolina Angarita, Nelson, "Falacias en torno a las discusiones de la firma digital", en *Ámbito Jurídico*, núm. 283, 2009, p. 15. Disponible en: http://gecti.uniandes. edu.co/columna.php?Op=columna.

[1] Éstas son algunas normas, expedidas con anterioridad a la ley 527 de 1999, que trataban temas sobre la materia en cuestión: leyes 8 de 1970, 27 de 1990 y 270 de 1996; decretos 1748 de 1995 y 1094 de 1996.

relacionados con los impuestos nacionales y poner especial énfasis en el mejoramiento y organización de las oficinas de Cobranzas y Ejecuciones Fiscales".

Con posterioridad a la ley 527, el marco legal colombiano se viene nutriendo de normas[2] relacionadas con mensajes de datos, firmas digitales, firmas electrónicas, entidades de certificación, tecnologías de información y comunicación, protección de datos personales, delitos informáticos, antecedentes disciplinarios y judiciales electrónicos, títulos valores electrónicos, teletrabajo, contratación electrónica, nombres de dominio, gobierno electrónico, factura electrónica, voto electrónico, y la utilización de medios electrónicos e informáticos en el cumplimiento de las funciones de Administración de Justicia. Esto pone de presente no sólo la inmersión masiva de lo "electrónico" en el sistema jurídico del país sino que cada día gran parte de los asuntos jurídicos cotidianos guardan relación con la amalgama derecho-tecnología.

La ley 527 de 1999 es producto de la labor de armonización que organismos internacionales han liderado con la finalidad de lograr a nivel mundial un consenso sobre fundamentos jurídicos mínimos para el desarrollo del comercio electrónico y el uso de los mensajes de datos como una nueva forma jurídica válida de manifestar la voluntad y como medio de prueba. La Organización de las Naciones Unidas (ONU), a través de la Comisión de las Naciones Unidas para el Desarrollo Mercantil Internacional (CNUDMI)[3] (o Uncitral, su acrónimo en inglés), publicó en 1996 la Ley Modelo sobre Comercio Electrónico, cuyos principales propósitos son los siguientes: 1) "ofrecer al legislador nacional un conjunto de reglas aceptables en el ámbito internacional que le permitan

[2] Las normas pueden ser consultadas en http://gecti.uniandes.edu.co/legislacion.php.

[3] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. Su principal función es la de fomentar la armonización y la unificación progresivas del derecho mercantil internacional.

[...] crear un marco jurídico que permita un desarrollo más seguro de las vías electrónicas de negociación designadas por el nombre de comercio electrónico",[4] y 2) "conceder igualdad de trato a los usuarios de mensajes consignados sobre un soporte informático que a los usuarios de la documentación consignada sobre papel".[5]

La precitada ley es una disposición cardinal en todo lo relacionado con el uso de los mensajes de datos como medio mediante el cual se manifiestan la voluntad y el soporte de documentos electrónicos. De allí surgieron equivalentes funcionales centrales para cualquier actividad y reglas atinentes a lo denominado evidencia digital o electrónica. Su importancia es indiscutible, razón para iniciar este libro haciendo referencia a ciertos tópicos trascendentales de ella que serán objetos de consideraciones a lo largo de la obra.

A. Principales aspectos de la ley 527 de 1999

La ley 527 de 1999 constituye el marco jurídico integral y general que avala, salvo algunas excepciones, el uso de los mensajes de datos en todas las actividades de los sectores público y privado. Su importancia es indiscutible, sin perjuicio de que con anterioridad a ella existieran ya algunas normas sectoriales que trataban ciertas cuestiones relacionadas con temas como la desmaterialización, la factura electrónica, la Administración de Justicia y los medios electrónicos, entre otros. En las siguientes líneas se hará referencia a varios de los principales aspectos de la citada ley.

[4] Los problemas básicos detectados en su momento y que se quieren solucionar con la ley modelo fueron los siguientes: 1) no validez jurídica al uso de los mensajes de datos como medio para manifestar la voluntad, 2) no aceptación de los datos almacenados en soportes informáticos como prueba en los litigios; 3) exigencia normativa y práctica de que los documentos estuviesen firmados o consignados sobre papel.

[5] Tanto la ley modelo como su guía explicativa pueden consultarse en http://www.uncitral.org/sp-index.htm.

1. Ámbito de aplicación

El campo de acción de la ley va más allá de las operaciones comerciales a través de medios electrónicos (comercio electrónico). Aunque regula aspectos de dicha materia y es conocida como la *ley de comercio electrónico,*[6] fue redactada de manera que comprenda, salvo las dos únicas excepciones que explícitamente menciona,[7] todas las actividades en donde se involucre el uso de mensajes de datos.[8] La ley 527, por ejemplo, tiene aplicación en las actividades del Estado con otras entidades estatales y con los particulares. Lo anterior se deriva del texto de la norma avalado y desarrollado en sentencias de la Corte Constitucional, así como por algunos conceptos de entidades públicas que hacen referencia a la ley aludida.[9] La Corte, concretamente, señaló: "[...] la ley 527 de 1999 no se restringe a las operaciones comerciales sino que hace referencia en forma genérica al acceso y uso de los mensajes de datos, lo que obliga a una comprensión sistemática de sus disposiciones con el conjunto de normas que se refieren a este tema dentro de nuestro ordenamiento jurídico".[10]

[6] Este término no sólo es utilizado por el común de la gente sino que también nuestros jueces lo emplean para referirse (de manera imprecisa o parcial) a la ley 527 de 1999. Así, el Consejo de Estado, mediante concepto 1376 del 11 de diciembre de 2001, da a entender que la ley 527 rige sólo el "comercio electrónico" y que ésta no contiene los postulados fundamentales para el uso de los mensajes de datos y las firmas digitales en todas las actividades hechas por particulares entre sí o con el Estado.

[7] 1) Las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales; y 2) Las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón del riesgo que implica su comercialización, uso o consumo.

[8] Cfr. ley 527 de 1999, artículo 1°.

[9] Por ejemplo, consultar el concepto 1007028, del 21 de marzo de 2001, de la Superintendencia de Industria y Comercio.

[10] Colombia, Corte Constitucional (2001), "Sentencia C-831".

Los mensajes de datos[11] son el núcleo fundamental de la ley porque se convierten en otro medio jurídicamente válido de manifestar la voluntad y, por ende, de realizar cualquier actividad (contratos). Su concepto legal[12] se redactó de manera que abarque los antiguos, actuales y futuros medios que permitan crear, archivar y comunicar información.

2. Principios

Existe un grupo de principios que irradian el alcance e interpretación de la ley. Algunos están incorporados explícitamente en ésta, mientras que otros forman parte de los mencionados en la Ley Modelo sobre Comercio Electrónico, de la Uncitral, los cuales no son sólo un elemento de interpretación sino un eje orientador en la fijación de algunas políticas públicas y de la reglamentación sobre la materia. Dentro de los principales principios se destacan los siguientes: internacionalidad, primacía de la autonomía de la voluntad, equivalencia funcional y neutralidad tecnológica. Cada uno de ellos será explicado a continuación.

a) *Internacionalidad*

El artículo 3° de la ley 527 envía un mensaje al operador de la ley (jueces, abogados y autoridades, entre otros) para que al momento de interpretarla siempre tenga en cuenta los principios y objetivos que inspiraron dicha regulación, así como la connotación que ella ha adquirido en el contexto internacional. Con esto se pretende que la labor interna-

[11] Es decir, a "toda 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" (artículo 2°, literal 2).

[12] Cfr. ley 527 de 1999, artículo 2°, literal a).

cional de armonización de normas no se diluya vía interpretación local de cada operador.

En virtud de lo anterior, el citado artículo ordena que a la hora de ser interpretada la ley deben tenerse en cuenta los siguientes factores: 1) su origen internacional; 2) la necesidad de promover la uniformidad de su aplicación, y 3) la observancia de la buena ley. Para el caso de temas regidos por la ley pero que no estén explícitamente resueltos por ella, se han de tener en cuenta los principios generales en que dicha norma se inspira, tales como: "[...] 1) facilitar el comercio electrónico en el interior y más allá de las fronteras nacionales; 2) validar las operaciones efectuadas por medio de las nuevas tecnologías de la información; 3) fomentar y estimular la aplicación de nuevas tecnologías de la información; 4) promover la uniformidad del derecho aplicable en la materia; y 5) apoyar las nuevas prácticas comerciales".[13]

Según la Uncitral, el artículo 3° de la ley en comento sigue lo señalado en el artículo 7° de la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías.

b) *Primacía de la autonomía de la voluntad*

La ley da prevalencia a la autonomía de la voluntad de las partes[14] sobre aspectos fundamentales en la realización de actividades a través del intercambio de mensajes de datos, a saber: ¿Cuándo se entiende perfeccionado un contrato electrónico? ¿Cuándo se entiende recibido el mensaje de datos? ¿Desde dónde se entienden enviados o recibidos los mensajes de datos? ¿Cómo sabrán las partes que el mensaje fue efectivamente enviado o recibido? ¿Cuándo una parte debe entender

[13] Cfr. Ley Modelo sobre Comercio Electrónico, de la Uncitral.

[14] Cfr. ley 527 de 1999, artículo 4°.

que el mensaje de datos recibido proviene de determinada persona y no de otra? ¿Cómo tener certeza de que un mensaje de datos fue enviado o recibido por la persona indicada y no por un tercero? ¿Si el destinatario recibe varios mensajes de contenido idéntico y provenientes del mismo remitente se debe entender que se trata de copias, o de que estamos frente a mensajes diferentes? ¿Cómo establecer que el contenido del texto no fue alterado o modificado? ¿Cómo determinar que durante la transmisión del mensaje de datos su contenido no fue leído por terceros?

La respuesta a estos interrogantes comprende un aspecto cardinal en el uso y comunicación de los mensajes, como lo es la absoluta certeza en cuanto a la transmisión de éstos y respecto de la integridad y confidencialidad del contenido de los mensajes de datos.

De no pactar nada las partes, en virtud del principio de la autonomía, entonces se dará aplicación a las respuestas que para cada caso trae la ley en los artículos 16 a 25.

c) *La equivalencia funcional*

Los equivalentes funcionales son los pares de instituciones del mundo material en el contexto digital. Se basan en un análisis de los objetivos y funciones del requisito tradicional con miras a determinar la manera de satisfacer sus fines en el contexto tecnológico. Así por ejemplo, a partir del conocimiento de las funciones y la labor jurídica que cumple el papel[15] como medio físico se diseñó una solución técnico-jurídica en

[15] Un documento en papel procura cumplir, entre otras, las siguientes funciones: 1) proporciona legibilidad a todos; 2) asegura su inalterabilidad a lo largo del tiempo; 3) permite su reproducción a fin de que cada una de las partes disponga de un ejemplar de lo escrito; 4) facilita la autenticación de los datos consignados suscribiéndolos con una firma; y 5) proporciona una forma aceptable para su presentación ante las autoridades públicas y los tribunales.

un medio electrónico que cumpla los mismos cometidos y, además, le imprima al documento electrónico las bondades propias de la tecnología (ahorro de tiempo, etcétera).

La ley 527 de 1999 no buscó establecer un equivalente informático para cada clase de documento, sino que incorporó pautas y condiciones aplicables a cualquier situación. La ley consagra los equivalentes funcionales[16] de escrito, firma y original en el contexto digital. Con éstos se busca que dichas instituciones cumplan las mismas funciones que tienen mediante el uso de medios tradicionales. Para la Corte Constitucional, la ley 527 "adoptó el criterio flexible de 'equivalente funcional', que tuviera en cuenta los requisitos de forma, fiabilidad, inalterabilidad y rastreabilidad, que son aplicables a la documentación consignada sobre papel, ya que los mensajes de datos por su naturaleza, no equivalen en estricto sentido a un documento consignado en papel".[17]

Los artículos 6°, 7° y 8° de la ley comparten una misma estructura en el sentido de señalar los requisitos o condiciones que debe cumplir un mensaje de datos para que entenderse que es "escrito", está "firmado" y se trata de un "original", tal como sucede con los documentos en medio físico.

d) *Neutralidad tecnológica*

Este principio reconoce algo evidente: la tecnología cambia constantemente. Si la ley se "casa" con una tecnología en particular, muy seguramente la norma quedará obsoleta pronto. Por eso es trascendental que las autori-

[16] Un desarrollo completo y crítico de este tema se puede encontrar en el artículo: Umaña Chaux, Andrés Felipe, "Algunos comentarios sobre el principio del equivalente funcional en la ley 527 de 1999", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, núm. 1, abril de 2005.

[17] Colombia, Corte Constitucional (2000), "Sentencia C-662". En igual sentido, consultar los siguientes conceptos de la Superintendencia de Industria y Comercio: 1007028, del 21 de marzo de 2001, y 3046333, del 25 de junio de 2003.

dades competentes observen este principio como, entre otras, una técnica legislativa y un factor relevante a la hora de valorar la evidencia digital.

La ley 527 exige algunos requisitos técnicos fundamentales, pero no señala la tecnología específica que se deba utilizar. Así las cosas, si la ley requiere utilizar tecnologías confiables para garantizar la integridad de un mensaje de datos, el operador puede escoger la que desee, siempre y cuando sea fiable a la luz del estado de la técnica y del momento histórico.

El artículo 26 de la ley 962 de 2005 es un ejemplo de una disposición legal explícitamente neutral en la medida en que no exige una tecnología concreta respecto de las facturas electrónicas: "[...] para todos los efectos legales, la factura electrónica podrá expedirse, aceptarse, archivarse y en general llevarse usando cualquier tipo de tecnología disponible, siempre y cuando se cumplan todos los requisitos legales establecidos y la respectiva tecnología que garantice su autenticidad e integridad desde su expedición y durante todo el tiempo de su conservación".

Este principio es crucial para el desarrollo y la competitividad de las actividades que se realicen a través del uso de las tecnologías. Por eso la "neutralidad tecnológica" es uno de los principios orientadores de la ley 1341 de 2009, que según el numeral 6 del artículo 2°, obliga al Estado a "garantizar la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible".

3. Reconocimiento jurídico de los mensajes de datos

Si existió duda sobre la validez jurídica de los mensajes de datos, el artículo 5° de la ley la elimina. Para la Corte Constitucional "el mensaje

de datos como tal debe recibir el mismo tratamiento de los documentos consignados en papel, es decir, que debe dársele la misma eficacia jurídica, por cuanto el mensaje de datos comporta los mismos criterios de un documento".[18] Ahora bien: si se da validez jurídica al medio que se utiliza para generar, enviar o archivar información, no quiere ello decir que automáticamente se dé plena aceptación al contenido incorporado en dicho medio,[19] porque éste pudo ser objeto de manipulaciones, fraudes, etcétera, lo cual también sucede con el contenido de documentos tradicionales.

El artículo 44[20] de la ley 527 otorga validez no sólo al contenido del texto del mensaje, sino a otros textos a los cuales hace referencia, pero sin que se transcriba su contenido. De esta manera, el texto por remisión cuenta con el mismo grado de validez jurídica como si fuese parte del texto del mensaje de datos. En este sentido, afirma la Uncitral:

> [...] las comunicaciones electrónicas están estructuradas normalmente de tal forma que se intercambian grandes cantidades de mensajes, cada uno de ellos con un breve contenido de información, y basándose con mucha mayor frecuencia que los documentos escritos en remisiones a información que puede obtenerse en otro lugar. No debe someterse a los usuarios de las comunicaciones electrónicas a la engorrosa obligación de sobrecargar sus mensajes de datos con abundante texto si pueden aprovechar fuentes externas de información, como bases de datos, glosarios o listas de códigos, y utilizar abreviaturas, códigos y otras remisiones a dicha información.

[18] Colombia, Corte Constitucional (2000), "Sentencia C-662 del 8 de junio". En este mismo sentido, consultar el concepto 3046333, del 25 de junio de 2003, de la Superintendencia de Industria y Comercio.

[19] Establece la Uncitral: "La forma en que se haya conservado o sea presentada cierta información no podrá ser aducida como única razón para denegar eficacia jurídica, validez o fuerza ejecutoria a esa información".

[20] Declarado exequible mediante sentencia C-662 del 8 de junio de 2000, de la Corte Constitucional.

4. Documento físico original y documento electrónico original

Tradicionalmente el concepto de documento lo vinculamos a un *corpus* o soporte material que plasma, representa o incorpora una expresión, un derecho, una obligación, etcétera. Ese corpus se ha considerado como la base esencial o el ser mismo del documento.

Dentro de las acepciones sobre la naturaleza del documento se destacan la teoría del escrito y la teoría de la representación. Según la primera, el documento siempre es un escrito, en algún soporte permanente o durable (tradicionalmente el papel). De conformidad con la teoría de la representación, el documento no es solamente un escrito sino todo objeto representativo o que pueda informar sobre un hecho o sobre otro objeto. Desde esta óptica, el concepto de documento no se restringe a la naturaleza del soporte, ni a la forma escrita como único elemento material. Esta última teoría es acogida por nuestra legislación al expresar que documento es todo objeto mueble que tenga carácter representativo o declarativo sin exigirse la presencia de un soporte material de él. En efecto, a la luz del artículo 251 del Código de Procedimiento Civil, los documentos son "escritos,[21] impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares". Respecto del término escrito, la ley

[21] La ley 527 de 1999 trata los términos "escrito" y "documento emitido en papel" en forma equivalente. En efecto, refiriéndose a los documentos de transporte, en el artículo 27 incluye expresamente dicha expresión para significar que en los casos donde la ley requiera que alguno de los actos enunciados en el artículo 26 de la citada ley "se lleve a cabo por escrito o mediante documento emitido en papel, ese requisito quedará satisfecho cuando el acto se lleve a cabo por medio de uno o más mensajes de datos".

prevé un equivalente funcional,[22] para cuya definición se examinaron, de una parte, la naturaleza de las exigencias legales de que determinadas operaciones comerciales o documentos consten por escrito y, de otra parte, las razones por las cuales se solicita la presentación de un escrito.[23] Con esa información se establecieron las pautas tecnológico-jurídicas mínimas que deben cumplir los mensajes de datos electrónicos para suplir éstos el requisito de un "escrito", centrándose en el concepto básico de que la información se reproduce y lee.

Según nuestra legislación, un documento original corpóreo "es la fuente primaria de información con todos los rasgos y características que permiten garantizar su autenticidad e integridad".[24] El documento será auténtico "cuando existe certeza sobre la persona que lo ha elaborado, manuscrito o firmado".[25] En el contexto digital el concepto de original no se vincula únicamente con la fuente primaria, sino también con el concepto de integridad del contenido. El artículo 8° de la ley 527 de 1999 considera original al documento electrónico que no ha sido alterado o

[22] Cfr. artículo 6°, declarado exequible mediante sentencia C-831, del 8 de agosto de 2001, de la Corte Constitucional. En la sentencia C-356 de 2003 la Corte realiza un estudio sobre el documento electrónico para efectos penales. El artículo 25 del decreto 2170 de 2002 constituye una aplicación explícita de este equivalente en materia de contratación estatal electrónica.

[23] Entre las principales razones, los antecedentes de la ley destacan las siguientes: "1) dejar una prueba tangible de la existencia y la naturaleza de la intención de las partes de comprometerse; 2) alertar a las partes ante la gravedad de las consecuencias de concluir un contrato; 3) proporcionar un documento que sea legible para todos; 4) proporcionar un documento inalterable que permita dejar constancia permanente de la operación; 5) facilitar la reproducción de un documento de manera que cada una de las partes pueda disponer de un ejemplar de un mismo texto; 6) permitir la autenticación, mediante la firma del documento, de los datos en él consignados; 7) proporcionar un documento presentable ante las autoridades públicas y los tribunales; 8) dar expresión definitiva a la intención del autor del 'escrito' y dejar constancia de dicha intención; 9) proporcionar un soporte material que facilite la conservación de los datos en forma visible; 10) facilitar las tareas de control o de verificación ulterior para fines contables, fiscales o reglamentarios; y 11) determinar el nacimiento de todo derecho o de toda obligación jurídica cuya validez dependa de un escrito".

[24] Artículo 3° de la ley 594 de 2000, "por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".

[25] Ley 794 de 2003, artículo 26.

modificado desde el momento en el cual se compuso por primera vez ("integridad"), pero no exclusivamente al primer documento creado.

En el "mundo" digital no se puede entender como documento original únicamente aquel en el que por primera vez se consigna la información, principalmente porque en la práctica el destinatario de un documento enviado vía electrónica recibe una copia y el remitente se queda con el que, en el contexto tradicional, conocemos como original. Sobre este punto, la misma Uncitral señaló en la nota explicatoria de la Ley Modelo sobre Comercio Electrónico: [...] "si por 'original' se entiende el soporte en el que por primera vez se consigna la información, sería imposible hablar de mensajes de datos 'originales', pues el destinatario de un mensaje de datos recibiría siempre una copia del mismo".

Nótese que el término "endoso" del artículo 9°[26] no hace referencia a la forma de negociación de títulos valores a la orden, sino, por ejemplo, a eventuales procedimientos o protocolos electrónicos para enviar o reenviar un mensaje de datos. Para la Uncitral,

> [...] mientras el contenido de un mensaje de datos sea completo y esté inalterado, las adiciones que sea necesario introducir no afectarán a su calidad de "original". Así, cuando se añada un certificado electrónico al final de un mensaje de datos "original" para certificar que es el "original" o cuando la red informática utilizada inserte automáticamente ciertos datos de transmisión al principio y al final de cada mensaje de datos transmitido, esas adiciones se considerarían escritos complementarios adjuntados a un escrito "original" o serían asimiladas al sobre y los sellos utilizados para enviar ese escrito "original".

[26] Este artículo establece que la información consignada en un mensaje de datos es íntegra si ha permanecido completa e inalterada.

5. Prueba y archivos electrónicos

El artículo 10[27] de la ley 527 acepta jurídicamente los mensajes de datos como otro medio de prueba que debe ser admitido y considerado por los jueces y los funcionarios públicos.[28] Sobre este aspecto la Corte Constitucional ha señalado:

> [...] cuando la ley 527 hace referencia a la definición de documentos del Código de Procedimiento Civil, le otorga al mensaje de datos la calidad de prueba, permitiendo coordinar el sistema telemático con el sistema manual o documentario, encontrándose en igualdad de condiciones en un litigio o discusión jurídica, teniendo en cuenta para su valoración algunos criterios como: confiabilidad, integridad de la información e identificación del autor.[29]

Los empresarios y las organizaciones deben adoptar medidas tecnológico-administrativas con miras a que la información contenida en medios electrónicos no sea cuestionada a la hora de ser presentada como prueba, por la falta de diligencia en la implementación de protocolos de seguridad y de tecnología apropiada para la creación, circulación y archivo de documentos electrónicos. Esto sucedería si, por ejemplo, no se ha utilizado la tecnología adecuada para mantener y garantizar frente a terceros, las autoridades y los jueces, la autenticidad, integridad e inalterabilidad de los documentos que día a día incorporan una organización o un comerciante en sus archivos.[30]

[27] Declarado exequible mediante sentencia C-662, del 8 de junio de 2000, de la Corte Constitucional.

[28] Consultar el concepto 1007028, del 21 de marzo de 2001, de la Superintendencia de Industria y Comercio.

[29] Colombia, Corte Constitucional (2000), "Sentencia C-662 de 2000".

[30] Mayor detalle sobre la importancia de este aspecto en la gestión empresarial puede ser consultado en: Rodríguez Parra, César Felipe, "Documentos electrónicos como pruebas claves en litigios empresariales", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, núm. 1, 2005.

En adición a la sana crítica, el artículo 11[31] establece los criterios a tomar en cuenta para *valorar probatoriamente un mensaje de datos*. Debe tenerse presente que seguridad y confiabilidad son aspectos fundamentales del derecho probatorio en el contexto digital. Si los documentos que pretendemos utilizar como prueba carecen de estos elementos, muy seguramente estarán destinados a no tener ninguna incidencia probatoria en un proceso.[32]

El artículo 12[33] consagra los mínimos que caracterizarán los archivos electrónicos y las reglas para la conservación de la información. En el inciso 1) se reproducen las condiciones enunciadas en el artículo 6° para poder un mensaje de datos satisfacer la regla que exige la presentación de un escrito. En el inciso 2) se ordena adoptar medidas apropiadas para garantizar la integridad de la información. El inciso 3) pretende el contarse con información adicional al texto del mensaje de modo que permita identificarlo en un momento dado teniendo en cuenta su origen, destino, fecha y hora, tanto de creación como de envío y de recepción, etcétera.

El artículo 28 de la ley 962 de 2005 recalca:

> [...] los libros y papeles del comerciante deberán ser conservados por un período de diez (10) años contados a partir de la fecha del último asiento, documento o comprobante, pudiendo utilizar para el efecto, a elección del comerciante, su conservación en papel o en cualquier medio técnico, magnético o electrónico que garantice su reproducción exacta.
>
> Igual término aplicará en relación con las personas, no comerciantes, que legalmente se encuentren obligadas a conservar esta información.

[31] Declarado exequible mediante sentencia C-662, del 8 de junio de 2000, de la Corte Constitucional.

[32] Consultar la sentencia C-662 de 2000, de la Corte Constitucional, y el concepto 3046333, del 25 de junio de 2003, de la Superintendencia de Industria y Comercio.

[33] Declarado exequible mediante sentencia C-662, del 8 de junio de 2000, de la Corte Constitucional.

Lo anterior sin perjuicio de los términos menores consagrados en normas especiales.

Esta disposición deja sin efecto el procedimiento de reproducción y destrucción de documentos previsto en el artículo 60 del Código de Comercio y las disposiciones contenidas en el artículo 134 del decreto 2649 de 1993 y en los artículo 2° y 3° del decreto 2620 de 1993.[34]

II. LA FIRMA ELECTRÓNICA Y LA FIRMA DIGITAL: REALIDADES Y RESTRICCIONES

Desde hace décadas el legislador ha previsto como firma otros medios diferentes a la tradicional firma autógrafa o manuscrita que se menciona, entre otras, en el artículo 826 del Código de Comercio y el parágrafo del artículo 28 de la ley 527 de 1999:

La firma es, pues, requisito imprescindible para que un documento tenga valor probatorio, ya que sin ella, salvo aceptación expresa de la parte o de sus causahabientes —según el caso—, no podrá establecerse con certeza quién es el autor, esto es, lisa y llanamente su autenticidad, siendo necesario recordar que, por firma, se entiende "la expresión del nombre del suscriptor o de alguno de los elementos que la integren o de un signo o símbolo empleado como medio de identificación personal" (C. de Co., art. 826), omnicomprensiva noción —*ex lege*— que está a tono, en la hora de ahora, con el empleo de los adelantos tecnológicos (cibernéticos, robóticos, informáticos, etc.), en virtud de los cuales se ha desarrollado el concepto de firma electrónica o digital que, según la *ley 527 de 1999*, se acota de paso, tiene idéntica fuerza y efectos de la

[34] En este sentido, ver el concepto 5054043, del 12 de octubre de 2005, de la Superintendencia de Industria y Comercio.

firma manuscrita, cuando se reúnan los requisitos —claro está— allí señalados relativos a la verificación de la individualidad de la misma.[35]

La firma electrónica, la firma digital, la firma digital avalada por una entidad de certificación cerrada y la firma digital certificada por una entidad de certificación abierta, son algunas formas de identificación personal en el contexto digital. La ley 527 de 1999 y la doctrina[36] tratan a la firma electrónica[37] como el género y a la digital como una especie de la primera. Lo propio hizo el Consejo Superior de la Judicatura mediante acuerdo PSAA 06-3334 del 2 de marzo de 2006,[38] al definir la firma electrónica como

> [...] los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos. Para efectos de la aplicación del presente acuerdo una firma digital es una clase de firma electrónica, adicionalmente la firma electrónica evidencia cualquier modificación al mensaje de datos posterior al envío.

[35] Sentencia de casación, Sala de Casación Civil, septiembre 4 de 2000, rad. 5565, M. P.: Jaramillo Jaramillo, C. I. Citada sentencia del 27 de agosto de 2003 (proceso 20166) de la Corte Suprema de Justicia (CSJ), M. P.: Pulido de Barón, M.

[36] En este sentido, ver: Ortega Díaz, Juan Francisco, *La firma y el contrato de certificación electrónicos*, Aranzadi, 2008, pp. 37-38.

[37] Ejemplos de normas que utilizan la expresión "firma electrónica": decreto 1791 de 2007, "por medio del cual se reglamenta el artículo 579-2 del Estatuto Tributario"; decreto distrital 55 de 2002, "por medio del cual se establece el Sistema de Declaración y Pago de Impuestos Distritales a través de medios electrónicos"; ley 1189 de 2008, "por medio de la cual se aprueba el Acuerdo de Libre Comercio entre la República de Colombia y la República de Chile - Protocolo adicional al Acuerdo de Complementación Económica para el Establecimiento de un Espacio Económico Ampliado entre Colombia y Chile (ACE 24) del 6 de diciembre de 1993", suscrito en Santiago, Chile, el 27 de noviembre de 2006.

[38] "Por el cual se reglamenta la utilización de medios electrónicos e informáticos en el cumplimiento de las funciones de administración de justicia".

El artículo 7° de la ley 527 de 1999 consagra el equivalente funcional y general de firma en los siguientes términos:

> Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:
>
> a) Se ha utilizado un método que permita identificar al iniciador de un mensaje de datos y para indicar que el contenido cuenta con su aprobación;
> b) Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

Doctrinariamente se ha establecido que este artículo se refiere a la firma electrónica, pues el concepto de firma digital se prevé en el literal c) del artículo 2° de esta norma. El equivalente de la firma electrónica se basa en el reconocimiento de las funciones que se atribuyen a una firma en los documentos físicos, las cuales deben ser cumplidas en los documentos electrónicos, enfocándose en las siguientes: 1) identificar a una persona (firmante); 2) dar certeza de la participación personal de esa persona en el acto de firmar; y 3) asociar a esa persona con el contenido de un documento (confirmación de que el autor aprueba el contenido). La norma citada se centra en las dos funciones básicas de la firma: la identificación del autor y la confirmación de que él aprueba el contenido del documento.

Lo esencial del tema radica en que se utilice un mecanismo de identificación fiable y apropiado. Para la Uncitral la firma electrónica es fiable si:

> 1) los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante; 2) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante; 3)

es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y 4) cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.[39]

Para determinar si el método utilizado es apropiado pueden tenerse en cuenta, entre otros, los siguientes factores jurídicos, técnicos y comerciales que destaca la Uncitral: 1) la perfección técnica del equipo utilizado por cada una de las partes; 2) la naturaleza de su actividad comercial; 3) la frecuencia de sus relaciones comerciales; 4) el tipo y la magnitud de la operación; 5) la función de los requisitos de firma con arreglo a la norma legal o reglamentaria aplicable; 6) la capacidad de los sistemas de comunicación; 7) la observancia de los procedimientos de autenticación establecidos por intermediarios; 8) la gama de procedimientos de autenticación que ofrecen los intermediarios; 9) la observancia de los usos y prácticas comerciales; 10) la existencia de mecanismos de aseguramiento contra el riesgo de mensajes no autorizados; 11) la importancia y el valor de la información contenida en el mensaje de datos; 12) la disponibilidad de otros métodos de identificación y el costo de su aplicación; 13) el grado de aceptación o no aceptación del método de identificación en la industria o esfera pertinente, tanto en el momento en que se acordó el método como cuando se comunicó el mensaje de datos, y 14) cualquier otro factor pertinente.

[39] Cfr. Ley Modelo de la CENUDMI sobre Firmas Electrónicas, de 2001, artículo 6°.

Junto al concepto de firma electrónica[40] se encuentra la firma digital, definida en los siguientes términos en el literal c) del artículo 2° de la ley 527 de 1999: "[...] valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación".

Aunque la ley 527 de 1999 y otras normas mencionan el término *firma digital*,[41] la denominación *firma electrónica* también ha sido utilizada explícitamente en normas de nuestro ordenamiento jurídico, otorgándole la misma validez que la firma autógrafa. Así por ejemplo, el artículo 2° del decreto 1791 de 2007[42] establece: "La firma electrónica de las declaraciones presentadas virtualmente surte los mismos efectos legales de la firma autógrafa". Valga anotar que este decreto concibe a la firma digital como una especie de firma electrónica.

Una breve distinción entre estas dos clases de firmas se puede sintetizar de la siguiente manera:[43]

[40] Se entiende por firma electrónica los "datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos" (Ley Modelo sobre Firmas Electrónicas [2001]), *Diario Oficial* núm. L 13 de 19/01/2000, pp. 12–20, en: http://www.uncitral.org/sp-index.htm). La directiva europea sobre Firmas Electrónicas las define como "los datos en forma electrónica anexos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación" (Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco común para la firma electrónica, en: http://europa.eu.int/scadplus/leg/es/lvb/l24118.htm).

[41] Cfr. ley 527 de 1999, artículo 2°, literal c). Adicionalmente consúltense las siguientes normas: artículo 32 de la ley 794 de 2003; artículo 1° del decreto 1747 de 2000; artículos 826-828 y 621 del Código de Comercio; artículos 28, 39, 40 de la ley 527 de 1999.

[42] Por medio del cual se reglamenta el artículo 579-2 del Estatuto Tributario.

[43] Los gráficos y gran parte de las afirmaciones sobre firma electrónica y firma digital se tomaron del siguiente artículo: Remolina Angarita, Nelson, "Aspectos legales del comercio electrónico, la contratación y la empresa electrónica", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*,

Firma electrónica (Ley modelo Uncitral y ley 527/1999)	Firma digital (ley 527/1999 y decreto 1747 de 2000)
Cualquier método confiable y apropiado que incorpore, adjunte o lógicamente asocie a un texto datos electrónicos que identifican al firmante.	No es cualquier método. Se trata de un valor numérico que se adhiere a un mensaje de datos estrechamente vinculado a la clave del iniciador y al texto del mensaje.
Permite: 1) identificar al firmante, y 2) establecer que el firmante aprueba la información contenida en el mensaje de datos.	Permite establecer que: 1) el texto ha sido firmado con la clave privada del iniciador; 2) el texto no ha sido modificado después de firmado (integridad).
El artículo 7º de la ley 527 establece que el método de identificación utilizado indica que el contenido del texto cuenta con la aprobación del firmante.	Cuando es fijada en un mensaje de datos el artículo 28 presume que el suscriptor tenía la intención de acreditar el mensaje y de ser vinculado con el contenido de éste.

Detrás de los conceptos jurídicos de firma digital y firma electrónica encontramos un soporte tecnológico que apunta a cumplir los fines señalados en el cuadro anterior. La tecnología de la firma digital de la cual trata la ley 527 de 1999 supone que el texto se suscribe con una clave privada y es verificado con una clave pública que permite establecer si, de una parte, éste fue creado con la clave privada del firmante y, de otra parte, si el contenido no fue alterado o modificado después de haber sido firmado. La clave privada y la clave pública reciben el nombre de "datos de creación de firma" y "datos de verificación de firma" en la directiva europea[44] sobre Firmas Electrónicas.[45]

núm. 2, Bogotá, Facultad de Derecho de la Universidad de los Andes, 2006, pp. 323-370. La revista puede ser consultada en: http://derechoytics.uniandes.edu.co.

[44] Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

[45] "Datos de creación de firma": datos únicos (códigos o claves criptográficas privadas) que el firmante utiliza para crear la firma electrónica; "datos de verificación de firma": datos (códigos o claves criptográficas públicas) que se utilizan para verificar la firma electrónica.

La regulación de la firma digital supone una serie de atributos jurídicos para que ésta sea válida y surta los mismos efectos de una firma manuscrita. Pero eso sólo no basta, también es necesario que el usuario de este tipo de firmas sea diligente en el uso y cuidado de ella; de no hacerlo, será responsable por su negligencia.[46] Los atributos de la firma digital[47] y los deberes del suscriptor[48] que la adquiere de una entidad de certificación se pueden resumir así:

ATRIBUTOS DE LA FIRMA DIGITAL	DEBERES DEL SUSCRIPTOR
➔Ser única a la persona que la usa. ➔Ser susceptible de verificación. ➔Estar bajo control exclusivo de la persona que la utiliza. ➔Estar ligada a la información de manera que si es modificada la firma se considera inválida. ➔Estar conforme a la reglamentación expedida por el Gobierno Nacional.	➔Recibir la firma digital de la entidad de certificación o generarla utilizando el método autorizado por ésta. ➔Suministrar la información que requiera la entidad de certificación. ➔Mantener el control de la firma digital. ➔Solicitar oportunamente la revocación de los certificados.

La seguridad de las firmas no sólo depende de la tecnología sino del correcto uso y diligencia del usuario de ellas. El titular será responsable de su conducta negligente respecto del uso de la firma tal, como sucede, por ejemplo, con el usuario de una tarjeta débito o crédito.

Si bien la ley 527 de 1999 y otras normas como el decreto 1747 de 2000 y la ley 794 de 2003 propenden por el uso de la firma digital, la utilización de la firma electrónica también tiene validez jurídica, como se desprende del artículo 7° de la ley 527 de 1999.

[46] Según el artículo 40 de la ley 527, el suscriptor no sólo es responsable por el incumplimiento de sus deberes sino por la falsedad, error u omisión de la información que suministre a la entidad de certificación.

[47] Cfr. ley 527 de 1999, artículo 28, declarado exequible mediante sentencia C-662 del 8 de junio de 2000, de la Corte Constitucional. Consúltense los artículos 1°, 15, 16 y 23 del decreto 1747 de 2000.

[48] Cfr. ley 527 de 1999, artículo 39.

Colombia lleva diez años hablando de firmas digitales, pero éstas no se han masificado. La firma electrónica, en cambio, se ha venido utilizando en el mundo desde la década de los sesenta bajo el contexto de los acuerdos EDI. En otras palabras, el tiempo se ha encargado de demostrar que desde los inicios del comercio electrónico la firma electrónica ha sido el instrumento empleado por los empresarios para identificarse y emitir documentos electrónico, mensajes de datos auténticos, etcétera.

No debe perderse de vista que la firma digital es buena mas su costo aún puede ser más accesible. Adquirir en Colombia una firma digital de una entidad certificadora debidamente registrada no es económicamente viable para muchos ciudadanos. Su precio ha hecho que se convierta en un instrumento excluyente, de acceso muy limitado a la mayoría de la población.

La firma digital no es la maravilla, ni ciento por ciento segura. Tampoco es plena prueba de que una persona firmó, sólo de que para firmar se utilizó la clave privada de alguien (que no es lo mismo). Adicionalmente, la firma digital fue la respuesta tecnológica que se dio a los colombianos en 1999 (hace diez años). La tecnología evoluciona rápidamente y es factible que la firma digital pronto sea tildada de obsoleta. Esto no sucede con la firma electrónica, pues de entrada se ha concebido como un medio ciento por ciento neutral pensado para perdurar a lo largo del tiempo y a tono con los avances tecnológicos o el estado de la técnica de cada época. Al igual que la firma digital, la utilización de la firma electrónica también tiene validez jurídica, como se desprende del artículo 7° de la ley 527 de 1999. De hecho, el sector privado (el sistema financiero, los operadores de telecomunicaciones y las empresas en general) recurre masivamente al uso de la firma electrónica por las diversas opciones que brinda en virtud del desarrollo, que genera más oferta a un menor costo, sin desmedro de la seguridad y, en últimas, de la certeza de los usuarios y de un eventual juzgador.

Como sucede en los temas relacionados con la tecnología, un punto crítico es la seguridad. Así como existen unas firmas "tradicionales" más seguras que otras,[49] lo propio sucede con las firmas en el contexto digital. Tenemos, entre otras, la firma electrónica, la firma digital (o "firma electrónica avanzada",[50] como se denomina en la directiva europea aludida) y la firma digital avalada por una entidad de certificación abierta o cerrada (o "firma electrónica avanzada basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma", como se le conoce en Europa). Todas son jurídicamente válidas y de entrada no puede afirmarse que unas sean más seguras que otras. Todo dependerá del grado de confiabilidad y seguridad de la tecnología y los procedimientos empleados para alcanzar los propósitos mencionados en el párrafo anterior.[51] No sobra tener claro: la firma digital avalada por una entidad de certificación abierta no es, *per se*, plena prueba de que el firmante efectivamente firmó, sino que meramente cumple el requisito del equivalente funcional de firma manuscrita y, esto podrá ser rebatido.

Vale la pena considerar algunos aspectos (que a continuación destacamos), de un estudio realizado en 2009 por la Uncitral o CNUDMI, de la ONU, titulado: "Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas".[52]

[49] No tiene el mismo nivel de seguridad firmar con el nombre que con un signo, un símbolo, una rúbrica o nuestra huella dactilar.

[50] Según la directiva europea, la "firma electrónica avanzada" se define como aquella que cumple los siguientes requisitos: 1) estar vinculada al firmante de manera única; 2) permitir la identificación del firmante; 3) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control; 4) estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de éstos sea detectable.

[51] 1) Identificar al firmante; 2) dar certeza de la participación personal del firmante en el acto de firmar, y 3) asociar al firmante con el contenido del documento.

[52] [Disponible en http://www.uncitral. org/pdf/spanish/publications/sales_ publications/ Promoting_ confidenceS.pdf].

Dice el estudio:

1) "La definición de 'firma electrónica' en los textos de la CNUDMI es deliberadamente amplia, para que *abarque todos los métodos de firma electrónica existentes o futuros*"[53] (resaltamos).

2) "Los métodos de autenticación y firmas electrónicas pueden clasificarse en tres categorías, a saber: los que se basan en lo que el usuario o el receptor emplea (por ejemplo, contraseñas, números de identificación personal (NIP)), los basados en las características físicas del usuario (por ejemplo, biometría) y los que se fundamentan en la posesión de un objeto por el usuario (por ejemplo, códigos u otra información almacenada en una tarjeta magnética). *(...) Entre las tecnologías que se usan en la actualidad figuran las firmas digitales en el marco de una infraestructura de clave pública (ICP), dispositivos biométricos, NIP, contraseñas elegidas por el usuario o asignadas, firmas manuscritas escaneadas, firmas realizadas por medio de un lápiz digital y botones de aceptación de tipo 'sí' o 'aceptar' o 'acepto'. Las soluciones híbridas basadas en la combinación de distintas tecnologías están adquiriendo una aceptación creciente*"[54] (resaltamos).

3) "La firma digital funciona bien como un medio para verificar las firmas que se crean durante el período de validez de un certificado. *Sin embargo, cuando el certificado caduca o se revoca la clave pública correspondiente pierde validez (...). Por ello, todo mecanismo de ICP requeriría un sistema de gestión de la firma digital para asegurar que la firma siga disponible a lo largo del tiempo*"[55] (resaltamos).

[53] ONU/Uncitral, "Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas", Viena, 2009, p. 15.

[54] Ibídem, p. 13.

[55] Ibídem, p. 26.

4) "Un volumen importante de operaciones comerciales electrónicas se lleva a cabo en redes cerradas, es decir, en grupos con un número limitado de participantes *a los que pueden acceder únicamente personas o empresas previamente autorizadas*"[56] (resaltamos). Un ejemplo que se cita de este tipo de redes son las instituciones financieras, las bolsas de valores, etcétera.

Como corolario de lo anterior, contamos con otros medios electrónicos de identificación que pueden ser más seguros y ofrecer mayor certeza de origen que las firmas digitales. No podemos equivocarnos en sostener que la firma digital debe utilizarse para todo. Si se trata de una cuestión de seguridad, pues con ese argumento todos los ciudadanos deberíamos movilizarnos en carros blindados y con escoltas.

Existen escenarios en donde la firma electrónica es más pertinente que la digital, y lo contrario. Ésta debe ser una decisión libre del empresario o una entidad pública y no una imposición legal o un discurso propagandístico en pro de la firma digital. En todo caso, no se debe cerrar jurídicamente la puerta al uso de la firma electrónica ni avalar un monumento ciego y acrítico, de adoración perpetua, a la firma digital.

En síntesis, y a título de resumen, queremos recalcar lo siguiente:

1) En Colombia es jurídicamente válido utilizar firmas electrónicas, digitales, o firmas digitales avaladas por una entidad de certificación cerrada o abierta.
2) Todas son admisibles como medio probatorio, sin que pueda afirmarse, *per se,* que unas sean más seguras que otras. Todo dependerá del grado de confiabilidad y seguridad de la tecnología y de los procedimientos empleados para alcanzar los siguientes propósitos:

[56] Ibídem, p. 37.

a) Identificar al firmante.
b) Dar certeza sobre la participación personal del firmante en el acto de firmar.
c) Asociar al firmante con el contenido del documento.

3) Recurrir a las entidades de certificación no es obligatorio y no necesariamente la intervención de ellas generará, por ese mero hecho, mayor certeza respecto del originador de un mensaje de datos o del creador de un documento electrónico. Se trata de una alternativa no infalible que incluso puede ser superada por mecanismos y procedimientos englobados dentro del concepto de firma electrónica.
4) Las firmas avaladas por una entidad de certificación abierta no son plena prueba de que el titular de una firma digital fue quien realmente firmó. En la práctica pueden existir firmas electrónicas o mecanismos aún más seguros que la propia firma digital avalada por una entidad de certificación abierta. En efecto, con el mero uso de la firma digital podemos establecer que durante el proceso de firma se utilizó la clave privada del titular de ésta, pero no se puede asegurar que dicha persona fue quien efectivamente firmó. Es como cuando una persona va a un cajero electrónico y digita una clave personal. Salvo al existir cámaras de video en el cajero, el banco siempre asumirá que la clave la digitó el titular de la tarjeta débito pero no puede asegurar que efectivamente fue así.
5) Es factible utilizar otros medios de prueba para generar el mismo convencimiento sobre una firma digital. Ello es así porque el equivalente del artículo 7° de la ley 527 no se circunscribe a la firma digital certificada y porque en materia probatoria impera el principio de la libertad de prueba, según el cual, sirve como

> tal cualquier medio útil para la formación del convencimiento del juez.[57]

Finalmente, no podemos dejar culminar este espacio sin mencionar lo siguiente: El administrador de una entidad de certificación abierta, afirmó: "Se ha calificado en algunos comentarios como 'chambón' *[sic]* la inclusión de la firma digital en actuaciones por medios electrónicos, pero esa descalificadora expresión es consecuencia del desconocimiento o desinformación de la firma digital". También dice respecto de la firma digital: 1) "el legislador estableció la equivalencia con respecto a esta figura y no a la firma electrónica", 2) "para que la firma digital sea válida requiere la intervención de un tercero de confianza, denominado entidad de certificación digital", 3) "a la luz de la legislación colombiana el equivalente idóneo de la firma manuscrita es la firma digital de una entidad de certificación abierta".[58]

Quienes escribimos tenemos la obligación de no perder de vista que, según el artículo 20 de la Constitución, los lectores tienen derecho a "recibir información veraz e imparcial". Consideramos las afirmaciones transcritas no consistentes con dicho mandato constitucional.

Es falso afirmar que el legislador estableció la firma digital como único equivalente de la firma manuscrita. Esta conclusión desconoce abiertamente el artículo 7° de la ley 527 de 1999. Tampoco es veraz aseverar que la validez de una firma digital depende de la intervención de una entidad de certificación. Eso no lo dice la ley. Ya vimos cómo respecto de esta clase de firma tenemos tres opciones: la digital, la digital avalada por una entidad de certificación cerrada, y la digital avalada por una entidad de certificación abierta.

[57] Cfr. Código de Procedimiento Civil, artículo 175.

[58] Rincón Cárdenas, Erick, "Discusiones alrededor de la firma digital", en *Ámbito Jurídico*, núm. 281, 2009, p. 13.

El artículo 28 de ley 527 de 1999 exige que la firma digital sea "susceptible de ser verificada" pero en ninguna parte ordena que para tener validez deba ser certificada por una entidad de certificación. La verificación se puede realizar con la clave pública sin que sea necesaria la intervención de una entidad de certificación. Recuérdese que a la luz del numeral 5 del artículo 1° del decreto 1747 de 2000 la clave pública es "*el valor o valores que son utilizados para verificar que una firma digital fue generada con la clave privada del iniciador*". En síntesis, verificar una firma no es lo mismo que certificarla, pues en éste último caso sí es necesaria la presencia de una entidad de certificación,[59] pero, se repite, lo que la ley ordena es que la firma digital sea verificada.

Recalcamos que la firma digital no es plena prueba de haber firmado una persona. Sólo nos dice que para firmar se utilizó la clave privada de alguien (lo cual no es lo mismo). La firma digital de una entidad de certificación puede ser un equivalente de firma manuscrita, pero no el único. Incluso, pueden existir firmas electrónicas más confiables y seguras que la precitada clase de firma digital.

Existen disposiciones que imponen el uso de la firma digital,[60] sin embargo se ha evidenciado la existencia de una cruzada para minar la legislación colombiana de disposiciones que obliguen a utilizar la firma digital

[59] En efecto, según el numeral 6 del artículo 1° del decreto 1747 de 2000, el "certificado en relación con las firmas digitales" es un "mensaje de datos firmado por la entidad de certificación que identifica, tanto a la entidad de certificación que lo expide, como al suscriptor, y contiene la clave pública de éste".

[60] Algunos ejemplos que corroboran esta afirmación son las siguientes normas: ley 1350 de 2009, "por medio de la cual se reglamenta la Carrera Administrativa Especial en la Registraduría Nacional del Estado Civil y se dictan normas que regulen la Gerencia Pública"; decreto 852 de 2009, "por medio del cual se modifica parcialmente el decreto 159 de 2002, modificado parcialmente por el decreto 072 de 2005, y se dictan otras disposiciones"; resolución 1339 de 2008 del Ministerio de Transporte, "por la cual se adopta el uso de la firma digital para los sujetos obligados a reportar información al Ministerio de Transporte"; resolución 1448 de 2006 del Ministerio de la Protección Social, "por la cual se definen las condiciones de habilitación para las instituciones que prestan servicios de salud bajo la modalidad de telemedicina"; ley 1111 de 2006, "por la cual se modifica el estatuto tributario de los impuestos administrados por la Dirección de Impuestos y Aduanas Nacionales", y circulares externas 3 de 2005 de la Superintendente de Industria y Comercio y 100-004 de la Superintendencia de Sociedades.

avalada por una entidad de certificación. Así por ejemplo, en el texto del proyecto de la nueva ley antitrámites (2009), el artículo 4°, denominado "Trámite administrativo electrónico", establece que "todo documento electrónico expedido por servidor público en ejercicio de sus funciones y firmado digitalmente tendrá la connotación de documento público". Remata el parágrafo diciendo: "cuando el trámite de las actuaciones administrativas se adelante por medios informáticos, las firmas autógrafas que la misma exija tendrán como equivalente *la firma digital emitida por una entidad de certificación digital abierta"* (destacamos).

Esta propuesta está pensada en favorecer a las entidades de certificación abierta , dejando de lado lo hecho por algunas entidades públicas de certificación cerrada (la Dirección de Impuestos y Aduanas Nacionales, DIAN, por ejemplo) y cerrando la posibilidad para que el Estado utilice la firma electrónica tratada en el artículo 7° de la ley 527 de 1999. Este tipo de iniciativas es conveniente como estrategia de comercialización de dicha clase de firmas, mas no necesariamente consulta los intereses de todos los ciudadanos y del país. También es desconcertante evidenciar cómo algunos funcionarios públicos afirman que lo único válido en Colombia es la firma digital avalada por una entidad de certificación abierta o sostienen que toda firma digital debe ser certificada por, valga la redundancia, una entidad de certificación.

La ley 527 prevé opciones para que cada uno seleccione el medio de identificación electrónica más apropiado para determinadas gestiones. Insistimos en existir escenarios en los cuales la firma electrónica es más pertinente que la digital, y lo contrario. Ésta debe ser una decisión libre por parte del empresario o de una entidad pública y no una imposición legal o un discurso propagandístico y mesiánico en pro de la firma digital por parte de las entidades de certificación abierta.

La firma digital no es mala; lo malo es imponerla por ley, a la fuerza, a las malas.

III. Entidades de certificación: escenarios y limitaciones probatorias

Las entidades de certificación son personas jurídicas autorizadas por la Superintendencia de Industria y Comercio (SIC) para

> [...] emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales.[61] Las entidades de certificación cerradas ofrecen los anteriores servicios pero "sólo para el intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello".[62]

Las entidades de certificación abierta,[63] por su parte, son un tercero imparcial que imprime mayor confianza respecto del uso de las firmas en el contexto digital. Recurrir a ellas no es obligatorio pero sí recomendable si se quiere tener más certeza sobre el originador de un mensaje de datos o el creador de un documento electrónico. Se denominan, en la directiva europea sobre Comercio Electrónico, como "prestadores de servicios de certificación" (PSC), y en la directiva europea sobre Firmas Electrónicas, por su parte, como "proveedores de servicios de certificación". En todo caso, su función principal consiste en expedir certificados, sin perjuicio de que puedan prestar otros servicios relacionados con las firmas en comento.

[61] Ley 527 de 1999, artículo 2°, literal d).

[62] Cfr. Decreto 1747 de 2000, artículo 1°, numeral 8.

[63] Cfr. ley 527 de 1999, literal d). Adicionalmente, consúltense las siguientes normas: artículos 30 y ss. de la ley 527; artículo 11 del decreto 1747 de 2000; numerales 6, 7, 8 y 9 del artículo 1° del decreto 1747 de 2000 (conceptos de certificado, estampado cronológico, entidades de certificación cerrada y abierta).

Conceptualmente[64] se deriva de la ley 527 de 1999 que para efectos de la verificación de una firma digital el receptor de un mensaje de datos tiene dos opciones:

La primera consiste en que él recibe la clave pública del iniciador[65] del mensaje de datos. Con ésta, establecerá si el mensaje de datos fue creado con determinada clave privada y si el texto ha sido alterado o modificado después de haber sido firmado. No obstante, surgen algunas dudas: ¿cómo sabe el destinatario que el iniciador del mensaje es quien dice ser y no otra persona?, ¿cómo tener certeza de que el iniciador realmente existe?

Los anteriores riesgos son mitigados con la segunda opción, consistente en solicitar un certificado digital a una entidad de certificación. En este caso, el destinatario de un mensaje de datos solicita a una entidad de certificación[66] un certificado digital[67] para corroborar la firma digital. Dicho certificado consta de un mensaje de datos firmado por la entidad que identifica tanto a la entidad de certificación que lo expide como al suscriptor de la firma, y contiene la clave pública de éste para poder el destinatario realizar el procedimiento de verificación.[68] Particularmente, contiene la siguiente información: 1) nombre, dirección y domicilio del suscriptor; 2) identificación del suscriptor nombrado en el certificado;

[64] Es importante precisar que las dos opciones citadas se derivan del texto de la ley 527 de 1999. No obstante, en el mercado se ofrecen firmas digitales para cuya verificación se siguen procedimientos diferentes a los citados en este escrito.

[65] Se trata de la persona que actuando por su cuenta, o en cuyo nombre se haya actuado, envía o genera un mensaje de datos (decreto 1747 de 2000, artículo. 1°).

[66] Uno de los principales deberes de las entidades de certificación consiste en emitir certificados digitales. Los deberes son señalados en el artículo 32 de la ley 527 de 1999.

[67] El cual consiste en un mensaje de datos firmado por la entidad de certificación que identifica tanto a la entidad de certificación que lo expide como al suscriptor, y contiene la clave pública de éste.

[68] Téngase presente que la firma digital se estructura a partir de la clave privada y la clave pública. Con la primera se genera la firma digital de un mensaje de datos, mientras que con la segunda se verifica que una firma digital fue generada con la clave privada del iniciador.

3) el nombre, la dirección y el lugar donde realiza actividades la entidad de certificación; 4) la clave pública del usuario; 5) la metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos; 6) el número de serie del certificado, y 7) fecha de emisión y de expiración del certificado.

El destinatario recibe el certificado de un tercero imparcial al que ha acudido el iniciador del mensaje para obtener su firma digital. De esta manera el receptor tiene la certeza de que la persona a quien corresponde la firma realmente existe y la clave pública es remitida por una entidad profesional y seria. Por eso, en principio, es válido afirmar el ser más confiable utilizar firmas digitales avaladas por entidades de certificación que firmas digitales carentes de dicho respaldo. No obstante, ello no quiere decir que las firmas digitales no certificadas sean inseguras. Al contrario, pueden ser incluso más confiables si están provistas de tecnologías y procesos más seguros y apropiados para establecer la plena identidad del firmante y que él efectivamente fue quien suscribió un documento. Todo dependerá de la tecnología utilizada y del buen uso y control que tenga el titular del sistema de identificación electrónico.

Debe aclararse que firma digital y certificado son dos conceptos jurídicamente diferentes. El primero hace alusión a un método de identificación especial[69] y el segundo a una forma de constatar ciertos aspectos frente a terceros respecto de la firma digital. Concretamente, el "certificado en relación con las firmas digitales" está definido como un "mensaje de datos firmado por la entidad de certificación que identifica, tanto a la entidad de certificación que lo expide, como al suscriptor, y contiene la clave pública de éste".[70]

[69] Cfr. ley 527 de 1999, artículo 2°, literal c).

[70] Cfr. decreto 1747 de 2000, artículo 1°, numeral 6.

No toda empresa que cree o utilice firmas digitales ha de convertirse en entidad de certificación cerrada ni toda firma digital debe ser certificada. La regla general consiste en que todas las empresas pueden emplear firmas digitales sin necesidad de adquirir la categoría de entidad de certificación cerrada. Sólo aquellas que presten servicios de entidades de certificación, como expedir certificados en el sentido anotado, deben acreditar ciertos requisitos ante la SIC con miras a que ella las autorice para realizar las labores propias de entidades de certificación.

En ese sentido, en el numeral 8.6 del título V de la circular única de la SIC se ordenó lo siguiente a las entidades que ofrecen servicios propios de las entidades de certificación:

> Todas aquellas personas jurídicas, públicas o privadas, de origen nacional o extranjero, las cámaras de comercio y las notarías o consulados, *que estén ejerciendo actividades como entidades de certificación, tales como: emisión de certificados en relación con las firmas digitales de personas, ofrecer o facilitar servicios de estampado cronológico de la transmisión y recepción de los mensajes de datos,* así como cumplir otras funciones relativas a las comunicaciones basadas en firmas digitales, sin autorización de la Superintendencia de Industria y Comercio, deberán presentar la correspondiente solicitud, so pena de la imposición de las sanciones a que haya lugar[71] (resaltado fuera del texto).

De una lectura armónica de los artículos 4° y 15 del decreto 1747 de 2000, junto con el parágrafo del artículo 28 de la ley 527 de 1999, se puede concluir que "los certificados emitidos por las entidades de certificación cerradas no tienen la misma fuerza y efectos que la firma

[71] Esta instrucción se introdujo mediante la circular externa 2 del 21 de febrero de 2002, publicada en el *Diario Oficial* núm. 44722, de febrero 26 de 2002.

manuscrita" ni los mismos privilegios probatorios que el decreto 1747 de 2000 le confirió a las firmas digitales de las entidades de certificación abierta. En palabras de la SIC,

> En virtud de la estipulación contenida en el artículo 4° del decreto 1747, tenemos entonces que los certificados emitidos por una entidad de certificación cerrada no cumplen los requisitos contenidos en los numerales 1 a 4 del artículo 15 citado, por lo cual no pueden darse por satisfechos los atributos exigidos para una firma digital contenidos en el parágrafo del artículo 28 de la ley 527.
>
> [...]
>
> Ahora bien, respecto al tercer punto, en el cual nos consulta si los efectos de los certificados emitidos por una entidad de certificación cerrada son diferentes a los emitidos por una entidad de certificación abierta, tenemos que, según lo antes anotado y conforme con la normatividad citada, la respuesta a dicha cuestión es que sí son diferentes por cuanto en la medida en que un certificado emitido por una entidad de certificación abierta cumpla con los requisitos establecidos en el artículo 15 del decreto 1747, uno de los cuales consiste en que el certificado digital que respalda la firma digital sea expedido por una entidad de certificación abierta, se entenderá que "se darán por satisfechos los atributos exigidos para una firma digital en el parágrafo del artículo 28 de la ley 527 de 1999".[72]

Los citados artículos del decreto en cuestión fueron más allá de lo que dice la ley 527, pues ésta no exige que el equivalente a una firma manuscrita únicamente corresponda a las firmas digitales avaladas por una entidad de certificación abierta.[73] Pese a los artículos 4° y 15, la

[72] Superintendencia de Industria y Comercio, concepto 5037703, de junio 14 de 2005.

[73] El parágrafo del artículo 28 de la ley 527 de 1999 reza lo siguiente:

SIC ha establecido que los atributos exigidos en el artículo 28 pueden ser demostrados y, por ende, un certificado emitido por una entidad de certificación cerrada podría tener el mismo valor probatorio que el expedido por una entidad de certificación abierta:

> Tenemos entonces que, si el certificado expedido por una entidad de certificación cerrada no cumple los requisitos enunciados en el artículo 15 del decreto 1747, según lo establece el mismo decreto en su artículo 4° de manera expresa, no podría, en principio, la firma digital que se encuentra respaldada mediante el certificado digital, cumplir con lo establecido en el parágrafo del artículo 28 de la ley 527, *salvo que se prueben dichos atributos*[74] (resaltado fuera del texto).

A pesar de establecer el artículo 2° del decreto 1747 que un sistema confiable utilizado para el ejercicio de las actividades de certificación sea aquel que cumpla los estándares establecidos por la Superintendencia de Industria y Comercio, ello no es óbice para que técnica, fáctica y jurídicamente existan mecanismos dispuestos demostrar la confiabilidad y generar convicción.

En el evento de presentarse un cuestionamiento sobre la confiabilidad de los sistemas de identificación, corresponderá demostrar que dicho método no sólo permite identificar al firmante, sino el ser confiable y apropiado para, por ejemplo, suscribir un documento electrónico.

"El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:

1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.
3. Está bajo el control exclusivo de la persona que la usa.
4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional".

[74] Superintendencia de Industria y Comercio, concepto 5037703, de junio 14 de 2005.

Pueden existir mecanismos aún más seguros que la propia firma digital avalada por una entidad de certificación abierta. En efecto, con el mero uso de la firma digital podemos establecer que durante el proceso de firma se utilizó la clave privada del titular de la firma digital, pero no se puede asegurar el haber sido dicha persona quien efectivamente firmó. Es como cuando una persona va a un cajero electrónico y digita una clave personal: salvo existir cámaras de video en el cajero, el banco siempre asumirá que la clave la digitó el titular de la tarjeta débito mas no puede asegurar que efectivamente fue así.

En otras palabras, jurídicamente es factible utilizar otros medios de prueba para generar el mismo convencimiento sobre una firma digital. Cuanto busca, en últimas, la tecnología, es garantizar que quien suscribe determinado documento sea efectivamente quien dice ser. La tecnología no es la panacea de la seguridad, pero definitivamente es un magnífico medio para garantizarlo. Si a la tecnología de identificación actual (uso de claves privadas, por ejemplo), se le incluyen otros medios de seguridad como sistemas biométricos tales como la huella o un video del firmante firmando, la sumatoria de éstos genera un altísimo convencimiento sobre la originalidad de un signatario.

Ello es así porque el equivalente del artículo 7° de la ley 527 no se circunscribe a la firma digital certificada y porque en materia probatoria impera el principio de la libertad de prueba, según el cual, sirve como prueba cualquier medio útil para la formación del convencimiento del juez.

IV. ¿Hacia una reglamentación de la firma electrónica?

En mayo de 2009 el Ministerio de Comercio, Industria y Turismo publicó el texto del proyecto de decreto "Por el cual se reglamenta

la firma electrónica"[75] (anexo). Si bien esta iniciativa aún no ha sido convertida en decreto, la misma merece algunos comentarios:

El decreto es necesario para la mayoría de la población colombiana y las empresas. Para un experto o profesor de comercio electrónico seguramente no lo es, pues si bien el artículo 7° de la ley 527 de 1999 consagra la firma electrónica, la mayoría de la población cree que en Colombia sólo existe y es válida la firma digital.

Colombia lleva diez años hablando de firmas digitales, pero éstas no se han masificado. La firma electrónica, en cambio, se ha venido utilizando en el mundo desde la década de los sesenta bajo el contexto de los acuerdos EDI a los cuales se refiere el proyecto de decreto. En otras palabras, el tiempo se ha encargado de demostrar que desde los inicios del comercio electrónico la firma electrónica ha sido el instrumento empleado por los empresarios para identificarse y emitir documentos electrónicos, mensajes de datos auténticos, etcétera.

Es muy positiva, entre otras, la consagración en el proyecto de lo atinente a los acuerdos EDI, ya que actualmente un porcentaje importante de los negocios electrónicos se realiza en mercados electrónicos cerrados *(e-marketplaces)* cuyo soporte jurídico son dichos acuerdos.

El decreto abre los ojos a los neófitos al respecto para que también exploren la firma electrónica como medio de identificación masivo en el contexto digital. Adicionalmente, pone a Colombia a tono con los países o bloques económicos con los cuales está suscribiendo tratados de libre comercio. En Estados Unidos y en Europa las leyes se refieren a la firma electrónica.

Es positiva y saludable la iniciativa para el país porque es neutral tecnológicamente, no concede privilegios y, sobre todo, es consistente con

[75] El texto fue publicado en http://www.mincomercio.gov.co/eContent/NewsDetail. asp?ID=6835 (última consulta: mayo 25 de 2009).

estándares internacionales y la misma ley 527 en lo pertinente. Nótese cómo el precitado proyecto de decreto sigue muy de cerca los siguientes documentos: 1) Ley Modelo sobre Firmas Electrónicas con la guía para su incorporación al derecho interno, 2001; 2) Recomendación de la Comisión de 19 de octubre de 1994 relativa a los aspectos jurídicos del intercambio electrónico de datos; 3) Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, 2005.

Otro aspecto favorable del proyecto de decreto es que deja intacta toda la regulación sobre firmas digitales. De esta manera se reabre al país una baraja de posibilidades de identificación tecnológica y se permite a las empresas y los consumidores seleccionar el mecanismo más apropiado para cada necesidad particular.

En el segundo semestre de 2009 han surgido elementos que refuerzan la tendencia de replantear lo sucedido a la fecha con las firmas digitales. Veamos:

En primer lugar, la Asobancaria publicó el 23 de octubre de 2009 el documento: "Avances y desafíos para los instrumentos electrónicos en Colombia". Allí se abordan varias cuestiones importantes para el país, dentro de las cuales se trae a colación el tema de la firma electrónica y digital. Apuntala la Asobancaria que "no es posible establecer la superioridad técnica de uno de los dos tipos de firma sobre el otro (cada uno tiene sus fortalezas y debilidades)". Adicionalmente, asevera: "la ley otorgó ventajas jurídicas injustificadas en materia probatoria a las firmas digitales, en particular a aquellas expedidas por entidades de certificación abiertas". Esta situación ha sido reforzada, en palabras de dicha entidad, por el decreto 1747 de 2000 y por "prácticas de diferentes entidades públicas, que han dado preferencia al uso de la firma digital". Recalca: "el costo de la firma digital constituye una barrera de entrada para el público en general, además de que no respeta el principio de neutralidad tecnológica".

Concluye la Asobancaria el ser necesario contar con "soluciones prácticas y de bajo costo" para dinamizar el comercio electrónico. Así las cosas, sugiere "analizar si el uso de la firma digital es lo más adecuado para el país. O si por el contrario, otras alternativas disponibles, como las firmas electrónicas [...] cumplen con los requisitos de seguridad para la acreditación y autenticación electrónicas".

En segundo lugar, en el documentos Conpes 3620 del 9 de noviembre de 2009, titulado "Lineamientos de política para el desarrollo e impulso del comercio electrónico en Colombia", se pone de presente que si bien la firma digital es "reconocida en la actualidad por sus altos estándares de seguridad, puede resultar limitada en el largo plazo de acuerdo a los cambios tecnológicos y su neutralidad". Adicionalmente, se destaca que en Colombia el precio de los certificados digitales emitidos por entidades de certificación abierta "son considerados relativamente altos en comparación de otros países de América Latina como por ejemplo Chile, lo cual puede representar un costo de oportunidad en materia de utilización de esta herramienta para las mypimes". En virtud de lo anterior, el Conpes recomienda realizar una revisión integral de la ley 527 de 1999 que promueva el uso de la firma electrónica como esquema alternativo de la firma digital.

Todo lo anterior ratifica la urgencia de repensar en las necesidades del país en el entorno electrónico, para ser más competitivos.[76] Por eso cobra relevancia convertir en decreto el proyecto de reglamentación sobre firmas electrónicas, de manera que éstas cuenten con las mismas bondades probatorias que durante más de diez años se han conferido a la firma digital de las entidades de certificación abierta.

[76] Véase: Rodríguez Turriago, Omar, "Diez años de la ley 527 de comercio electrónico: reflexiones sobre la necesidad de su modernización", en *Ámbito Jurídico*, agosto de 2009, p. 14; Remolina Angarita, Nelson, "La protección de datos personales y las firmas digitales: dos temas para repensar y actuar", en *Ámbito Jurídico*, noviembre de 2009. Disponibles en: http://gecti.uniandes.edu.co/columna.php?Op=columna.

Como era de esperarse, esta propuesta no ha sido bien recibida por el representante legal de una entidad de certificación abierta. Recientemente el administrador de una de ellas[77] se opuso a serles concedidos a las firmas electrónicas los mismos privilegios probatorios que han tenido durante una década las firmas digitales certificadas por las entidades de certificación abierta. Esta posición es entendible en la medida en que si vía decreto se le confiere igual valor probatorio a una firma electrónica que a una firma digital certificada por una entidad de certificación abierta, puede afectarse el negocio de las empresas de certificación abierta, pero ello no significa que la propuesta de decreto sea mala o inconveniente para el país.[78]

[77] Rincón Cárdenas, Erick. "Sobre el proyecto de reglamentación de firmas electrónicas", en *Ámbito Jurídico*, núm. 289, 2010, pp. 14-15.

[78] Sobre la discusión en torno al proyecto de decreto reglamentario de la firma electrónica, consúltese el Documento GECTI núm. 10 titulado "Pensar en las necesidades del país o mantener a ultranza un *statu quo* para la firma digital de las entidades de certificación abierta –ECA–", Bogotá, marzo de 2010. Disponible en: http://gecti.uniandes.edu.co/documentos.php.

V. ANEXO

Texto publicado del proyecto de decreto sobre firma electrónica:

República de Colombia
Ministerio de Comercio, Industria y Turismo
Decreto número ( ) de 2009

"Por el cual se reglamenta la firma electrónica"

El Presidente de la República de Colombia, en uso de sus facultades constitucionales y legales, especialmente de las que le confiere el numeral 11 del artículo 189 de la Constitución Política,

Considerando:

Que se ha considerado al comercio electrónico como motor de crecimiento de la economía del siglo XXI y factor que contribuye a fomentar la competitividad empresarial de las pymes y mipymes a través del uso de las tecnologías de información y comunicación;

Que para impulsar el desarrollo del comercio electrónico, internacionalmente se [ha] recomendado promover enfoques apropiados para el reconocimiento legal de firmas electrónicas bajo principios de neutralidad tecnológica;

Que la firma electrónica representa un medio de identificación electrónico flexible y tecnológicamente neutro que se adecua *[sic]* a las necesidades de los particulares, las empresas y el Estado;

Que ante la evolución de las innovaciones tecnológicas, es necesario establecer criterios para el reconocimiento jurídico de las firmas electrónicas independientemente de la tecnología utilizada;

Que en [el] documento Conpes 3419 del 17 de abril de 2006 se destacó que la falta de legalización de la firma electrónica presenta un obstáculo al crecimiento de los canales virtuales;

Que es indispensable, tanto en el comercio como en el gobierno electrónico y todas las demás actividades que se realizan a través del uso e intercambio de mensajes de datos o documentos electrónicos, avalar jurídicamente el uso de las nuevas tecnologías de identificación personal;

Que en el artículo 7° de la ley 527 de 1999 se consagró la firma electrónica como equivalente funcional de la firma;

Que se hace necesario reglamentar la firma electrónica para generar mayor entendimiento sobre la misma, dar seguridad jurídica a los negocios que se realicen a través de medios electrónicos y facilitar el uso masivo de la firma electrónica en todo tipo de transacciones entre particulares y frente al Estado;

DECRETA:

Artículo 1°. *Definiciones.* Para los fines del presente decreto se entenderá por

a) *Acuerdo* EDI. Acuerdo de voluntades mediante el cual se estipulan las condiciones legales a que se ajustarán las partes para realizar comunicaciones, efectuar transacciones, crear documentos electrónicos o cualquier otra actividad mediante el uso del intercambio electrónico de datos (EDI).

b) *Datos de creación de la firma electrónica.* Datos únicos y personalísimos, tales como códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

c) *Firma electrónica.* De conformidad con el artículo 7° de la ley 527 de 1999, se entenderá como firma electrónica cualquier procedimiento, método o dispositivo electrónico, óptico o similar tales como, entre otros, códigos, contraseñas, datos biométricos o claves criptográficas privadas que el firmante utiliza para suscribir documentos electrónicos o mensajes de datos y que:

i) Permite identificar al firmante de un mensaje de datos o un documento electrónico y para indicar que el contenido cuenta con su aprobación;
ii) Sea tanto confiable como apropiado para el propósito por el cual el mensaje o documento electrónico fue generado o comunicado, atendidas todas las circunstancias del caso, inclusive todo acuerdo EDI aplicable entre las partes.

d) *Firmante.* Persona que posee los datos de creación de la firma y que actúa en nombre propio o por cuenta de la persona a la que representa.

Artículo 2°. *Neutralidad tecnológica e igualdad de tratamiento de las tecnologías para la firma electrónica.* Ninguna de las disposiciones del presente decreto será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método, procedimiento, dispositivo o tecnología para crear una firma electrónica que cumpla los requisitos señalados en el literal c) del artículo 1° de este decreto.

Artículo 3°. *Confiabilidad de la firma electrónica.* La firma electrónica se considerará confiable si:

a) los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;

c) es posible detectar cualquier alteración no autorizada de la firma electrónica hecha después del momento de la firma.

Parágrafo. Lo dispuesto anteriormente se entenderá sin perjuicio de la posibilidad de que cualquier persona:

a) demuestre de otra manera que la firma electrónica es confiable y apropiada para los fines que suscribió un documento electrónico o se generó o comunicó un mensaje de datos; o

b) aduzca pruebas de que una firma electrónica no es confiable.

Artículo 4°. *Atributos jurídicos de la firma electrónica.* Cuando una firma electrónica haya sido fijada en un mensaje de datos o en un documento electrónico se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos o documento electrónico y de ser vinculado con el contenido del mismo.

El uso de una firma electrónica tendrá la misma fuerza y efectos que el uso de la firma, la firma manuscrita u otros tipos de firma diferentes a la firma digital, si aquélla incorpora los siguientes atributos:

a) Es única a la persona que la usa.

b) Es susceptible de ser verificada por cualquier medio útil para la formación del convencimiento del juez, los particulares o las entidades públicas.

c) Está bajo el control exclusivo de la persona que la usa.

d) Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma electrónica es invalidada.

Artículo 5°. *Obligaciones del firmante.* El firmante debe:

a) mantener control y custodia sobre los datos de creación de la firma;

b) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;

c) Dar aviso oportuno a cualquier persona que posea, haya recibido o va a recibir documentos o mensajes de datos firmados electrónicamente por el firmante, si:

i) el firmante sabe que los datos de creación de la firma han quedado en entredicho; o

ii) las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho.

Parágrafo. Se entiende que los datos de creación del firmante han quedado en entredicho cuando éstos, entre otras, han sido conocidos ilegalmente por terceros, corren peligro de ser utilizados indebidamente, o el firmante ha perdido el control o custodia sobre los mismos, y en general cualquier otra situación que ponga en duda la seguridad de la firma electrónica o que genere reparos sobre la calidad de la misma.

Artículo 6°. *Firma electrónica pactada mediante acuerdo* EDI. Salvo prueba en contrario, se presume que los mecanismos o técnicas de identificación personal o autenticación electrónica que acuerden utilizar las partes mediante acuerdo EDI, cumplen los requisitos de firma electrónica.

Las partes que suscriban acuerdos EDI en el [sic] que pacten utilizar la firma electrónica como medio de identificación personal no negarán a la misma admisibilidad y valor probatorio entre sí o ante terceros.

Artículo 7°. *Admisibilidad y valor probatorio.* La firma electrónica será admisible como prueba en toda actividad de naturaleza pública o privada frente a particulares, las autoridades públicas, la Administración de Justicia y en general frente a todas las ramas del Poder Público, los órganos de control y la Organización Electoral.

De conformidad con el artículo 11 de la ley 527 de 1999, para la valoración de la fuerza probatoria de la firma electrónica, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado la firma electrónica y conservado la integridad de la información, y cualquier otro factor pertinente.

Artículo 8°. *Criterios para establecer el grado de seguridad de las firmas electrónicas.* Para determinar si los procedimientos, métodos o dispositivos electrónicos que se utilicen como firma electrónica son seguros, y en qué medida lo son, podrán tenerse en cuenta los siguientes factores:

a) El grado de cumplimiento de los estándares establecidos para el efecto por la Superintendencia de Industria y Comercio.

b) El concepto técnico emitido por un órgano independiente y especializado.

c) La existencia de una auditoría especializada, periódica e independiente sobre los procedimientos, métodos o dispositivo electrónicos que una parte suministra a sus clientes o terceros como mecanismo electrónico de identificación personal.

d) Cualesquiera otros factores pertinentes.

Artículo 9º. El presente decreto rige a partir de su publicación en el *Diario Oficial* y deroga todas las normas que le sean contrarias.

Publíquese y cúmplase.

Dado en Bogotá, D. C., a los [...]

El Ministro de Comercio, Industria y Turismo

Luis Guillermo Plata Páez

VI. Bibliografía

Organización de las Naciones Unidas (onu)-Uncitral, "Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas", Viena, 2009.

Ortega Díaz, Juan Francisco, *La firma y el contrato de certificación electrónicos*, Aranzadi, España, 2008.

Remolina Angarita, Nelson, "Aspectos legales del comercio electrónico, la contratación y la empresa electrónica", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, núm. 2, Bogotá, Facultad de Derecho de la Universidad de los Andes, 2006.

— "Falacias en torno a las discusiones de la firma digital", en *Ámbito Jurídico*, núm. 283, 2009.

— "La protección de datos personales y las firmas digitales: dos temas para repensar y actuar", en *Ámbito Jurídico*, noviembre de 2009.

— Documento gecti núm. 10 titulado "Pensar en las necesidades del país o mantener a ultranza un *statu quo* para la firma digital de las entidades de certificación abierta –eca–" Bogotá, marzo de 2010. Disponible en: http://gecti.uniandes.edu.co/documentos.php

Rincón Cárdenas, Erick, "Discusiones alrededor de la firma digital", en *Ámbito Jurídico*, núm. 281, 2009.

— "Sobre el proyecto de reglamentación de firmas electrónicas", en *Ámbito Jurídico*, núm. 289, 2010.

Rodríguez Parra, César Felipe, "Documentos electrónicos como pruebas claves en litigios empresariales", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, núm. 1, 2005.

Rodríguez Turriago, Omar, "Diez años de la ley 527 de comercio electrónico: reflexiones sobre la necesidad de su modernización", en *Ámbito Jurídico*, agosto de 2009.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Conceptos:

— 1007028, del 21 de marzo de 2001.

— 3046333, del 25 de junio de 2003.

— 5037703, del 14 de junio de 2005.

UMAÑA CHAUX, Andrés Felipe, "Algunos comentarios sobre el principio del equivalente funcional en la ley 527 de 1999", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, núm. 1, abril de 2005.

CAPÍTULO II

VALORACIÓN DE LA EVIDENCIA DIGITAL: ANÁLISIS Y PROPUESTA EN EL CONTEXTO DE LA ADMINISTRACIÓN DE JUSTICIA EN COLOMBIA

Andrea Rueda Plazas y Jeimy J. Cano

Si la inseguridad jurídica es la norma
en un mundo interconectado,
la administración de la evidencia digital
debería ser la constante
Jeimy J. Cano

I. Introducción

Con la llegada de las nuevas ciencias aplicadas, que controvierten y modifican en gran medida la actividad humana, es claro que el derecho y la tecnología son dos conceptos inherentes a las sociedades modernas. La revolución en el campo de las telecomunicaciones se ha dado gracias al advenimiento de nuevas redes de comunicación por medios informáticos, los cuales le han otorgado al hombre la disposición de novedosos canales de transmisión de información, como el correo y el comercio electrónico. Así, conceptos tales como la Internet, el mensaje de datos, la firma electrónica y demás, están tomando cada vez más fuerza,

relevancia y aceptación en las constantes relaciones y negocios celebrados entre particulares.

En Colombia tal problemática no es ajena a la realidad jurídica. En la actualidad su sistema legal cuenta con normas como la ley 527 de 1999, que incursiona el nuevo concepto del equivalente funcional, y la ley 962 de 2005 (conocida también como ley antitrámites o de racionalización de éstos), la cual, en cierta medida, agiliza los procedimientos judiciales; normatividades que dan respuesta a una práctica social creciente entre comerciantes y entre ciudadanos del común. Lo anterior, con el objetivo de generar un mínimo de seguridad jurídica a la hora de efectuar transacciones y negocios, ya no por el medio escrito tradicional, sino mediante correos electrónicos, páginas *web* y demás campos de acción ofrecidos por la Internet.

A pesar de contar con normatividades que regulan la materia, en Colombia sigue latente la problemática sobre la valoración de las pruebas digitales aportadas en un proceso en cuanto generan dudas sobre la confidencialidad, la integridad y la autenticidad de la información presentada en un formato de mensaje de datos o en otro tipo de documento electrónico.

Lo anterior arroja como consecuencia principal que, en la mayoría de los casos, dichas pruebas sean valoradas como meros indicios o por el concepto técnico de un perito. Ambos, a pesar de ser idóneos a la hora de brindarle certeza al juez sobre los hechos, además de restarle eficiencia y eficacia al proceso judicial abruman la fuerza probatoria de la evidencia digital, impidiéndole que entre al proceso por la puerta principal, es decir, como una prueba en sí.

En el presente capítulo se hará un breve recuento de la situación actual de la prueba electrónica en el derecho comparado, especificando las regulaciones con las que cuentan algunos países. Así mismo, se analizará la problemática de la prueba electrónica en Colombia y sus posibilidades

de valoración. Además, se estudiará la necesidad de implementar un plan de buenas prácticas para la admisión y valoración de la evidencia digital y, en consecuencia, se planteará una propuesta de buenas prácticas para la admisión y valoración de la prueba digital en el ordenamiento jurídico colombiano, bajo los preceptos planteados por el documento HB 171:2003, que se encuentre acorde con sus propias necesidades. La propuesta representará, por lo tanto, una respuesta para los operadores jurídicos frente a la evidencia digital en determinado proceso. Finalmente, se expondrán unas breves conclusiones.

II. La prueba electrónica en el derecho comparado

En todos los países se ha vuelto indispensable adaptar las leyes vigentes a las nuevas concepciones técnicas y tecnológicas, con el fin de dar respuestas a las necesidades derivadas de la práctica jurídica[1] y a las exigencias propias de un mundo globalizado, en los asuntos comerciales, civiles, entre otros. Lo anterior tiene como objetivo principal que cada uno de los sistemas jurídicos posea la capacidad de regular los cambios de sus sistemas económicos y sociales, permitiendo, con ello, que el propio derecho no se vuelva arcaico e ineficaz.

Es claro que tanto la Internet como los medios electrónicos se han convertido en los instrumentos más rápidos para realizar negocios a nivel nacional e internacional, por cuanto a través de ellos se pueden perfeccionar y concretar transacciones en cuestión de segundos, transacciones que traen consigo efectos e implicaciones jurídicas.

Las pruebas electrónicas de dichas transacciones, susceptibles de ser aportadas a un proceso determinado, se pueden ver afectadas por una

[1] La práctica jurídica hace alusión al diario vivir de los abogados y los operadores jurídicos, que se enfrentan constantemente con casos expuestos a la luz del derecho y de su normatividad.

valoración deficiente por parte del juez. Esto, en cuanto no existen criterios o requisitos que guíen la actividad valorativa de la evidencia digital a nivel nacional e internacional, dejando tal acción al libre albedrío de la razón y de la sana crítica. Éstos, si bien son útiles y suficientes en determinados casos, en el campo de la informática y, más específicamente, de la evidencia digital, dada su especialidad, requieren de una valoración más clara y detallada que cualquier otro medio probatorio.

Los países pioneros en regular la materia en la Comunidad Europea fueron Alemania, Italia y España. En este último se sancionó el real decreto ley 14 sobre la firma electrónica, en el año 1999,[2] en donde se le otorgó a dicha firma el mismo valor jurídico de la manuscrita. El decreto, a su vez, recaudó los elementos suficientes para proteger la seguridad y la integridad de las comunicaciones telemáticas en las que se emplee la firma electrónica.

Sumado a lo anterior, también se expidió el real decreto ley 1906 de 1999,[3] el cual regula la contratación telefónica o electrónica general. Éste se justifica por la necesidad de desarrollar el artículo 5° de la ley 7 de 1998, del 13 de abril, sobre condiciones generales de la contratación, que en su apartado 3 dice textualmente: "en los casos de contratación telefónica o electrónica será necesario que conste en los términos que reglamentariamente se establezcan la aceptación de todas y cada una de las cláusulas del contrato, sin necesidad de firma convencional. En este supuesto, se enviará inmediatamente al consumidor justificación escrita de la contratación efectuada, donde constarán todos los términos de la misma".

En Estados Unidos, por su parte, gracias a la costumbre y a desarrollos jurisprudenciales, ha sido generalizada la aceptación de la evidencia

[2] Ministerio de Industria, Turismo y Transporte de España, real decreto ley 14, consultado el 8 de noviembre de 2005. Disponible en: http://www.setsi.mcyt.es/legisla/internet/rdley14_99.htm.

[3] Real decreto ley 1906 de 1999, de España, consultado el 8 de noviembre de 2005. Disponible en: http://www.aeat.es/normlegi/ecomercio/rd171299.htm.

digital como prueba válida dentro de los procesos judiciales. La codificación de la costumbre fue lograda bajo lo estipulado por las *Uniform Rules of Evidence*[4] y las *Federal Rules of Evidence*.[5] La segunda normatividad regula la introducción de la evidencia en los procedimientos civiles y criminales en las Cortes federales de los Estados Unidos.

En concordancia con lo anterior, una de las leyes más recientes sancionadas por dicho país es la *Electronic Signatures in Global and National Commerce Act* del 2000, la cual establece principios generales como:

> [...] "1) El desarrollo y uso de los registros electrónicos y la firma electrónica deberían ser regulados por los principios de libre mercado y autorregulación antes que la fijación estatal de reglas; 2) Los principios de neutralidad y no discriminación entre proveedores de tecnología para el registro electrónico y la firma electrónica; 3) Las partes en una transacción pueden establecer requerimientos relativos al uso de la firma electrónica aceptables para esas partes; 4) Las partes pueden determinar los procedimientos de autenticación y ellos deben ser aceptados, dándoles ejecutabilidad y debiendo ser reconocidos como prueba; 5) No puede negarse validez y efecto a los registros electrónicos y la firma electrónica otorgados en una forma aceptada por las partes, sobre la base de que no son escritos; 6) No se debe discriminar en favor de una tecnología, proceso, técnica específica de creación, generación, almacenamiento, registro, comunicación o autenticación de firmas".[6]

[4] *Uniform Rules of Evidence*, consultado el 8 de noviembre de 2005. Disponible en: http://www.law.upenn.edu/bll/ulc/ure/evid1200.htm.

[5] *Federal Rules of Evidence*, consultado el 8 de noviembre de 2005. Disponible en: http://www.law.upenn.edu/bll/ulc/ure/evid1200.htm.

[6] *Electronic Signatures in Global and National Commerce Act*, del año 2000, consultado el 8 de noviembre de 2005. Disponible en: http://www.ricardolorenzetti.com.ar/secciones/comercio_electronico1.htm.

Las anteriores normatividades fueron expedidas con la intención de lograr una mayor seguridad jurídica para aquellos negocios celebrados por medios electrónicos.

Así las cosas, la comisión de las Naciones Unidas, desde la década de los sesenta, se ha propuesto la tarea de facilitar los procedimientos del comercio internacional por medio de normas que agilicen los trámites y disminuyan los requisitos excesivos. Por lo anterior, dicho organismo, desde comienzos de los años noventa, ha venido promoviendo la elaboración de leyes modelos para el Intercambio Electrónico de Datos (EDI), por medio de la Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional (CNUDMI), conocida también como la Uncitral.

Tales esfuerzos se vieron materializados con la reciente Ley Modelo sobre Comercio Electrónico de Uncitral,

> [...] la cual fue inspirada en la convicción de que al dotársele de fundamentación y respaldo jurídicos, se estimularía el uso de los mensajes de datos y del correo electrónico para el comercio, al hacerlos confiables y seguros, lo cual, de contera, redundaría en la expansión del comercio internacional, dadas las enormes ventajas comparativas que gracias a su rapidez, estos medios ofrecen en las relaciones de índole comercial entre comerciantes y usuarios de bienes y servicios.[7]

El proyecto tiene como novedad el concepto del *equivalente funcional*, la cual consiste en suplir las exigencias formales como la firma, el requisito que conste por escrito, entre otros, por equivalentes electrónicos que cumplan con la misma función, más eficaces para los fines del comercio electrónico. A su vez, resuelve el problema de admisibilidad y fuerza probatoria de los mensajes de datos, pues suple tal dificultad por *la regla de la mejor*

[7] Colombia, Corte Constitucional (2000), "Sentencia C-662", M. P.: Morón Díaz, F.

prueba. Dicha solución no opera en los países de corte continental o civil, en cuanto su aplicación no ha sido aceptada por sus Tribunales y Cortes.

En los países latinoamericanos también se han sancionados leyes que regulan el comercio electrónico. Aunque su llegada ha sido tardía, en la actualidad cuentan con una normatividad sólida y estable sobre el tema. Tal es el caso de Perú, que en el año 2000 sancionó la ley 27269, de firmas y certificados;[8] Argentina, que promulgó la ley 25506,[9] sobre la firma digital; Venezuela, que reguló las firmas digitales, los certificados electrónicos y los proveedores de servicios de certificación; Chile, que sancionó la ley 19789, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma;[10] Ecuador, que promulgó la ley 57 de 2002, la cual regula el comercio electrónico, las firmas y los mensajes de datos; México, que en el año 2000 sancionó la ley 500 sobre el comercio electrónico; entre otras.

Todas las regulaciones mencionadas tuvieron como fuente de derecho y como espíritu la ley modelo del proyecto Uncitral, que ha inspirado las normatividades nacionales y a su vez les ha brindado el fundamento necesario y las herramientas para regular un tema tan novedoso como lo es el comercio electrónico y todos sus derivados.

De la mano de todas las normatividades expuestas se puede decir que el tema del comercio electrónico y en especial del mensaje de datos, se encuentra debidamente regulado por las normatividades internacionales. Ello por cuanto la práctica electrónica pasó, de desconocida, a ser promovida por los Estados, pues facilita las transacciones propias del mundo global en el que vivimos.

[8] Ley 27269, de firmas y certificados, de Perú, consultado el 8 de noviembre de 2005. Disponible en: http://www.indecopi.gob.pe/upload/crt/firmasDigitales/reglamentods019-2002-jus.PDF.

[9] Ley 25506, sobre la firma digital, de Argentina, consultado el 8 de noviembre de 2005. Disponible en: http://www.safjp.gov.ar/digesto2/index/normas/LEY%2024241/Ley25506.htm.

[10] Ley 19789, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, de Chile, consultado el 8 de noviembre de 2005. Disponible en: http://www.cedi.uchile.cl/docs/Ley19799.pdf.

III. PROBLEMÁTICA SOBRE LA VALORACIÓN DE LA PRUEBA ELECTRÓNICA EN COLOMBIA

Para comprender la problemática de la prueba electrónica en Colombia será necesario analizar la doctrina general de la prueba y su regulación, esta última establecida en el Código de Procedimiento Civil. Es así como, a continuación, se estudiarán la normatividad y cada uno de los conceptos desarrollados por la doctrina jurídica.

La prueba judicial, aunque tiene un sentido polifacético, es definida por la doctrina como "el conjunto de motivos o razones que nos suministran el conocimiento de los hechos, para los fines del proceso, que de los medios aportados se deducen".[11]

Los principales elementos de la prueba judicial son:

1. *El objeto de la prueba*: son los hechos susceptibles de ser probados. Éstos son esgrimidos por la doctrina como todos los sucesos, acontecimientos, hechos o actos humanos, voluntarios o involuntarios, individuales o colectivos, que sean perceptibles; sus circunstancias de tiempo, modo y lugar; los hechos de la naturaleza en que no interviene actividad humana; las cosas o los objetos materiales y cualquier situación de la realidad material sean o no producto del hombre, incluyendo los documentos; la persona física humana, su existencia y características.[12]
2. *El tema de la prueba*: se refiere a los elementos fácticos que demanda la norma demostrar para establecer la aplicación de ésta. En palabras del doctor Jairo Parra Quijano, el tema de la prueba "está constituido

[11] Devis Echandía, Hernando, *Teoría general de la prueba judicial*, t. I, Medellín, Biblioteca Jurídica Dike, 1987, p. 25.

[12] Devis Echandía, Hernando, *Compendio de derecho procesal, pruebas judiciales*, t. II, 7ª edición, Bogotá, ABC, 1982, p. 46.

por aquellos hechos que son necesarios de probar, por ser los supuestos de las normas jurídicas cuya aplicación se discute en un determinado proceso".[13]

3. *El fin de la prueba*: es la creación de la certeza en el juez, es decir, la prueba busca indagar la verdad de los hechos ocurridos en el pasado para que en el presente y en la conciencia del juez se pueda fallar acorde con la realidad de las cosas y no ante hechos hipotéticos.

El artículo 174 del Código de Procedimiento Civil establece: "toda decisión judicial debe fundarse en la prueba regular y oportunamente allegada al proceso", es decir, toda sentencia ha de estar soportada por pruebas legales que reposen en el expediente, estableciendo como requisito principal la necesidad de la prueba. Lo anterior significa que el juez no tendrá la facultad de dirimir la controversia planteada sin pruebas fundamentando su convicción. Esto con el fin de evitar decisiones arbitrarias y discrecionales.

Acorde a lo anterior, la sentencia de la Corte Suprema de Justicia de marzo 27 de 1998 desarrolla el artículo 174 del Código de Procedimiento Civil, aduciendo:

> [...] las pruebas producidas, con el objeto de que cumplan con su función de llevar al juez el grado de convicción suficiente para que pueda decidir sobre el asunto materia de la controversia, además de ser conducentes y eficaces, deben allegarse y practicarse en los términos y condiciones establecidos de antemano en el ordenamiento positivo, ya que de lo contrario no es posible que cumplan la función señalada, así lo estipula el artículo 174 del

[13] Parra Quijano, Jairo, *Manual de derecho probatorio*, 7ª edición, Bogotá, Librería del Profesional, 1986, p. 78.

Código de Procedimiento Civil, al tenor del cual "toda decisión judicial debe fundarse en pruebas regular y oportunamente allegadas al proceso".[14]

Siguiendo con la línea argumentativa planteada, y teniendo en cuenta el precepto legal del artículo 174 del Código de Procedimiento Civil, el juez debe dirimir toda controversia a partir de las pruebas que consten en el proceso, con base en la valoración que éste haga de cada una de ellas. La doctrina se ha pronunciado al respecto y determinado como sistemas para la valoración de la prueba *la tarifa legal* y *la libre convicción*. La primera es aquella donde el legislador señala el valor de la prueba, es decir, que determina los parámetros de valoración; mientras que la segunda es cuando el juez puede y debe libremente valorar la prueba[15] bajo los conceptos de la sana crítica y de la razón.

En tanto lo anterior, en Colombia el artículo 187 del Código de Procedimiento Civil[16] indica que el juez deberá apreciar las pruebas en conjunto, o sea que no podrá fallar por la simple apreciación de una de éstas sino por el convencimiento derivado de la pluralidad de pruebas oportuna y regularmente aportadas al proceso. La acción del juez en la valoración e interpretación de ellas habrá de seguir los criterios de la sana crítica y de la razonabilidad, tal como lo establece la ley. De lo anterior se esgrime que el sistema probatorio colombiano se basa en el sistema de la *libre convicción*, por cuanto es el juez quien tiene la facultad de darle valor probatorio a las pruebas.

[14] Colombia, Corte Suprema de Justicia, Sala de Casación Civil (1998), "Sentencia de marzo 27", expediente 4943, M. P.: Jaramillo Schloss, C. E.

[15] Ob. cit., Parra Quijano, Jairo, *Manual de derecho probatorio*, p. 109.

[16] Código de Procedimiento Civil, artículo 187: *Apreciación de las pruebas*. Las pruebas deberán ser apreciadas en conjunto, de acuerdo con las reglas de la sana crítica, sin perjuicio de las solemnidades prescritas en la ley sustancial para la existencia o validez de ciertos actos.

El juez expondrá siempre razonadamente el mérito que le asigne a cada prueba.

Así las cosas, es pertinente mencionar que un determinado proceso no podrá constar de pruebas legalmente prohibidas o ineficaces, ni impertinentes o superfluas, pues el artículo 178 del Código de Procedimiento Civil[17] lo prohíbe. Al respecto, la sentencia del Tribunal Superior de Bogotá ha dicho que el Código de Procedimiento Civil *ha entendido* por

> [...] pruebas legalmente prohibidas aquellas tendientes a demostrar hechos que la ley prohíbe investigar, como son aquellas en defensa de la moral. [...] Por ineficaces cuando se trata de un medio por el cual es jurídica o legalmente imposible probar el hecho a que se refiere ya sea porque se exige un medio por el cual es jurídica o legalmente imposible probar el hecho a que se refiere ya sea porque se exige un medio determinado de prueba (ej. escritura pública o documento privado para determinados actos o contratos). [...] Por impertinentes aquellas que tratan de probar un hecho que nada tiene que ver con lo discutido dentro del proceso y por superfluas aquellas que se hacen innecesarias en virtud de haberse practicado ya dentro del proceso suficientes pruebas para darle la plena certeza sobre un hecho determinado.[18]

Antes de "aterrizar" toda la teoría y regulación planteada a la prueba electrónica, será necesario detenernos en los conceptos básicos del equivalente funcional, conceptos que fueron inmersos en el sistema jurídico colombiano por la ley 527 de 1999.

Ahora bien, en este punto es preciso detenerse y comprender el alcance general del principio del equivalente funcional, el cual tiene como finalidad adaptar y darle la misma fuerza probatoria de los documentos consignados en papel a los contenidos en formato de mensajes

[17] Código de Procedimiento Civil, artículo 178: *Rechazo* in limine. Las pruebas deben ceñirse al asunto materia del proceso y el juez rechazará *in limine* las legalmente prohibidas o ineficaces, las que versen sobre hechos notoriamente impertinentes y las manifiestamente superfluas.

[18] Colombia, Tribunal Superior de Bogotá (1978), "Auto de junio 19", M. P.: Rodríguez Robayo, H.

de datos, firmas electrónicas y demás conceptos tecnológicos. Lo anterior pretende cumplir con los mandatos estipulados por la ley, al incorporarle los requisitos de forma a los documentos electrónicos, como son, fiabilidad, inalterabilidad y rastreabilidad. Es decir, el principio en mención establece que un mensaje de datos que cumpla con la función de declaración o representación tendrá los mismos efectos jurídicos propios de los medios de prueba tradicionales.

En conclusión, los documentos electrónicos o mensajes de datos están en la capacidad de brindar equivalentes grados de seguridad que los documentos consignados en papel y, en muchos casos, un mayor nivel de confiabilidad y rapidez. Para poder predicar un grado de seguridad confiable se deberá cumplir con los requisitos técnicos y jurídicos plasmados en la ley, cuestión que se hace palpable en el derecho colombiano con la llegada del principio del equivalente funcional.

Es preciso decir que la ley 527 de 1999 surge como una norma interpretativa de la regulación actual, por cuanto los equivalentes funcionales esgrimidos en ella permiten una interpretación actualizada y acorde con las necesidades de la realidad tecnológica, adaptando las normatividades ya vigentes al mundo contemporáneo.

Así las cosas, el mensaje de datos es definido por la ley 527 como "la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el EDI, la Internet, el correo electrónico, el telegrama, el télex o el telefax".[19]

Los requisitos de forma exigidos para las diversas actuaciones quedarán suplidos para la información consignada en mensaje de datos de la siguiente forma:

[19] Ley 527 de 1999, artículo 2°: *Definiciones*. Para los efectos de la presente ley se entenderá por: a) Mensaje de datos. 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; (...).

1. *Equivalente funcional del escrito*: a pesar de que el escrito cumple un sinnúmero de funciones, la ley 527 consideró que la más relevante es la de permitir el acceso de la información almacenada en el mensaje de datos con posterioridad a su creación. Lo anterior se deriva del artículo 6° de la ley en cuestión, el cual consagra:

> Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta. Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso de que la información no conste por escrito.[20]

2. *Equivalente funcional de la firma*: las funciones generales de la firma son las de identificar a alguien y vincular a esa persona con el contenido del documento. La legislación comercial define la firma como: "...la expresión del nombre del suscriptor o de alguno de los elementos que la integren o de un signo o símbolo empleado como medio de identificación personal".[21] El equivalente de firma manuscrita es la firma electrónica o la firma digital. Aunque no son iguales ni estamos hablando de lo mismo, las dos son jurídicamente válidas.
3. *Equivalente funcional del original*: a diferencia de los demás equivalentes, la función de éste sufre una gran modificación, por cuanto el acceso a la información consignada en formato de mensaje de datos necesariamente implica realizar una copia de la información consignada en ella. Por tal motivo, el original se suple en los mensajes de

[20] Umaña Chaux, Andrés Felipe, "Algunos comentarios sobre el principio del equivalente funcional en la ley 527 de 1999", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, vol. I, Bogotá, Universidad de los Andes, 2005, pp. 75-111.

[21] Cfr. Código de Comercio, artículo 826.

datos siempre y cuando exista una garantía confiable de que la información almacenada se ha conservado íntegra desde el momento de su creación de forma final. El artículo 8° de la ley 527 es el encargado de regular la materia en los siguientes términos:

> Cuando cualquier norma requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos, si: a) Existe alguna garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma; b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona que se deba presentar. Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

Los equivalentes funcionales de escrito y firma se armonizan con la realidad gracias al principio de neutralidad tecnológica consagrado en los artículos 6° y 7° de la ley 527, los cuales establecen que no será necesario el uso de una tecnología específica para lograr el equivalente de cada uno de ellos, por cuanto éstos quedan satisfechos con el cumplimiento de las funciones establecidas para cada caso en concreto, cuestión que servirá para que un mensaje de datos se entienda firmado o conste por escrito.[22]

Todo lo anterior nos permite analizar la problemática de la prueba electrónica en Colombia y, en especial, la valoración de ésta. Ello, teniendo en cuenta que la prueba electrónica es otro tipo de prueba

[22] Ob. cit., *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, p. 88.

físicamente concebida, que encuentra su soporte en un medio magnético, sin perjuicio de que por regla general sea considerada una prueba documental.[23]

Es así como la valoración de la prueba electrónica, además de contener y cumplir las normas consagradas en los artículos 174 y siguientes del Código de Procedimiento Civil, deberá reunir los requisitos establecidos por la ley 527 de 1999, analizados con anterioridad.

Los requisitos de admisibilidad de la evidencia digital se encuentran desarrollados en el artículo 10 de la mencionada ley, que estipula:

> 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 Código de Procedimiento Civil. En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho [de] que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.

A partir del precepto anterior, el juez no podrá negarle fuerza probatoria ni admisibilidad a los mensajes de datos por el simple hecho de ser mensaje de datos. Esto por cuanto se presentaría una ilegalidad[24] por parte de éste, al contrariar los mandatos establecidos en la ley.

Sabiendo de antemano que las pruebas en el régimen probatorio civil

[23] La evidencia documental está constituida por todo tipo de escritos, grabaciones de audio o video, grabaciones de diversos sistemas de información, fotografías, reportes de exámenes médicos o cualquier objeto similar o análogo a éstos. Tomado de *La prueba en el sistema penal acusatorio*, cap. 7. Disponible en: http://www.fiu.edu. co/fiu/dp/cdinteractivo/Manuales%20y%20Formatos/Modulo%20de%20Pruebas.pdf.

[24] La conducta antes descrita se encuentra tipificada por el artículo 230 de la Constitución, en cuanto el juez en sus providencias sólo está sometido al imperio de la ley y deberá cumplir a cabalidad con cada uno de sus preceptos. La normatividad establece: "Los jueces, en sus providencias, sólo están sometidos al imperio de la Ley. La equidad, la jurisprudencia, los principios generales del derecho y la doctrina son criterios auxiliares de la actividad judicial".

deberán ser valoradas por la sana crítica y la razonabilidad del juez, para el caso de la prueba electrónica éste también deberá cumplir con la normatividad estipulada por la ley 527 de 1999. Es decir que, sumado a los criterios de la sana crítica y de la razonabilidad, el juez —como consecuencia de la especialidad de la evidencia digital— deberá "estudiar y valorar la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje; la confiabilidad en la forma en que se haya conservado la integridad de la información; y la forma en la que se identifique a su iniciador y cualquier otro factor pertinente".[25]

A continuación se esgrimirán cada uno de los elementos mencionados, que son también entendidos como las garantías de la información en documento electrónico:

- *Autenticidad:* hace referencia a la capacidad de determinar si una persona ha establecido su reconocimiento y vinculación sobre el contenido del documento electrónico. Lo anterior se comprende de dos elementos principales: en primera medida, "que dicha evidencia haya sido generada y registrada en el lugar de los hechos", y la segunda, "que muestre 'la no alterabilidad de los medios originales', es decir, que los registros correspondan efectivamente a la realidad y que son un fiel reflejo de la misma".[26]

[25] Ley 527 de 1999, artículo 11. "*Criterio para valorar probatoriamente un mensaje de datos.* Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente".

[26] Mosquera González, José Alejandro; Certain Jaramillo, Andrés Felipe; Cano, Jeimy J., "Evidencia digital: contexto, situación e implicaciones nacionales", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, vol. I, Universidad de los Andes, 2005, p. 186.

Ello se vislumbra en el sistema jurídico colombiano a partir de dos normatividades, ya sean documentos públicos o privados. [27] Los primeros de ellos se entienden auténticos siempre y cuando no obre prueba en contrario o no se hayan tachado de falsos;[28] mientras que a los segundos la ley sólo los considera auténticos en los siguientes casos:

> [...] i) Si ha sido reconocido ante el juez o notario, o si judicialmente se ordenó tenerlo por reconocido; ii) Si fue inscrito en un registro público a petición de quien lo firmó; iii) Si habiéndose aportado a un proceso y afirmado estar suscrito, o haber sido manuscrito por la parte contra quien se opone, ésta no lo tachó de falso oportunamente, o los sucesores del causante a quien se atribuye dejaren de hacer la manifestación contemplada en el inciso segundo del artículo 289. Esta norma se aplicará también a las reproducciones mecánicas de la voz o de la imagen de la parte contra quien se aducen, afirmándose que corresponde a ella; iv) Si fue reconocido implícitamente de conformidad con el artículo 276; v) Si se declaró auténtico en providencia judicial dictada en proceso anterior, con audiencia de la parte contra quien se opone en el nuevo proceso, o en la diligencia de reconocimiento de que trata el artículo 274.[29]

[27] Para comprender con precisión la terminología jurídica en este caso, el documento, la ley y más exactamente el artículo 251 del Código de Procedimiento Civil, lo definen de la siguiente forma: "Son documentos los escritos, impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares. Los documentos son públicos o privados. Documento público es el otorgado por funcionario público en ejercicio de su cargo o con su intervención. Cuando consiste en un escrito autorizado o suscrito por el respectivo funcionario, es instrumentos público; cuando es otorgado por un notario o quien haga sus veces y ha sido incorporado en el respectivo protocolo, se denomina escritura pública. Documento privado es el que no reúne los requisitos para ser documento público".

[28] Código de Procedimiento Civil, artículo 252, modificado por la ley 794 de 2003: "Es auténtico un documento cuando existe certeza sobre la persona que lo ha elaborado, manuscrito o firmado. El documento público se presume auténtico, mientras no se compruebe lo contrario mediante tacha de falsedad. [...]".

[29] Código de Procedimiento Civil, artículo 252, modificado por la ley 794 de 2003, inciso 2, numerales 1 al 5.

A su vez, se presume la autenticidad de los documentos enviados por el iniciador cuando se hayan aplicado los procedimientos acordados para la emisión de mensajes de datos con miras a establecer que los mismos provenían de éste, tal como lo establece el artículo 17 de la ley 527. Mientras, los demás documentos, por el momento, son aptos para el estudio realizado por un perito experto en la materia, quien por medio de habilidades técnicas podrá determinar su autoría y su autenticidad.

a) *Originalidad:* se entiende por original cualquier obra literaria, artística, científica, entre otras, emanadas de la creación e imaginación de su autor. Como se mencionó en el equivalente funcional de original, una de las dificultades más grandes en el campo electrónico e informático consiste en que el original del documento electrónico en realidad es aquel que se encuentra en el equipo o en el computador donde su autor digitó o creó dicho escrito, o aquel que es extraído del dispositivo electrónico con técnicas o metodologías informáticas que conservan las características iniciales[30] de dicho archivo o documento digital. Por tal motivo, cualquier copia, impresión y demás, son reproducciones de éste, es decir, copias que ya pierden la garantía de ser originales.

Una excepción a la regla anterior para el caso colombiano se encuentra consignada en el artículo 254 del Código de Procedimiento Civil, el cual establece que las copias tendrán el mismo valor que el original, en los casos taxativamente señalados por él, los cuales son:

[30] La verificación de las características iniciales se puede adelantar con la validación de las características del archivo mediante una función de Hash. Esta función calcula un número único al aplicarse sobre un archivo y denota cambios en su resultado si al mismo documento se le han efectuado variaciones en su estructura o contenido.

"i) Cuando hayan sido autorizadas por notario, director de oficina administrativa o de policía, o secretario de oficina judicial, previa orden del juez, donde se encuentre el original o una copia autenticada; ii) Cuando sean autenticadas por notario, previo cotejo con el original o la copia autenticada que se le presente; iii) Cuando sean compulsadas del original o de copia autenticada en el curso de inspección judicial, salvo que la ley disponga otra cosa".

Siempre y cuando se cumpla con cualquiera de los casos descritos, las copias se tomarán como originales y por tal motivo pierden la calidad de copias. Las anteriores situaciones pueden ser aplicadas en los documentos electrónicos, en cuanto se verifiquen las características de copia digital idéntica, es decir, que se conservan las características iniciales del archivo identificado en el dispositivo electrónico.

- *No repudio:* es definida por la doctrina como "la capacidad de probar a una tercera parte que una determinada comunicación ha sido originada, admitida y enviada a una determinada persona".[31] El no repudio permite establecer el vínculo existente entre la voluntad de la persona y el contenido del documento. La diferencia principal entre la autenticidad y el no repudio es que lo primero logra establecer quién es el autor y cuál es su destinatario, mientras que con el *no repudio* se prueba que el emisor envió la comunicación y el destinatario la recibió sin error alguno.
  A pesar de la escasez de regulación sobre la *no repudiación* del contenido del documento, la ley 527 de 1999 en su artículo 23 establece que sin pacto en contrario entre el emisor y el receptor el tiempo del

[31] Ramos Suárez, Fernando, "Eficacia jurídica de una transacción electrónica. La figura del no repudio" en *Alfa-Redi*, núm. 12, consultado el 1° de diciembre de 2005. Disponible en: http://www.alfa-redi.org/rdi-articulo.shtml?x=300.

envío de un mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo control del iniciador o de la persona que envió el mensaje de datos en nombre de éste.[32] En ese instante, el mensaje queda por fuera de la esfera del emisor, cuestión que no le permite desistir de su contenido.

A su vez, el artículo 24 de la ley 527[33] consagra el tiempo de la recepción de un mensaje de datos, el cual será determinado a partir de cualquiera de las siguientes hipótesis:

a) Si el destinatario ha designado un sistema de información para la recepción de mensaje de datos, la recepción tendrá lugar: 1. En el momento en que ingrese el mensaje de datos en el sistema de información designado; o 2. De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos; b) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar cuando el mensaje de datos ingrese a un sistema de información del destinatario. Lo dispuesto en este artículo será aplicable aun cuando el sistema de información esté ubicado en lugar distinto de donde se tenga por recibido el mensaje de datos conforme al artículo siguiente.

[32] Ley 527 de 1999, artículo 23: "*Tiempo del envío de un mensaje de datos*. De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido cuando ingrese en un sistema de información que no esté bajo control del iniciador o de la persona que envió el mensaje de datos en nombre de éste".

[33] Ley 527 de 1999, artículo 24: "*Tiempo de la recepción de un mensaje de datos*. De no convenir otra cosa el iniciador y el destinatario, el momento de la recepción de un mensaje de datos se determinará como sigue: a) Si el destinatario ha designado un sistema de información para la recepción de mensaje de datos, la recepción tendrá lugar: 1. En el momento en que ingrese el mensaje de datos en el sistema de información designado; o 2. De enviarse el mensaje de datos a un sistema de información del destinatario que no sea el sistema de información designado, en el momento en que el destinatario recupere el mensaje de datos; b) Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar cuando el mensaje de datos ingrese a un sistema de información del destinatario. Lo dispuesto en este artículo será aplicable aun cuando el sistema de información esté ubicado en lugar distinto de donde se tenga por recibido el mensaje de datos conforme al artículo siguiente".

Tal garantía es cumplida cuando se prueba que la información emitida por el emisor fue satisfactoriamente recibida por el receptor y que éste tiene una estrecha relación con el contenido del mensaje de datos.

- *Integridad*: un documento se considera íntegro cuando "contiene toda la información que constaba al momento de su emisión, y que desde entonces no ha sido alterado".[34]

  Al respecto, la legislación colombiana no ha regulado la materia a cabalidad. Su normatividad se encuentra más encaminada a proteger la originalidad de los documentos, sin hacer mayores alusiones sobre la integridad de ellos. No obstante, sin importar la falta de normatividad al respecto, se puede decir que un documento por el simple hecho de ser auténtico goza de integridad, pero no necesariamente un documento considerado íntegro tendrá la característica de auténtico. Lo anterior significa que una de las características principales de la autenticidad es la integridad.

- *Confidencialidad*: dicha característica "garantiza que un documento sólo pueda ser leído por su destinatario, nos asegura que nadie más sabrá su contenido".[35]

  Esta garantía es propia del campo de las telecomunicaciones debido a que se trata de un medio en donde el usuario pretende realizar comunicaciones privadas, a diferencia de los medios de comunicación masivos, los cuales tienen por fin comunicar a la mayor cantidad de personas posible. Es por esto que quien realiza la comunicación es el que le da el carácter de privado o público a la información que pretende transmitir.

[34] Riofrío, Juan Carlos, *La prueba electrónica*, Bogotá, Temis, 2004, p. 105.

[35] Ibídem, p. 117.

En el caso de los mensajes informáticos que tienen como soporte una firma electrónica, ésta, "por tener una clave privada combinada con la pública, naturalmente ofrece un grado muy alto de confidencialidad que no le debe pasar inadvertido al juez".[36]

En conclusión, el régimen probatorio colombiano en la actualidad cuenta con un soporte jurídico apto para la aceptación y valoración de la evidencia digital o prueba electrónica. No obstante, vale la pena indicar que en la práctica jurídica tales preceptos legales son de difícil aplicación o desconocidos por los jueces. Lo anterior, por cuanto en el ordenamiento jurídico aquellas pruebas, como es el caso del mensaje de datos, no adquieren la misma fuerza probatoria o consistencia que cualquier otro medio de prueba, pues el juez decreta peritazgos o simplemente las valora como indicios graves, para su admisión y tratamiento. Esto, sabiendo de antemano que la prueba digital en sí ya se constituye como un medio probatorio idóneo para otorgarle al juez el convencimiento necesario sobre los hechos fundamento de la demanda y del proceso.

IV. Análisis de posibilidades probatorias

Una vez analizada la problemática de la prueba electrónica en Colombia, es preciso mencionar que el sistema de medios probatorios colombiano está compuesto por un catálogo abierto. Lo anterior significa que los medios referidos por él simplemente son enunciados o enumerados. Esto permite la incursión de nuevas técnicas probatorias pertinentes para cada caso en concreto. Tal interpretación se desprende del artículo 175 del Código de Procedimiento Civil, el cual menciona: "sirven como pruebas, la declaración de parte, juramento, el

[36] Ibídem, p. 122.

testimonio de terceros, el dictamen pericial, la inspección judicial, los documentos, los indicios y cualesquiera otros medios que sean útiles para la formación del convencimiento del juez. El juez practicará las pruebas no previstas en este código de acuerdo con las disposiciones que regulen medios semejantes o según su prudente juicio".

Al ser el artículo 175 del Código de Procedimiento Civil un catálogo no taxativo, la ley faculta al juez para decretar nuevos medios probatorios que no estén contemplados por dicha lista, los cuales, en determinado momento, pueden llegar a ser más eficaces a la hora de esclarecer los hechos objeto del litigio.

En concordancia con lo anterior, es pertinente mencionar que el equivalente funcional es simple y llanamente una norma interpretativa de las leyes ya vigentes. Permite, por lo tanto, expandir la concepción humana a nuevas posibilidades tecnológicas igual de idóneas a las tradicionales. Es así como, es posible asemejar las normas jurídicas a los hechos provenientes del mundo actual, permitiendo que éstos se encuentren debidamente regulados por el derecho y brindándole a las nuevas prácticas soporte y seguridad jurídica.[37]

Sin embargo, en la actualidad Colombia cuenta con dos alternativas jurídicas de valoración de la prueba electrónica que, a pesar de ser idóneas y eficaces para esclarecer los hechos de un caso, cuentan con problemas de tiempo, costos, especialidad y uso de tecnología

[37] En el Código de Procedimiento Penal —Ley 906 de 2004— se encuentra previsto el tema de pruebas novel en su artículo 422, que reza:

Artículo 422. "*Admisibilidad de publicaciones científicas y de prueba novel.* Para que una opinión pericial referida a aspectos noveles del conocimiento sea admisible en el juicio, se exigirá como requisito que la base científica o técnica satisfaga al menos uno de los siguientes criterios:

1. Que la teoría o técnica subyacente haya sido o pueda llegar a ser verificada.

2. Que la teoría o técnica subyacente haya sido publicada y haya recibido la crítica de la comunidad académica.

3. Que se haya acreditado el nivel de confiabilidad de la técnica científica utilizada en la base de la opinión pericial.

4. Que goce de aceptabilidad en la comunidad académica".

especial para la identificación y valoración de este tipo de prueba, problemas que pueden llegar a obstruir la eficiencia en la resolución del litigio.

En primer lugar, los hechos pueden ser valorados a través de un peritazgo decretado por el juez, el cual no es obligatorio y sí susceptible de ser objetado por cualquiera de las partes. El peritazgo es un medio de prueba tradicional enunciado en el catálogo abierto del artículo 175 del Código de Procedimiento Civil. La segunda alternativa que tiene el juez recae en la valoración de las pruebas electrónicas como meros indicios, por cuanto el mensaje de datos que determina la existencia de un hecho dentro del proceso podría no llegar a cumplir con los requisitos mínimos de seguridad jurídica, cuestión que puede no proporcionarle al juez confianza sobre la autenticidad de la información almacenada en un documento electrónico. Lo anterior trae como consecuencia el restarle fuerza probatoria a la evidencia aportada en formato de mensaje de datos, sin tener en cuenta que ésta es una prueba apta para darle certeza al juez sobre los hechos del caso en particular.

Así las cosas, la doctrina define el peritazgo como "una actividad procesal desarrollada, en virtud de encargo judicial, por personas distintas de las partes del proceso, especialmente calificadas por sus conocimientos técnicos, artísticos o científicos, mediante la cual se suministra al juez argumentos o razones para la formación de su convencimiento respecto de ciertos hechos cuya percepción o cuyo entendimiento escapa a las actitudes del común de las gentes".[38]

De esta forma, y como el juez no puede tener conocimiento de todas las ciencias, técnicas o áreas del conocimiento, es necesario recurrir a los peritos como auxiliares de la justicia. Ellos ayudan a resolver un

[38] Devis Echandía, Hernando, *Teoría general de la prueba*, t. II, 3ª edición, Buenos Aires, 1974, pp. 286 y ss.

determinado litigio, al esclarecer el saber del juez sobre los hechos objeto del experticio, otorgándole total certeza sobre éstos.[39]

Como se mencionó, el peritazgo, a pesar de ser un medio eficaz para brindarle certeza al juez sobre los hechos objeto del proceso, su práctica en el medio informático presenta problemas de costos, tiempo y probabilidades de éxito que llegan a dilatar el proceso. A su vez, y de no haber estándares para adelantar el procedimiento forense y valorar las pruebas recabadas en este proceso, se podría caer en ineficiencia en la resolución de eventuales litigios.

La experiencia estadounidense[40] ha demostrado que a un experto suele tomarle entre 10 y 50 horas su labor, dependiendo de las habilidades y destrezas del implicado dentro de un proceso específico, lo que dificulta el desempeño del perito. En cuanto a costos, éstos son de alrededor de 2 mil dólares en los casos pequeños o de menor cuantía y de 100 mil dólares en los grandes.[41]

Así las cosas, el peritazgo, a pesar de ser óptimo a la hora de suplir las necesidades del juez y esclarecer los hechos del caso, es una labor compleja la cual amerita tiempo y dinero, limitaciones que pueden llegar a perjudicar la eficacia de la justicia y la resolución de los conflictos.

Como segunda medida, los operadores jurídicos también valoran la prueba electrónica como un mero indicio, definido por la doctrina como "un hecho del cual se infiere otro desconocido. Debe quedar suficientemente claro que el indicio es, por así decirlo, un hecho especialmente cualificado, porque tiene la propiedad de salirse de sí mismo y mostrar otro".[42]

[39] Parra Quijano, Jairo, "Tratado de la prueba judicial", en *La prueba pericial y la inspección judicial*, t. V, 3ª edición, Bogotá, Librería del Profesional, 1988, p. 7.

[40] Para mayor información sobre casos en Estados Unidos, consultar: http://www.cybercrime. gov.

[41] Ob. cit., *La prueba electrónica*, p. 144.

[42] Parra Quijano, Jairo, *Tratado de la prueba judicial, indicios y presunciones*, t. IV, 3ª edición, Bogotá, Librería del Profesional, 1988, p. 21.

En el sistema jurídico colombiano los artículos 248 y siguientes del Código de Procedimiento Civil desarrollan el tema de los indicios, indicando que para considerarse un hecho como tal deberá estar debidamente probado dentro del proceso.[43] A su vez, el juez habrá de valorar los indicios en conjunto,[44] junto con las demás pruebas que reposen en el acervo probatorio del caso en concreto.

De esta forma, el indicio es el producto de una deducción lógica realizada por el juez de un hecho demostrado dentro del proceso, que afirma la existencia de otro desconocido, del cual no obra prueba alguna en el acervo probatorio. Por tal motivo, y en este caso en particular, es claro que los medios informáticos no entrarían como prueba sumaria, pues queda en manos del juez el otorgarle la fuerza probatoria y el grado de convencimiento a los medios informáticos bajo los criterios de la razón y de la sana crítica.

Como en el peritazgo, es pertinente y necesario aclarar que si bien estos medios de prueba son aptos para esclarecer los hechos de un determinado proceso, es comprensible que si un medio electrónico u óptico se vincula a un proceso por medio de dichas alternativas el juez le estaría restando eficacia a la evidencia electrónica.

V. HACIA UN ESTÁNDAR DE VALORACIÓN DE LA PRUEBA ELECTRÓNICA

De la misma forma, y aunque el peritazgo y el indicio son mecanismos eficientes y eficaces a la hora de esclarecer los hechos de un caso, claramente éstos sufren problemas de costos, tiempo y especialidad que, en determinado momento, pueden llegar a dilatar la decisión del juez.

[43] Código de Procedimiento Civil, artículo 248: "Para que un hecho pueda considerarse como indicio, deberá estar debidamente probado dentro del proceso".

[44] Código de Procedimiento Civil, artículo 250: "El juez apreciará los indicios en conjunto, teniendo en consideración su gravedad, concordancia y convergencia y su relación con las demás pruebas que obren en el proceso".

Por tal motivo, y con el fin de proporcionarle una herramienta eficiente al operador jurídico, se hace necesario fijar unos parámetros de valoración de la prueba electrónica cuyo principal propósito consista en evitar que los hechos de un determinado caso sean valorados como meros indicios o mediante peritazgos largos y costosos y, por lo tanto, lograr que el juez los admita como elementos formales. Es importante anotar que si bien de manera general las pruebas electrónicas son consideradas pruebas documentales, requieren de procedimientos técnicos y científicos específicos para su valoración como tales.

Lo anterior tiene como finalidad determinar en qué casos una evidencia digital debe ser admitida en un proceso como prueba plena, es decir, cuándo ésta cumple con la totalidad de los requisitos establecidos en la ley,[45] requisitos tanto de seguridad como de legalidad. A su vez, permite que el juez vislumbre si se hace necesario acudir a otros medios de prueba cuando las pruebas no satisfagan la totalidad de los requisitos y por ende no sean idóneas para crear un pleno convencimiento suyo sobre los hechos bajo estudio.

A continuación se explicarán las razones, tanto legales como de seguridad, que determinan la eficacia, alcance y eficiencia de la evidencia digital. Ello, en concordancia con la fuerza probatoria otorgada a los mensajes de datos por la ley 527 de 1999.

Las pruebas informáticas gozan de una eficacia natural por el simple hecho de ser documentos electrónicos. A pesar del deber existente en cabeza del legislador y del derecho positivo de regular y determinar el alcance de cada una de ellas, el alcance probatorio otorgado por el

[45] Los requisitos para el caso de los mensajes de datos son el equivalente funcional de escrito, firma, original, entre otros, y las formalidades para el perfeccionamiento de algunos negocios jurídicos celebrados por particulares, con el fin de que éstas sean cumplidas a cabalidad bajo el criterio y parámetros electrónicos. A su vez, la ley determina que un mensaje de datos deberá cumplir con requisitos de confidencialidad, integridad, no repudio, entre otros, los cuales brindan confianza al juez sobre la veracidad de la información contenida en el mensaje de datos.

derecho positivo no elimina la aptitud probatoria que reposa en los *documentos* electrónicos. En el caso colombiano, la ley 527 determina el alcance probatorio de la información contenida en forma de mensaje de datos, elevando la eficacia natural de éstos a mandatos legales y asimilando su fuerza probatoria a la de los documentos tradicionales.

A su vez, y en virtud de los principios de confidencialidad, integridad y autenticidad de los mensajes de datos, será necesario establecer pasos y requisitos mínimos a la hora de recolectar la prueba electrónica y de aportarla al proceso, con el fin de no ser ésta alterada o modificada por terceros.[46] Ello cumpliendo con una cadena de custodia que vinculará al recolector con el material recopilado y donde él deberá seguir cada paso, sin omisión alguna. De lo contrario el mensaje de datos podría perder fuerza probatoria.

En este sentido, y siempre y cuando se reúnan los requisitos legales y de seguridad informática, el juez podrá valorar los hechos provenientes de una evidencia electrónica como una prueba en sí, sin necesidad de acudir a los auxiliares de la justicia o de otorgarle la fuerza de un indicio. Lo anterior, en tanto se cumplan los requisitos de confidencialidad, integridad y autenticidad que tanto preocupan a los operadores jurídicos.

VI. PROPUESTA PARA COLOMBIA

Como se mencionó, la propuesta pretende otorgarle las herramientas suficientes al juez para la admisión y valoración de la prueba electrónica, pruebas que deberán cumplir con los requisitos establecidos en la ley, en procura de la conservación de la integridad, autenticidad y confidencialidad de la información contenida en el archivo electrónico.

[46] Lo que se exige en este proceso es asegurar la cadena de custodia del elemento material probatorio informático, lo cual se traduce en procedimientos propios de la informática forense al procesar una escena del crimen con componentes de alta tecnología.

Es pertinente mencionar que la neutralidad jurídica y tecnológica juega un papel de enorme importancia en el caso bajo estudio. Ello por cuanto las normatividades se encuentran redactadas con el ánimo de no quedar encasilladas a una técnica específica. Lo anterior permite que sus preceptos queden abiertos a las formas tecnológicas provenientes de nuevos avances científicos, garantizando así que las regulaciones no se limiten a una destreza concreta de seguridad, sino dejando latente la posibilidad de implementar nuevas pericias, provenientes de la constante evolución del hombre.

De esta forma, el siguiente estándar propondrá un conjunto de buenas prácticas para el sistema jurídico colombiano que tendrá como fundamento jurídico principal el documento HB 171-2003 del *Handbook of Guidelines for the Management of IT Evidence*.[47] Este estándar justificará la admisión y la valoración de la evidencia digital que cumpla, en su totalidad, con los pasos o requisitos planteados a continuación. Lo anterior promueve que la información se conserve integralmente, es decir, protegiendo la confiabilidad en la forma como se haya generado, archivado o comunicado el mensaje y se haya conservado la integridad de la información, señalando cómo se identifica a su iniciador y cómo se realizó la recopilación de la evidencia digital.[48]

A su vez, la propuesta de buenas prácticas recomienda la aplicación de una etapa de recolección de la prueba electrónica donde se

[47] El documento HB 171-2003 es una propuesta para el ordenamiento jurídico australiano que plantea una serie de buenas prácticas y de requisitos para la admisión de la prueba electrónica en dicho país.

[48] Ley 527 de 1999, artículo 11. "*Criterio para valorar probatoriamente un mensaje de datos.* Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente".

proteja la evidencia por medio de una cadena de custodia a cargo de un informático forense.[49] Esto con el fin de prevenir la alteración del documento por parte de terceros, una vez se haya recopilado y aportado al proceso todo el acervo probatorio digital.

La propuesta es la siguiente:

1. El juez deberá establecer qué pruebas son electrónicas y cuáles no, para determinar a cuáles evidencias digitales se les aplicará el estándar de valoración.
2. La persona natural o jurídica que pretenda hacer valer pruebas electrónicas dentro de un determinado litigio ha de diseñar o contar con un sistema computacional para la evidencia electrónica que permita verificar e identificar el documento electrónico y esté disponible a la hora de la creación, alteración y recolección de él.

   Con el fin de garantizar la efectividad y eficacia del diseño computacional, se requiere identificar al autor del documento electrónico y establecer fecha y hora de su creación o alterabilidad y la autenticidad del contenido del mensaje de datos mediante la confiabilidad de los programas computacionales que permitan la no incursión de terceros de mala fe en la información contenida en el medio informático.

   Los programas informáticos deberán fijar la autenticidad del documento electrónico mediante la identificación del documento original y sus posibles alteraciones. Es decir, el sistema computacional ha de tener la capacidad de detectar cualquier alteración del documento con respecto a la información del original.

[49] El informático forense funcionaría como un auxiliar de la justicia, encargado de vigilar y proteger la evidencia digital que se pretenda hacer valer dentro de un proceso determinado.

Es así como, el juez tendrá que valorar los métodos de seguridad implementados por las partes emisora y receptora. En este punto juegan un papel preponderante los sistemas de identificación y autenticación, criptografía, biométricos, entre otras técnicas ya implementadas, así como las que traiga la tecnología en el futuro. Es decir, el juez estudiará si el documento electrónico se encuentra sometido a un determinado método de seguridad para garantizar, con ello, la confiabilidad sobre el contenido del mensaje de datos.

3. En la etapa de elaboración del documento ha de contarse con un sistema que cumpla con la fase operacional de los pasos que se pretenden plantear, pues se requiere determinar qué computador específicamente fue el instrumento utilizado para la creación del mensaje de datos, estableciendo la fecha y la hora de ésta. A su vez, establecer que el programa computacional, en el momento de la creación o alteración del contenido del mensaje, funcionaba a cabalidad, sin error alguno. Lo anterior con el fin de no alterar la confiabilidad del documento y su integridad, sabiendo de antemano si el almacenamiento del mensaje de datos pudo contar con algún inconveniente técnico. De ser así, se desvirtuaría la seguridad de la técnica particular utilizada.

   De acuerdo con la técnica de seguridad implementada, el juez establece el grado de confianza que ella le brinde, esto es, analiza si el sistema implementado tanto por el emisor como por el receptor es confiable. Lo anterior significa que si el sistema utilizado es el de autenticación y clave, el juez —según su propio criterio y discrecionalidad— evaluará qué tan confiable pudo ser la clave y qué tan secreta.

4. En la fase de recolección de la evidencia, ésta deberá llevarse a cabo por un informático forense,[50] especializado en la materia.

[50] Ley 906 de 2004, artículo 236. "*Recuperación de información dejada al navegar por Internet u otros medios tecnológicos que produzcan efectos equivalentes.* Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para

Contar con dicho funcionario le daría mayor fuerza probatoria a la prueba electrónica, ya que el procedimiento le otorgará la confianza suficiente para admitir la prueba como evidencia dentro del acervo probatorio.

El informático forense debe hacer un recuento de cada uno de los procedimientos utilizados (captura de la evidencia volátil, la generación de la imagen idéntica (bit a bit) del medio, el aseguramiento del equipo o dispositivo electrónico, entre otros), los datos de fechas y horas de los documentos del computador, para generar la línea de tiempo de lo ocurrido con éstos. Así mismo, identificar a cada uno de los autores de los mensajes de datos (si es viable) y los hechos inmersos en el sistema computacional.

Sumado a lo anterior, será necesario implementar una cadena de custodia[51] de las evidencias recolectadas y allegadas al proceso, con el fin de evitar posibles intromisiones y alteraciones de terceros. Por tal motivo, parece conveniente seguir con los planteamientos del artículo 28851 del Código de Procedimiento Penal, el cual establece que se deberá aplicar la cadena de custodia a los elementos físicos materia de prueba, con el ánimo de garantizar la

inferir que el indiciado o el imputado ha estado transmitiendo información útil para la investigación que se adelanta, durante su navegación por Internet u otros medios tecnológicos que produzcan efectos equivalentes, ordenará la aprehensión del computador, computadores y servidores que pueda haber utilizado, disquetes y demás medios de almacenamiento físico, para que expertos en informática forense descubran, recojan, analicen y custodien la información que recuperen". [...]

[51] Código de Procedimiento Penal, artículo 288. "*Cadena de custodia*. Se debe aplicar la cadena de custodia a los elementos físicos materia de prueba, para garantizar la autenticidad de los mismos, acreditando su identidad y estado original, las condiciones y las personas que intervienen en la recolección, envío, manejo, análisis y conservación de estos elementos, así mismo, los cambios hechos en ellos por cada custodio. La cadena de custodia se inicia en el lugar donde se obtiene, encuentre o recaude el elemento físico de prueba y finaliza por orden de la autoridad competente. Son responsables de la aplicación de la cadena de custodia todos los servidores públicos y los particulares que tengan relación con estos elementos, incluyendo al personal de servicios de salud que dentro de sus funciones tengan contacto con elementos físicos que puedan ser de utilidad en la investigación. El Fiscal General de la Nación reglamentará lo relacionado con el diseño, aplicación y control del sistema de cadena de custodia, conforme con los avances científicos y técnicos".

autenticidad de los mismos y acreditar tanto su identidad y estado original, envío, manejo, análisis y conservación de estos elementos, como los cambios hechos en ellos por cada custodio.

Esta cadena ha de iniciarse en el lugar donde se obtiene la prueba y finalizar por orden judicial de la autoridad competente. Todos aquellos que tengan acceso a la evidencia digital serán responsables de llevar a cabo la cadena de custodia y se identificarán con el procedimiento implementado.

5. Si se cumplen los pasos mencionados, el juez debe admitir y aceptar el mensaje de datos como una prueba electrónica dentro del acervo probatorio del proceso. Además, dependiendo de la confidencialidad y el cumplimiento de los pasos planteados, podrá otorgarle —bajo su discrecionalidad— la fuerza probatoria que estime conveniente.

   A las partes les queda la posibilidad de controvertir la validez de la prueba o de tachar de falsa la información inmersa en el documento electrónico.

VII. Conclusiones

1. La propuesta de buenas prácticas para la admisión y valoración de la prueba electrónica, y la incursión de ellas en el sistema jurídico colombiano, tiene como principal ventaja el simple hecho de tener el juez una herramienta legal que le proporcionará seguridad, confiabilidad y certeza a la hora de admitir y valorar la evidencia digital, por cuanto tal práctica ya no queda sujeta a los criterios de la sana crítica y de la razonabilidad. Por lo tanto, el juez tendrá que entrar a analizar si la propuesta fue aplicada a cabalidad en la etapa de creación, de almacenamiento y de recopilación de la prueba digital, pues si alguno de los pasos llegare a faltar el juez

no le podrá otorgar la misma fuerza probatoria de aquel que haya cumplido a cabalidad con el estándar planteado. Es así como la tarea del juez ya no queda bajo su discrecionalidad, sino bajo los preceptos legales.

2. Una limitante para el sistema jurídico colombiano consiste en que, a pesar de contar en la actualidad nuestro ordenamiento jurídico con múltiples normatividades que regulan el nuevo campo de acción entre los particulares y la actividad estatal, todavía no existe una conciencia ni una cultura informática. Es decir, a pesar de existir regulaciones claras que le otorgan plena seguridad a las transacciones celebradas por medios electrónicos, los operadores jurídicos y los mismos particulares hoy en día no cuentan con un acceso y dominio del tema, convirtiéndolos en personas escépticas a la consecución de este tipo de prácticas.
3. Algunas condiciones esenciales para la aplicación de la propuesta de buenas prácticas en la admisión y valoración de la prueba digital en el sistema jurídico colombiano es la necesidad existente de incluirla en el ordenamiento jurídico como ley de la República. Esto con el ánimo de que los jueces estén sometidos a sus preceptos, tal como lo establece la Constitución en el artículo 230,[52] el cual estipula que ellos, en sus providencias, sólo están sometidos al imperio de la Ley.

   A su vez, será necesario incentivar y propagar el uso de la Internet como campo de acción entre la actividad de los particulares y la estatal, creando conciencia sobre la seguridad de los negocios celebrados por medios informáticos.

[52] Constitución Política de Colombia, artículo 230. "Los jueces, en sus providencias, sólo están sometidos al imperio de la Ley. La equidad, la jurisprudencia, los principios generales del derecho y la doctrina son criterios auxiliares de la actividad judicial".

4. Por último, para las personas interesadas en seguir esta investigación será necesario estudiar permanentemente los avances tecnológicos que innovan en gran medida la actividad humana y a su vez las necesidades provenientes de las prácticas internas, por cuanto la complejidad y la amplitud del campo de la informática será cada vez mayor. Ello le dará mayores retos al derecho y por consiguiente a sus operadores jurídicos, al establecer éstas nuevas necesidades en el contexto en el que se encuentren.

VIII. Bibliografía

Devis Echandía, Hernando, *Teoría general de la prueba,* t. II, 3ª edición, Buenos Aires, Buenos Aires, 1974.

—, *Compendio de derecho procesal, pruebas judiciales,* t. II, 7ª edición, Bogotá, ABC, 1982.

—, *Teoría general de la prueba judicial,* t. I, Medellín, Biblioteca Jurídica Dike, 1987.

Federal Rules of Evidence.

HB 171–2003, *Handbook of Guidelines for the Management of IT Evidence,* Published by Standards Australia International Ltd.

International Association of Chiefs of Police Advisory Committee for Police Investigative Operations, "Best Practices for Seizing Electronic Evidence".

Ministerio de Industria, Turismo y Transporte de España.

Mosquera González, José Alejandro; Certain Jaramillo, Andrés Felipe; CANO, Jeimy J., "Evidencia digital: contexto, situación e implicaciones nacionales", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* vol. I, Bogotá, Universidad de los Andes, 2005.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, "Computer Security Division".

PARRA QUIJANO, Jairo, *Manual de derecho probatorio,* 7ª edición, Bogotá, Librería del Profesional, 1986.

—, *Tratado de la prueba judicial, indicios y presunciones,* t. IV, 3ª edición, Bogotá, Librería del Profesional, 1988.

—, "Tratado de la prueba judicial", en *La prueba pericial y la inspección judicial*, t. V, 3ª edición, Bogotá, Librería del Profesional, 1988.

RAMOS SUÁREZ, Fernando, "Eficacia jurídica de una transacción electrónica. La figura del no repudio", en *Alfa-Redi*, núm. 12, 1999.

REMOLINA ANGARITA, Nelson, "Aspectos legales del comercio electrónico, la contratación y la empresa electrónica", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, núm. 2, Bogotá, Facultad de Derecho de la Universidad de los Andes, 2006.

— "La firma electrónica es esencial en los negocios", columna de opinión publicada en portafolio.com.co el 20 de mayo de 2009.

RIOFRÍO, Juan Carlos, *La prueba electrónica,* Bogotá, Temis, 2004.

UMAÑA CHAUX, Andrés Felipe, "Algunos comentarios sobre el principio del equivalente funcional en la ley 527 de 1999", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* vol. I, Bogotá, Universidad de los Andes, 2005.

UNCITRAL, o CNUDMI, de la Organización de las Naciones Unidades (ONU), "Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas", Viena, 2009.

Uniform Rules of Evidence.

A. Regulación

Ley 446 de 1998, "Por la cual se adoptan como legislación permanente algunas normas del decreto 2651 de 1991, se modifican algunas del Código de Procedimiento Civil, se derogan otras de la ley 23 de 1991 y del decreto 2279 de 1989, se modifican y expiden normas del Código Contencioso Administrativo y se dictan otras disposiciones sobre descongestión, eficiencia y acceso a la justicia".

Ley 527 de 1999, "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones en la legislación colombiana".

Ley 906 de 2004, "Por medio de la cual se expide el Código de Procedimiento Penal".

Código de Procedimiento Civil Colombiano.

Código de Procedimiento Penal Colombiano.

Electronic Signatures in Global and National Commerce Act del 2000.

Ley de firmas y certificados núm. 27269, de Perú.

Ley 25506, de Argentina.

Ley 19789, de Chile.

CAPÍTULO III

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

Javier Pimentel Calderón y Jeimy José Cano M.

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*

I. Introducción

En un mundo globalizado en el que las personas celebran contratos mediante el simple intercambio de mensajes de datos y en el cual 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

* Larrea Holguín, Juan, *La prueba electrónica* (prólogo), Bogotá, Temis, 2004.

y jurídicos necesarios para ofrecer certeza sobre la integridad de la evidencia obtenida en entornos digitales.

Este capítulo procura dar un vistazo a los estándares y prácticas internacionales más importantes en materia de peritaje informático, siempre con el cometido de establecer cuáles son los conocimientos informáticos, técnicos, jurídicos, y en general cuáles son las prácticas que se deben exigir a un experto para ser sus dictámenes 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 Estados le han dado al reto antes de crear nuestros propios estándares y procedimientos en materia de peritaje informático.

Inicialmente se realizará una breve contextualización en el tema del peritaje considerado en abstracto para luego ahondar en la definición de peritaje informático y así hacer un análisis de algunos de los estándares y prácticas internacionales que rigen actualmente dicha materia. La meta que nos hemos impuesto es la de llevar a cabo una evaluación del estado actual del peritaje informático en Colombia y adelantar una propuesta sobre los conocimientos y destrezas mínimas que se deben afianzar en quienes se desempeñarán como peritos informáticos en nuestro país. Para lograr ese cometido necesariamente hemos de llevar a cabo 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 trasplantarlos 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 efectuar una sugerencia informada

para ayudar a la implementación de lo que sería el estándar colombiano de buenas prácticas en materia de peritaje informático.

II. ¿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 surgidas 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 "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]

[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*, 14ª edición, Bogotá, Ediciones del Profesional, 2004, p. 143.

[2] Ibídem, p. 628.

[3] Ídem.

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 ser verdaderos expertos con el fin de que su dictamen revista verdadera importancia y autoridad. En ese orden de ideas, se preferirá necesariamente a quienes demuestren "una reconocida solvencia profesional, ética y moral",[5] además de una formación idónea y una experiencia adecuada en el área del conocimiento sobre la cual versará el dictamen. No obstante, lo anterior no implica necesariamente que se deba acreditar un título profesional para obrar como perito, pues resulta obvio que alguien puede ser un experto en un determinado tema y no poseer un título profesional confirmando tal experticia, 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 acreditados en el caso *sub júdice*. 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 proveniente, a todas luces, de alguien inexperto en los temas sobre los que versa la pericia. En España, por ejemplo, se admite la posibilidad

[4] Colin Sánchez, Guillermo, citado por Bailón Baldovinos, Rosalío, *Derecho procesal penal*, Limusa, 2002, p. 84.

[5] Rodríguez Jouvencel, Miguel, *Manual del perito médico. Fundamentos técnicos y jurídicos*, Madrid, Díaz de Santos, 2002, p. 251.

de que una persona entendida en un determinado tópico y no titulada oficialmente pueda obrar como perito:

> Así, la Ley de Enjuiciamiento Civil (LEC), art. 340, en su párrafo primero, al referirse a las (*sic*) condiciones de los peritos, dispone: los peritos deberán poseer el título oficial que corresponda *(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: "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 Código de Procedimiento Civil, que establece: "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 reviste la mayor importancia para efectos de este trabajo en tanto permite vislumbrar el primer error en el que podría

[6] Ídem.

[7] Parra Quijano, Jairo, ob. cit., p. 633.

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; no sólo de un conocimiento en la materia sobre la cual versará su informe, sino además, 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 por cuanto 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".
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 (artículo 235 del Código de Procedimiento Civil).
5. En Colombia el dictamen debe seguir los lineamientos establecidos en el numeral 6 del artículo 237 del Código de Procedimiento Civil.

[8] Ibídem, p. 636.

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.

III. Aproximación al derecho informático

No es un secreto que el mundo está en constante cambio y que la informática[9] juega un papel muy importante en la actualidad debido a su convergencia con las telecomunicaciones. Así las cosas, tampoco causa sorpresa el haber nacido una nueva disciplina "que se encarga de poner orden [*sic*] 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 encargada de estudiar y regular las nuevas relaciones jurídicas que la informática y las TIC 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]

[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 necesariamente, con la ayuda de ordenadores y sistemas de telecomunicación como instrumentos", Altmark, Daniel, *Informática y Derecho*, vol. 1, Buenos Aires, Depalma, 1987, p. 6.

[10] Bencomo Yarine, Edel, "Reseña de la legislación informática en Cuba", en *Alfa-Redi*, núm. 102, 2007. Disponible en: http://www.alfa-redi.com/rdi-articulo.shtml?x=8408.

[11] Riofrío Martínez-Villalba, Juan, "La pretendida autonomía del derecho informático", en *Alfa-Redi*, núm. 50, 2002. Disponible en: http://www.alfa-redi.com/rdi-articulo.shtml?x=1448.

[12] Bencomo Yarine, Edel, ob. cit.

Mucho se ha discutido sobre la posibilidad de considerar al derecho informático como una rama autónoma del derecho. En nuestra reflexión entenderemos que el informático no es en sí mismo una rama del derecho en tanto su estudio resultaría imposible sin la enseñanza de la dogmática y los conceptos de otras áreas de éste. 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, [*sic*] ¿qué nos quedará? En una palabra: nada.[13]

Entendido lo anterior, y en aras de evitar centrarnos en discusiones no esenciales para el tema que nos ocupa y extender excesivamente

[13] Riofrío Martínez-Villalba, Juan, ob. cit.

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.

IV. 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.

[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 en forma humanamente comprensible'", Remolina Angarita, Nelson, "Desmaterialización, documento electrónico y centrales de registro", en *Comercio Electrónico*, GECTI, Bogotá, Legis, 2005, p. 150.

[15] Ley 527 de 1999, artículo 2°, literal a).

Lo cierto al respecto es que no existe una definición amplia y genérica de prueba electrónica. La doctrina usa y expone múltiples definiciones, entre las cuales podemos destacar la siguiente: "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 ya se expresó, las legislaciones no abundan en definiciones en cuanto respecta al concepto de prueba electrónica; al parecer los legisladores prefieren mantener una cierta prudencia que a nuestro juicio obedece al temor típico que los embarga en el momento de verse apremiados a fijar conceptos en términos jurídicos estrictos, en materias que trascienden el dogma y la teoría del derecho, para abarcar otros 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 sólo los mensajes de datos y los

[16] Torrente, Diego, "Conferencia AEEC: en busca de una definición para 'prueba electrónica'", en *E-Newsletter de Cybex*, núm. 27, 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, ob. cit.

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 Código 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, la cual no constituye documento o mensaje de datos alguno, puede ofrecer certeza o convencimiento sobre unos hechos determinados.

Un buen ejemplo serían las huellas dejadas por 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 diversas 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, las cuales sólo se pueden vislumbrar en un entorno digital, constituyen un mensaje de 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 como se llevó a cabo un determinado *cibercrimen* y por ende, a la luz de la definición operativa expuesta, constituir verdaderas pruebas electrónicas.

Por último, con ánimo meramente enunciativo, sería pertinente señalar algunas de las formas como se puede encontrar la evidencia digital:

[18] Ley 527 de 1999, artículo 10.

— Contenido de un archivo: "Usualmente, las palabras y figuras en un documento o reporte, imágenes (...), *e-mails*, páginas *web*",[19] entre otros.
— Metadata: en términos simples, la metadata podría vislumbrarse como información sobre la información. En efecto, este tipo de evidencia sería muy útil en la medida de consistir en "datos sobre los datos, que no son inmediatamente visibles pero que indican, por ejemplo, quién creó un archivo, cuántas veces ha sido editado y cuántas 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*: éstos 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

[19] Sommer, P. "Directors and corporate advisors', guide to digital investigations and evidence", 2005 [versión electrónica, accesada en mayo de 2007]. Disponible en: http://www.iaac.org.uk/Portals/0/Evidence%20of%20Cyber-Crime%20v12-rev.pdf.

[20] Ídem.

[21] Ídem.

[22] Ídem.

[23] Ídem.

medios de almacenamiento que no sería normalmente visto, como por ejemplo, archivos que no han sido debidamente eliminados",[24] entre otros.

— Interpretaciones de expertos: éstos podrían constituir pericias electrónicas en los términos del acápite siguiente y pueden versar sobre cualquiera de las formas de evidencia señaladas.

V. 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 es 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 poseído por 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.

[24] Ídem.

[25] Cano, Jeimy, "Estado del arte del peritaje informático en Latinoamérica", en *Alfa-Redi*, p. 8. Disponible en: www.alfa-redi.org.

El trabajo del perito informático es, entonces, el de 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 habrá de tener ciertos conocimientos jurídicos y determinadas destrezas criminalísticas y forenses. En los capítulos siguientes analizaremos los estándares que requieren cumplir los peritos informáticos en el mundo para garantizar la idoneidad de sus dictámenes y 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 adquirir un perito informático, así como las exigencias que se hacen en cuanto a las destrezas y consideraciones que ha de observar cualquier persona con aspiración de llevar a cabo un verdadero peritaje informático.

VI. ¿Por qué es necesario un perito informático?

En 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 la Uncitral es un buen ejemplo) tienden a permitir el

[26] Ídem.

[27] De la Torre, Juan; Agud Andreu, Sergio, "Pruebas electrónicas: una nueva realidad", en *E-Newsletter de Cybex*, núm. 27, abril de 2007.

perfeccionamiento de contratos y negocios jurídicos mediante un simple intercambio de mensajes de datos.

Los criminales, por su parte, ven en la 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 la Internet ha sido determinante en algunos fraudes bancarios millonarios y que los *hackers* maliciosos, los *crackers,* y en general los cibercriminales, se sienten más seguros al sentirse menos vulnerables que un criminal común, sentados frente a una pantalla de computador a una distancia considerable del lugar en el cual 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 mil 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 donde se plantea la inexistencia o nulidad de un determinado contrato de compraventa celebrado mediante el intercambio de mensajes de datos, ¿quién 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, ¿quién 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

[28] "Los delitos informáticos, en aumento", en *El Tiempo*, 7 de mayo de 2007, p. 2.

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 hechas 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]

[29] Cano, Jeimy, "Evidencia digital: conceptos y retos", en *Comercio Electrónico*, GECTI, Bogotá, Legis, 2005, p. 185.

[30] Ídem.

[31] Ibídem, p. 186.

— "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 ésta 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 cuales se hizo referencia en acápites anteriores y que se especificarán en los siguientes, máxime si se tiene en cuenta que tratándose de pericias informáticas y en casos en donde 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 del experto en cuestión. En esos casos las consecuencias de escoger a una persona inexperta para rendir dictamen serían funestas, pues la decisión del juez se vería distorsionada por el análisis y las conclusiones equivocadas hechas 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 en el mundo para prevenir problemas como el descrito en el párrafo anterior y evitar que sus dictámenes y las pruebas electrónicas analizadas sean descartadas por los jueces o puestas en duda por las partes interesadas en un litigio.

VII. Peritaje informático y manipulación de evidencia digital en Europa

La forma disímil en la que estos temas son tratados en los países de Europa nos obligaría a dar un vistazo a la legislación y doctrina de cada

[32] Ídem.

uno de ellos 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 "tienen 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 llevarse a cabo la manipulación de la prueba electrónica por expertos. Entendido lo anterior, causa sorpresa el no existir en Europa una regulación vigente la cual fije los requisitos y características que deben reunir quienes pretendan ostentar el título de expertos en informática forense. Sobre este tema 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.

[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, "La admisibilidad de las pruebas electrónicas ante los tribunales", 2006 [revisado el 7 de mayo de 2007]. Disponible en: http://www.cybex. es/agis2005/docs/libro_ aeec_sp.pdf.

[35] Ídem.

En cuanto al proceso de recolección de evidencia, en el Reino Unido se han tenido en cuenta los diversos problemas que plantea la manipulación de las pruebas electrónicas, y por ende la Asociación de Jefes de Policía (Association of Chief Police Officers - ACPO) sugiere ceñirse a un procedimiento forense estandarizado que normalmente consta de cuatro etapas:

1) Etapa de recolección: implica la búsqueda, reconocimiento, recolección y documentación de la evidencia electrónica.[36]
2) Proceso de examen de la evidencia: como lo explica la ACPO, este proceso 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, y 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 y la información pertinente obtenida mediante dicho proceso, y contener un análisis del investigador enfocado en esos dos aspectos. En esta etapa, la asociación hace hincapié en que las notas tomadas por 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

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

> 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 usarán en sus investigaciones, para asegurar que la información original no resulte comprometida.

De la bibliografía revisada se puede extraer que además de las consideraciones específicas impuestas en cada legislación 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 y de los parámetros de legalidad de la prueba, entre otras, 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 niveles 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 uno 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:

[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, "La admisibilidad

1) La experticia del especialista a seleccionar.
2) Su experiencia en el tipo de trabajo que se le encomendará.
3) Su nivel de entendimiento sobre la naturaleza de las investigaciones en Gales y el Reino Unido en aspectos específicos como el ritmo en el que éstas se realizan y su confidencialidad.
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 quienes efectúan 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 actual 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]

de las pruebas electrónicas ante los tribunales", 2006 [revisado el 7 de mayo de 2007]. Disponible en: http://www.cybex. es/agis2005/docs/libro_aeec_sp.pdf.

[38] Ídem.

VIII. 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 estadounidense estableció ciertos límites para la búsqueda y recolección de evidencia al establecer que las personas gozan del derecho a no ser objeto de búsquedas o apoderamientos arbitrarios o irracionales en sus personas, casas, papeles y efectos personales.

Las Cortes en Estados Unidos han desarrollado y delimitado tal derecho en cuanto 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.

Una de las principales preocupaciones de los estadounidenses 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 como se debe interpretar la Cuarta Enmienda en los casos que involucren pruebas electrónicas.

Además de la analogía mencionada anteriormente, las Cortes estadounidenses han establecido otra subregla importante, la cual 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 cederse 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 esa no sea la intención, se entiende el extinguirse también su expectativa razonable de privacidad en lo que atiende 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 Estados Unidos[39] hace 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

[39] United States, Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", 2002. Disponible en: http://www.cybercrime. gov/s&smanual2002.htm#_IB3.

y expone los resultados de la misma a un agente del Estado".[40] Un precedente considerado pertinente para ilustrar un caso en el que las Cortes típicamente aplicarían la excepción comentada es el *United States v. Hall (142 F.3d 988)*, en el que un individuo llevó su computadora a reparación donde un especialista, quien decidió llevar a cabo una investigación al encontrar indicios de que en el disco duro 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, después de la denuncia, la policía había obtenido la debida autorización judicial para hacer 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 observados reiteradamente en las investigaciones criminales y en procesos de indagación que impliquen la manipulación de pruebas electrónicas en ese país. Al respecto, el citado Manual del Departamento de Justicia reconoce que si bien 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 ofrecidos por la manipulación de pruebas electrónicas enunciados en el acápite 2.4 del presente trabajo, a la volatilidad de los archivos de

[40] Ídem.

[41] *Computer technologies frequently force agents to execute computer searches in nontraditional way.*

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 recorriendo 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 a ser 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 cuales 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 dónde 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 hará 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

[42] Ídem.

[43] Ídem.

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 búsqueda se hará en el sitio en donde se encuentra el sistema a revisar, o si por el contrario se removerá el hardware para inspeccionarlo en un laboratorio o en alguna otra locación; si se sacarán copias de los discos duros o de archivos individuales; y en general, cuál 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 cuáles procedimientos 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 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

[44] Un *warrant*, en el *common law* (derecho común, o derecho anglosajón), 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. . *Dictionary of Law Containing Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern*, 1891, p. 1234. Disponible en la base de datos *Hein Online*, en la colección *Legal Classics*.

de la autoridad competente. En efecto, dada la complejidad de los procesos investigativos recaídos 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 citadas, el Departamento de Justicia hace ciertas alusiones a las objeciones y argumentos típicos que esgrimen las partes en los procesos donde hay comprometidas 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 el ser 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 contra 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 los cuales 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 anonimato propio de las pruebas electrónicas para poner en duda la identidad de su autor. Con el fin de enfrentar este tipo de argumentos el investigador debe tomar todas las medidas posibles para superar el anonimato de la prueba, valiéndose primordialmente de su experticia en computación.

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

Como se dijo, 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 escapar al alcance de este trabajo el tratar de hacer una recopilación o resumen de todas ellas, dicha tarea resultaría infructuosa en la medida en que la mayoría de esos procedimientos tienden a ser muy específicos en aras de sortear los retos a los cuales se puede enfrentar el investigador en el momento de recolectar

[45] Mohd, M., "An Overview Of Disk Imaging Tool In Computer Forensics", 2000, p. 3. [Versión electrónica, accedida 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-.

o allegar pruebas a un determinado proceso en los tribunales estadounidenses. Lo pretendido 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 al 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 reglas de exclusión de la prueba, el régimen de la ilicitud e inconstitucionalidad de éstas, y previendo las formas como los operadores jurídicos explotarán 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 estadounidense en bien 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 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 su entrenamiento 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]

[47] Myers, L. J., "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, 2000, p. 45.

A manera de conclusión, podemos señalar algunos principios básicos y generales seguidos en Estados Unidos al 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 examinados:

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]

IX. 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 donde presentaba su estándar de directrices y pautas para la manipulación de evidencia electrónica. En este acápite repasaremos el estándar de manipulación de evidencia digital a la luz de dicho documento, el cual puede dar luces sobre el avance de la cooperación asiático-pacífica (APEC) en los temas que nos ocupan.

[48] Scientific Working Group on Digital Evidence, "Best Practices For Computer Forensics", 2006 [versión electrónica, accesada en mayo de 2007. Disponible en: http://ncfs. org/swgde/documents/swgde2006/Best_Practices_for_Computer_Forensics%20July06.pdf.

[49] Ídem.

Para efectos de este artículo, es preciso comenzar nuestra revisión de las directrices enfatizando 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 y la fecha y hora de creación de éstos, sobre la identidad de su autor, y por último, sobre la fiabilidad del procedimiento para su custodia y manipulación.[50]
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.
4) Determinar si se están manipulando registros originales o copias de ellos. Así mismo, sería pertinente documentar apropiadamente cualquier tipo de acción tomada sobre los registros de evidencia. En este aspecto, el artículo australiano reitera que la evidencia original debe permanecer inalterada y en el evento en que su alteración sea inevitable se debe documentar dicha alteración adecuadamente.

[50] Ghosh, Ajoy, "*Guidelines for the Management of* IT *Evidence*", APEC Telecommunications and Information Working Group 29th Meeting, Hong Kong, 21-26 March, 2004, p. 12.

[51] Ídem.

[52] Ídem.

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 E.E. UU., el artículo australiano resalta la importancia de efectuar este tipo de procedimientos. En efecto, en él se cita una decisión judicial significativamente influenciada por el hecho de que el demandante omitió copiar 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. 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]

Igualmente, 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 participantes 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, qué acciones específicas se llevaron a cabo sobre los registros de evidencia.
2) Los individuos participantes en procesos de recopilación de evidencia digital deben ser capaces de discernir entre los datos de un sistema que pueden ser útiles y aquellos que no lo son.

[53] Ídem.

[54] Ibídem, p. 21. La decisión judicial citada por Ajoy es: *Gates Rubber Company vs Bando Chemical Industries Ltd. 167* FRD *90 (D. Colorado) at 90 and 112.*

3) Cuando se recolecta evidencia digital se ha de intentar descubrir información de difícil visibilidad, en aras de obtener material forense recuperado,[55] y 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 cuales se verá enfrentado un acervo probatorio constituido principalmente por pruebas electrónicas. Así mismo, en múltiples ocasiones el documento enfatiza sobre la importancia de la preparación y formación de expertos que sean capaces de manipular este tipo de pruebas de una manera adecuada.

X. 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] relativa a la aproximación legislativa respecto de 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, implicando necesariamente la adopción de una postura prudente que reconozca la

[55] Véase el acápite 2.2 del artículo.

[56] Seng, Daniel; Chakravarthi, Sriram, "Computer Output as Evidence Final Report", Singapure, Academy of Law [revisado en mayo de 2007]. Disponible en: http://www.agc.gov. sg/publications/docs/Computer_Output_As_Evidence_Final_Dec_2004.pdf.

rapidez con la cual cambia la tecnología. En ese sentido, el legislador debería evitar cualquier tipo de preferencia o inclinación hacia una tecnología en particular con el fin de impedir que la legislación no contemple otra tecnología ya existente o el quedar obsoleta muy rápidamente debido a su veloz expansión.

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 propósito 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 específica.

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, particularmente renuente a abordar el tema de las pruebas electrónicas en concreto. 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 el 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.

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

[57] Plazas Rueda, Andrea; Cano, Jeimy, "Valoración de la evidencia digital: análisis y propuesta en el contexto de la administración de justicia en Colombia", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, vol. 1, 2006, p. 103.

de revisar 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) las cuales permitan darle luces al juez sobre ciertos tipos de evidencia electrónica en particular 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.

XI. 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 maximizar la posibilidad de éxito de sus búsquedas y la admisibilidad del material probatorio recopilado. En ese orden de ideas, algunos países han optado por estandarizar los procesos de búsqueda y recolección de evidencia digital como una forma de evitar la improvisación y de guiar a sus funcionarios en procura de poder 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 esgrimidas en contra de las pruebas electrónicas. Dichas argucias, como sabemos, se valen de la mencionada volatilidad y fácil 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 como 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 énfasis en la importancia de que las organizaciones administren correctamente sus registros electrónicos con la finalidad de dotarlos de verdadera eficacia probatoria y nos dicta ciertas pautas para llevar a cabo una exitosa toma 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.

XII. BIBLIOGRAFÍA

ALTMARK, Daniel, *Informática y derecho,* vol. 1, Buenos Aires, Depalma, 1987.

BENCOMO YARINE, Edel, "Reseña de la legislación informática en Cuba", en *Alfa - Redi,* núm. 102, 2007.

BLACK, H. C., *Dictionary of Law Containing Definitions of the Terms and Phrases of American and English Jurisprudence, Ancient and Modern,* 1891.

CANO, Jeimy, "Estado del arte del peritaje informático en Latinoamérica", en *Alfa-Redi.*

CANO, Jeimy, "Evidencia digital: conceptos y retos", en *Comercio Electrónico, GECTI,* Bogotá, Legis, 2005.

CYBEX, "La admisibilidad de las pruebas electrónicas ante los tribunales", 2006.

De La Torre, Juan; Agud Andreu, Sergio, "Pruebas electrónicas: una nueva realidad", en *E-Newsletter de Cybex*, núm. 27, 2007.

Ghosh, Ajoy, *Guidelines for the Management of IT Evidence*, APEC Telecommunications and Information Working Group 29th Meeting, Hong Kong, 2004.

Mohd, M., "An Overview Of Disk Imaging Tool In Computer Forensics", 2000.

Myers, L. J., "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, 2000.

Parra Quijano, Jairo, *Manual de derecho probatorio*, 14ª edición, Bogotá, Ediciones del Profesional, 2004.

Plazas Rueda, Andrea; Cano, Jeimy, "Valoración de la evidencia digital: análisis y propuesta en el contexto de la administración de justicia en Colombia", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, vol. 1, 2006.

Remolina Angarita, Nelson, "Desmaterialización, documento electrónico y centrales de registro", en *Comercio Electrónico, Gecti*, Bogotá, Legis, 2005.

Riofrío Martínez-Villalba, Juan, "La pretendida autonomía del derecho informático", en *Alfa - Redi*, núm. 50, 2002.

Rodríguez Jouvencel, Miguel, *Manual del perito médico. Fundamentos técnicos y jurídicos*, Madrid, Díaz de Santos, 2002.

Scientific Working Group on Digital Evidence, "Best Practices For Computer Forensics", 2006.

Seng, Daniel; Chakravarthi, Sriram, *Computer Output as Evidence Final Report*, Singapure, Academy of Law, 2004.

Sommer, P., Directors and Corporate Advisors', guide to digital investigations and evidence, 2005.

Torrente, Diego, "Conferencia aeec: en busca de una definición para 'prueba electrónica'", en *E-Newsletter de Cybex,* núm. 27, 2007.

United States, Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division, "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", 2002.

CAPÍTULO IV

CONTEXTO ACTUAL DE LA FORMACIÓN DEL PERITO INFORMÁTICO EN EL ESCENARIO INTERNACIONAL Y SU REALIDAD EN COLOMBIA

Ángela María Ramírez Caballero y Jeimy J. Cano M.

Cuando sea necesario que una persona acceda
a una evidencia digital original,
*dicha persona debe estar entrenada para esa tarea**

I. Introducción

La propagación de la tecnología de la información hace que el país dependa cada vez más de sistemas y dispositivos automatizados. El funcionamiento de las infraestructuras críticas en varios sectores (sistema financiero, sistemas de generación de energía, de telecomunicaciones, de distribución y transporte de combustibles, entre otros), se realiza a través de sistemas en red que, de ser sometidos a acciones perturbadoras, generarían impacto negativo en la economía y la seguridad de la nación de una magnitud imprevisible. La delincuencia transnacional que afronta Colombia, como lo son los delitos del narcotráfico y el terrorismo, ponen

* Traducción libre de: IOCE - International Organization on Computer, "G8 Proposed Principles for the procedures relating with digital evidence". Disponible en: http://www.ioce.org/core.php?ID=5.

de presente la necesidad de actuar desde varios frentes, y por todos los medios, contra la ciberdelincuencia.[1]

Cuando nos asomamos al fenómeno de la denominada *era digital* es inevitable llegar a la conclusión de que el peritaje informático, como lo vimos en la primera parte del trabajo,[2] se ha convertido en una demanda creciente en la moderna sociedad de la información. Con mayor frecuencia los procesos judiciales incorporan elementos informáticos, elemento tanto central como accesorio. Este cambio de paradigma ha provocado importantes impactos en la estructura socioeconómica del mundo, en virtud de la realidad incuestionable de que la informática nos rodea y se encuentra inmersa en todos los aspectos de la vida del hombre. Como lo afirma el Dr. Hugo Daniel Carrión, "La informática se presenta como una nueva forma de poder, es un instrumento de expansión ilimitada e inimaginable del hombre que potencia y multiplica de manera insospechada las posibilidades de desarrollo científico y social".[3]

Actualmente hay 1300 millones de usuarios de Internet en el mundo. En el año 2010 esta cifra alcanzará los 1800 millones. Los desplazamientos internacionales se duplicarán entre hoy y 2020, año en que sumarán 1400 millones, y muchos viajeros llevarán consigo datos electrónicos almacenados en diversos dispositivos, dando lugar a un aumento considerable del número de investigaciones sobre asuntos que podrían afectar a naciones enteras, en las cuales se contará con pruebas electrónicas.[4]

[1] Comisión de Regulación de Telecomunicaciones, "Recomendaciones al Gobierno Nacional para la implementación de una estrategia de ciberseguridad", diciembre de 2007.

[2] Cano, J.; Pimentel, J., "Consideraciones sobre el estado del arte del peritaje informático y los estándares de manipulación de pruebas electrónicas en el mundo", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, Bogotá, Universidad de los Andes, diciembre de 2007.

[3] Carrión, Hugo Daniel, "Auditoría informática frente a un caso de espionaje informático dentro de una empresa". Disponible en: http://www.delitosinformaticos.com (consultada el 14 de diciembre de 2007).

[4] Información contenida en el documento de la Interpol sobre los computadores decomisados a las Fuerzas Armadas Revolucionarias de Colombia (Farc) el 1° de marzo de 2008.

La información, en consecuencia, ha adquirido un alto valor desde el punto de vista económico, constituyéndose en un bien sustrato del tráfico jurídico, adquiriendo eminente relevancia jurídico-penal por ser posible objeto de conductas reprochables. Ante este panorama, deviene la necesidad de que exista un procedimiento sólido el cual contemple las políticas de seguridad necesarias de poner en práctica para que no se borren, manipulen ni alteren las pruebas; de manera que se le pueda hacer seguimiento a la información a través de los rastros dejados a su paso por el acto ilícito.[5]

Así entonces aparece la informática forense como una "disciplina auxiliar de la justicia moderna"[6] para detectar si en determinados ambientes sistematizados nos encontramos frente a alguna de estas conductas, recolectando evidencia y generando la documentación probatoria requerida para poder manejar el caso ante la justicia, considerando la importancia del manejo de la evidencia, factor fundamental en el nuevo sistema penal acusatorio. Si la prueba no es bien recolectada es muy probable que en el juicio el caso no sea exitoso, por no obtener la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso. Al ser la informática forense una ciencia aplicada naciente, y considerando que en Colombia aún no existen programas académicos regulados sobre los criterios de idoneidad para la formación de los peritos informáticos que apoyen las labores tanto en la Administración de Justicia como en investigaciones organizacionales internas, se convierte en un reto para Colombia iniciar las reflexiones sobre la formación de una especialidad en este campo.

Teniendo en cuenta lo anterior, recientemente en Colombia se produjo un hecho que ha puesto a reflexionar no sólo al alto Gobierno, sino

[5] Guerrero, Alberto, en *Revista de Derecho Informático*, núm. 110, septiembre de 2007. Disponible en: http://www.Alfa-Redi.Org/Rdi.Shtml.

[6] Cano Martínez, Jeimy José, "Introducción a la informática forense. Una disciplina técnico-legal", en *Sistemas*, núm. 96, abril-junio de 2006.

también a las autoridades judiciales y a quienes deben propender por el éxito en las investigaciones: el caso de los computadores hallados en un campamento de las Fuerzas Armadas Revolucionarias de Colombia (FARC), decomisados al guerrillero Raúl Reyes. En esta ocasión, y ante las dificultades de carácter diplomático que podrían surgir de la información allí contenida, las autoridades colombianas solicitaron a la Interpol[7] la realización de un análisis forense de tres ordenadores portátiles, dos discos duros externos y tres memorias USB, decomisados en el campamento de las FARC, en Ecuador, el 1° de marzo de 2008. Concretamente, las autoridades colombianas solicitaron la asistencia técnica independiente de la Interpol en materia de investigación informática forense para que se examinaran los archivos contenidos en las ocho pruebas instrumentales de carácter informático decomisadas a las FARC y se determinara si alguno de dichos ficheros de usuario se había creado, modificado o eliminado el 1° de marzo de 2008 o después de esta fecha. Para ese estudio se contó con la participación de dos especialistas de la Interpol procedentes de Australia y Singapur y la colaboración de expertos provenientes del ámbito académico, del sector privado y de las fuerzas policiales, lográndose el examen de 609,6 gigabytes de datos.[8]

En el informe de la Interpol se presentan para Colombia varias recomendaciones en materia de informática forense. La primera se refiere a la *necesidad de formar un personal especializado capaz de ejercer el peritaje informático que se requiere para atacar la ciberdelincuencia.* La segunda, al manejo de procedimientos, pues la Interpol descubrió varios problemas con respecto a la ejecución de análisis in-

[7] La Interpol es la mayor organización policial internacional del mundo; tiene como objetivo facilitar la cooperación policial transfronteriza y prestar apoyo y ayuda a las organizaciones, autoridades y servicios cuyo cometido sea prevenir o combatir la delincuencia internacional.

[8] Información contenida en el documento de la Interpol sobre los computadores decomisados a las FARC el 1° de marzo de 2008. Disponible en: http://www. interpol. int/Public/ICPO/PressReleases/PR2008/pdfPR200817/ipPublicReportNoCoverES.pdf.

formáticos forenses internacionales y el manejo de las pruebas electrónicas por parte de los funcionarios de los organismos encargados de la aplicación de la ley, especialmente de aquellos que intervienen primero en el lugar de los hechos. Estos problemas no sólo afectan directamente a Colombia, sino que igualmente a los agentes de los servicios encargados de la aplicación de la ley en los 186 países miembros de la Interpol.

Considerando el panorama colombiano, se sabe que la tecnología requerida es limitada con relación al delito informático y por consiguiente es necesario la preparación y calificación apta para satisfacer el contexto del nuevo sistema penal acusatorio. En este punto es donde cobra importancia la formación que debe recibir un perito informático, capaz de cumplir con las características establecidos en el actual artículo 236 del nuevo Código de Procedimiento Penal, refiriéndose a los expertos en informática forense, para que descubran, recojan, analicen y custodien la información. Por lo tanto, se deben comprender las estrategias antiforenses, con el fin de fortalecer las investigaciones y herramientas tecnológicas disponibles que permitan generar valor y confianza tanto a las organizaciones e individuos como a la Administración de Justicia y sus organismos asociados. Es importante recordar en este punto que la informática forense nace para enfrentar los desafíos y técnicas de los intrusos informáticos y como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.[9]

En este contexto, el presente capítulo pretende analizar el estado actual de la formación del perito informático en el concierto internacional, específicamente en Estados Unidos y Australia, dado su desarrollo en el tema, con el propósito de recoger esas experiencias y aplicarlas en Colombia, proponiendo líneas de acción a mediano y corto plazo en

[9] Cano, Jeimy, ob. cit., p. 1.

esta especialidad hasta fortalecer y modernizar la Administración de Justicia en el nuevo sistema penal acusatorio.

II. Manifestaciones por parte de los organismos internacionales sobre la necesidad de profundizar en el tema de la profesionalización del perito informático

Son varias las manifestaciones de organismos internacionales sobre la necesidad de profundizar en el tema de la profesionalización del perito informático, las cuales se expondrán a continuación:

El primer tratado internacional sobre crímenes cometidos a través de la Internet y otras redes de computación fue la Convención del Delito Cibernético (Convention on Cybercrime), realizada en el 2001 en Budapest por el Consejo de Europa (CoE),[10] dirigido particularmente hacia violaciones a los derechos de autor, al fraude relacionado con el ciberespacio, la pornografía infantil y las violaciones a la seguridad de la red informática.

En enero de 2001 la Asamblea General de las Naciones Unidas aprobó la resolución 55 de 1963 sobre la "lucha contra la utilización de la tecnología de la información con fines delictivos", en la cual se establecen los procedimientos para impedir el uso indebido de ésta. En el ordinal d) de estos procedimientos se dice que "El personal encargado de hacer cumplir la ley debe contar con *capacitación* y equipo adecuado para hacer frente a la utilización de la tecnología de la información con fines delictivos" (énfasis fuera del texto).[11]

[10] CoE, Convention on Cybercrime, 2001 [acceso: 3 de junio de 2008]. Disponible en: http://Conventions.Coe.Int/Treaty/En/Treaties/Html/185.Htm.

[11] Comisión de Regulación de Telecomunicaciones, ob. cit., p. 20.

Por otra parte, en el año 2002 la Asamblea General de las Naciones Unidas aprobó la resolución 56/121, a través de la cual se invita a los Estados Miembros a que se tengan en cuenta, al elaborar leyes y políticas nacionales, según proceda, la labor y logros de la Comisión de Prevención del Delito y Justicia Penal, junto con las de otras organizaciones internacionales y regionales.[12]

Entre los 5 subgrupos del Grupo de Lyon creados para implementar las 40 recomendaciones adoptadas por los jefes de Estado del G8 en 1996, se encuentra el "Grupo de Crimen de Alta Tecnología, para prevenir, investigar y procesar los crímenes que implican las computadoras, las redes de comunicaciones y otras nuevas tecnologías". La misión se ha ampliado para incluir el trabajo conjunto con otros países y asuntos tales como los usos de la Internet para combatir el terrorismo y las infraestructuras críticas de la información. Este subgrupo cuenta con investigadores y expertos sobre delitos informáticos, análisis forense y acuerdos internacionales de cooperación.

En la 6ª Conferencia Internacional de la Interpol sobre ciberdelincuencia, celebrada en El Cairo (Egipto) del 13 al 15 de abril de 2004, se aprobó una resolución en la cual se pedía [...] "Que la formación y la asistencia técnica sigan considerándose prioritarias en la lucha internacional contra la ciberdelincuencia [...]". Igualmente lo ha registrado el Convenio sobre Ciberdelincuencia, del CoE: en su artículo 35 estipula que se debe disponer de *personal bien formado y equipado* de manera permanente, a fin de garantizar el poderse prestar ayuda inmediata en las investigaciones o procedimientos sobre delitos relacionados con datos y sistemas informáticos, o para la recopilación de pruebas en formato electrónico vinculadas con un delito (*Trained and equipped personnel are available* [...] *on a twenty-four hour, seven-day-a-week*

[12] Ibídem, p. 22.

basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence) [énfasis fuera del texto]. Hasta ahora, 22 países han firmado el convenio.

Se observa, a través de las manifestaciones expuestas, la importancia internacional adquirida por el tema de formar especialistas en informática forense que puedan apoyar las labores de peritaje tanto en la Administración de Justicia como en investigaciones organizacionales internas.

III. ¿Quién es un perito informático?

Las tecnologías de la información y las comunicaciones son equivalentes en el mundo moderno a lo que fue la revolución industrial, en términos de la transformación que representan para la sociedad. Esta transformación cobija todos los ámbitos: el social, el político, el económico y el personal. Pero al lado del avance positivo, el de ser uno de los fenómenos más importante en la Historia, no puede faltar su utilización nociva, existiendo personas que utilizan su privilegiado talento y conocimiento en informática para tratar de sacar provecho de ello en detrimento de sus semejantes, recurriendo a conductas que por lo novedosas no se encuentran aún tipificadas, o que si lo están, su aplicación concreta tiene relativa dificultad, pues la adecuación típica no es lo suficientemente clara como se quisiera; a estas personas se las conoce como *intrusos informáticos.*[13]

Teniendo en cuenta lo anterior, esta parte de la investigación pretende, a través de un estudio comparado, dar respuesta a la siguiente pregunta: ¿quién es un perito informático y qué conocimientos, habilidades y actitudes

[13] República de Colombia, Cámara de Representantes, proyecto de ley 42 de 1997, exposición de motivos.

requiere para facilitar la efectiva detección, investigación y persecución del crimen de alta tecnología?

Así como se estableció en la primera parte de este trabajo, los peritos son personas con capacidades y conocimientos técnico-científicos en temas desconocidos por el juez y por lo tanto rinden dictámenes que brindan certeza sobre tópicos de su experticia, ajenos a los de éste. En sentido general, se sabe que cuando en el proceso se requieran conocimientos especializados, es decir, "aquellos que escapan a la cultura de las gentes, puede y debe recurrirse a quienes por sus estudios, experiencia, etcétera, los posean".[14] 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, 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".[15] A partir de la anterior definición, tenemos que el perito es un verdadero experto.

Es muy importante notar que el perito informático no solamente requiere de una adecuada educación y entrenamiento para realizar el examen y probar con rigor, sino que también es indispensable el ser capaz de comunicar esa información y esos resultados a las Cortes, que con frecuencia no cuentan con el conocimiento suficiente para entender el tecnicismo. Las técnicas, el equipo y los instrumentos usados por el perito deben tener una validación científica y producir un resultado preciso y demostrable. De esa forma, así como lo establece este autor, cuando la gente, los equipos y los protocolos funcionan, se pueden verificar los resultados de la informática forense.[16]

[14] Quijano Parra, Jairo, *Manual de derecho probatorio*, 14ª edición, Bogotá, Ediciones del Profesional, 2004, p. 143.

[15] Colin Sánchez, Guillermo, *Derecho procesal penal*, México, Limusa, 2002, p. 84.

[16] Ibídem, p. 16.

A. El perito informático en Estados Unidos

Varios estudios revelan que las consecuencias económicas ocasionadas por los crímenes de alta tecnología se han ido incrementando de manera sorprendente en los últimos años. La Oficina Federal de Investigaciones (Federal Boureau of Investigations, FBI) estimó en el año 2004 una pérdida de 400 billones de dólares a causa de la ciberdelincuencia y casi un total de 500 corporaciones las afectadas electrónicamente por los cibercriminales. Esta institución considera que las pérdidas dejadas por los delitos informáticos ascienden a por lo menos un total de 10 billones de dólares anuales.

Un estudio recientemente elaborado en Estados Unidos por la Sociedad Americana para la Seguridad Industrial (ASIS) reportó que el número de incidentes en relación con la pérdida de propiedad intelectual y copia ilegal de software ha aumentado en un 323%. Se ha probado que las industrias estadounidenses han perdido casi un total de 24 millones de dólares anuales a causa de los "ladrones" de propiedad intelectual. Se probó que aproximadamente 60 por ciento de las pérdidas en propiedad intelectual se deben a los procesos de manufacturación de los procedimientos de información, y además, que en el 75% de los casos el personal interno de las organizaciones estaba involucrado.

Por otro lado, un estudio nacional de directores en corporaciones de seguridad, conducido por Carter y Katz, reveló que el 98% de las organizaciones fueron víctimas de crimen informático. Los responsables son personas que trabajan en las empresas, principalmente, pero existe el denominado grupo del *Computer Cracker,* típico personaje que ingresa al sistema y ocasiona daño.[17]

[17] Myers Jay, Larry, "High Technology Crimen Investigation: A Curricular Needs Assesment Of The Largest Criminal Justice And Criminology Programs In The United States", tesis doctoral, 2000, p. 2.

Ante este panorama, y frente a la preocupación principalmente económica, Estados Unidos ha sido el país más consciente de la problemática y por lo tanto el más proactivo en buscar soluciones. Durante los últimos años, universidades y entidades tanto públicas como privadas se han encargado de elaborar e investigar el crimen de alta tecnología con el fin de definirlo y así poderle dar el tratamiento adecuado. Con este objetivo, varios documentos se han publicado no sólo para darle una definición al concepto "crimen tecnológico", que aún no termina de ser elaborado, sino también para unificar y darle coherencia a la figura del "informático forense", o "perito informático", como es conocido en Colombia.

Lo primero que se intentó crear fue una alianza entre las corporaciones y el sistema jurídico con el fin de mantener la integridad del sistema de información y seguir las investigaciones de manera adecuada para solucionar el problema del crimen de alta tecnología. También se planteó fortalecer la educación y capacitar al personal de investigación. Igualmente, las agencias policiales, reconociendo la necesidad de ser más proactivas en el manejo de esta modalidad delictiva, crearon unidades de investigación en entidades como, por ejemplo, el FBI y la Asociación contra el Crimen de Alta Tecnología.[18]

Sin embargo, y a pesar de los esfuerzos realizados por combatir y crear políticas eficientes en torno a erradicar o por lo menos reducir las consecuencias que trae este delito, no se han podido obtener los resultados esperados, pues las políticas empleadas no han sido suficientes. Los expertos, en consecuencia, han concluido que el problema fundamental consiste en la escasez de personal con el conocimiento, la formación suficiente, las habilidades y capacidades necesarias para investigar y perseguir el crimen de alta tecnología.[19]

[18] Ibídem, p. 25.

[19] Ídem.

Uno de los estudios más detallados sobre la materia es la tesis doctoral escrita por Larry Myers en el año 2000. Este trabajo tuvo como objetivo principal proponer un modelo de investigador debidamente capacitado para afrontar los crímenes de alta tecnología, prevenir la impunidad respecto a estos delitos y fortalecer a la Administración de Justicia para combatirlos. Dicha investigación representa un trabajo formal para determinar el perfil requerido.

A tal fin, el autor establece unos criterios básicos que ha de tener un perito informático, o "investigador de crimen de alta tecnología", para la efectiva detección, investigación y persecución de esta clase de delitos, indicando que, además, requiere de cierto nivel de conocimiento en las áreas de justicia penal y criminología, principios de contabilidad y auditoría, tecnologías de información y operación de computadores.

La complejidad que rodea a esa materia propone un gran reto para los responsables de investigar ese tipo de crímenes. Diariamente evolucionan conceptos y programas que generan nueva clase de delitos tecnológicos, y por tanto las técnicas clásicas no serán siempre las adecuadas para solucionarlos.

> Es fundamental que los peritos no sólo sean expertos en sistemas de información, sistemas operativos, seguridad informática, configuración y auditoría de hardware y herramientas de protección informática, programación, conocimiento sobre protocolos de comunicaciones (especialmente TCP/IP), capas de red, sino además, a nivel personal, tener disposición para el aprendizaje diario ya que las tecnologías son evolutivas y con cambios y dinámicas constantes, ser analítico y con un altísimo grado de perseverancia en la búsqueda de rastros y huellas que generalmente el delincuente informático intentará borrar durante o después de la comisión de su ilícito.[20]

[20] Entrevista al ingeniero Javier Ortiz.

Se ha comprobado, igualmente, que es indispensable tener conocimientos en seguridad informática y justicia criminal. Normalmente los peritos tratan el problema y la solución como una cuestión técnica, y muchas veces el problema abarca el estudio de diferentes ciencias, lo que dificulta encuadrarlo dentro del tecnicismo. Su análisis debe ir acompañado de un buen manejo en temas jurídicos, por lo cual es fundamental saber cómo funciona el sistema penal, al igual que conocer los principios de la investigación criminal y la recolección de elementos materialmente probatorios, o evidencia física; entre éstos, el ejemplo más claro es el de respetar la cadena de custodia.

Por último, el investigador debe tener conocimientos en auditoría y contabilidad, con el fin de cumplir de manera exitosa la búsqueda del fraude. Esta característica se relaciona principalmente con la revisión de los estándares y protocolos manuales y de procedimientos que buscan evidencia o elementos materialmente probatorios.

La ausencia de estas habilidades, tanto técnico-legales como de auditoría, puede causar un impedimento en la solución del problema, ya que el personal no estaría apropiadamente capacitado. Si no se cuenta con niveles adecuados de educación y capacitación la prueba digital, que en este caso es el material más importante para analizar el delito, podría ser manipulada de forma inadecuada y eso ocasionaría su invalidez o inadmisibilidad en los estrados judiciales, generando impunidad. Los grupos de trabajo han comenzado a plantearse qué implicaciones penales puede tener el incumplimiento por parte de las fuerzas y cuerpos de seguridad del Estado en el tratamiento de los crímenes de alta tecnología cuando este incumplimiento signifique una vulneración de la normativa de protección de datos, llegando a la conclusión de que la prueba no sólo debe ser correctamente practicada durante la tramitación procesal, sino que, cuando ésta sea una prueba obtenida extraproceso, obliga a ser correctamente obtenida e incorporada al proceso.

La vulneración de esos principios ocasionarán la nulidad de ella, mientras que las violaciones de cuestiones formales o de procedimiento podrán entrar en el ámbito de la irregularidad, sin poderse determinar su valor.[21]

Al final del capítulo presentamos el modelo propuesto por Larry Myers sobre las habilidades y conocimientos que debe tener un perito informático[22] (figura 1, en anexos).

B. El perito informático en Australia

Como se mencionó, la Interpol hizo referencia a la destacada preparación y actuación de los técnicos forenses australianos que colaboraron en la investigación sobre los computadores de las FARC, lo cual comprueba que las autoridades en este país están afrontando con gran dinámica el delito informático, logrando grandes avances en armonizar la legislación y perseguir de manera debida la ciberdelincuencia.

Los investigadores forenses, o policía judicial (*forensic investigators* o *law enfocement officers*), son los encargados de obtener la evidencia relacionada con el crimen. La informática forense constituye una rama que se encarga de recuperar evidencias digitales de ordenadores o equipos informáticos; en Australia es lo más cercano al estudio del crimen de alta tecnología, como es llamado en Estados Unidos. Para ello las autoridades australianas han sido muy enfáticas en la necesidad de cooperación entre los agentes y las organizaciones que facilite el acceso a la información y los datos de prueba, al igual que la colaboración de los expertos en informática para asistir y proveer herramientas de investigación.

[21] Domínguez Peco, Elena, "Nuevas tecnologías, proceso penal y la protección de datos: el caso de la dirección IP", consultado en marzo de 2008. Disponible en: Http://Www.Cybex.Es/E-Newsletter/Pqojyrchnxcj4v/Indice_Nl0803.Htm.

[22] Myers, Larry, ob. cit., p. 55.

Australia se concentra en el principio rector de la asistencia mutua, un trabajo en equipo entre las autoridades y los expertos con el fin de perseguir los crímenes de alta tecnología. Las Cortes australianas se han pronunciado respecto de los casos que corresponden al delito tecnológico y la evidencia digital, y las dificultades que presentan. Las quejas más frecuentes provenientes de los jueces y jurados son aquellas relacionadas con la complejidad y el tecnicismo en la presentación y obtención de la prueba digital; frente a este problema se refirieron a la necesidad de obtener la opinión de un experto en los casos de crímenes de alta tecnología o *technology-enabled crime*, con el propósito de obtener una mejor comprensión de los elementos y la evidencia.

Se pronunciaron, igualmente, sobre la necesidad de desarrollar habilidades y conocimientos por parte de los jueces, el jurado y los abogados en relación con los eventos que involucran crímenes de alta tecnología y la importancia de capacitar a los profesionales del campo jurídico en el de la informática, especialmente en relación con la evidencia y su procedimiento de recolección. Se busca, mediante este ejercicio de capacitación, organizar a los grupos que manejan el tema forense y trabajan en el Gobierno para que incidan en las organizaciones y se pueda por medio de un trabajo colectivo lograr resolver de manera efectiva cada caso presentado.[23]

C. El perito informático en Colombia

De acuerdo con lo mencionado en esta investigación, y dada la presencia de delitos que han traspasado las fronteras, tales como el narcotráfico, el terrorismo y aun los que se producen internamente como la Farc-

[23] Raymond Choo, Kim-Kwang; Smith, Russell G.; Mccusker, Rob, "Future Directions in Technology-Enabled Crime: 2007-2009", Australian Institute of Criminology. Disponible en: http://www.aic.gov.au/publications/rpp/78/rpp78.pdf.

política y la parapolítica, Colombia requiere de expertos informáticos que contribuyan al análisis de las pruebas halladas continuamente en computadores y en elementos tecnológicos, que son de gran valor para la comprobación del delito.

El artículo 8° del Código de Procedimiento Civil establece para los peritos los siguientes lineamientos: "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".

El artículo 233 del mismo código indica: "la peritación es procedente para verificar hechos que interesen al proceso y requieran especiales conocimientos científicos, técnicos o artísticos".

Por su parte, el artículo 236 del Código de Procedimiento Penal dispone:

> Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o el imputado ha estado transmitiendo información útil para la investigación que se adelanta, durante su navegación por Internet u otros medios tecnológicos que produzcan efectos equivalentes, ordenará la aprehensión del computador, computadores y servidores que pueda haber utilizado, disquetes y demás medios de almacenamiento físico, para que expertos *en informática forense* descubran, recojan, analicen y custodien la información que recuperen (énfasis fuera del texto).

Más allá de los artículos mencionados, en Colombia no se cuenta con una definición formal de quién es un perito informático. Existe, de manera expresa, en el Código de Procedimiento Penal, la frase "expertos en informática forense", pero, ¿quién es un experto en informática forense? Aún no se ha tomado conciencia universal sobre el valor con-

ceptual de este tipo de profesional, lo que dificulta el entendimiento del oficio y su exacta aplicación.

Aún hoy en día la figura del peritaje informático se encuentra apenas consagrada en los artículos citados de manera genérica, pese a que el perito informático es la persona encargada de analizar y darle aplicabilidad técnica y jurídica a los sucesos de tipo penal.

Respecto del perito informático, existen dos clasificaciones principales: el perito de parte y el perito de oficio. El primero es aquél especializado en el área de las tecnologías de la información que, de acuerdo con el tema requerido, puede ser seleccionado para una labor de análisis, de la cual ofrece un dictamen técnico y científico. Generalmente se selecciona de listados en asociaciones, agremiaciones o colegios donde se cuenta con registros de profesionales en las diversas áreas informáticas o tecnológicas.[24]

El perito de oficio, además de las características mencionadas para el de parte, requiere de una formación más exigente y detallada en procedimientos legales, legislación nacional e internacional, así como fundamentos de criminalística y psicología que le permitan un conocimiento profundo sobre los casos de análisis. Un perito de oficio es garante de la verdad en un proceso, pues su estatus de funcionario de Estado le exige estar en las condiciones y competencias requeridas para defender al inocente y contar con testimonios y pruebas transparentes.[25]

La diferencia fundamental entre los peritos de parte y de oficio está

> [...] en que los primeros son especialistas y expertos en sus áreas de conocimiento y tienen una profesión que procura el desarrollo de la ciencia y la

[24] Cano Martínez, Jeimy José, "Estado del arte del peritaje informático", en *Alfa-Redi*. Disponible en: www.Alfa-Redi.Org, p. 9.

[25] Ídem.

tecnología; mientras que el perito de oficio, es parte integral del proceso legal, custodio de las pruebas y cadena de custodia, consciente de que su actuación le da al proceso la confiabilidad y formalidad, pues su formación en ciencias criminalísticas y forenses le ofrece mayores elementos de juicio para fortalecer las relaciones que verifiquen las pruebas que hagan brillar la verdad en el caso.[26]

Los artículos 200 al 203 del Código de Procedimiento Penal definen la Policía Judicial como la función que cumplen algunos organismos del Estado para apoyar la investigación penal en los campos investigativo, técnico, científico y operativo, por iniciativa propia o por orden impartida del fiscal de ésta, recaudando los elementos materiales probatorios o la evidencia física que permita determinar la ocurrencia de la conducta punible y la responsabilidad de los autores.

Con la nueva implementación del Sistema Penal Acusatorio los peritos que hacen parte de la Policía Judicial asumen un compromiso de trascendental importancia. En ellos recae la responsabilidad del éxito de la investigación penal, en la búsqueda de una justa y equitativa Administración de Justicia que garantice a los ciudadanos la convivencia pacífica y la armonía social.

Se requiere un servidor de policía judicial integral, suficientemente capacitado para el desempeño de las funciones técnicas, investigativas y operativas; que aplique correctamente los procedimientos y sea respetuoso de los principios que rigen las actuaciones procesales y de los derechos y garantías del ser humano.[27]

Dentro de las unidades de policía judicial se encuentran los peritos encargados de las investigaciones que se llevan a cabo sobre delitos informáticos.

[26] Ibídem, p. 9.

[27] República de Colombia, Consejo Nacional de Policía Judicial, *Manual Único de Policía Judicial*, Bogotá, Imprenta Nacional de Colombia.

En Colombia, el grupo de peritos que trabajan en la Unidad de Delitos Informáticos del Cuerpo Técnico de Investigación (CTI), de la Fiscalía General de la Nación, al responder un cuestionario preparado por los autores estableció que en la entidad los funcionarios que desarrollan actividades periciales son principalmente ingenieros de sistemas, algunos con especialización en seguridad de redes y en auditoría, y con experiencia de entre cinco y quince años en el apoyo a diligencias judiciales. Han recibido entrenamiento en el manejo de herramientas forenses (hardware y software) directamente por las casas productoras, y mediante programas de asistencia de la Embajada de los Estados Unidos. Además tienen formación en legislación, códigos Penal y de Procedimiento Civil, entre otros; cadena de custodia; y entrenamiento a través de los programas básicos de policía judicial dictados por la Fiscalía. Sin embargo, dejan presente el no existir en la actualidad una institución en el país que otorgue el título de perito informático.

IV. Acciones legislativas y políticas

La concientización sobre la problemática existente con respecto a la falta de regulación en este tema, que cada día cobra más importancia nacional e internacional, ha hecho que las legislaciones penales se actualicen acorde con las actividades delictivas que vienen surgiendo al tiempo con el avance tecnológico e informático; por esta razón, iniciativas parlamentarias y del propio Gobierno se han presentado a consideración del Congreso de la República, entre ellas los siguientes proyectos de ley:

Proyecto 49 de 2007, Senado, por el cual se reglamenta el ejercicio profesional del tecnólogo en criminalística y ciencias forenses. Puntualiza su principal objetivo, el de definir la actividad profesional de los tecnó-

logos en criminalística y ciencias forenses, reglamentando su ejercicio o prácticas; determina su naturaleza y campo de aplicación; señala su organización y acreditación por parte del Gobierno Nacional.

El ponente de la ley consideró necesario reglamentar la materia con el fin de lograr uniformidad en cuanto a los requisitos que se exijan para el desarrollo profesional de esta disciplina y determinar la obligatoriedad por parte de todas las instituciones debidamente reconocidas por el Ministerio de Educación Nacional para que ofrezcan el programa de tecnología en ciencias forenses o criminalística aplicando esos requisitos.

La justificación del proyecto se explica frente a la aplicación del Sistema Penal Acusatorio en la mayoría de departamentos de la República, lo cual ha determinado que por su naturaleza la recolección de pruebas por los aparatos estatales ofrecidos en la implementación del nuevo modelo no son suficientes para el óptimo desarrollo de éste, en tanto que los elementos probatorios se convierten en el pilar fundamental de las decisiones judiciales. De allí la importancia de que el tecnólogo en criminalística y ciencias forenses cuente con todas las garantías y control del Ministerio de Educación y del Gobierno Nacional, en cuanto a formar investigadores judiciales y científicos que efectúen una eficaz recolección de evidencias bajo los parámetros fijados por la cadena de custodia y según los protocolos establecidos para tal fin, ya que su labor debe ser justificada en el juicio. Este proyecto enfatiza en el tratamiento de la prueba judicial y en el derecho probatorio, para controlar en buena forma el alto índice de impunidad, y si bien contiene algunos componentes que debería tener el estudio de la informática forense, no son suficientes por carecer del rigor técnico y práctico sobre la materia.

A. Plan Nacional de TIC

El Gobierno de Colombia, a través del Ministerio de Comunicaciones, creó el Plan Nacional de Tecnologías de la Información y las Comunicaciones (TIC) teniendo como objetivo fundamental la lucha por que Colombia no se quede rezagada en el proceso de adopción y masificación de las tecnologías ni corra el riesgo de aislarse. Igualmente, lo guía el propósito de no permitir que los grupos más desfavorecidos de la población se marginen de la adopción y uso de las TIC, pues se acentuaría la desigualdad social. Con esto en mente, el Gobierno Nacional se ha comprometido con un Plan Nacional de Tecnologías de la Información y Comunicaciones 2008-2019 que busca durante este período lograr que la población colombiana se informe y comunique usando las TIC de tal manera que éstas mejoren la inclusión social y aumenten la competitividad.

Con el desarrollo de programas legislativos y gubernamentales se vuelve cada día más importante definir y capacitar a aquellas personas que van a ser las indicadas para aplicar de manera eficiente estos nuevos retos, y por la creación del Plan mayor cantidad de personas van a tener acceso a la Internet. Se pretende que toda la información y la documentación pasen a nivel virtual y digital; de ahí la necesidad de crear un sistema penal que enfrente las conductas delictivas de los intrusos informáticos. Y de todo esto, lo más importante es formar al perito informático, quien es en últimas el encargado de analizar e interpretar debidamente la información y adecuarla en el sistema penal.

Un estudio exploratorio sobre el estado actual del peritaje informático en Latinoamérica, adelantado por el profesor Cano, buscó establecer un marco referencial base de esta profesión en aspectos técnicos y jurídicos que procurara generar y fortalecer iniciativas multidisciplinarias para la modernización y avance de la Administración de Justicia en el contexto

de una sociedad digital y de la información, concluyendo que el peritaje informático es asumido principalmente por licenciados en informática e ingenieros de sistemas, eléctricos y electrónicos, basados exclusivamente en su formación académica.[28] También determinó que, debido a la falta de definición respecto al tema, ha sido necesario el formarse los peritos sean formados fuera de los países latinoamericanos, específicamente en Estados Unidos.[29]

En este mismo orden de ideas, el estudio estableció cinco requisitos fundamentales que debe tener un perito informático:

1. Honestidad: querer trabajar en el área, malicia para detectar debilidades, formación profesional en informática, certificaciones en seguridad informática, alto conocimiento y experiencia en administración de procesos, formación académica.
2. Experiencia: no menor de diez años; conocimientos técnicos en análisis de sistemas funcionales y de contraloría; estudios profesionales en tecnologías de información, análisis y crítica de los resultados.
3. Acreditar formación en seguridad de tecnologías de información y en legislación nacional e internacional; trabajo en equipo con abogados versados en estas tecnologías; profesionalismo e independencia; formación en análisis forenses en equipos electrónicos; estudios básicos en procedimientos civiles y penales.
4. Reconocimiento de imparcialidad y seriedad; formación en leyes nacionales e internacionales, así como en sistemas operacionales y manejo de evidencia digital.
5. Oportunidad y claridad en la preparación y comunicación de sus resultados.

[28] Cano Martínez, Jeimy José, ob. cit.

[29] Ídem.

Cuando nos referimos a un perito informático no solamente lo estamos haciendo respecto de sus conocimientos y calidades profesionales. Es fundamental tener presente sus habilidades, tal como lo establece la tesis doctoral antes analizada; entre éstas, se encuentra el manejo de los procedimientos para garantizar las medidas de seguridad y control a la hora de adelantar sus labores. En este sentido, el profesor Cano analizó algunos elementos que deben ser considerados para mantener la idoneidad del procedimiento forense:

1) *Esterilidad de los medios informáticos de trabajo:* este punto se refiere a la certificación de los medios de información utilizados por los profesionales, de tal manera que se pueda garantizar que éstos no han sido expuestos a variaciones magnéticas ópticas o similares, so pena de contaminar las copias de la evidencia. La esterilidad de los medios es una condición fundamental para el inicio de cualquier procedimiento forense.
2) *Verificación de las copias en medios informáticos:* las copias efectuadas en los medios informáticos, previamente esterilizadas, deben ser idénticas al original del cual fueron tomadas. Su verificación ha de ser hecha mediante métodos y procedimientos que establezcan la completitud de la información. Es muy importante usar técnicas de control que permitan comprobar la idoneidad de la información.
3) *Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados:* el investigador debe ser el custodio de su propio proceso, es por esto obligatorio que en cada uno de los pasos los resultados estén claramente documentados para que cualquier persona externa pueda revisarlos, validarlos, e inclusive reproducirlos, usando la misma evidencia.
4) *Mantenimiento de la cadena de custodia de las evidencias digitales:* la custodia de los elementos allegados al caso deben responder a

una diligencia y formalidad especial para documentar cada uno de los eventos realizados con la evidencia: quién la entregó, cuándo, en qué estado, cómo se ha transportado, quién ha tenido acceso a ella, etcétera.

5) *Informe y presentación de resultados de los análisis a medios informáticos:* una inadecuada presentación de los resultados puede llevar a falsas expectativas o tergiversación de los hechos. Esto puede poner en entredicho la idoneidad del investigador. Por lo tanto, la claridad, el uso adecuado de un lenguaje sin tecnicismos, redacción impecable y sin juicios de valor, son elementos críticos a la hora de defender un informe de las investigaciones.
6) *Administración del caso:* los investigadores en informática forense deben prepararse para declarar ante un jurado o juicio en el momento que lo solicite la investigación, por lo tanto han de mantener en un sistema automatizado la documentación de expedientes de los casos bajo una adecuada cuota de seguridad y control, con el fin de salvaguardar las investigaciones y cumplir con el debido cuidado, diligencia y previsibilidad profesional exigibles a quienes participan en ellas.
7) *Auditoría de los procedimientos realizados en la investigación:* es recomendable que el profesional investigador mantenga un ejercicio de autoevaluación de sus procedimientos para contar con la solidez de una buena práctica de investigaciones forenses.

Según el ingeniero Javier Edgardo Ortiz Acosta, investigador de la Sección de Análisis Criminal del CTI de la Fiscalía General de la Nación, dentro de los delitos más habituales investigados en el año 2007 se encuentran:

- Protección al menor: posesión, producción y distribución de pornografía infantil.

- Fraude en las comunicaciones: locutorios telefónicos clandestinos.
- *Dialers*: modificación oculta del número de teléfono de destino.
- Producción y distribución de decodificadoras de televisión privada.
- Fraudes en Internet: estafas, subastas ficticias y ventas fraudulentas.
- *Carding*: uso de tarjetas de crédito ajenas o fraudulentas.
- *Phising*: redirección mediante correo electrónico a páginas falsas, simuladas, trucadas.
- Cartas nigerianas: son mensajes enviados con el fin de engañar a un tercero mediante la promesa de obtener un beneficio económico por el manejo de una herencia o fortuna de su remitente.
- Seguridad lógica: virus, ataques de denegación de servicio, sustracción de datos, *hacking*, descubrimiento y revelación de secretos, suplantación de personalidad, sustracción de cuentas de correo electrónico.
- Delitos de injurias, calumnias y amenazas a través del correo electrónico, *news* (noticias), foros, *chats* (charlas) o *SMS* (mensaje de texto).
- Robos de código: como en el caso de los juegos *Dark Age of Camelot* y *Half-Life 2*, o de los sistemas *Cisco IOS* y *Enterasys Dragon IDS*.
- Recuperación de evidencias en discos.

Con el problema incrementándose cada año, se comprueba que existe escasez de funcionarios con el suficiente nivel de conocimiento, habilidades y actitudes para detectar, investigar y perseguir el crimen de alta tecnología. Actualmente "Las pruebas tradicionales están migrando desde el papel hacia un entorno virtual, donde los procesos de gestión y criterios de admisibilidad cambian por completo".[30]

[30] Herrero Tejedor, Fernando, consultado en: http://www.Cybex. Es/E-Newsletter/Pqojyrchnxcj4v/Indice_Nl0803.Htm.

Teniendo en cuenta lo anterior, es fundamental que los Estados, mediante sus aparatos judiciales, cumplan con la obligación de establecer un marco jurídico capaz de identificar, prevenir y sancionar adecuadamente los delitos relacionados con el crimen tecnológico y pongan a disposición funcionarios con conocimientos informáticos, jurídicos y técnicos suficientes para ofrecer certeza sobre la integridad de la evidencia obtenida en entornos digitales. Tal obligación positiva de protección por parte del Estado forma parte inherente del contenido de los derechos fundamentales de las personas, garantizados por las normatividades internas e internacionales.[31]

V. Formación de un perito informático

En el acápite anterior vimos quién es un perito informático, su importancia dentro del nuevo contexto global y la necesidad de capacitarlo debidamente para que pueda cumplir con los objetivos que esta nueva disciplina impone. Ha sido demostrado a lo largo de esta investigación el gran interés por el campo de la informática forense, que ha conducido a una proliferación de opciones en la educación académica y programas de entrenamiento profesional; sin embargo, pocos estudios han procurado definir cualidades y calidades, o medidas de excelencia, para esos programas. Por dicha razón, esta parte del trabajo busca establecer los criterios de idoneidad que debe tener un perito informático, analizar concretamente cómo debe ser la formación académica y personal que requiere recibir, y formular una propuesta clara de cómo debería ser esta educación en Colombia.

El campo de la informática forense está creciendo rápidamente. Hasta el momento los esfuerzos de académicos, predicadores y practicantes del

[31] Ídem.

área no han podido converger en el punto de aproximarse y producir un modelo pedagógico para esta disciplina, pues por un lado tenemos a la comunidad académica, que aparece inmersa en un *contraataque tecnológico* desviado de la detección de los intrusos, y por otro, a los encargados de recuperar la evidencia de los delitos e identificar a perpetradores y víctimas, y el campo jurídico.[32]

El reto sería el de cerrar la brecha existente entre la teoría y la práctica, y proponer un sistema de educación superior que satisfaga los aspectos más relevantes en la formación de un perito informático, los requerimientos teóricos, técnicos y prácticos.[33]

Es importante recordar en este punto que la informática forense es por naturaleza una ciencia multi e interdisciplinaria, debido principalmente a que en su universo de acción convergen varias materias: la informática, el derecho, la criminología, las ciencias informáticas, la ética, los sistemas de seguridad informática, los procedimientos y herramientas forenses, la correcta escritura y redacción de los dictámenes rendidos ante las Cortes, los protocolos y las prácticas seguras, entre otras, y por eso un programa de educación o certificación debe abarcar su estudio.

Estados Unidos ha sido el país líder en la investigación y el desarrollo de la informática forense. No solamente ha sido pionero respecto de las definiciones, sino que también el gran creador de programas y cursos de capacitación en esa área. A continuación se hace un análisis comparado de los programas existentes en Estados Unidos para poder desarrollar con mayor exactitud uno en Colombia teniendo en cuenta las iniciativas existentes y los recursos con los que cuenta nuestro país.

[32] Yasinsac, A.; Erbacher, R.; Marks, R.; Pollitt, M.; Sommer, P., "Computer Forensics Education", en IEEE *Security and Privacy*, vol. 1, núm. 4, 2003, pp. 15-23.

[33] Forza I. R., "Digital forensics investigation framework that incorporates legal issues". Disponible en: http://www.dfrws.org/2006/proceedings/4-Ieong.pdf.

A. Programas sobre informática existentes en Estados Unidos

Estados Unidos ha comprendido la importancia de proveer seguridad, garantías y confianza en los sistemas de información a tal punto que es una de las prioridades nacionales, de ahí su dedicación a preparar profesionales en informática forense para poder lograr este objetivo.[34]

Un estudio estadounidense publicado en agosto de 2003 por el IEEE Computer Society estableció que existen cuatro categorías para estructurar los temas de estudio en el campo de la informática forense. La primera es la recolección de evidencia; la segunda, preservación de ésta; la tercera, su presentación; y por último, la preparación forense. Teniendo esto en cuenta, analizaremos cada una de ellas.[35]

En cuanto a la recolección de evidencia se destaca que la esencia de cualquier ciencia forense es la información, de modo que la evidencia es la información presentada ante una Corte. La evidencia digital puede ser dividida en tres categorías:

— Registros almacenados en el equipo de tecnología informática (correos electrónicos, archivos, imágenes, etcétera).
— Registros generados por los equipos de tecnología informática (de auditoría, de transacciones, de eventos).
— Registros que parcialmente han sido generados y almacenados en los equipos de tecnología informática (hojas de cálculo financieras, consultas especializadas en bases de datos, vistas parciales de datos).[36]

[34] Herath, A.; Herath, S.; Samarasinghe, P.; Herath, J., "Computer forensics, information security and law: a case study", en *Proceedings of Systematic Approaches to Digital Forensic Engineering*, 2005.

[35] Yasinsac, A.; Erbacher, R.; Marks, R.; Pollitt, M.; Sommer, P., ob. cit.

[36] Cano Martínez, Jeimy José, ob. cit., p. 3.

Las características propias de la evidencia digital, como son su volatilidad; su anonimato; su fácil duplicación, modificación y eliminación, hacen que no todo el mundo tenga la capacidad de recolectarla. Por esta razón, y considerando su carácter indispensable, es fundamental saber dónde y cómo buscarla, respetando los procedimientos técnico-legales. Éste es quizás uno de los puntos más importantes en esta disciplina. Se necesita ser un experto imparcial para garantizar la transparencia del proceso, capaz de extraer y recuperar los datos en caso de que hayan sido borrados, manipulados, o el disco duro se haya dañado, sin maltratar la evidencia. Al referirse a este punto, los autores lo describen como el corazón de la informática forense.[37]

Respecto de la preservación de evidencia, se establece que una vez la información es recuperada lo importante es tomar las medidas necesarias para preservarla hasta el momento de ser presentada ante la Corte.

Sobre la presentación de la evidencia sabemos que la información digital es difícil de presentar ante una Corte debido a su naturaleza esencialmente abstracta; así la gente esté familiarizada con los computadores, la mayoría tiene muy poco entendimiento tecnicista y sobre las redes de información digital, lo que dificulta entender la evidencia extraída de ellos; aquí es donde cobra importancia la labor que realizan los informáticos forenses, pues son quienes tienen la capacidad de presentarla ante la Corte de forma que los jueces o el jurado entiendan cómo fue recolectada y su contenido.

Por último, el estudio hace referencia a la preparación del forense. Esta categoría se refiere al nivel de educación que éste debe tener para prevenir la ocurrencia de delitos informáticos, etapa anterior a la recolección, preservación y presentación de la evidencia. Dicha preparación también capacita a los expertos para que puedan comunicar estrategias útiles a los usuarios relativas a medidas informáticas preventivas.

[37] Herath, A.; Herath, S.; Samarasinghe, P.; Herath, J., ob. cit.

Con estas cuatro categorías en mente, el estudio adelantado por el IEEE elaboró un currículo en esta materia que incluye una variedad de temas, algunos académicos y otros prácticos, para desarrollar habilidades en programas informáticos. Se destacó en el aspecto técnico el conocimiento para usar las herramientas y seguir los procedimientos adecuados, y en la teoría la manera de presentar la información y rendir el dictamen pericial ante la Corte (tabla 1, en anexos).

Como se puede observar en la tabla, la parte académica está enfocada en ofrecer los fundamentos básicos del peritaje e introducir a los estudiantes en la problemática mundial y en la importancia de su papel para la sociedad con el fin de proponer soluciones mediante su correcto desempeño en la detección, persecución y aprehensión de los cibercriminales. Además, como en todo proceso académico, inmiscuye a los estudiantes en el aspecto jurídico de la informática forense, y a través del estudio de casos reales ellos observan los problemas que se presentan diariamente y aprenden a solucionarlos desde el enfoque ofrecido por la especialidad.[38]

La parte práctica alude al desempeño de los estudiantes en los laboratorios forenses. Es importante enseñarles a manipular y familiarizarse con la evidencia usando las herramientas disponibles en el mercado. Hablar de informática forense sin revisar algunas ideas sobre herramientas es hacerlo sólo en un contexto teórico. Las herramientas informáticas son esenciales para analizar las evidencias digitales, siendo fundamental manejarlas de tal forma que se pueda validar su confiabilidad en los resultados y la formación y conocimientos del investigador que las utiliza.[39] La tabla 2 muestra algunas de las herramientas frecuentemente utilizadas en procedimientos forenses.

[38] Ibídem, p. 5.

[39] Cano Martínez, Jeimy José, ob. cit.

Teniendo en cuenta lo anterior, se concluye en este punto que la informática forense es un proceso que determina y relaciona información y evidencia digital con el fin de establecer hechos fácticos en un proceso judicial. Ieong Forza, en su artículo "Digital forensics investigation framework that incorportate legal issues", establece que para cumplir esos requisitos los principales fundamentos o principios de esta ciencia incluyen: el reconocimiento, la confiabilidad y la pertinencia, refiriéndose a la evidencia y a los procedimientos (figura 2).[40]

A continuación se enuncian algunos de los programas académicos y certificaciones más relevantes en materia de informática forense con el objetivo de despejar el interrogante de quién está capacitando a la siguiente generación en informática forense y qué estándares están siendo aplicados, para con los resultados realizar un estudio comparado aplicado a Colombia que establezca cuáles programas funcionan o serían viables en nuestro país.

B. Programas académicos[41]

A medida que la demanda de profesionales entrenados en el campo de la informática forense ha venido aumentando, y debido a la creciente preocupación por la seguridad nacional, varias universidades estadounidenses han optado por desarrollar programas técnicos y profesionales de dos y cuatro años de duración, respectivamente, de maestría y de certificación.[42]

[40] Forza, I. R., "Digital forensics investigation framework that incorporate legal issues". Disponible en: www.Sciencedirect.Com, p. 2.

[41] Taylor, Carol; Endicott-Popovsky, Barbara; Phillips, Amelia, "Forensics Education: Assessment And Measures Of Excellence", en IEEE *Computer Society*, 2007, p. 3.

[42] Ibídem, p. 2.

1. Carreras técnicas

El objetivo de la carrera técnica en informática forense, de dos años de duración, es el de capacitar en conocimientos, habilidades y herramientas de informática digital y ciencias informáticas. Estas últimas son puntuales en hacer hincapié en habilidades que apoyan el análisis de información forense tales como sistemas operativos o de seguridad informática, con poco énfasis en programación, estructura de datos y otras materias típicas de la carrera. Algunas de las universidades que cuentan con estos programas técnicos son: Highline Community College, Spokane Falls Community College, Butler County Community College y Tompkins Cortland Community College.

2. Pregrado

Existe, igualmente, el pregrado en informática forense, el cual tiene una duración de cuatro años. El enfoque de este programa puede variar, dependiendo del Departamento o la Facultad que lo ofrezca. Entre los Departamentos se encuentran los de contabilidad, criminalística, economía e informática, todos concentrados en informática forense. La naturaleza de los programas es interdisciplinaria e incluye cursos en forensia digital, ciencia informática, derecho informático y criminología, los cuales, a diferencia de las carreras técnicas, parecen hacer menos realce en el desarrollo de habilidades forenses y conceder más importancia a las materias relacionadas con criminología y aplicación de la ley. Se ofrecen en universidades como Champlain College, Purdue College y John Hopkins University.

3. Maestrías

Por otra parte, algunas universidades ofrecen maestrías en ciencias informáticas. Estos programas no parecen tener un currículo estándar,

pues en este nivel de educación es entendible la diversidad en cuanto a su aplicación, considerando los diferentes panoramas. Varias maestrías profundizan en la recolección de evidencia y el manejo probatorio, procesal y técnico ante el juzgado; otras se enfocan en justicia criminal, seguridad informática, etcétera. Estas maestrías se dictan en universidades como Purdue University, University of Rhode Island, George Washington University, entre varias.

Otro ejemplo de un programa de maestría complementario al de pregrado en computación e informática forense lo creó la Universidad de Champlain. Teniendo en cuenta que el pregrado en informática forense combina aspectos de tecnologías de red y computacional, criminalística, crímenes cibernéticos y otros aspectos técnicos, esta universidad decidió educar a la próxima generación de informáticos forenses en los aspectos administrativos de la profesión, creando la maestría en administración de investigación digital, con el propósito de darle un enfoque especializado que lidiara con los aspectos administrativos de la investigación forense.

Por otro lado, ciertos programas académicos ofrecen certificaciones en informática forense. Estos programas, al igual que la concentración de grado, dependen fundamentalmente del Departamento de origen: Justicia Criminal, Administración, etc. Dicha certificación se ofrece en instituciones como University of Rhode Island, Champlain College y Cal State Fullerton.

4. Programas profesionales de certificación

Se entiende por programas de certificación aquellos mediante los cuales se le reconoce a un individuo poseer conocimientos, habilidades y capacidades para desempeñar una función específica, adquiridos a través de la educación, el entrenamiento o la experiencia. La certificación

no se compara con un programa académico en cuanto a formación; sin embargo, de una certificación se puede establecer que la persona posee un nivel básico de conocimiento.

A continuación se enuncian las certificaciones profesionales más reconocidas en informática forense en Estados Unidos:

1. Certified Computer Examiner (CCE). Expedida por la international Society of Forensics Computer Examiners.
2. GIAC Certified Forensics Analyst (GCFA). Del SANS Global Information Assurance Organization.
3. Certified Computer Crime Investigator (CCCI) and Certified Computer Forensics Technician. En la international Association of Computer Investigators.
4. Certified Forensic Computer Examiner. Por la International Association of Computer Investigative Specialists.
5. Cyber Security Forensics Analyst. Ofrecida por el CSFA Cyber Security Institute.

Teniendo en cuenta la internacionalización adquirida por esta disciplina, se ha exigido la implementación de certificaciones globales; sin embargo, ha sido difícil lograrlo, principalmente porque hasta el momento se están desarrollando los programas nacionales. De todas maneras, todo esto son grandes avances que ayudan a profundizar en la materia, a orientar esta disciplina y lograr consolidar cada vez más su estructura para poder formar cada día mejor a los peritos informáticos.

Como se observa, los programas en informática forense dependen en gran medida del nivel de educación ofrecido, sea pregrado, maestría o certificación. No obstante, varios estudios son enfáticos en concluir que es posible identificar algunas características generales claves en cuanto a la educación que debe recibir un perito informático para ser ella de alta

calidad en cualquier nivel. (Estos componentes de excelencia se detallan en la tabla 3).[43]

C. Programas existentes en Colombia

Como lo estableció la Unidad de Delitos Informáticos del CTI, "La importancia de formar un perito informático en el país es muy alta, el constante crecimiento del país en materia de tecnología y su uso generalizado en todos los ambientes pone la información como un nuevo bien susceptible de ser vulnerado y que por ende necesita ser protegido".

Colombia actualmente no cuenta con un programa académico a nivel de pregrado, especialización o maestría en informática forense, ni siquiera con una carrera técnica. La formación de los peritos informáticos en el país ha sido muy abstracta, por cuanto aún no se han establecido criterios de idoneidad regulados respecto de su adecuada formación. Esta afirmación se pudo establecer después de realizar una investigación de campo en algunas entidades del Estado encargadas del manejo de "delitos informáticos".

El mayor Freddy Bautista, director de Delitos Informáticos de la DIJIN —Dirección de Investigación Criminal—, afirma que existen dos postulados muy importantes para acreditar la idoneidad de estos expertos: estudio y experiencia. Para la Fiscalía General de la Nación, Unidad de Delitos Informáticos del CTI, la conclusión fue exactamente la misma: no existen criterios de idoneidad certificados, la formación de los peritos informático en Colombia se va dando por la experiencia y los estudios adelantados por los profesionales que ocupan estos cargos, y frecuentemente quienes ejercen estas labores son graduados en ingeniería de sistemas, algunos con especialización en seguridad de redes y auditoría.

[43] Taylor, Carol; Endicott-Popovsky, Barbara; Phillips, Amelia, ob. cit., p. 6.

En los estrados judiciales la idoneidad es reconocida por el tiempo de servicio y la experiencia de los funcionarios de la policía judicial, sumado a los programas de formación general y capacitación que reciben por parte de las instituciones y la Embajada de los Estados Unidos. Las capacitaciones, fundamentalmente, son en temas como: formación en legislación, Códigos Penal y de Procedimiento, cadena de custodia y entrenamiento en procedimientos a través de los programas básicos de policía judicial, reiterando que todavía no hay una institución en el país la cual ofrezca programas otorgando el título de perito informático o de informático forense.

En posgrados existen varios programas de seguridad informática, en universidades como la de los Andes, la Javeriana, la Nacional, la Católica, entre otras; pero esto es sólo un componente de la informática forense orientado hacia la parte de auditoría, haciendo falta en esta ciencia multidisciplinaria el análisis y la formación en aspectos igualmente importantes como los técnicos, los jurídicos, los relacionados con la criminalística, la criminología, etcétera.

También se reseña que en Colombia existe la Unidad de Investigación Criminal, concedida al Ministerio de Defensa Nacional mediante resolución 2045 del 15 de junio de 2007. Esta Unidad, que forma parte de la Policía Nacional, contiene programas académicos impartidos por la Facultad de Criminalística y la Escuela de Policía Judicial e Investigación. Con el fin de conocer los que se estaban adelantando en esa institución, se contactó al teniente coronel Hugo Agudelo Sanabria, director de la Escuela de Investigación Criminal, quien explicó que la Facultad otorga el pregrado en investigación criminal, el cual consta de tres módulos básicos: 1) criminalística, 2) policía judicial, y 3) medicina legal y ciencias forenses. Además, en esa dependencia existen dos especializaciones: investigación criminal e investigación de accidentes de tránsito.

El pregrado tiene una duración de cinco años y contiene los siguientes programas: Profesional en Criminalística, Tecnología de Investigación Criminal, Técnico Profesional en Dactiloscopia, Técnico Profesional en Identificación de Automotores, Técnico Profesional en Balística, Técnico Profesional en Documentología, Técnico Profesional en Explosivos, Técnico Profesional en Fotografía Judicial, Técnico Profesional en Topografía, Técnico Profesional en Policía Judicial, Curso Básico de Policía Judicial, Diplomados y Seminarios.

La especialización en investigación criminal tiene una duración de dos semestres y una metodología presencial. Este programa se encuentra dirigido a profesionales en áreas como derecho, administración, ingeniería, salud, humanidades, física, química, integrantes de la Fuerza Pública, y campos afines a la investigación criminal. Se busca con él que el egresado salga capacitado para desempeñarse como auxiliar de la justicia, asesor judicial y de policía judicial, asesor de entidades públicas y privadas, investigador y docente de instituciones con programas universitarios en el campo de la investigación criminal. En el primer semestre se dictan las materias de procedimiento penal (dos créditos), criminalística (cinco créditos), ciencias forenses I (dos créditos), investigación criminal I (dos créditos), metodología de la investigación científica I (un crédito) y electiva I (un crédito). El segundo semestre contiene las siguientes: procedimiento penal en el sistema acusatorio (tres créditos), ciencias forenses II (dos créditos), criminología y victimología (dos créditos), investigación criminal II (tres créditos), metodología de la investigación científica II (un crédito) y electiva II (un crédito).

Como se puede observar, el pregrado y la especialización solamente tratan temas jurídicos, de criminología, criminalista y ciencias forenses. Sin embargo, no tienen en cuenta materias técnicas ni de procedimiento con respecto a las pruebas y herramientas orientadas a la informática forense y la ciberdelincuencia. Por lo tanto, así esos programas conten-

gan temas afines a la informática forense, no logran satisfacer los requisitos que esta ciencia impone. Este programa resulta muy parecido a lo que se pretende con el mencionado proyecto de ley 49 de 2007.

Los funcionarios de las entidades visitadas concluyeron que uno de los problemas más graves en Colombia respecto del delito informático consiste en que, así éste se llegue a tipificar en el Código Penal, habrá limitaciones en el proceso probatorio dada la dificultad inherente en cuanto a su claridad, aplicación y calificación al momento de ser analizado. Lo anterior es importante teniendo en cuenta el contexto del nuevo Sistema Penal Acusatorio, pues el tema de las pruebas es un componente crítico para apoyar a la Administración de Justicia. En este sentido, y considerando el crecimiento y uso de las tecnologías de información, las pruebas de los hechos ahora se encuentran en mayor proporción en medios digitales, lo cual exige apoyo por parte de personal especializado en esta área.

Así pues, surge la necesidad de contar con peritos informáticos que conociendo ampliamente las implicaciones técnicas soporten investigaciones que permitan esclarecer los hechos de un delito. Se trata, en otras palabras, de que el ordenamiento penal colombiano se sume a las políticas penales globalizadas en materia del combate frontal contra la llamada criminalidad del ciberespacio y le brinde herramientas a la comunidad internacional para la persecución de estos flagelos.

VI. Propuesta sobre la formación de peritos informáticos en Colombia

A lo largo de este estudio comparado hemos podido apreciar quién es un perito informático y la formación que debe recibir este especialista para cumplir como profesional con excelencia. Con esto en mente, y considerando la importancia del tema al igual que la precariedad en

cuanto a los programas existentes en Colombia, se hace un llamado al Gobierno, a la Academia, y a quienes deben proteger el debido proceso en el mundo de la investigación, para contextualizar la práctica de los peritos informáticos y aplicar líneas de acción a mediano y corto plazo en esta especialidad con el objeto de fortalecer y modernizar la Administración de Justicia en el país.

Para nadie es desconocido el hecho de que hoy enfrentamos una problemática delincuencial compleja. Los grupos delictivos se transformaron en las últimas décadas en verdaderas empresas criminales de alcance internacional, en su mayoría asociados al narcotráfico, al tráfico de armas, al terrorismo, al secuestro y a otras conductas que afectan por igual a todos los Estados. Por consiguiente, cada día es mayor la responsabilidad del investigador y de las autoridades. Para ello es imperativo el acceso a nuevos conocimientos en la tecnología de punta, la actualización en sus procedimientos y la normatividad legal.

Con este fin, se propone una medida de acción a corto plazo que consiste en crear un posgrado en informática forense, ya sea como parte de un programa universitario o como especialización en la Facultad de Investigación Criminal de la Policía Nacional, vigente en la Escuela General Santander.

Consistiría en una especialización de un año, con un contenido multidisciplinario, pues como lo vimos en la segunda parte de esta investigación, un perito informático es aquél que debe tener conocimientos en aspectos técnico-legales, económicos, en administración, en principios de contabilidad y revisión; en justicia penal, criminología y criminalística; en seguridad informática, principios de auditoría y contabilidad ocupacional, conceptos financieros, operación de sistemas de procedimiento criminal y recolección de evidencia.

Es sustancial establecer que esta especialización necesita no sólo de la parte académica del contenido, sino además resulta fundamen-

tal la práctica; es en esta área donde el estudiante desarrolla las habilidades procedimentales que deben seguirse para el buen manejo de las herramientas y los procedimientos relacionados con la evidencia en la escena del crimen, como son: identificación, preservación, extracción, análisis, interpretación, documentación y presentación de las pruebas en el contexto de la situación bajo inspección de la evidencia, con el fin de obtener claridad en la preparación y comunicación de los resultados.[44] Para esto se utilizarían los laboratorios y equipos con los cuales cuentan actualmente instituciones del país como la Dirección de Investigación Criminal de la Policía Nacional de Colombia (DIJIN), el Cuerpo Técnico de Investigación (CTI), el Departamento Administrativo de Seguridad (DAS) y la Policía Nacional.

Se colige que tanto la parte académica como la práctica se pueden unir al momento de estudiar casos reales. La idea de esta especialización es trabajar a partir del estudio de hecho ocurridos, así los estudiantes se pueden familiarizar con el entorno y las posibles soluciones al delito que se les propone como material de estudio.

De esta forma concluimos que quienes se dedican a esta disciplina emergente como lo es la informática forense, deben ser profesionales con los más altos niveles de ética y respeto por las instituciones, honestos, con experiencia, imparciales y serios en sus dictámenes, pues en ellos está el soporte de las decisiones que sobre los hechos analizados se tomen.

En cuanto a la formación pudimos observar que en Estados Unidos existen múltiples programas académicos y de certificaciones, mientras que en Colombia no existe esa cultura ni el desarrollo de la informática forense en ese país, razón por la cual se dificulta más aplicar esta teoría. Existe preocupación y deseos por avanzar en el tema, pero no se toman acciones a corto plazo ni mucho menos a futuro, de acuerdo con las necesidades urgentes que la problemática afronta.

[44] Cano Martínez, Jeimy José, "Estrategias antiforenses en informática: repensando la computación forense", p. 2.

Se debe, como lo recomienda el estudio de la Comisión de Regulación de Telecomunicaciones, evaluar las actuales autoridades legales, para su adecuación. El país requiere revisar su Código Penal con el fin de determinar si está actualizado para encarar los actuales y futuros delitos contra la ciberseguridad; desarrollar un entendimiento entre fiscales, jueces, legisladores, sobre ese aspecto, y capacitar al personal destinado a ejercer las funciones de perito informático.

La justificación de esta propuesta se explica ante la aplicación del nuevo Sistema Penal Acusatorio, que por su naturaleza: la recolección de pruebas y los aparatos estatales ofrecidos a la implementación del nuevo modelo, no son suficientes para su efectivo desarrollo. De allí la importancia y la necesidad de darle vida a un individuo con características muy particulares, encargado de velar por la investigación del crimen informático, de darle un tratamiento rápido y efectivo, y que cumpla a cabalidad con todas las exigencias, profesional al cual denominamos perito informático o informático forense, quien cuenta tanto con todas las garantías en su preparación con el fin de modernizar la legislación penal colombiana y ponerla a la par de la de otros países, como con los controles del Ministerio de Educación y del Gobierno Nacional. Esta invitación a las autoridades se convierte en una solución a corto plazo, sin dejar de lado la posibilidad de crear pregrados, maestrías y certificaciones a futuro que permitan desarrollar el conocimiento de los interesados y crear una nueva era de informáticos forenses capaces de cumplir con los retos impuestos por la actual sociedad digital y la Administración de Justicia.

VII. Conclusiones

Del estudio realizado se pueden derivar varios aspectos importantes. El primero se refiere a la conciencia existente actualmente en los países

respecto de las consecuencias tan nocivas que trae el crimen de alta tecnología y, por consiguiente, la importancia de darle un tratamiento rápido y efectivo. Esto, sin duda alguna, es una de las características comunes más importantes, pues no sólo muestra cómo los países apuntan hacia un mismo fin, sino que se puede percibir la necesidad de unificar y armonizar las legislaciones, considerando que se trata de un delito globalizado.

Otra característica importante consiste en que los países reconocen la importancia y la necesidad de formar peritos informáticos, individuos de características muy particulares encargados de velar por la investigación del crimen informático.

Del estudio comparado se desprende que el crimen de alta tecnología contiene elevado grado de especialidad por tratarse de un delito multidisciplinario, cargado de complejos grados de tecnicismo y conocimientos jurídicos. Éste es quizás el punto más importante y sobre el cual los Estados han hecho gran énfasis. Cuando se pensó en la definición de perito informático todos coincidieron en que no basta con los conocimientos técnicos relacionados con la materia, pero tampoco era suficiente tener únicamente los jurídicos y procedimentales. Se busca implementar en los sistemas jurídicos la figura del perito informático como auxiliar de la justicia encargado de investigar y analizar aquellos casos en los cuales el juez no tiene los conocimientos suficientes, y pese a no ser la solución meramente técnica, se requiere que el perito sepa manejar el procedimiento y el correcto orden en la búsqueda de los rastros digitales dejados en la comisión de un delito informático, que es quizás lo más complejo de adelantar, y por lo tanto que sea un experto en la interpretación de ellos y en la recolección y manipulación de la prueba.

En términos generales, se puede decir que son pocas las diferencias establecidas en los países con relación a la definición de perito informático. Mas se puede decir que tanto en Australia como en Colombia la

definición se centra en base a los conocimientos en materia de tecnología y los aspectos jurídicos y de criminología, sin tener en cuenta los de auditoría y contabilidad, tal como lo propone Estados Unidos.

La informática forense es una ciencia relativamente nueva que está adquiriendo gran significado debido al aumento del valor de la información y al uso que se le da a ésta. Cuando se materializa un crimen relacionado con la informática la información queda almacenada en forma digital, dificultándose su recolección y utilización, razón por la cual debe realizarse por medios diferentes a los tradicionales.

Y no basta con darle una solución técnica al problema del crimen de alta tecnología, pues se deben tener conocimientos sobre el sistema jurídico, la criminología y la criminalística que permitan darle un adecuado manejo a la prueba y seguir paso a paso el procedimiento sin violar la cadena de custodia, debiéndose considerar también la posibilidad de crear procesos de capacitación en nuevas tecnologías y entrenamiento avanzado en sistemas operativos y bases de datos, políticas y lineamientos, para las entidades de acceso público.

Es evidente que existe una amenaza económica importante sobre las naciones, pues los sistemas jurídicos han demostrado no estar preparados para combatir el delito de alta tecnología y a consecuencia de ello, como fue demostrado en el caso estadounidense, se perdieron millones de dólares por falta de personal capacitado e idóneo. Si bien se cuenta con personas capacitadas en temas técnicos, no es suficiente, pues se ha comprobado a lo largo de este estudio comparado que por la naturaleza del crimen es imprescindible contar con personas versadas en temas de criminología, criminalística y procedimiento legal, al igual que aptas para elaborar dictámenes conforme a las normas de procedimiento vigentes.

Además, como vimos, es importante también que el perito informático sea capaz de efectuar la correcta recolección de evidencia y de mantener

debidamente la cadena de custodia. De igual forma, los jueces, jurados o abogados llamados a analizar un caso de informática se verán en aprietos debido al tecnicismo que requiere el análisis. En este punto es cuando se pide asesoría a un experto que dé respuesta a cada caso de manera profesional, constituyéndose en fuente confiable a la hora de juzgar y decidir sobre la veracidad de los hechos en un delito.

Cuando se ha optado por una legislación o un capítulo especial que comprenda los llamados delitos informáticos se ha partido de la base de elevación a bien jurídico tutelado el derecho a la información, referida al dato informático (información almacenada, procesada y transmitida mediante sistemas informáticos), o si se quiere, el bien jurídico a salvaguardar es la seguridad de la información, teniendo en cuenta que a través de su ataque se pueden vulnerar otros bienes como la intimidad, la propiedad, la libre competencia y hasta la misma seguridad del Estado. Es por ello que algunos "doctrinantes" catalogan a ese derecho a la información o a la seguridad informática como bien jurídico intermedio digno de la tutela penal por su propio valor y por el peligro potencial que encierra su quebrantamiento para los demás bienes jurídicos.[45]

VIII. Bibliografía

A. Doctrina y publicaciones

Bailon Valdovinos, Rosalío, *Derecho procesal penal*, México, Limusa, 2002.

Cano Martínez, Jeimy José, "Estrategias antiforènses en informática: repensando la computación forense", 2008.

—, "Estado del arte del peritaje informático", 2005.

—, "Introducción a la informática forense. Una disciplina técnico-legal, en *Sistemas*, núm. 96, 2006.

[45] Cano Martínez, Jeimy José, "Introducción"..., ob, cit.

CARRIÓN, Hugo Daniel, "Auditoría informática frente a un caso de espionaje informático dentro de una empresa".

CoE, Convention on Cybercrime, 2001.

DOMÍNGUEZ PECO, Elena, "Nuevas tecnologías, proceso penal y protección de datos: el caso de la dirección IP", 2008.

FORZA, IEONG R., "Digital forensics investigation framework that incorporate legal issues", 2006.

GUERRERO, Alberto, *Alfa-Redi*, núm 110, 2007.

HERATH, A.; HERATH, S.; SAMARASINGHE, P.; HERATH, J., "Computer forensics, information security and law: a case study", en *Proceedings of Systematic Approaches to Digital Forensic Engineering*, 2005.

HERRERO TEJEDOR, Fernando, consultado en http://www.cybex.es/e-newsletter/pqojyrchnxcj4v/indice_nl0803.htm.

MYERS JAY, Larry, "High Technology Crime Investigation: A curricular needs assessment of the largest criminal justice and criminology programs in the United States", tesis doctoral, 2000.

PARRA QUIJANO, Jairo, *Manual de derecho probatorio,* 14ª edición, Bogotá, Ediciones del Profesional, 2004.

RAYMOND CHOO, Kim-Kwang; SMITH RUSSELL, G.; MCCUSKER, Rob, "Future Directions in Technology-Enabled Crime: 2007–2009", Australian, Institute of Criminology.

TAYLOR, C.; ENDICOTT-POPOVSKY, B.; PHILLIPS, A., "Forensics Education: Assessment and Measures of Excellence", en *Proceedings of Systematic Approaches to Digital Forensic Engineering*, SADFE, 2007.

YASINSAC, A.; ERBACHER, R.; MARKS, R.; POLLITT, M.; SOMMER, P., "Computer Forensics Education", en IEEE *Security and Privacy*, vol. 1, núm. 4, 2003.

B. Documentos del Gobierno

Comisión de Regulación de Telecomunicaciones, documento: "Recomendaciones al Gobierno Nacional para la implementación de una estrategia de ciberseguridad", 2007.

Interpol, información contenida en los computadores decomisados a las farc el 1° de marzo de 2008.

Ministerio de Comunicaciones, Plan Nacional de Tecnologías de la Información y las Comunicaciones (tic).

C. Códigos, proyectos de ley y manuales

Código Penal Colombiano, Legis, 2006.

Código de Procedimiento Penal Colombiano, Legis, 2006.

Manual Único de Policía Judicial, República de Colombia, Consejo Nacional de Policía Judicial, Bogotá, Imprenta Nacional de Colombia.

Proyecto de ley 49 de 2007, Senado.

Proyecto de ley 23 de 2007, Cámara.

Proyecto de ley 42 de 2007, Cámara.

D. Trabajo de campo

Entrevistas; algunas formales, y otras informales debido a que varios entrevistados por razones de trabajo no pudieron diligenciar el cuestionario; el detalle de estas últimas no está disponible en este documento.

Las formales se les hicieron a:

Ingeniera Mónica del Pilar Camargo Rodríguez, perita informática en la Unidad de Delitos Informáticos de la Fiscalía General de la Nación, cti.

Ingeniero Javier Ortiz Acosta, investigador de la Sección de Análisis Criminal, CTI, Fiscalía General de la Nación.

Mayor Freddy Bautista, director del Grupo de Delitos Informáticos de la DIJIN.

Teniente coronel Hugo Javier Agudelo, director nacional de la Escuela de Investigación Criminal de la Policía Nacional.

IX. Anexos

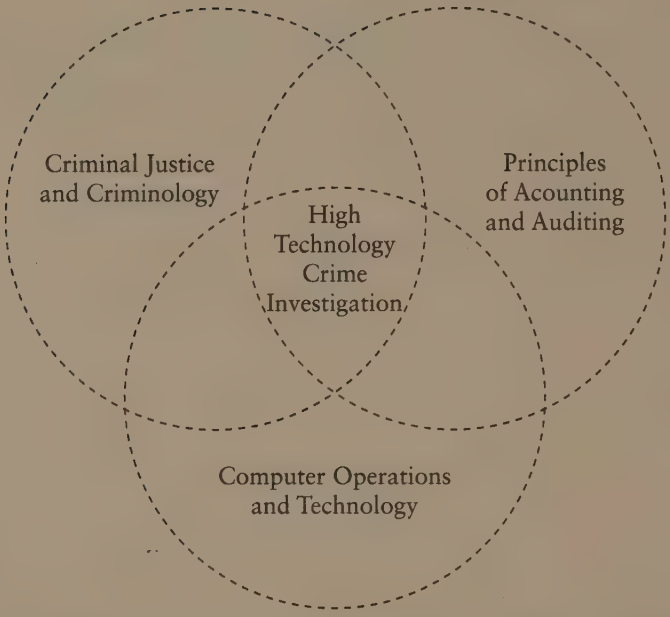

Figura 1. Modelo propuesto en la tesis doctoral de Larry Myers Jay sobre las habilidades y conocimientos que debe tener un perito informático[46]

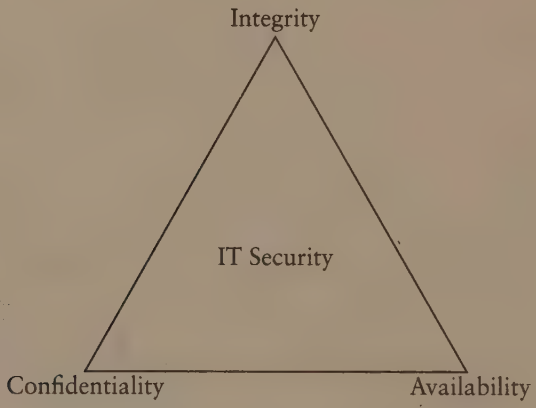

Figura 2[47]

[46] Myers Jay, Larry, ob. cit.

[47] Forza Ieong R., ob. cit., p. 2.

Tabla 1. **Programas informáticos**

Computing forensic training plan	
Education	Training
Introduction to forensic science Introduction to computer science Introduction to computer hardware Introduction to operating systems Introduction to criminal and civil law	A+training Net+training Basic computer seizure Basic data recovery and duplication
Information management Forensic science Information assurance Knowledge management Enterprise architecture	Survey or seminar courses in information assurance, legal issues, and CNF techniques
All of CNF technical items Upper-level BS/MS courses in information systems, network systems, architecture, and criminal, civil, and procedural law	All of CNF technician training plus advanced data recovery and moot court training
Doctorate-level education or a master degree with extensive experience in computer forensics	Specific research areas are difficult to project, but researchers should receive hands-on training in the research areas

Fuente: Yasinsac, A.; Erbacher, R.; Marks, R.; Pollitt, M.; Sommer, P.

Tabla 2. **Herramientas más utilizadas en procedimientos forenses**

	Licencia	Imágen	Control integridad	Análisis	Admón. Caso
ENCASE	Sí	Sí	Sí	Sí	Sí
FORENSIC TOOLKIT	Sí	Sí	Sí	Sí	Sí
WHINEX (Forensic edition)	Sí	Sí	Sí	Sí	Sí

ENCASE - http://www.encase.com/products/ef_index.asp.
FORENSIC TOOLKIT - http://www.accessdata.com/products/utk/.
WINHEX - http://www.x-ways.net/forensics/index-m.html.
Fuente: Cano Martínez, Jeimy José.

Para mayor información sobre otras herramientas forenses en informática se sugiere revisar el enlace: http://www.e-evidence.info/vendors.html.

Tabla 3.[48] **Components of excellence in DF education and Subjects covered in a forensics course**

1. Multi-disciplinary content 2. Hands-on exercises 3. Knowledgeable instructors 4. Real world case examples

Computer Forensic Tools and Techniques Investigative procedures Computer Laws Relating to Digital Forensics Ethics Relating to Computer Security

[48] Taylor, C.; Endicott-Popovsky, B.; Phillips, A., "Forensics...", ob. cit.

CAPÍTULO V

LA FORMACIÓN DE LOS JUECES EN TEMAS DE DELITO INFORMÁTICO Y LA EVIDENCIA DIGITAL EN EL CONTEXTO INTERNACIONAL Y SUS IMPLICACIONES EN LA ADMINISTRACIÓN DE JUSTICIA EN COLOMBIA

Martha Lucía Segrera y Jeimy J. Cano M.

Nadie puede diseñar un sistema
que alguien más no pueda comprometer o vulnerar
Russell Ackoff

I. Introducción

Los avances en la informática y las telecomunicaciones han logrado reducir significativamente las distancias y las barreras de comunicación entre las personas, razón por la cual somos más eficientes y a la vez más dependientes tanto de los sistemas como de la tecnología. Esta dependencia y vinculación es tal que, podríamos afirmar, el desarrollo de la vida personal, institucional y comercial actual está completamente fundamentado en los avances tecnológicos, en los computadores y las telecomunicaciones.

Lo anterior ha tenido efectos positivos, pues es indiscutible que nuestras industrias, economías, Gobiernos, y en general nuestras vidas, han

mejorado con los avances en las aplicaciones de la informática y de las tecnologías de telecomunicación. Sin embargo, como resultado del mal uso de los avances tecnológicos, informáticos y telemáticos se ha incrementado el número de incidentes peligrosos y de producción de consecuencias graves.

Aunque en Colombia este tipo de conductas ya se han venido manifestando hace algún tiempo, nuestro ordenamiento aún alberga vacíos normativos y disposiciones obsoletas. Estas circunstancias ponen de presente múltiples retos y desafíos, principalmente a la hora de enfrentar la criminalidad en medios informáticos. De ahí, la necesidad de potenciar las herramientas de prevención, control y sanción del derecho penal en los escenarios donde la tecnología actúe como medio o fin para configurar conductas ilícitas.

La revisión de esta realidad desde la óptica de la seguridad informática sugiere la necesidad de valorar la respuesta institucional frente a este tipo de criminalidad, a la par de procurar la regulación de las medidas que debe adoptar la legislación colombiana en el contexto formativo y educativo de la rama judicial en temas de delito informático y evidencia digital.

El vertiginoso incremento de las tasas de vulnerabilidades y formas de acceder a la información privilegiada contenida en sistemas informáticos advierte la necesidad de entrenar a los funcionarios de la rama judicial para enfrentar adecuadamente la investigación y el juzgamiento de los delitos en contra de las infraestructuras de computación y comunicaciones.

Considerando esa realidad, este capítulo pretende hacer un análisis extensivo del estado actual de la formación de jueces en delitos informáticos y evidencia digital en el contexto internacional, a fin de recoger experiencias que permitan desarrollar el tema en Colombia y así proponer líneas de acción a mediano y corto plazo encaminadas a fortalecer y modernizar la Administración de Justicia.

II. Planteamiento del problema jurídico

Los continuos avances en las tecnologías de información y telecomunicaciones, además de incrementar el número y nivel de los delitos relacionados con sistemas informáticos, han generado una preocupación en el sistema de Administración de Justicia. Esta preocupación se ha manifestado, en términos de informática forense, en tres grandes aspectos:

La omnipresencia de la ciberdelincuencia en todas las esferas y disciplinas de la realidad, ilustrada en la figura 1, plantea diversas cuestiones problemáticas, tales como: ¿Estamos frente a un fenómeno novedoso? ¿No es simplemente crimen? ¿Es necesario hacer algo más que judicializar a los ciberdelincuentes usando la normativa tradicional?

III. Indeterminación en la definición de los delitos informáticos

Figura 1. El cibercrimen emerge como una disciplina nueva (Edgard-Nevill & Stephens, 2008)

No obstante, el reconocimiento del desarrollo, conformación y superposición del delito informático en torno a una amplia gama de

disciplinas y la dificultad para determinar el grado real de los denominados delitos informáticos y la amenaza que éstos implican para la sociedad, generan grandes dificultades. Tales dificultades se centran en torno a dos cuestiones fundamentales: en primer lugar, que no existe una definición de delito informático universalmente aceptada; en segundo lugar, que el nivel de detección de dichos crímenes, al igual que los métodos establecidos para determinar los daños monetarios resultantes de éstos, son considerados inadecuados.[1]

La falta de un acuerdo en torno a la definición de delitos informáticos sólo puede entorpecer el juzgamiento de dichos crímenes, pues en muchos de los casos los jueces se han inclinado por entender los delitos informáticos como una forma novedosa de cometer fechorías tradicionales. En consecuencia, muchos de estos delitos son procesados como crímenes tradicionales.[2]

Si bien las conductas punibles existentes en los estatutos penales son en una buena parte de los casos lo suficientemente genéricas como para adecuar un crimen de tipo informático a una conducta tradicional, existen situaciones en las cuales no es procedente, pues hay conductas que son exclusivas de la delincuencia informática, como por ejemplo, el *electronic browsing*, dando espacio a la configuración de un margen de impunidad.[3]

Algunos investigadores, respondiendo a dichas críticas, han publicado estudios indicando el adecuado juzgamiento de los delitos informáticos junto con las cifras de las pérdidas monetarias resultantes de

[1] Myers, L. J., *High Technology Crime Investigation: A Curricular Needs Assessment of the Largest Criminal Justice and Criminology Programs in the United States*, Florida, Texas, A & M University, 2000, pp. 6-7.

[2] United States Sentencing Comission [acceso el 12 de junio de 2008]. Disponible en: http://www.ussc.gov/publicat/cmptfrd.pdf.

[3] Ídem.

cibercrímenes; sin embargo, éstas sólo pueden considerarse aproximaciones. Si no hay una definición universal de delito informático ¿cómo podríamos determinar las pérdidas económicas derivadas de este tipo de actividad criminal? Lo que algunos consideran delito informático, podría no encuadrar dentro de la definición de otros.[4]

IV. Incremento y perfeccionamiento de los delitos informáticos

El rápido avance de las aplicaciones informáticas facilita a los individuos la comisión de conductas delictivas con alto nivel de sofisticación. Las herramientas proporcionadas por la informática dan al crimen organizado posibilidades nuevas, ya que pueden explotar la conectividad global, la integración económica y el crecimiento mundial de los servicios financieros.

Adicionalmente, el aspecto transnacional del crimen se conjunta con desarrollos tecnológicos que hacen difícil la identificación de quienes cometen actos delictivos y, por ende, el acopio de evidencia. La evidencia digital es frágil, transitoria, y las técnicas predigitales de recolectarla son poco efectivas. La creciente sofisticación de los criminales cibernéticos es un reto para la policía. La habilidad de planear y ejecutar estrategias de largo plazo para cometer crímenes es realmente peligrosa.[5]

Con el tiempo ha venido acrecentándose la constatación del elevado número y nivel de delitos relacionados con sistemas de procesamiento y transferencia automática de datos, que ya no sólo afecta a los países del área occidental o altamente tecnificada (EE. UU., la Unión Europea, Australia, Japón), sino incluso a otros de ámbito socialista como la

[4] Myers, L. J., ob. cit., supra, nota 1.

[5] Daltabuit, E., *Alfa-Redi*, p. 9, consultado el 20 de junio de 2008. Disponible en: http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/daltabuit_2007.pdf.

Federación Rusa, los actuales países anteriormente integrados en la extinta URSS o de su antiguo ámbito de influencia, China y otros Estados en donde se ha producido desde la década de los años noventa una apertura a los nuevos avances tecnológicos. Dicha situación ya no implica un riesgo sólo para las empresas privadas, la economía y la sociedad de un país, sino también para la sociedad mundial.[6]

V. INEXISTENCIA DE JUECES FORMADOS Y ESPECIALIZADOS EN TEMAS DE DELITO INFORMÁTICO Y EVIDENCIA DIGITAL

El vertiginoso crecimiento de los índices de criminalidad informática anualmente pone de presente la escasez de justicia criminal y personal corporativo con suficientes conocimientos, habilidades y aptitudes para detectar, investigar y juzgar los delitos informáticos.[7]

La presencia del crimen organizado en los medios informáticos y tecnológicos obliga a los legisladores y a los abogados a estar enterados del funcionamiento de la tecnología que usan estos delincuentes; también, a los desarrolladores de tecnología, a estar al día con la normatividad, la legislación y las recomendaciones que tienen que ver con su buen uso. La colaboración entre especialistas de disciplinas tan distantes requiere de una comprensión mutua.[8]

De lo contrario, la complejidad y la dinámica de la delincuencia informática en manos de un personal carente de las herramientas adecuadas impedirían la adecuada judicialización, creando para la víctima una situación de indefensión difícil de resolver por cuanto las acciones

[6] Rovira del Canto, E., *Delincuencia informática y fraudes informáticos*, Granada, Comares, 2002, pp. 9-10.

[7] Myers, L. J., *High Technology Crime Investigation*..., p. 7.

[8] Daltabuit, E., *Alfa-Redi*, p. 16.

directas, esto es, la investigación y el juzgamiento, poco aportarían.[9] Por eso resulta pertinente la formación de jueces en temas de delito informático y evidencia digital.

Teniendo en cuenta lo anterior, esta parte de la investigación pretende a través de un estudio comparado dar respuesta al siguiente interrogante: ¿qué conocimientos, habilidades y aptitudes requiere un juez para lograr la efectiva persecución y judicialización de los crímenes de alta tecnología?

VI. Necesidad de una justicia especializada en delito informático y evidencia digital

El uso de sistemas informáticos para la comisión de crímenes se ha venido incrementando en los últimos años a raíz de la dependencia y vinculación generada a las tecnologías de información y telecomunicaciones por parte de los individuos y los empresarios. Tal incremento pone de presente la ausencia de conocimiento y adecuada preparación de los jueces para lograr la correcta judicialización de los crímenes de alta tecnología. Es por esto que, ya tradicionalmente, el sistema de Administración de Justicia se ha visto amenazado por los desafíos generados e impuestos por los nuevos sistemas.

Cuando en el curso de una investigación criminal básica el juez encuentra por casualidad equipos informáticos —hardware y software— conteniendo evidencia digital importante, la pregunta que normalmente surge es: ¿qué debe hacer el juez? Este interrogante no puede ser resuelto con una respuesta simplista, como "ciérrelos y olvídelo". Por el contrario, los jueces necesitan conocer las opciones existentes

[9] Campoli, G. A., *Alfa-Redi*, 2005. Disponible en: http://www.alfa-redi.org/rdi-articulo.shtml?x=974.

para estar en capacidad de perseguir y judicializar radicalmente los delitos informáticos.[10]

A pesar de la posición asumida por el ordenamiento jurídico colombiano frente al valor probatorio y la admisibilidad de las nuevas tecnologías y sus productos en los procesos judiciales, la presentación de evidencia digital ante los jueces implica grandes dificultades. No es suficiente descifrar el lenguaje técnico a los términos de un abogado, como se traduciría una lengua extranjera al español, pues las complejidades técnicas de este tipo de casos frecuentemente sobrepasa los conocimientos y la experiencia de los funcionarios judiciales. Incluso algunos elementos de la evidencia digital pueden parecer intangibles para los funcionarios digitales dada su naturaleza "virtual" o sus confusas similitudes con otros elementos de evidencia. Esto podría ilustrarse en la realidad a través de un caso en el que tuviese que explicarse a un juez las diferencias entre la fecha del último acceso y la de la última modificación de un archivo en el sistema de archivos NT File System (NTFS) en un sistema informático.[11]

A diferencia de un documento escrito, las pruebas contenidas en un ordenador deben ser allegadas a un proceso judicial junto a una interpretación exacta, que claramente identifique su importancia en el contexto donde fueron encontradas. Por ejemplo, el disco duro de una computadora comprende datos binarios e ignora tipos de datos más complejos, que pueden estar codificados como simples códigos binarios, códigos binarios decimales, o datos hexadecimales. Es por esto que la interpretación de la evidencia digital debe estar en manos de personal

[10] McLean, S. J., "British & Irish Law, Education and Technology Association", 1999, p. 1, consultado el 16 de julio de 2008. Disponible en: http://www.bileta.ac. uk/Document%20Library/1/Basic%20Considerations%20in%20Investigating%20Computer%20Crime,%20Executing%20Computer%20Search%20Warrants%20and%20Seizing%20Equipment.pdf.

[11] Kennedy, I., "Investigating Digital Crime", en R. Bryant, *Investigating Digital Crime*, England, Wiley, 2008, p. 52.

calificado, con fines de poder ser presentada en forma accesible para su posterior examen por un Tribunal. No obstante, la simplificación excesiva puede resultar peligrosa, en la medida en que puede implicar una interpretación muy abierta de la evidencia.[12]

En la práctica es importante que las investigaciones referentes a la informática forense tengan en cuenta diversos aspectos, tales como la educación de los funcionarios judiciales en cuanto a disciplinas científicas y la aplicabilidad de las normativas pertinentes a la materia, con el fin de lograr que éstas sean exitosas.

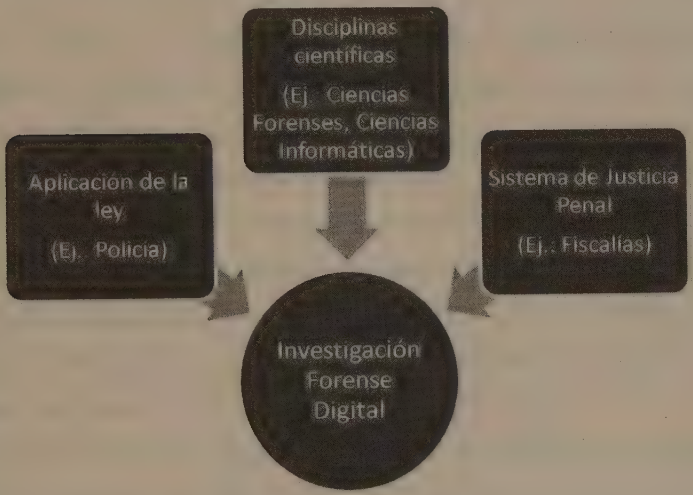

Figura 2. Factores de incidencia en una investigación forense digital (Kennedy, 2008)

Los factores de incidencia en una investigación de informática forense son ilustrados de manera general en la figura 2. Para que una investigación pueda coadyuvar a un correcto juzgamiento de las conductas delincuenciales a través de sistemas tecnológicos, informáticos o telemáticos, es menester que el sistema de justicia penal esté orientado hacia

[12] Ibídem, p. 53.

una aplicación de la ley basada en estudios previos, principalmente en tres áreas de conocimiento: informática básica, evidencia digital y delitos informáticos.

El conocimiento de temas de delito informático y evidencia digital es de suma importancia para un juez que se vea enfrentado a un caso donde se involucre la utilización de sistemas informáticos y tecnológicos. La labor es crítica, ya que él debe procurar al máximo recolectar la evidencia digital disponible en el equipo y además preservarla, objetivo completamente posible si el funcionario judicial cuenta con entrenamiento especializado y buenas herramientas de trabajo.

Es importante para el sistema de Administración de Justicia la comprensión de las especiales circunstancias en las que se encuentran inmersos los crímenes perpetrados a través de medios informáticos, pues las barreras investigativas en muchos de los casos resultan difíciles de romper por cuanto la información contenida en los ordenadores puede encontrarse alterada, protegida, parcialmente borrada, comprimida u oculta.[13] El problema cobra aún mayor importancia si se considera que históricamente la delincuencia informática no ha sido una de las prioridades del sistema judicial colombiano; aun cuando la revolución informática continúa evolucionando y cambiando la forma como se desarrollan las actividades criminales, muy poca atención se le ha dado al fomento de conocimiento y desarrollo de habilidades en tecnologías de información y telecomunicaciones entre los funcionarios judiciales.

Si el sistema judicial colombiano pretende ser suficientemente competente en la lucha contra el crimen es menester invertir tiempo y recursos en el entrenamiento de jueces especializados en temas de delito informático y evidencia digital, de lo contrario habrá perdido irremediablemente sus esfuerzos por hacer cumplir la legislación penal. Así mismo, no sólo

[13] McLean, S. J., "British & Irish Law, Education and Technology Association", 1999, p. 4.

es perentorio sino inexorable promover la inclusión de estos temas en las Facultades de Derecho Procesal y Penal.

VII. Administración de Justicia en temas de delito informático

Los ordenadores y la delincuencia informática inevitablemente acarrean consigo un carácter transnacional, el cual puede dar lugar a complejas cuestiones jurisdiccionales que involucran personas, cosas y actos presentes en todos los países. Esto puede ser tan cierto para los actos de criminalidad individuales como para las organizaciones delictivas multinacionales. Aun cuando el delincuente y la víctima se encuentren ubicados bajo una misma jurisdicción, la evidencia relevante puede encontrarse en otra, como por ejemplo, en una cuenta de *hotmail* (correo electrónico). Como la mayor parte de los aspectos de las actividades basadas en la Internet, los conceptos legales y los principios tradicionales se ven muchas veces desafiados por la naturaleza del entorno. Consecuentemente, los legisladores y poderes judiciales han tenido dificultades para encaminar las cuestiones alusivas a la criminalidad informática en varios campos.[14]

La aceptación de esta realidad ha llevado a los legisladores y a los funcionarios judiciales a luchar por el establecimiento y la funcionalidad de un marco legal que refleje el ciberespacio como un medio internacional de información. Es por esto que algunos mecanismos tradicionales de control han sido erradicados, y los nuevos o resultan confusos o simplemente están en proceso.[15]

[14] Walden, I., *Computer Crimes and Digital Investigations*, Nueva York, Oxford, 2007, p. 297.

[15] Ibídem, p. 298.

A. Delito informático en Estados Unidos

Durante los últimos años se ha puesto de manifiesto un incremento en el promedio de estimación de las pérdidas tanto físicas como financieras a causa de la ciberdelincuencia. Un estudio reciente elaborado en Estados Unidos por el Computer Crime Institute ha tasado una pérdida de 350.424 millones de dólares en el año 2007, esto es, 182.424 millones de dólares más que en el anterior.[16]

Considerando la importancia y la peligrosidad de este panorama, Estados Unidos ha logrado configurar una de las legislaciones, en lo que a delitos informáticos se refiere, más amplias y eficientes que existen. Durante los últimos años las instituciones de la vida social, política, educativa y corporativa se han encargado de producir iniciativas encaminadas a la efectiva judicialización y persecución de los crímenes de alta tecnología. Este enfoque ha constituido la columna vertebral de las disposiciones y publicaciones que pretenden unificar y otorgar coherencia al juzgamiento de los delitos informáticos.

El primer documento federal orientado a detener la criminalidad informática fue creado por el Congreso de Estados Unidos en 1984 y es conocido con el nombre de Computer Fraud and Abuse Act (CFAA). Esta regulación tuvo por objetivo la protección de la confidencialidad, integridad y disponibilidad de los datos y las comunicaciones. En ese sentido, la CFAA reconoció expresamente cómo delitos las siguientes conductas: 1) cometer espionaje, accediendo a la información sin autorización o excediendo el acceso autorizado, 2) acceder a información sin autorización o excediendo el acceso autorizado, 3) acceder a cualquier ordenador privado del Gobierno, 3) acceder a cualquier ordenador con la intención de cometer fraude, 4) intencionalmente, dañar

[16] Computer Security Institute, *Computer Crime and Security Survey*, CSI Publications, 2007.

un computador, 5) tráfico fraudulento de contraseñas, y 6) amenazar a una computadora protegida con la intención de hacer una extorsión y obtener dinero a cambio.

El punto relevante en la valoración de la conducta, por parte del juez, se encuentra entonces en la determinación de si la persona ingresó o no a una computadora sin autorización. Un caso de la Corte estadounidense de 1991 ilustra este punto: Morris, un estudiante de ciencias de la computación, creó un programa de computador para demostrar las vulnerabilidades de la seguridad en Internet. Entonces, liberó un gusano, diseñado con la característica de poder duplicarse utilizando las partes automáticas de un sistema operativo, generalmente invisibles para el usuario. Sin embargo, éste se reprodujo más rápido de lo esperado, ocasionando graves daños en cerca de 6200 computadores de universidades, unidades militares y hospitales. En opinión del juez Newman, el acusado infringió la ley al ingresar a sistemas de interés común sin la debida autorización. Morris, por su parte, adujo que su conducta a lo sumo alcanzaría el grado de acceso a la información excediendo la autorización otorgada, pues él contaba con la autorización de las universidades de Cornell, Harvard y California, en Berkeley, para comunicarse con otros computadores enviando correos electrónicos e investigar información de otros usuarios. No obstante, el juez indicó que el virus fue diseñado con el fin de extenderse a otros sistemas, para lo cual no tenía autorización, y por lo tanto Morris fue condenado.[17]

Inicialmente la CFAA fue eficiente para el juzgamiento de conductas delictivas cometidas a través de medios informáticos. Sin embargo, con el surgimiento de nuevos avances en las tecnologías de información y telecomunicaciones, éstas adquirieron un elevado nivel de sofisticación y fue necesario el desarrollo de reformas y nuevas legislaciones.

[17] *United States vs. Morris, 928 F.2d 504 (2nd. Cir.)*, Supreme Court, 1991.

En ese sentido, la CFAA fue reformada en 1994 con fines de darle solución a la nueva problemática, a saber, el "código malicioso", como por ejemplo, virus, gusanos o cualquier otro programa diseñado para alterar, dañar o destruir la información contenida en un ordenador. Como quedó establecido en el caso Morris, la CFAA únicamente sancionaba a quien ingresaba sin autorización en un sistema, no pudiendo perseguir y sancionar adecuadamente a quienes transmitían programas, datos o comandos con intenciones de dañar bien sea la computadora o la información contenida en ella.[18]

Como resultado de las incertidumbres y vacíos legales, un número significativo de nuevas regulaciones se produjo durante la década de los noventa. En octubre de 1994 surgió el Communications Assistance for Law Enforcement Act (CALEA), que exigía a proveedores del servicio de Internet construir capacitores en sus redes que le permitiesen llevar a cabo vigilancia electrónica a determinados individuos. Cabe anotar que el CALEA no elimina la necesidad de una orden judicial antes de llevarse a cabo la vigilancia, simplemente otorga los permisos en caso de que fuera necesario, para dar impulso a un proceso judicial.[19]

En 1996 fue aprobado el Economic Espionage Act (EEA), que condena el robo o apropiación indebida de secretos profesionales a través de computadoras u otros medios. La definición de secreto profesional dada por este acto es bastante amplia, con el fin de incluir cualquier información que sea razonablemente protegida de la divulgación pública, pues ésta es una de las muestras más claras de cómo los delitos informáticos pueden derivar en una reducción de la competitividad, se obtenga provecho o no. En un caso reciente, el FBI arrestó a unos desarrolladores de

[18] May, M., SANS Institute, 2004, p. 2, consultado 3 de agosto de 2008. Disponible en: http://www.sans.org/reading_room/whitepapers/legal/1446.php.

[19] Ídem.

software de Lucent Technologies por robar una tecnología denominada *PathStar* para venderla en China a Datang Telecom.[20]

En 1998 nace otra regulación, bajo el nombre de Digital Millenium Copyright Act (DMCA), cuyo propósito fundamental obedecía a la implementación de leyes encaminadas a la protección de la propiedad intelectual de acuerdo con las nuevas tecnologías, según las recomendaciones impartidas por la Organización Mundial para la Propiedad Intelectual, reformando definitivamente el título 17 del Código estadounidense. En fecha reciente un estudiante del Instituto Tecnológico de Massachusetts encontró la forma de eludir el sistema de seguridad del *Xbox* de Microsoft y publicó su reporte en una página *web* de acceso público. Sin embargo, no pudo ser procesado por violar el DMCA. Bajo las disposiciones del DMCA no es un crimen descifrar los dispositivos contra la piratería con el propósito de realizar investigaciones u otros trabajos académicos.[21]

Con posterioridad a los acontecimientos ocurridos el 11 de septiembre de 2001, muchas cosas parecen haber cambiado. Con el consenso unánime del Senado de los Estados Unidos, el presidente Bush firmó el Patriot Act (*Provide Appropriate Tools Required to Intercept and Obstruct Terrorism*), el cual marca un hito en la lucha contra la criminalidad globalizada.[22]

La Ley Patriótica, como también es denominada, amplía el poder del Estado a fin de garantizar la seguridad nacional y la lucha contra el terrorismo. Entre sus disposiciones, ésta da plenas facultades a las instituciones estatales para interceptar llamadas telefónicas, correos electrónicos, historias clínicas, financieras y de otros tipos; disminuye las

[20] Ferrera, G. et ál., *Cyberlaw: Text and Cases*, Maryland, Thompson, 2004, pp. 430-431.

[21] Ibídem, pp. 429-430.

[22] Guerrero, M. F., *La ciberdelincuencia*, Bogotá, Procuraduría General de la Nación, 2004, p. 23.

restricciones en cuanto a la recolección de datos de inteligencia sobre los extranjeros dentro de Estados Unidos y aumenta la discrecionalidad de las autoridades de inmigración en lo que a la detención y deportación de inmigrantes sospechosos de terrorismo respecta.

Los desarrollos más extensos de la Ley Patriótica han encontrado sustento en una relación triangular llamada "lo estratégico preventivo", que se explica partiendo del supuesto según el cual si la tecnología puede ser utilizada como instrumento por la delincuencia, también constituye el recurso idóneo, del cual se deben servir las autoridades, para contrarrestar la actividad delictiva.[23] En la práctica, "lo estratégico preventivo" en la Ley Patriótica se traduce en la aplicación de sistemas computarizados —software— que se utilizan para prevenir y conjurar los efectos adversos del ciberterrorismo.[24] Dichos sistemas son básicamente dos: Echelon y Enfopol.

Echelon y Enfopol son sistemas de redes de espionaje y análisis globales cuya funcionalidad básica es la de interceptar comunicaciones electrónicas; pueden capturar comunicaciones por radio y satélite, llamadas de teléfono, faxes y correos electrónicos en casi todo el mundo, generando análisis automáticos y clasificación de las interceptaciones, las cuales son de tan grandes proporciones que el número de comunicaciones llegadas al sistema se calcula en tres millones por día.

La presencia de estos sistemas ha generado fuertes reacciones, mostrando una situación preocupante por las eventuales violaciones de principios y valores fundamentales, entre los cuales se encuentra principalmente el de la protección de datos personales.

Es de resaltar de toda la legislación penal estadounidense en su conjunto la flexibilidad con la que se interpretaban, y se siguen interpretando,

[23] Ibídem, p. 64.

[24] Ibídem, p. 65.

las figuras delictivas clásicas, lo cual suponía que no siendo indispensable la realización de reformas, ni la existencia de una demanda social urgente para ello, o un requerimiento de los Tribunales en este ámbito, dichas reformas se han venido promoviendo fundamentalmente por razones preventivas generales.[25]

B. Delito informático en Europa

La ciberdelincuencia ha adquirido, con el paso del tiempo, dimensiones tan problemáticas que han requerido la atención de los Gobiernos, legisladores y autoridades judiciales de los países europeos. En ese sentido las jurisdicciones europeas, independientemente de sus grados de desarrollo, se han visto forzadas a evaluar la adecuación de sus sistemas jurídicos a los nuevos avances de las tecnologías de información y telecomunicaciones con el propósito de hacer frente a la expansión de la delincuencia en el ciberespacio.

La forma como los Estados han establecido disposiciones sobre el delito informático en sus códigos penales evidencia esfuerzos para establecer doctrinas legales respecto de la naturaleza y fenomenología de este tipo delictivo. A ese respecto, y dadas las peculiaridades de cada legislación interna, es preferible, para su exposición, analizarlas separadamente.

1. España

Probablemente este país es el que más experiencia ha obtenido en casos de delitos informáticos en Europa. Es por eso que desde el año 1995 la legislación española ha contado con normas específicas para

[25] Rovira del Canto, E., *Delincuencia informática...*, ob. cit., p. 349.

la tipificación de este tipo de conductas dentro de su Código Penal. No obstante, no debe pensarse que toda la normativa referente a la ciberdelincuencia se encuentra circunscrita a él. Existe también en su derecho un cuerpo legislativo adicional que regula estos aspectos de la sociedad de la información.

Los tipos delictivos en donde los datos o sistemas informáticos son instrumentos de comisión o el objeto del delito, establecidos en el Código Penal español de 1995, son los siguientes:

1) Delitos relacionados con el contenido

   a) *Artículo 186*. La distribución por cualquier medio de material pornográfico entre menores de edad o discapacitados.
   b) *Artículo 189*. La distribución de pornografía infantil a través de Internet.

2) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

   a) *Artículo 197*. Las conductas encaminadas al apoderamiento de mensajes de correo electrónico o acceso a documentos privados sin la autorización de sus titulares.
   b) *Artículo 264.2*. La destrucción, alteración, inutilización o daño de datos, programas o documentos electrónicos ajenos, contenidos en redes, soportes o sistemas informáticos.
   c) *Artículo 278.1*. El apoderamiento por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos a fin de descubrir secretos empresariales.

3) Delitos informáticos

a) *Artículo 248.2.* Estafa valiéndose de alguna manipulación informática o artificio semejante, consiguiendo la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.
a) *Artículo 256.* Utilización no consentida de un ordenador sin la autorización de su dueño, causándole un perjuicio económico superior a 300,50 euros.

4) Delitos contra la propiedad intelectual y derechos afines

a) *Artículo 279.1.* La copia no autorizada de programas de ordenador o de música.
b) *Artículo 270.3.* La fabricación, distribución o tenencia de programas que vulneren las medidas de protección contra la piratería de los programas.
c) *Artículo 273.* Comercio a través de Internet de productos patentados sin la debida autorización del titular de la patente.

Así mismo, es importante para la regulación de la sociedad de la información en España el desarrollo de otras leyes distintas de las disposiciones acuñadas en el Código Penal, dado que se requiere conocer y cumplir los requisitos de ellas para poder adoptar comportamientos eficaces en caso de delitos. Dentro de las más significativas, encontramos las siguientes:

- Ley Orgánica 15 de 1999 – Protección de Datos de Carácter Personal (LOPD). Tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas,

y especialmente de su honor, intimidad y privacidad personal y familiar. El órgano de control del cumplimiento de la normativa de protección de datos dentro del territorio español, con carácter general, es la Agencia Española de Protección de Datos (AEPD).

En un caso reciente, la AEPD sancionó con una multa de 150 mil euros a una clínica ginecológica de Bilbao por considerar que no "custodió con el debido sigilo" los datos de 11.300 pacientes y éstos acabaron circulando por Internet. El problema se debió a que uno de los empleados de la clínica utilizaba un programa de intercambio de archivos (P2P), lo cual permitió que cuantos incluían información ginecológica circulasen por la red.[26]

- Real Decreto Legislativo 1 de 1996, por medio del cual se aprueba el texto de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre este tema. En ese sentido, constituye la principal referencia relativa a la regulación de la propiedad intelectual en España.

Es importante destacar de la legislación penal española la minuciosidad con que son sancionadas conductas tales como la obtención o violación de secretos, el espionaje, la divulgación de datos privados, las estafas electrónicas, entre otras, aplicando penas de prisión y multas.

2. Alemania

En Alemania la legislación penal en materia de delitos informáticos surgió como consecuencia de la insuficiencia y deficiencias de las normas tradicionales y de tipo clásico previstas en ellas. Por tal razón, el 15 de

[26] Agencia Española de Protección de Datos, "Delitos informáticos", consultado el 18 de junio de 2008. Disponible en: http://www.delitosinformaticos.com/04/2008/proteccion-de-datos/sancion-a-una-clinica-de-bilbao-por-la-perdida-de-datos-de-11300-pacientes-en-redes-p2p.

mayo de 1986, luego de intensos debates, se adoptó la segunda ley de lucha contra la criminalidad económica.

Esta ley introdujo modificaciones en el Código Penal alemán, mas es de notar que no sólo se limitaron a la modificación de disposiciones ya existentes, sino a la creación de nuevos tipos y figuras penales.

Entre las nuevas figuras reguladas por esta ley se encuentran:

- *Espionaje de datos (párrafo 202.a)*. La punibilidad de este tipo se extiende a datos que están especialmente protegidos contra el acceso no autorizado, tales como contraseñas, contenedores cerrados o encriptados.
- *Estafa informática (párrafo 263.a)*. Se prescinde de los conceptos restrictivos de los elementos clásicos de la estafa que dificultan la aplicación de la ley a las defraudaciones cometidas a través de computadores. Es por esto que el perjuicio patrimonial que se comete en la estafa informática consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la apropiación no autorizada de datos o a través de una intervención ilícita.
- *Falsificación de datos probatorios (párrafo 269)*. El tipo penal limita la acción a la modificación de datos ya almacenados o al almacenamiento de datos nuevos con fines de engañar al tráfico jurídico.
- *Alteración de datos (párrafo 303.a)*. La disposición menciona cuatro acciones típicas: el borrado, la eliminación, la inutilización y la alteración de datos, protegiendo los no inmediatamente perceptibles en el sentido del párrafo 202.a.
- *Sabotaje informático (párrafo 303.b)*. La creación de este tipo diferenciado de alteración de datos obedece a la intención del le-

gislador de sancionar con mayor severidad las acciones que atentan contra información que sea de esencial importancia para una industria o empresa.

Inicialmente el legislador alemán introdujo un número significativo de nuevos preceptos penales. Con la aparición de nuevas formas de agresión durante los últimos años la protección del derecho penal vigente no puede garantizar adecuadamente la protección de todos los bienes jurídicos, haciendo necesario el desarrollo de herramientas más eficaces.

3. Francia

Desde 1978 existía en Francia una ley con disposiciones penales (artículos 41 a 44) configurando ciertos tipos de naturaleza informática que se complementaban con normas administrativas de protección de datos, amparando los datos personales en el ciclo operativo de los sistemas informáticos. Las contravenciones administrativas quedaban fuera y las penas privativas de libertad podían ser de hasta cinco años.[27]

Más adelante el legislador francés inició el tratamiento específico de la criminalidad informática con la ley 85-660 del 3 de julio de 1985, integrada en la Ley de Propiedad Intelectual, relativa a la piratería del software.[28]

Con la ley 88-19, de modificación del Código Penal, de enero 5 de 1988, relativa al fraude informático, también conocida como *loi Godfrain*, se complementa el sistema de represión penal contra la criminalidad informática. El legislador recogió en un nuevo capítu-

[27] Rovira del Canto, E., *Delincuencia informática...*, ob. cit., p. 387.

[28] Ídem.

lo del Código Penal, bajo la rúbrica "Sobre ciertas infracciones en materia informática" (especialmente los delitos vinculados a la piratería, intrusión, traba al funcionamiento —esto es, virus— y ciertas asociaciones que pueden ser de *hackers*), toda la nueva realidad criminal compleja vinculada a las nuevas tecnologías de información, pero siempre y cuando no tuvieran una adecuada inclusión bajo figuras clásicas existentes. En este sentido, la utilización frecuente del término *informaticé* sobre el *informatique*, ha hecho pensar a la doctrina que el legislador se ha preocupado por proteger la información en su conjunto y no sólo aquella en soporte informático, es decir, que su afán se ha centrado en las conductas fraudulentas de acceso y uso ilícito de los sistemas de tratamiento automatizado de datos, absteniéndose de regular las manipulaciones informáticas con ánimo de lucro y en perjuicio patrimonial de tercero, núcleo principal del fraude informático.[29]

Es así como el título genérico de la ley hace referencia al fraude informático, en el que enunciado, en su texto no aparece ninguna referencia específica a él. Es más, la ley sanciona concretamente la falsedad informática sólo cuando el dato alterado se encuentre sobre un soporte informático.[30] Dicho esto, queda claro que las defraudaciones patrimoniales por medios informáticos permanecen sin una regulación particular dado que de conformidad con la jurisprudencia de la Corte y de los Tribunales de Casación franceses, éstas venían siempre subsumidas sin problemas en la figura clásica de estafa del artículo 405 del Código Penal, sancionándose al que haciendo uso de falsas cualidades, bien empresas de un poder o crédito imaginario, o para hacer nacer la esperanza o la creencia de un suceso, de

[29] Biblioteca del Congreso Nacional de Chile, Centro de Estudios de Justicia de las Américas, 2004, consultado el 13 de agosto de 2008. Disponible en: http://www.cejamericas.org/doc/documentos/cl-bcn-delitos-informaticos.pdf.

[30] Ídem.

un accidente o de cualquier otro acontecimiento imaginario, se haya hecho reintegrar o traspasar fondos, muebles, obligaciones, disposiciones, billetes, promesas, deducciones o desgravaciones, y hubiera por uno de estos medios defraudado o intentado defraudar la totalidad o parte de la fortuna de otro.[31]

La Ley de Reforma Penal del 22 de julio de 1992, vigente a partir de marzo de 1994, introdujo algunas mejorías en el texto legal de las disposiciones informáticas, que incluso trasladaron a otra parte del código, esto es, al libro III, título II, capítulo III, "De los atentados contra los sistemas de tratamiento automatizado de datos", tales como la falsificación informática, antes regulada en los artículos 462-5 y 462-6, que se refiere a la adulteración y el uso de documentos electrónicos falsos, actualmente en el nuevo artículo 411-1; el acceso fraudulento en sistemas informáticos, en el actual 323-1; o los daños a datos informáticos, ahora recogidos en el 323-3.

4. Gran Bretaña

El más importante cambio en la legislación penal sustantiva del Reino Unido, en materia de delincuencia informática, tuvo lugar con la entrada en vigor del *Computer Misuse Act,* del 29 de agosto de 1990. La aparición de dicha normativa surgió con ocasión de una importante decisión de la Cámara de los Lores en 1988, cuando se pronunció sobre el famoso caso *R versus Gold & Schifreen,* que marcó un hito por cuanto puso de manifiesto la necesidad de una legislación referente al *hacking.*

El contenido de dicha ley hace referencia exclusivamente a tres ilícitos mayores, estructurados en las tres primeras secciones, en base a la conducta del acceso no autorizado a una computadora.

[31] Rovira del Canto, E., *Delincuencia informática* ..., ob. cit., p. 392.

En la primera sección se sanciona el acceso no autorizado e intencionado, no imprudente, a un sistema informático o a su contenido con realización de operaciones o manipulaciones informáticas; pero no un simple contacto físico con un ordenador y la simple revisión o lectura de datos sin interacción alguna con el ordenador, sino que es necesario el activarse un dispositivo de seguridad o el ofrecimiento de un registro del menú informático.[32]

En la segunda sección se recoge como una forma calificada del anterior tal acceso no autorizado hecho con la intención de cometer cualquier otro delito, entre los cuales podría estar la estafa y por tanto, aparecer como supuesto agravado la finalidad o intención defraudatoria patrimonial.[33]

En la tercera sección se recoge la misma figura pero referida además a la causación de daños a los datos o a un sistema informático, o impedir o cambiar su función.[34]

Este sistema de legislación penal adoptado en el ámbito anglosajón es atractivo para el legislador por varias razones. Por un lado, porque pueden incluirse nuevas conductas ilícitas y sostenerse su punición por la norma sobre bases analógicas, argumentando para ello que al ser las acciones ilícitas de *hacking* similares a las figuras ya existentes, las nuevas modalidades de hacking pueden ser vistas como una ampliación necesaria de un concepto establecido al entorno moderno, donde entrar en un ordenador puede realizarse electrónicamente. Por otro lado, porque sobre la base inicial de acceso no autorizado, no hay necesidad de definir con precisión la conducta final perseguida por la persona que realiza el acceso.[35]

[32] Ibídem, pp. 370-371.

[33] Ibídem, p. 371.

[34] Ibídem, p. 372.

[35] Wasik, M., *Crime and the Computer*, Oxford, Clarendon Press, 1991, p. 693.

C. Delito informático en Asia

En la región Asia-Pacífica la incidencia de los ataques maliciosos en contra de la confidencialidad, integridad y disponibilidad de la información y sistemas; los crímenes vinculados a ordenadores, tales como falsificación o fraude; y aquellos en cuanto a los contenidos, como el caso de la pornografía infantil y los derechos de propiedad intelectual, es significativa. Amenazas a la infraestructura y a los intereses nacionales derivados del uso de la Internet para perpetrar actividades delictivas son una temática de creciente preocupación. Los daños ocasionados en las empresas, los Gobiernos y los individuos en los países de la región están adquiriendo cada vez mayor importancia, pues la ciberdelincuencia ha puesto en peligro la aplicación de las tecnologías de información y telecomunicaciones a los servicios públicos, el comercio y la banca. A medida que los usuarios pierden la confianza en las transacciones y los negocios, los costos de oportunidad se incrementan.

Los desafíos a la región residen básicamente en la falta de conciencia generalizada sobre la rápida evolución de la complejidad, capacidad y alcance de las tecnologías de información; el anonimato que ofrecen dichas tecnologías; la naturaleza transaccional de las redes de comunicación; y en general, la seguridad informática. Muy pocos países de la región Asia-Pacífico han adecuado los marcos normativos y jurídicos para hacer frente a esta realidad. Aun cuando la conciencia de estos temas se ha ido incrementando paulatinamente en los últimos años, la eficacia de las legislaciones y las tecnologías para detectar y responder a los delitos informáticos es muy baja.

1. China

La Comisión de Supervisión de la Seguridad de la Información, del Ministerio de Seguridad Pública de la República Popular China, estima

que en 2002 había aproximadamente 48,8 millones de usuarios de Internet, alrededor de 30 millones de computadores y 150.000 *websites* en esta nación. Menos de 5000 delitos informáticos fueron reportados en el año 2001, aproximadamente 2900 en el 2000 y cerca de 400 en 1999. A mediados de 2002 la Comisión había reportado algo más de 3000 casos. Así mismo, estimó que para fines del año 2005 manejó alrededor de 350 casos de intrusión en sistemas y por encima de 800 sobre daños en ordenadores. Según lo evaluado por ella, las tasas de delincuencia informática han alcanzado cifras abrumadoras, aun cuando muchos de los eventos no fueron reportados. Gran parte de los infractores eran jóvenes (18-30 años), que ocultaban su identidad mediante la conexión a través de *http* o *sock proxy*, direcciones de IP falsas y empleo de criptografía o esteganografía.[36]

Actualmente la Comisión carece de leyes específicas, de definiciones explícitas de evidencia digital y de procedimientos apropiados para la recuperación de pruebas. Aunque las legislaciones presentes relativas a la delincuencia informática son complejas, no poseen detalles para permitir su aplicación exitosa.

Antes de 1997 no existía ninguna ley en contra de la delincuencia informática. Todos los delitos vinculados a computadores eran procesados en virtud de lo dispuesto en la legislación penal tradicional de la República Popular China (RPC). A partir del 1° de octubre de 1997 la legislación penal de la RPC fue sustancialmente modificada con fines de sancionar conductas delictivas en la red, pero aún no se creaba un capítulo o sección independiente para los crímenes de alta tecnología. Sin embargo, hay tres disposiciones sancionatorias de cibercrímenes en el capítulo VI de la legislación penal de la RPC:

[36] Broadhurst, R. & Grabosky, P., "Computer-Related Crime in Asia: Emergent Issues", en R. Broadhurst & P. Grabosky, *Cyber-crime: The Challenge in Asia*, Hong Kong, Hong Kong University Press, 2005, p. 8.

- *Artículo 285*. Invasión de los sistemas de información de computadores en los ámbitos de asuntos estatales o de la construcción avanzada de aparatos tecnológicos relativos a la seguridad nacional.
- *Artículo 286*. La cancelación, modificación, aumento o creación de trabas en las funciones de los sistemas informáticos que hagan imposible el funcionamiento normal del sistema.
- *Artículo 287*. El uso de computadores para cometer crímenes tales como fraude financiero, hurto, malversación de fondos, indebida apropiación de fondos públicos y el robo de secretos estatales.

En breve, las sanciones están asociadas a las conductas de ingresos sin autorización a sistemas informáticos, la contaminación de datos o información contenida en un ordenador y el uso de computadores como instrumentos para perpetrar conductas delictivas.

La legislación penal no ha sido la forma predominante de represión de la ciberdelincuencia en China. Tradicionalmente las autoridades han usado las regulaciones administrativas y el control policivo para combatirla. Por ejemplo, el 5 de abril de 1995 el Ministerio de Seguridad Pública propagó un aviso pidiendo un esfuerzo concertado con el fin de frenar el uso de ordenadores para la duplicación, difusión y venta de material pornográfico.[37]

Las regulaciones administrativas en cuanto a la seguridad informáticas pueden agruparse en tres grandes categorías, a saber, red de vigilancia y control, información de red de seguridad del sistema de protección y registro de nombres de dominio. Estas regulaciones, junto con las disposiciones de la ley penal, proporcionan un marco para que el Gobierno chino monitoree y controle el flujo de la información en Internet, realice

[37] Wong, K; Wong, G., "Cyberspace Governance and Law Regulation in China", en B. Roderic, G. Peter, *Cyber-crime: The Challenge in Asia*, Hong Kong, Hong Kong University Press, 2005, p. 67.

seguimiento y vele por los usuarios de Internet , y regule y supervise los prestadores del servicio de la red.[38]

Es importante para este país la implementación de políticas encaminadas prioritariamente a la prevención de la ciberdelincuencia, además de la protección de sistemas de computador, mediante la educación y propaganda referente a la seguridad de la información y de los ordenadores. Es por esto que se hace necesario el desarrollo de nuevas políticas que hagan despegar la industria de la seguridad de la información y mejorar el nivel de cooperación entre las naciones para la efectiva persecución de crímenes transfronterizos.

2. La India

La compañía de propiedad estatal Videsh Sanchar Nigam Ltd introdujo por primera vez la Internet comercialmente el 15 de agosto de 1995, siendo sus inicios de muy lento crecimiento. Tomó tiempo para sus usuarios ponerse al día, pero actualmente la tendencia está cambiando. Durante la década de los noventa se produjo un auge en la apertura de cibercafés en la India, y un enorme crecimiento durante los años 2000 a 2002, con lo cual aumentó el número de personas que accedían a Internet.

El crecimiento y la rápida adopción de Internet en la India han implicado un significativo avance en términos económicos, fortaleciendo la industria del software y el desarrollo de nuevas tecnologías de información y telecomunicaciones. Los indios, sin embargo, han empezado a usar las computadoras, y más específicamente la Internet, para lograr accesos no autorizados y otras conductas delincuenciales. De acuerdo con las estadísticas recientes, entre febrero de 2000 y diciembre de 2002

[38] Ídem.

el Gobierno indio y las páginas web corporativas fueron "hackeadas" y modificadas cerca de 800 veces. Los primeros reportes de conductas delictivas a través de sistemas informáticos estremecieron a los legisladores, quienes inmediatamente sintieron la necesidad de regular legalmente este nuevo blanco de infracciones.[39]

Inicialmente el Código Penal de 1860 era muy compresivo y difícilmente dejaba impune alguna conducta de tipo delictivo. Con el surgimiento de las nuevas tecnologías de información y telecomunicaciones, la detonación de los actos delincuenciales vinculados a sistemas informáticos fue tan amplia que el Código Penal quedó insuficiente y se hizo necesario el desarrollo de nuevas regulaciones que combatieran la ciberdelincuencia.

El Código Penal de la India fue modificado en el año 2000 por el *Information Technology Act 2000 (IT Act)*, aprobado por ambas Cámaras del Parlamento el 17 de mayo de 2000; recibió sanción presidencial el 9 de junio de 2000 y finalmente entró en vigor el 17 de octubre de 2000. Las modificaciones contenidas en el IT Act simplemente correspondían a la adecuación de ciertas categorías de delito del Código Penal a los nuevos registros electrónicos, dejando por fuera una gran cantidad de conductas criminales.[40]

El capítulo IX del IT Act detalla determinados tipos de comportamientos que han sido designados como cibercrímenes:

- *Sección 65*. Causar daño al código fuente de un computador.
- *Sección 66*. Hacking.
- *Sección 67*. Publicar información electrónica obscena.
- *Sección 68*. Incumplir las órdenes impartidas por el contralor de las autoridades de certificación.

[39] Duggal, P. "Cyber-Crime in India: The Legal Approach", en R. Broadhurst, P. Grabosky, *Cyber-Crime: The Challenge in Asia*, Hong Kong, Hong Kong University Press, 2005, p. 185.

[40] Ibídem, pp. 185-186.

- *Sección 69.* Fracasar en la cooperación a cualquier agencia gubernamental en la ampliación de las instalaciones de descifrado cuando se ha sido exhortado por ella para hacerlo.
- *Sección 70.* Acceder o intentar garantizar el acceso a un sistema protegido.
- *Sección 71.* Tergiversación o supresión de hecho de cualquier material del contralor de las autoridades de certificación cuando se obtiene alguna licencia o certificado de firma digital.
- *Sección 72.* Violación de la confidencialidad y privacidad.
- *Sección 73.* Publicación de un certificado de firma digital que sea falso en determinados particulares.
- *Sección 74.* Publicación de un certificado de firma digital con fines fraudulentos o ilegales.
- *Sección 75.* Aplicación del IT Act para cometer delitos o contravenciones por fuera de la India.

Los desarrollos legislativos de la India, dentro de un contexto global, ponen de presente el interés por la promulgación de disposiciones específicas para la ciberdelincuencia. En ese sentido, se espera que este país pronto evolucione hacia un código diferenciado para los delitos informáticos, complementando el Código Penal y el IT Act, y sea el precursor de una amplia jurisprudencia alusiva a la delincuencia informática.[41]

3. Japón

El desarrollo de las industrias de tecnologías de información y telecomunicaciones está afectando el crecimiento de muchos aspectos de la economía y la sociedad japonesa. No obstante, esta revolución industrial

[41] Ibídem, p. 196.

y tecnológica ha estado acompañada por un vertiginoso incremento de las conductas delictivas en el ciberespacio. En ese sentido, los empresarios, de la mano del Gobierno y la policía, han diseñado medidas encaminadas a contrarrestar la ciberdelincuencia.

En el año 2001 el Gobierno japonés promulgó la *Basic Law on the Formation of an Advanced Information and Telecommunications Network Society (Basic IT Law)*, ayudando a garantizar que todos los ciudadanos japoneses pudieran gozar la emergente sociedad del conocimiento y sus beneficios plenamente. Sin embargo, la ciberdelincuencia es uno de los mayores desafíos para la revolución tecnológica.[42]

La Agencia Nacional de Policía divide los crímenes de alta tecnología en tres categorías: crímenes en contra de los computadores y la información, crímenes en la Internet, y acceso indebido a computadores. Los primeros incluyen el fraude, la producción ilegal de registros electromagnéticos, la obstrucción a la actividad empresarial a través de la destrucción de ordenadores, la destrucción de documentos públicos y la de documentos privados. Estas conductas fueron adicionadas a la ley penal en 1987 con fines de combatir el cibercrimen. Así mismo, los crímenes en contra de los computadores y la información incluyen la producción ilegal de registros electromagnéticos para tarjetas de pago como las de crédito o bancarias, agregadas en 2001. Los crímenes a través de Internet, entendidos como aquellos que ocurren cuando el delincuente está usando la Internet o cuando ésta es un factor esencial, incluyen una gran variedad de conductas, tales como fraude, difamación, intimidación, infracción de las leyes de propiedad intelectual, prostitución infantil, distribución de material obsceno y delitos relacionados con estupefacientes. El acceso indebido a computadores penaliza aquellas conductas en las que el

[42] Tatsuzaki, M., Cyber-Crime: "Current Status and Countermeasures in Japan", en R. Broadhurst, P. Grabosky, *Cyber-Crime: The Challenge in Asia*, Hong Kong, Hong Kong University Press, 2005, p. 169.

delincuente roba el código de identificación referente al control de acceso de otro y los ataques a las vulnerabilidades de los sistemas.[43]

Japón, a diferencia de las demás naciones del continente asiático, ha demostrado un gran liderazgo en cuanto al desarrollo de medidas orientadas a la lucha en contra de la delincuencia informática. Sus esfuerzos se ponen de presente en el desarrollo de legislaciones con referencias tanto nacionales como internacionales.

D. Delito informático en América Latina

Desafortunadamente América Latina está inundada de delitos "tradicionales" como robos, secuestros, narcotráfico, homicidios, entre otros. Más desafortunado aún es el hecho de que muchos de esos delitos ahora son apoyados por la tecnología. Y a todo esto, la pregunta es: ¿qué tan preparada está Latinoamérica para enfrentarlos?

1. Venezuela

El 30 de octubre de 2001 se publicó en Venezuela la Ley Especial sobre Delitos Informáticos, cuyo objetivo es proteger los sistemas que utilicen tecnologías de información, así como prevenir y sancionar los delitos cometidos contra, o mediante, el uso de ellas. Se trata de una ley que además de tipificar ciertas conductas restringe los conceptos a los cuales se refiere mediante definiciones explícitas.

Los términos que la ley delimita son los que siguen: tecnología de la información, sistema, data, documento, computadora, hardware, *firmware*, software, programa, procesamiento de datos o de información, seguridad, virus, tarjeta inteligente, contraseña y mensaje de datos.

[43] Ibídem, p. 170.

Una vez establecidas las nociones demarcadoras de lo que se regula, procede la ley a establecer las conductas consideradas típicas a través de la creación de cinco categorías de delitos: contra los sistemas que utilizan tecnologías de información, contra la propiedad, contra la privacidad de las personas y de las comunicaciones, contra niños y adolescentes, y contra el orden económico.

Los delitos contra los sistemas que utilizan las tecnologías de información incluyen las siguientes conductas: acceso indebido (art. 6°); sabotaje o daño a sistemas (art. 7°); sabotaje o daños culposos (art. 8°); acceso indebido o sabotaje a sistemas protegidos (art. 9°); posesión de equipos o prestación de servicios de sabotaje (art. 10); espionaje informático (art. 11); y falsificación de documentos (art. 12).

Los delitos contra la propiedad básicamente responden a las siguientes conductas: hurto a través del uso de tecnologías de información (art. 13); fraude mediante el uso indebido de sistemas de información (art. 14); manejo fraudulento de tarjetas inteligentes o instrumentos análogos (art. 16), apropiación de tarjetas inteligentes o instrumentos análogos (art. 17); provisión indebida de bienes o servicios (art. 18) y posesión de equipo para falsificaciones (art. 19).

Los delitos contra la privacidad de las personas y de las comunicaciones se resumen en tres conductas fundamentalmente: violación de la privacidad de la data o información de carácter personal (art. 20); violación de la privacidad de las comunicaciones (art. 21) y revelación indebida de data o información de carácter personal (art. 22).

Los delitos contra niños y adolescentes obedecen a conductas tipificadas con fines de proteger a los menores de la pornografía y la prostitución, esencialmente.

Los delitos contra el orden económico, por su parte, tipifican conductas encaminadas a la protección de la propiedad industrial y las ofertas comerciales.

La legislación venezolana es una de las más amplias en Latinoamérica en lo que a la ciberdelincuencia se refiere, pues su articulado recoge una gran cantidad de conductas típicas acuñadas bajo el título de delitos informáticos, sin necesidad de recurrir a las conductas penales tradicionales. Sin embargo, múltiples deficiencias y problemas en la técnica legislativa empleada y los conceptos usados, así como diversas lagunas y contradicciones, la hacen insuficiente como complemento del resto de la legislación.

2. Chile

Chile fue el primer país latinoamericano en sancionar una Ley contra Delitos Informáticos. La ley 19223, publicada en el *Diario Oficial* el 7 de junio de 1993, en un corto articulado tipifica y sanciona la destrucción o inutilización de un sistema de tratamiento de información.

La ley pretende proteger un nuevo bien jurídico surgido con el uso de las modernas tecnologías computacionales: la calidad, la pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de ésta, y de los productos que de su operación se obtengan.

No obstante, no sólo se protege ese bien, sino que además concurren otros, tales como: el patrimonio; la privacidad, intimidad y confidencialidad de los datos; la seguridad y fiabilidad del tráfico jurídico y probatorio; el derecho de propiedad sobre la información y sobre los elementos físicos.

La ley contempla cuatro artículos que, si bien corresponden cada uno a un tipo de conducta distinta, se pueden clasificar en dos grandes figuras delictivas: el sabotaje informático y el espionaje informático.

El sabotaje informático (arts. 1° y 3°) comprende aquellas conductas tipificadas atendiendo al objeto que se afecta o atenta con la acción

delictual, y que puede ser un sistema de tratamiento de la información o de sus partes componentes, el funcionamiento de un sistema de tratamiento de la información, o los datos contenidos en un sistema automatizado de tratamiento de la información. El atentado a estos objetos puede ser a través de su destrucción, inutilización, obstaculización o modificación.

El espionaje informático (arts. 2° y 4°) comprende aquellas figuras delictivas que atienden al modo operativo ejcutable y pueden ser, en primer lugar, delitos de apoderamiento, uso o conocimiento indebidos de la información, cometidos interfiriendo, interceptando o meramente accediendo al sistema de tratamiento de datos. Estas figuras corresponden a lo conocido comúnmente como hacking. En segundo lugar, comprende también los delitos de revelación indebida y difusión de datos contenidos en un sistema de tratamiento de la información.

La existencia de nuevas acciones informáticas que pueden tener el grado de delito es una problemática con presencia actualmente en Chile. Los riesgos de que este país no legisle sobre esta materia son enormes, si se tiene en cuenta que la ciberdelincuencia no tiene fronteras. En ese sentido, y dado el limitado alcance de la normativa chilena frente a nuevas conductas, es necesario desatar nuevos proyectos encaminados a combatir el cibercrimen.

3. Argentina

El 4 de junio de 2008 finalmente se convirtió en la ley 26388 el proyecto contra los delitos informáticos, con 172 votos a favor y ninguno en contra.[44] Esta ley modifica el Código Penal argentino para incluir esos delitos y sus respectivas penas.

[44] Sobre el tema de delitos informáticos en Argentina antes de 2008, consúltese la obra: Palazzi, Pablo, *Delitos informáticos*, Buenos Aires, AD-HOC, 2000.

La importancia de esta novedosa norma es que llena un vacío legal, el cual hasta ahora sólo contenía incertidumbre, pues en el ordenamiento positivo argentino el delito informático no constituía por sí mismo una categoría delictiva, sino que lo limitaba a los usos indebidos de cualquier medio informático, dejando un gran espacio para que los ciberdelincuentes continuaran en la impunidad.

Actualmente, gracias a la reciente reforma, el Código Penal argentino contempla los siguientes tipos de delitos:

- Distribución y tenencia, con fines de distribución, de pornografía infantil.
- Violación de correo electrónico.
- Acceso ilegítimo a sistemas informáticos.
- Daño informático y distribución de virus.
- Daño informático agravado.
- Interrupción de comunicaciones.

Esta reforma probablemente requerirá en el futuro de nuevos debates y actualizaciones, pero para Argentina es muy importante el haber tenido lugar, dado que el Código Penal, por su antigüedad, no contemplaba la categoría de delitos informáticos.

4. México

La legislación penal mexicana cuenta con importantes disposiciones en lo que a delitos informáticos respecta. Así, vale la pena destacar las leyes de carácter federal presentes en el Código Penal Federal, en el libro II, título IX, capítulos I y II:

- *Artículo 211 bis 1.* Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos

de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

- *Artículo 211 bis 2.* Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.
- *Artículo 211 bis 3.* Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.
- *Artículo 211 bis 4.* Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
- *Artículo 211 bis 5.* Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Aunque en México las nuevas transformaciones relativas a la ciberdelincuencia se han venido manifestando paulatinamente, el ordenamiento jurídico aún no le ha dado un tratamiento adecuado a ella y con contadas excepciones el país está retrasado a la hora de legislar sobre aspectos de trascendencia nacional e internacional como la evidencia digital. En ese

sentido, es clara la necesidad de ciertas reformas y adiciones legislativas las cuales le permitan establecer unos parámetros claros y precisos que aseguren el adecuado juzgamiento de los delitos informáticos.

5. Colombia

En la década pasada se consideraba, tanto en el ámbito nacional como en el internacional, que la inseguridad jurídica respecto del valor probatorio de los mensajes de datos era el principal obstáculo para el desarrollo del comercio electrónico y que su regulación, por tanto, era un asunto de suma importancia. La expedición de la ley 527 de 1999 obedeció a esta necesidad jurídica de dar seguridad jurídica a las transacciones electrónicas.[45]

En la regulación de los medios electrónicos por la ley 527 el legislador, con fines de adaptar el régimen jurídico existente a las nuevas realidades, creó el criterio del equivalente funcional. Dicho criterio puede ser enunciado como sigue: "Si un mensaje de datos cumple con los mismos objetivos y tiene las mismas funciones que un medio tradicional o físico de transmisión de información, dicho mensaje tendrá los mismos efectos jurídicos que dicho medio físico". En ese sentido, no pueden negarse efectos jurídicos, validez o fuerza a cierta información por el solo hecho de que esté en forma de mensaje de datos.

No obstante lo anterior, el que no pueda negarse efecto jurídico a los mensajes de datos no significa que todos los mensajes de datos tengan el mismo valor probatorio, y ni siquiera, que tengan alguno. Por eso el legislador consideró prudente establecer unos parámetros básicos para determinar cuándo un mensaje de datos tiene valor probatorio. Así, se

[45] Umaña Chaux, A. F., "Algunos comentarios sobre el principio del equivalente funcional en la ley 527 de 1999", en *Revista de Derecho: Comunicaciones y Nuevas Tecnologías*, 2005, pp. 78-79, consultado el 2 de octubre de 2008. Disponible en: http://derechoytics. uniandes.edu.co/pdfs/R1_A3.pdf.

tiene que, para saber si un mensaje de datos presta valor probatorio, deberá seguirse el siguiente razonamiento: 1) establecer las funciones probatorias que un determinado mensaje de datos cumplió respecto de señalados hechos; 2) hallar un documento o medio de prueba que cumpla con estas mismas funciones; 3) definir si el mensaje de datos cumple dichas funciones con la suficiente confiabilidad, de acuerdo con las reglas de la sana crítica.[46]

Es importante resaltar que los equivalentes funcionales son criterios de interpretación, esto es, son artículos interpretativos. Su función principal es permitir la interpretación de otros artículos de la normatividad, a saber, aquellos que imponen requisitos formales para ciertos actos o que exigen la prueba de éstos. En esa medida, no se requiere de normas particulares que establezcan equivalentes funcionales para cada una de las oportunidades en donde se imponen esos requisitos formales, puesto que los artículos de la ley 527 de 1999 se aplican de manera directa a los casos.[47]

El criterio del equivalente funcional es tal vez uno de los principales avances de la legislación colombiana en cuanto al uso de nuevas tecnologías se refiere. Su consagración permitió una primera aproximación al tema de la evidencia digital y más concretamente a su tratamiento, pues se trata de un criterio de interpretación de las normas del ordenamiento jurídico que regulan el valor probatorio.

Si bien esta normativa tiene un importante impacto en el desarrollo del comercio electrónico en Colombia, su uso todavía está lejos de no ser problemático. La ciberdelincuencia es uno de los mayores desafíos para su aplicación.

[46] Ibídem, p. 79.

[47] Ibídem, p. 80.

El delito informático en Colombia no está tipificado expresamente como una categoría delictiva individual y autónoma. El Código Penal colombiano cuenta con un único artículo, el 195, que bajo el epígrafe de "Acceso abusivo a un sistema informático" (hacking en otras legislaciones), establece una sanción de multa, sin especificar la cuantía, para quienes abusivamente se introduzcan en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo.

Es importante tener en cuenta que, sin perjuicio de existir o no una definición de qué es o qué no es un delito informático, el Código Penal trae definidos, delimitados y regulados muchísimos delitos susceptibles de ser cometidos en un entorno informático. Y, es allí precisamente, donde el juzgador y los investigadores deben encontrar la relación, con fines de evitar la impunidad en cuanto a la ciberdelincuencia.[48]

En ese sentido, no es totalmente cierto que cuanto hay en la legislación colombiana sea inaplicable. Sin embargo, no puede desconocerse que el delito informático requiere de unas condiciones especiales y diferentes a las contempladas dentro del ámbito jurídico nacional tradicional, pues no se puede pretender aplicar a rajatabla normas escritas para regular otros aspectos y otros momentos.

En materia normativa los mayores vacíos están relacionados con las restricciones generales y abstractas que tiene el juez para procurar y analizar las fuentes informáticas que colaborarían en gran medida a emitir una decisión más rápida y justa. Otro aspecto, entendido como "vacío", es la no existencia exhaustiva y taxativa de normas.[49]

[48] Gamboa, R. H., *Clic jurídico para combatir el delito informático*, *Sistemas*, núm. 92, 2005.

[49] Ídem.

En cuanto al punto de las restricciones generales y abstractas mencionadas, están aquellas que se le imponen al juzgador y a las partes, en el sentido de no poder acceder con anterioridad a la totalidad de la información sino sólo a una parte determinada. Y únicamente se permite analizar un disco duro hasta pasadas varias semanas de la notificación de la demanda. Esto genera que el investigado tenga la posibilidad de alterar o eliminar datos, haciendo muy difícil —si no imposible— la consecución de pruebas.[50]

Por otra parte, en materia penal se dice que "nadie puede ser juzgado sino por un delito preexistente" y se intenta asociar este principio a la no enunciación exhaustiva de todos los delitos informáticos que puede haber, llegando incluso a afirmar que para existir una sanción debe haber regulación previa y exacta de la conducta que se pretende sancionar. Esto no puede ser así, pues recordemos que el medio tecnológico no es más que eso: un medio a través del cual se realizan conductas ya tipificadas como delitos.

Un último aspecto que se puede considerar como vacío aunque no es normativo, es el de la carencia de medios. Muchas veces existe personal capacitado, certeza del hecho, pero se carece de las herramientas para desentrañar la verdad. Es como un coche sin ruedas, que no puede echarse a andar por carencia de elementos, y se da el saber algo pero no poderse probar. Lo cual confirma, una vez más, el principio de que "tanto vale no tener derecho como no poder probarlo".[51]

Dado lo anterior, resulta evidente la necesidad de expedir una reglamentación especial y específica para las conductas alusivas a la delincuencia informática. El rezago de Colombia con respecto a este tipo de delitos genera no sólo vacíos normativos, sino también permite que las

[50] Ídem.

[51] Ídem.

acciones punibles surgidas paralelamente a los avances tecnológicos, queden impunes. Es por lo tanto indispensable la adecuación de la legislación penal a la realidad tecnológica actual, así como el desarrollo de nuevos mecanismos que respondan a los nuevos desafíos.

Parte de esta necesidad fue acogida mediante la ley 1273 de 2009, a la cual haremos referencia posteriormente.

VIII. Formación de jueces en temas de delito informático

Uno de los axiomas de la gestión tanto en el sector público como en el privado es el de que "la información es poder". En muchas de las esferas sociales la gestión de la información es ahora considerada como una de las claves para un liderazgo efectivo, sobre todo en las organizaciones en continua transformación. Para los directores del sector de la justicia penal los recientes avances en las tecnologías de información y telecomunicaciones ofrecen oportunidades para introducir mejoras en el control de la operación, la toma de decisiones y la planificación estratégica, esenciales para el éxito de la policía, los Tribunales, organismos y correccionales. No obstante, los cambios en las tecnologías de información y telecomunicaciones también crean una diversidad de problemas para los directores del sector de la justicia penal, particularmente en relación con el desarrollo analítico, el conocimiento y el tratamiento de funcionarios de niveles medio y superior de gestión.[52]

Tradicionalmente los problemas alusivos a la delincuencia informática encontraban solución en programas y controles informáticos, pues se partía de que la respuesta a la máquina estaba en ella. Sin embargo,

[52] Byrne, J; Buzawa, E., "Information, Technology and Criminal Justice Education", en A. Pattavina, *Information Technology and the Criminal Justice System*, California, Sage, 2005, p. 243.

con el surgimiento de nuevos sistemas de prevención y protección los ciberdelincuentes encuentran a su vez nuevas formas de violentarlos. Es por esto que los funcionarios del sector penal, reconociendo la complejidad de los crímenes de alta tecnología, deben contar con conocimientos especiales que les permitan adelantar la adecuada investigación y prosecución de crímenes de alta tecnología.

No obstante lo anterior, y aun cuando los crímenes de alta tecnología continúan incrementándose cada año, hay gran escasez de jueces penales con un nivel suficiente de conocimientos para detectar, investigar y juzgar este tipo de crímenes. La naturaleza compleja y dinámica de los delitos informáticos determina la necesidad de personal especializado, con conocimientos, habilidades y aptitudes basadas en un entrenamiento permanente en tecnologías de información y telecomunicaciones.[53]

La ausencia de las habilidades más básicas y fundamentales para la investigación de los crímenes de alta tecnología impide su apropiado juzgamiento. Sin un nivel de educación y entrenamiento adecuado los jueces podrían pasar por alto o malinterpretar evidencia crítica para la resolución de un caso que involucre sistemas informáticos.[54]

A. Programas existentes en Estados Unidos

El National Center for State Courts estima que, colectivamente, los Tribunales estadounidenses gastan alrededor de US$ 500 millones en tecnologías de información. Estos dólares se destinan a la planificación de nuevas aplicaciones automatizadas, especificando sus necesidades, la compra de hardware, el desarrollo o la adquisición de software, la

[53] Myers, L. J., *High Technology Crime Investigation...*, p. 49.

[54] Ibídem, p. 50.

instalación de nuevos sistemas, la capacitación de los usuarios sobre cómo operarlos y el apoyo a las operaciones.

Desafortunadamente, en muchos sistemas judiciales los administradores de los Tribunales han intentado cambiar o mejorar sus sistemas de información existentes sin una clara comprensión de esta nueva tecnología, de sus costos y de sus limitaciones inherentes.[55]

El adecuado manejo de las tecnologías de información y telecomunicaciones se ha convertido en una necesidad para los sistemas judiciales en Estados Unidos. En ese sentido, la educación puede y debe jugar un papel importante en la preparación de profesionales que puedan proveer seguridad, garantías y confianza en los Tribunales encargados del juzgamiento de los delitos informáticos.

Existen tres áreas relevantes para estructurar los temas de estudio en lo que a la formación de jueces en temas de delito informático y evidencia digital respecta. La primera es el desarrollo de aptitudes; la segunda, el desarrollo de análisis; y la tercera, el desarrollo de conocimientos. Teniendo en cuenta esto, como mínimo los cursos deben ofrecer las siguientes temáticas: información sobre el diseño del sistema y los Tribunales; planificación estratégica, tecnologías de información y telecomunicaciones y los Tribunales; y las nuevas y potenciales aplicaciones de los sistemas informáticos en la configuración de los Tribunales.[56]

A medida que la demanda de una justicia cualificada con una apropiada combinación de formación en investigación y conocimientos técnicos en tecnologías informáticas se ha venido incrementando, varias instituciones estadounidenses han optado por desarrollar programas que incluyen principalmente cursos de entrenamiento permanente y educación superior, y de exposición a las tecnologías informáticas.

[55] Byrne, J; Buzawa, E., "Information, Technology and Criminal Justice Education"..., p. 248.

[56] Ídem.

1. Cursos de entrenamiento

El objetivo de los cursos de entrenamiento es el de introducir al personal encargado de la Administración de la Justicia penal en los temas de tecnologías de información y telecomunicaciones y concientizarlo sobre la forma como los sistemas informáticos pueden ser utilizados para perpetrar crímenes. El énfasis de estos cursos consiste en ofrecer un entrenamiento más especializado en las herramientas de investigación y judicialización de la ciberdelincuencia, logrando que los jueces desarrollen o avancen en sus conocimientos, habilidades y aptitudes concernientes a las tecnologías de computadores. Algunas de las instituciones que cuentan con estos cursos de entrenamiento son: National Consortium for Justice Information and Statistics (SEARCH), Federal Law Enforcement Training Center (FLETC), International Assóciation of Computer Investigative Specialists (IACIS), United States Secret Service, International Revenue Service (IRS) y Federal Bureau of Investigation (FBI).

2. Cursos de educación superior

El personal encargado de la justicia penal podría desarrollar sus conocimientos, habilidades y aptitudes concernientes a las tecnologías de computadores ya sea mediante programas técnicos o profesionales. El principal objetivo de los cursos de educación superior es el de dar a conocer a los estudiantes las demandas tanto reales como potenciales de la justicia penal, así como de la sociedad en general. Para lograrlo, la mayoría de estos programas académicos están integrando el uso de computadores con los esquemas tradicionales de justicia criminal.[57]

[57] Myers, L. J., *High Technology Crime Investigation*..., p. 53.

Los programas técnicos existentes en Estados Unidos se caracterizan básicamente por brindar a los estudiantes las herramientas fundamentales para que puedan participar en la correcta investigación y juzgamiento de las conductas punitivas a través de ordenadores. Algunos ejemplos de universidades que ofrecen estos programas son: Tompkins Cortland Community College y Highline Community College.

Los programas profesionales ofrecidos por las universidades estadounidenses cuentan con una naturaleza esencialmente interdisciplinaria en lo que a tecnologías de computadores y aplicaciones de los sistemas de información se refiere. Entre otras, estos programas pueden adelantarse en universidades como Purdue College.

Tales programas de educación superior constituyen una herramienta fundamental para la detección y juzgamiento de las conductas ciberdelictivas, pues se encargan de entrenar apropiadamente a quienes habrán de tomar las riendas de la justicia penal en temas de delito informático. El juzgador ideal de los crímenes de alta tecnología debe tener un enfoque multidisciplinario en cuanto a tecnologías de información y telecomunicaciones.

IX. Exposición a las tecnologías informáticas

Con fines de desarrollar o actualizar los conocimientos, habilidades y aptitudes del personal encargado de la justicia penal, las Cortes deben equipar a sus funcionarios, y más específicamente a los jueces, de modernos equipos tecnológicos. La exposición constante a tecnologías informáticas podría contribuir a que se familiaricen con las operaciones y procedimientos computacionales básicos; con esos conocimientos mínimos fundamentales los jueces penales estarían en capacidad de mejorar su habilidad para comprender la naturaleza de los crímenes informáticos.[58]

[58] Ibídem, p. 52.

De acuerdo con lo anterior, el National Center for State Courts ha trabajado considerablemente en la temática de tecnologías en general y en el desarrollo de estándares para automatizar los tribunales. Así, han resultado relevantes las iniciativas de las Cortes de Pensilvania, Florida y California en la constitución de programas como el *Off shore programming service* —permite adelantar procesos de personas en otras partes a través de sistemas informáticos— o *Live from your Court* (permitía que estudiantes de universidades vieran a través de Internet, en tiempo real, lo acontecido en las Cortes).

X. Reflexiones sobre la formación de jueces en temas de delito informático en Colombia

En la actualidad Colombia no cuenta en informática forense con ningún tipo de programa académico, ni carrera técnica, mucho menos de pregrado, especialización o maestría. La formación del personal encargado de la justicia penal en el país es aún una utopía, por cuanto no se han establecido los criterios idóneos para que gocen de una adecuada formación. Ha sido posible llegar a esta conclusión a raíz de investigaciones de campo en las entidades estatales encargadas del manejo del área de la delincuencia informática.

Con ellas se encontró que en Colombia apenas existe una institución encargada de la educación y la formación de los funcionarios del sector justicia, la Escuela Judicial de Formación de Jueces Rodrigo Lara Bonilla. Ésta ofrece básicamente programas de formación a los integrantes de la rama judicial que aspiran a ingresar a su servicio, con el fin de afianzar y fortalecer aquellos principios, valores, actitudes, habilidades, competencias, destrezas, estructuras de pensamiento y conceptos fundamentales necesarios para prestar una atención de calidad y oportuna a los ciudadanos que acuden a la Administración de Justicia en las

diversas jurisdicciones y especialidades. Así, la actividad de la Escuela se concentra en las áreas de formación inicial y continuada, según lo dispuesto por la ley 270 de 1996:

> Artículo 177. *Escuela Judicial.* La Escuela Judicial Rodrigo Lara Bonilla se constituirá en el centro de *formación inicial y continuada* de funcionarios y empleados al servicio de la Administración de Justicia.

En dicha Escuela, desde el año 2002, se ha venido ofreciendo a todos los funcionarios del país el Ciclo de formación y capacitación de magistrados y jueces, compuesto por cuatro proyectos de formación y uno de capacitación: el primero, "Fundamentos de la función judicial"; el segundo, "Elementos de la decisión judicial"; el tercero, "Ejercicio de la función judicial"; el cuarto, "Capacitación especializada"; y el quinto, "Informática jurídica".

El programa completo tiene una duración de cinco años. En el primero se dictan las materias: filosofía del derecho, ética judicial, derechos humanos y Derecho Internacional Humanitario, y tutela. El segundo año contiene las de interpretación constitucional, interpretación judicial, argumentación jurídica y estructura de la sentencia. El tercer año incluye: la Administración de Justicia en la Constitución Política, el juez director del Despacho, el juez director del proceso y optimización del talento humano y del servicio. En el cuarto año se ven las materias derecho civil, de familia, laboral, penal y administrativo. El último año incluye informática básica y especializada, y software de gestión judicial.

Como se desprende de la lectura del programa, los cursos de formación ofrecidos por la Escuela Judicial solamente tratan temas filosóficos y jurídicos; y si bien tocan algunas materias pertinentes para el área de la informática, dejan por fuera las técnicas procedimentales con respecto a las pruebas y herramientas orientadas a la informática

forense y la ciberdelincuencia. En ese sentido, no quedan satisfechas las recomendaciones de organismos internacionales, ni las normativas de países avanzados en la materia, tales como Estados Unidos o Inglaterra, para el adecuado entrenamiento del personal encargado del sector de la Administración de Justicia.

La Dirección de la División Académica de la Escuela Judicial de Formación de Jueces "Rodrigo Lara Bonilla", al ser inquirida acerca de la formación de jueces en temas de delitos informáticos y los programas ofrecidos por ella orientados a dichos fines, prefirió guardar reserva. Así las cosas, y sin perder de vista las deficiencias en los programas de formación ofrecidos por esta institución sobre los asuntos de evidencia digital y ciberdelincuencia, Colombia deja entrever su falta de preocupación y de acción frente a un fenómeno criminal que contrae un alto grado de peligrosidad.

XI. PROPUESTA SOBRE LA FORMACIÓN DE JUECES EN TEMAS DE DELITO INFORMÁTICO Y EVIDENCIA DIGITAL EN COLOMBIA

La investigación desarrollada en este documento esboza los conocimientos, habilidades y aptitudes que requiere un juez para adelantar el adecuado juzgamiento de las conductas delictivas vinculadas a sistemas informáticos. En ese sentido, sin ignorar la importancia que han venido adquiriendo en los últimos años las tecnologías de información y telecomunicaciones, se exhorta al Gobierno Nacional y en general a los funcionarios judiciales a tomar conciencia sobre la urgencia de formar a los jueces en evidencia digital y delitos informáticos, para poder fortalecer y modernizar la Administración de Justicia en Colombia y evitar que nuestro país continúe siendo un paraíso para los ciberdelincuentes.

Con esta finalidad, se propone una medida de acción a mediano plazo consistente en la creación de diplomados que permitan la actualización

permanente de los funcionarios judiciales frente a los constantes avances en las tecnologías de información y telecomunicaciones, vinculada específicamente a la evidencia digital y a la criminalidad informática. Estos diplomados pueden desarrollarse en la Escuela de Formación de Jueces Rodrigo Lara Bonilla y consistirían básicamente de 3 cursos, con una duración estimada de 120 horas cada uno, estructurados en 3 ciclos: el de formación básica, el de contextualización y el de especialización.

El ciclo de formación básica tendría como fin cimentar en los funcionarios judiciales las bases de la formación en informática, la cual se estudiaría integrando los conceptos y materias fundamentales que componen la columna vertebral de esta ciencia, de modo tal que se logre en el funcionario una visión de conjunto la cual le permita conocer y relacionar los conceptos informáticos.

El ciclo de contextualización estaría encaminado a la formación de los estudiantes dentro de una óptica interdisciplinaria que les permita abordar los problemas de manera contextualizada. Así, se estudiaría la evidencia digital y sus implicaciones, con el propósito de lograr que los conceptos informáticos básicos sean abordados desde una perspectiva de inmersión en la realidad jurídica.

El ciclo de especialización permite al funcionario formado previamente en informática y en evidencia digital responder mejor a su vocación de juez a través del estudio en profundidad de los delitos informáticos y de la adecuada forma de aplicación de las disposiciones presentes en el ordenamiento jurídico colombiano.

Con fines de ilustrar lo anotado, se procede a elaborar unas tablas que reflejan con mayor detalle la justificación, los objetivos y las materias a estudiarse en cada ciclo.

CICLO I - FORMACIÓN BÁSICA Diplomado en Informática Básica	
Justificación	El tratamiento racional, automático y adecuado de la información por medio del computador para el diseño y desarrollo de estructuras y aplicaciones especiales orientadas a la búsqueda de seguridad e integridad de ésta, son factores necesarios para garantizar la eficiencia y competitividad en la recta impartición de justicia en un mundo digitalizado.
Objetivo	El diplomado está orientado a brindar los conceptos básicos de la informática y la computación para obtener un conocimiento general sobre las tecnologías de la información y de las telecomunicaciones.
Dirigido a	Abogados, jueces, fiscales, y en general, a todas aquellas personas que están relacionadas con la investigación y el juzgamiento de los delitos informáticos.
Metodología	Se implementará la metodología del aprendizaje activo, que combina la exposición magistral de los temas a cargo de los profesores, con el objeto de exponer la actualidad de los diversos conceptos, junto con el esquema de participación del estudiante, que involucra la lectura previa de material debidamente seleccionado.
Temas	Ayer y hoy de la informática, estructuras de datos, la información y el ordenador, la arquitectura fundamental del ordenador, las memorias, los periféricos, almacenamiento de información, el software, desarrollo del software, Internet, redes y comunicaciones, aplicaciones de la informática, seguridad de la información, gestión empresarial.
Duración del programa, hora y lugar	El programa tendrá una duración de 100 horas. Hora: Viernes, de 6:00 p. m. a 8:00 p. m. Sábados, de 8:00 a. m. a 12:00 m. Lugar: Escuela de Formación de Jueces "Rodrigo Lara Bonilla"
Profesores	Funcionarios y técnicos encargados de los asuntos de computación y seguridad informática, en la Escuela Judicial de Formación de Jueces.

CICLO II - CONTEXTUALIZACIÓN Diplomado en Evidencia Digital y sus Aplicaciones	
Justificación	La investigación criminal y criminalística, binomio que permite dar calidad de investigación científica a los delitos informáticos, afronta en la actualidad un reto dentro de la etapa de juzgamiento dada la gran cantidad de conductas delictivas concretadas mediante sistemas informáticos.
Objetivo	El diplomado está orientado a lograr una aproximación hacia el fenómeno de la ciberdelincuencia, esto es, a las nuevas técnicas de comisión de delitos informáticos, a su investigación, y a los principios básicos de seguridad.
Dirigido a	Abogados, jueces, fiscales, y en general, a todas aquellas personas que están relacionadas con la investigación y juzgamiento de los delitos informáticos, previamente formadas en el Diplomado de Informática Básica.
Metodología	Se implementará la metodología del aprendizaje activo, que combina la exposición magistral de los temas a cargo de los profesores, con el objeto de exponer la actualidad de los diversos conceptos, junto con el esquema de participación del estudiante, que involucra la lectura previa de material debidamente seleccionado y el análisis de casos prácticos.
Materias	Prueba electrónica, identificación y seguridad de fuentes de pruebas electrónicas, seguridad en las tecnologías de información y telecomunicaciones, incautación y registro de evidencias digitales, preservación de la evidencia digital, investigación de evidencias digitales, sistemas de seguridad en tecnologías informáticas.
Duración del programa, hora y lugar	El programa tendrá una duración de 120 horas. Hora: Viernes, de 6:00 p. m. a 9:00 p. m. Sábados, de 8:00 a. m. a 1:00 p. m. Lugar: Escuela de Formación de Jueces "Rodrigo Lara Bonilla"
Profesores	Profesores de las diversas universidades del país que cuentan con programas y desarrollos avanzados en seguridad informática, como los Andes y la Javeriana. Esto, en virtud de convenios que podría adelantar la Escuela de Formación de Jueces con ellas.

CICLO III - ESPECIALIZACIÓN Diplomado en Delito Informático	
Justificación	El avance tecnológico en la informática y su influencia en casi todas las esferas de la vida social, ha dado lugar a una serie de comportamientos ilícitos, acuñados bajo el término genérico "delitos informáticos", haciendo necesario el conocimiento profundo de éstos con el fin de realizar un juzgamiento adecuado.
Objetivo	El diplomado está orientado a ofrecer ideas sobre cómo se realizan estos delitos, estadísticas, efectos en varias áreas, cómo combatirlos, y finalmente, cómo poder minimizar su repercusión y sus daños.
Dirigido a	Abogados, jueces, fiscales, y en general, a todas aquellas personas que están relacionadas con la investigación y juzgamiento de los delitos informáticos, previamente formadas en los Diplomados de Informática Básica y Evidencia Digital y sus Aplicaciones.
Metodología	Se implementará la metodología del aprendizaje activo, que combina la exposición magistral de los temas a cargo de los profesores, con el objeto de exponer la actualidad de los diversos conceptos, junto con el esquema de participación del estudiante, que involucra la lectura previa de material debidamente seleccionado y el análisis de casos prácticos.
Materias	Conceptualización y generalidades en torno a los delitos informáticos, legislaciones sobre delitos informáticos a nivel nacional e internacional, tipificación de los delitos informáticos, impacto sobre la Administración Pública por la falta de regulación en materia de delitos informáticos, análisis de la incorporación de medios informáticos para la comisión de delitos y su impacto en la Administración Pública, detección de delitos informáticos, prosecución de delitos informáticos.
Duración del programa, hora y lugar	El programa tendrá una duración de 120 horas. Hora: Viernes, de 6:00 p. m. a 9:00 p. m. Sábados, de 8:00 a. m. a 1:00 p. m. Lugar: Escuela de Formación de Jueces "Rodrigo Lara Bonilla"

CONTINÚA...

...CONTINUACIÓN

CICLO III - ESPECIALIZACIÓN Diplomado en Delito Informático	
Profesores	Profesores de las diversas universidades del país que cuentan con programas y desarrollos avanzados en seguridad informática, como la de los Andes y la Javeriana. Esto, en virtud de convenios que podría adelantar la Escuela de Formación de Jueces con ellas.

XII. Bibliografía

Agencia Española de Protección de Datos, "Delitos informáticos", 2008.

Biblioteca del Congreso Nacional de Chile, Centro de Estudios de Justicia de las Américas.

Broadhurst, R.; Grabosky, P., "Computer-Related Crime in Asia: Emergent Issues", en R. Broadhurst & P. Grabosky, *Cyber-crime: The Challenge in Asia,* Hong Kong, Hong Kong University Press, 2005.

Byrne, J.; Buzawa, E., "Information, Technology and Criminal Justice Education", en A. Pattavina, *Information Technology and the Criminal Justice System,* California, Sage, 2005.

Campoli, G. A., *Alfa-Redi.* Disponible en: http://www.alfa-redi.org/rdi-articulo.shtml?x=974 [acceso el 3 de julio de 2008].

Computer Security Institute, *Computer Crime and Security Survey,* csi Publications, 2007.

Daltabuit, E., *Revista de Derecho Informático Alfa-Redi, 2007.*

Duggal, P. "Cyber-Crime in India: The Legal Approach", en R. Broadhurst, P. Grabosky, *Cyber-Crime: The Challenge in Asia,* Hong Kong, Hong Kong University Press, 2005.

Edgard-Nevill, D.; Stephens, P. "Countering Cybercrime", en R. Bryant, *Investigating Digital Crime,* England, Wiley, 2008.

Ferrera, G.; Lichtenstein, S.; Reder, M.; Bird, R.; Schiano, W., *Cyberlaw: Text and Cases,* Maryland, Thompson, 2004.

Gamboa, R. H., "Clic jurídico para combatir el delito informático" *en Sistemas,* núm. 92, 2005.

Guerrero, M. F., *La ciberdelincuencia,* Bogotá, Procuraduría General de la Nación, 2004.

Kennedy, I., "Investigating Digital Crime", en R. Bryant, *Investigating Digital Crime,* England, Wiley, 2008.

May, M. Sans Institute, 2004

McLean, S. J., British & Irish Law, Education and Technology Association, 1999

Myers, L. J. *High Technology Crime Investigation: A Curricular Needs Assessment of the Largest Criminal Justice and Criminology Programs in the United States,* Florida, Texas, A&M University, 2000.

Palazzi, Pablo, *Delitos informáticos*, Bogotá, ad-hoc, 2000.

— "Análisis legal del accionar de un virus informático en el derecho penal argentino y comparado", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* núm. 2, Bogotá, Universidad de los Andes, 2006.

Posada Maya, R., "Aproximación a la criminalidad informática en Colombia", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* núm. 2, Bogotá, Universidad de los Andes, 2006.

Reyna, L., "El bien jurídico en el delito informático", en *Alfa-Redi*, 2007.

Rovira del Canto, E., *Delincuencia informática y fraudes informáticos,* Granada, Comares, 2002.

TATSUZAKI, M., "Cyber-Crime: Current Status and Countermeasures in Japan", en R. Broadhurst, P. Grabosky, *Cyber-Crime: The Challenge in Asia,* Hong Kong, Hong Kong University Press, 2005.

UMAÑA CHAUX, A. F., "Algunos comentarios sobre el principio del equivalente funcional en la ley 527 de 1999", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías, 2005.*

UNITED STATES SENTENCING COMISSION.

UNITED STATES *vs.* MORRIS, 928 F.2d 504 (2nd. Cir.) Supreme Court, 1991.

WALDEN, I., *Computer Crimes and Digital Investigations,* New York, Oxford, 2007.

WASIK, M., *Crime and the Computer,* Oxford, Clarendon Press, 1991.

WONG, K.; WONG, G., "Cyberspace Governance and Law Regulation in China", en B. Roderic, G. Peter, *Cyber-crime: The Challenge in Asia,* Hong Kong, Hong Kong University Press, 2005.

CAPÍTULO VI

ANOTACIONES SOBRE LA LEY 1273 DE 2009

Nelson Remolina Angarita

El fenómeno del delito informático ha vivido el ciclo constante de casos no cubiertos por la legislación y la reforma posterior a la ocurrencia de hechos resonantes[1]

Pablo A. Palazzi

I. Introducción

Poco a poco se nutre la regulación penal colombiana tipificando conductas centrales de lo que se engloba bajo el término delitos informáticos. La ley 1273 de 2009[2] modificó el Código Penal y estableció la protección de la información y de los datos como nuevo bien jurídico tutelado. Esta norma tiene varias implicaciones:

En primer lugar, adiciona el artículo 58 para establecer como circunstancia de agravación el uso de medios informáticos, electrónicos o telemáticos en la realización de conductas punibles. Se trata de un

[1] Palazzi, Pablo, *Delitos informáticos*, Buenos Aires, AD-HOC, 2000, p. 53.

[2] "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado 'de la protección de la información y de los datos', y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

reconocimiento a los efectos en masa, e ilimitados, que puede ocasionar el empleo de dichos medios en fines criminales.

En segundo lugar, crea el título VII *bis*, denominado "De la protección de la información y de los datos". Bajo dicho manto precisa y amplía el delito de acceso abusivo a un sistema informático, previsto en el artículo 195 de la ley 599 de 2000, el cual de manera explícita quedó derogado.

En tercer lugar, retoma e incorpora una serie de términos en nuestra jerga jurídica, como "sistema informático", "dato informático" y "sistema de tratamiento de información". Lamentablemente la ley no los define, lo cual podría generar problemas a la hora de sancionar porque la tipificación no es precisa. Recuérdese que el artículo 10 del Código Penal exige que la conducta sea definida de manera "inequívoca, expresa y clara".

De otra parte, la ley 1273 tipificó varios delitos, distribuidos en dos capítulos. En el primero se describen los siguientes: obstaculización ilegítima de sistema informático o red de telecomunicación (art. 269b); interceptación de datos informáticos (art. 269c); daño informático (art. 269d); uso de *software* malicioso (art. 269e); violación de datos personales (art. 269f); suplantación de sitios web para capturar datos personales (art. 269g). En el capítulo segundo se incorporan estos tipos penales: hurto por medios informáticos y semejantes (art. 269i) y transferencia no consentida de activos (art. 269j).

II. ANTECEDENTES

Esta ley fue antecedida de varias iniciativas legislativas hasta que finalmente se condensó en el proyecto de ley 281 de 2008 Senado, 42 y 123 de 2007 Cámara, acumulados.[3] Durante su trámite existieron al

[3] No existe información sobre las razones que se tuvieron en cuenta para conciliar los textos aprobados en la Cámara y el Senado. Solamente encontramos la siguiente frase, publicada en la *Gaceta del Congreso* 931, del 11 de diciembre de 2008: "Luego de un análisis detallado de los textos, cuya

menos dos posturas sobre el tema. Para un sector el proyecto no era necesario porque con las disposiciones actuales de la ley 599 de 2000 era suficiente para sancionar penalmente muchas de las conductas previstas en el proyecto. Para otros, los delitos informáticos sí ameritan una regulación explícita y especial para abordar correctamente el tema desde la óptica penal y para poner a tono a Colombia con el estándar internacional. No se trataba de optar por una "globalización" acrítica de delitos informáticos, sino de una "glocalización", aterrizada a la realidad colombiana, aunque, valga insistir en ello, el fenómeno de la delincuencia informática no conoce fronteras y por ello frente a un fenómeno o problema internacional no podemos pretender solucionarlo con meras respuestas locales. Se trata de un primer paso, pero como tal es insuficiente.

De conformidad con los antecedentes publicados en la *Gaceta del Congreso* se puede destacar que el proyecto buscaba, entre otras finalidades, modernizar la regulación penal colombiana a modo de quedar a tono con el Convenio sobre Cibercriminalidad suscrito en Budapest el 23 de noviembre de 2001.[4] Vale la pena traer a colación que el citado convenio se consideró necesario para

> [...] prevenir los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos, asegurando la incriminación de dichos comportamientos, como los descritos en el presente Convenio, y la

aprobación por las respectivas Plenarias presenta diferencias, hemos acordado acoger como soporte de esta nueva ley el texto aprobado por el honorable Senado de la República" (Informe de Conciliación al proyecto de ley 281 de 2008 Senado, 042 y 123 de 2007 Cámara (acumulados).

[4] Uno de los principales motivos que dieron origen al Convenio sobre Cibercriminalidad fue el de "la necesidad de llevar a cabo, con prioridad, una política penal común destinada a prevenir la criminalidad en el ciberespacio y, en particular, de hacerlo mediante la adopción de una legislación apropiada y la mejora de la cooperación internacional" (preámbulo).

> atribución de poderes suficientes para permitir una lucha eficaz contra estas infracciones penales, facilitando la detección, la investigación y la persecución, tanto a nivel nacional como internacional, y previendo algunas disposiciones materiales al objeto de una cooperación internacional rápida y fiable.[5]

Particularmente, la iniciativa aspiraba a regular los diversos atentados que se cometan contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como de su uso fraudulento.

> Se trata, en otras palabras, [de] que el ordenamiento penal colombiano se sume a las políticas penales globalizadas en materia del combate frontal contra la llamada criminalidad del ciberespacio y le brinde herramientas a la comunidad internacional para la persecución de estos flagelos; al mismo tiempo, se busca brindar una adecuada tutela jurídica a un bien jurídico de tanta trascendencia en el mundo de hoy como lo es el atinente a la protección de la información y de los datos.[6]

III. Comentarios sobre algunos tipos penales

Sin pretender realizar un análisis profundo de cada tipo penal, a continuación realizaremos algunas observaciones al respecto:

A. Delito de acceso abusivo a un sistema informático

Éste es catalogado por el profesor Ricardo Posada Maya como una forma de *intrusismo informático*, que a la vez consiste en una hipótesis de delito informático en sentido criminológico:

[5] Cfr. preámbulo del Convenio sobre Cibercriminalidad.

[6] Informe de ponencia, segundo debate del proyecto de ley 281 de 2008 Senado, 42 de 2007 Cámara, publicado en la *Gaceta del Congreso* núm. 911, del 9 de diciembre de 2008.

Por esta modalidad delictiva —en sentido general— se puede entender la conducta de arrogarse ilegalmente —de forma no autorizada— el derecho o la jurisdicción de intrusarse o "ingresar" en un sistemas informático o red de comunicación electrónica de datos, con la consecuente transgresión de las seguridades dispuestas por el *webmaster* o prestador del servicio al *webhosting* u *owner*, con el fin de proteger los servicios de transmisión, almacenamiento y procesamiento de datos que ofrece frente a posibles abusos de terceros (ingreso en cuentas de *e-mail* ajenas).[7]

El artículo 2° de la Convención sobre Cibercriminalidad lo denomina "acceso ilícito", sancionando penalmente a quien dolosamente y sin autorización acceda a todo o parte de un sistema informático. Dice la Convención que para la tipificación de este delito se podrá exigir "que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrá requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático". Luis Reyna coincide con Ricardo Posada al denominar esta conducta "intrusismo informático", consistente en

> [...] la introducción a sistemas de información o computadoras infringiendo medidas de seguridad destinadas a proteger los datos contenidos en ellas. Vemos que, aunque en ocasiones se afecten los datos computarizados o programas informáticos, ello no es determinante para la configuración del injusto, basta tan sólo el ingreso subrepticio a la información (con valor económico de empresa) para la concreción del comportamiento.[8]

[7] Posada Maya, Ricardo, "Aproximación a la criminalidad informática en Colombia", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, núm. 2, Bogotá, Universidad de los Andes, 2006, p. 23. Disponible en: http://derechoytics.uniandes.edu.co.

[8] Reyna, Luis. "El bien jurídico en el delito informático". Disponible en: http://www.alfa-redi.org/revista/data/34-14.asp.

Este delito fue inicialmente consagrado en el artículo 195 de la ley 599 de 2000. Posteriormente se modificó mediante la ley 1273 del 5 de enero de 2009, pero a los dos meses fue nuevamente "modificado" por la ley 1288 del 5 de marzo de 2009. A la fecha no sabemos de otro delito en la historia de Colombia que haya sido reformado por el Congreso tan apresuradamente y sin explicación. En la exposición de motivos de la ley 1288 no se da razón alguna para justificar tan súbito cambio. Adicionalmente anotamos que la ley 1288 de 2009 modificó un artículo que ya no existía en la regulación, pues el artículo 4° de la ley 1273 de 2009 derogó explícitamente el artículo 195 del Código Penal.

Comparemos la tipificación de esta conducta en las tres normas:

Ley 599 de 2000	Ley 1273 de 2009	Ley 1288 de 2009
Artículo 195. ***Acceso abusivo a un sistema informático.*** *El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa.*	Artículo 269a. ***Acceso abusivo a un sistema informático.*** *El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.*	Artículo 25. ***Modificación de penas para los delitos de divulgación y empleo de documentos reservados y acceso abusivo a un sistema informático.*** *[...]* Artículo 195. ***Acceso abusivo a un sistema informático.*** *El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en pena de prisión de cinco (5) a ocho (8) años.*

Como se observa, a la luz de la ley 1288 de 2009 quedó vigente la misma conducta consagrada en la ley 599 de 2000, aunque con una

pena sustancialmente mayor, consistente en prisión de cinco a ocho años. En otras palabras, la ley 1288 simplemente aumentó la pena, dejando intacta la conducta tipificada en el año 2000. La manera como fue tipificada la conducta ha sido objeto de serias y cuidadosas críticas por parte de la doctrina, razón por la cual no nos referiremos a ellas, pero sugerimos abordar este aspecto a partir del trabajo realizado por el profesor Ricardo Posada Maya.[9]

La razón del incremento de la sanción obedece, según el artículo 25 de la ley 1288, a "garantizar la reserva legal de los documentos de inteligencia y contrainteligencia y evitar su divulgación por parte de los miembros de organismos que llevan a cabo este tipo de actividades". Debemos anotar que el delito de acceso abusivo a un sistema informático no se restringe a los que contienen documentos de inteligencia y contrainteligencia. Su aplicación es amplia, abarcando cualquier sistema informático.

La ley 1273 trató de precisar más la conducta penal, sancionándola con prisión de cuatro a ocho años. Se sostuvo en el Congreso:

> El artículo 269a introduce como punible el acceso abusivo a un sistema informático, conducta criminal caracterizada porque sus autores quieren demostrarle al sistema de seguridad al que acceden, lo capaces que son de vulnerarlo; este comportamiento es, sin duda, uno de los delitos de mayor ocurrencia puesto que el pirata informático, al realizar otros comportamientos informáticos, ingresa abusivamente al sistema. En otras palabras: el actuar criminoso llevado a cabo por el sujeto activo va asociado a otras conductas punibles.[10]

[9] Cfr. Posada Maya, ob. cit., supra, nota 8, pp. 25-32.

[10] Informe de ponencia..., ídem.

En adición al aumento de la pena, los cambios que incluyó la efímera disposición legal pueden resumirse en los siguientes términos: en primer lugar, resguardaba penalmente a sistemas informáticos protegidos o no con medida de seguridad. Para las leyes 599 y 1288 el sistema informático debe estar protegido con sistema de seguridad. En este sentido, la conducta penal de la ley 1273 comprendía todo tipo de sistema informático, sin ser relevante si el mismo contaba o no con sistemas de seguridad, lo cual nos parece más apropiado que frente al escenario restringido de las precitadas leyes 599 y 1288.

En segundo término, las leyes 599 y 1288 sancionan penalmente al que se "introduzca abusivamente a un sistema informático", sin especificar cuándo ese ingreso es "abusivo". La ley 1273, en lugar de utilizar esa expresión, prefirió delimitar la conducta a acceder a un sistema "sin autorización" del titular de éste, o cuando contando con dicha autorización, quien accede al mismo se excede de lo autorizado o permitido por el titular.

B. Delito de obstaculización ilegítima de sistema informático o red de telecomunicación

Esta conducta penal quedó tipificada en el artículo 269b. Sanciona a aquel que sin estar facultado para ello "impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones". Para el legislador, dicho delito "también se conoce como ´bloqueo ilegítimo´ o ´extorsión informática´, pues el delincuente bloquea, asedia, o acorrala el sistema. Uno de los casos[11] más emblemáticos es el de los piratas

[11] Sobre casos de delitos informáticos consúltese: Kerr, Orin S, *Computer Crime Law*, 2ª edición, American Casebook Series, US, WEST, 2009.

turcos y eslovenos que tomaron como rehén la página de un equipo de fútbol colombiano, el Envigado Fútbol Club".[12]

La ley no define "sistema informático", pero si ésta se basa, aunque sea parcialmente, en el Convenio de Cibercriminalidad de 2001, podría utilizarse la definición prevista allí, según la cual el sistema informático "designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos que aseguran, en ejecución de un programa, el tratamiento automatizado de datos".[13] Lo propio sucede con la expresión "datos informáticos", que a la luz del precitado convenio hace alusión a "toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función".[14]

C. Delito de interceptación de datos informáticos

Consagrado en el artículo 269c, recalca la necesidad de que en regímenes democráticos exista una orden judicial previa al momento en el cual particulares o funcionarios del Estado procedan a interceptar sistemas informáticos para, entre otros propósitos, obtener datos informáticos. El artículo parece problemático, pues si nos atenemos rígidamente a su texto, encontramos difícil interceptar "datos informáticos", como lo dice la ley. Creemos más bien que se interceptan son sistemas de comunicación para acceder a la información circulante a través de ellos.

No obstante lo anterior, el propio Convenio de Budapest utiliza dichas expresiones en el artículo 3°, con miras a sancionar "la

[12] Informe de ponencia..., ídem.

[13] Literal a) del artículo 1° del Convenio sobre Cibercriminalidad de 2001.

[14] Literal b) del artículo 1° del Convenio sobre Cibercriminalidad de 2001.

interceptación, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos —en transmisiones no públicas— en el destino, origen, o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos".

D. Delito de daño informático

Previsto en el artículo 269d. Se trata de una especie de daño en bien ajeno tipificado en el artículo 265 del Código Penal. La particularidad radica en los bienes objeto de daño, que en este caso son los datos informáticos, o los sistemas de tratamiento de información o sus partes o componentes lógicos. Para el legislador, este delito "castiga la obstaculización grave, cometida de forma dolosa y sin autorización, contra el funcionamiento de un sistema informático, a través de la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos, o mediante la realización de esas conductas en relación con un sistema de tratamiento de información o sus partes o componentes lógicos". Una figura similar a ésta prevé el artículo 264.2 del Código Penal español de 1995, en los siguientes términos: "2) La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos. Es el caso también de quien introduzca los denominados virus informáticos a un sistema de datos".[15]

Esta nueva conducta penal es producto de la mixtura de los artículos 4° y 5° de la Convenio sobre Cibercriminalidad, donde bajo los nombres de "Atentados contra la integridad de los datos" y "Atentados contra la integridad del sistema" se procura sancionar, de una parte,

[15] Informe de ponencia..., ídem.

la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos, y de otra, *la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.*

E. Delito de uso de *software* malicioso

Incorporado a nuestra legislación penal mediante el artículo 269 de la ley 1273 de 2009. Se considera que incurre en esta conducta penal quien, "sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos".

Como puede observarse, estamos frente a otra clase especial de daño en bien ajeno que se materializa a través del uso de software creado para causar daños a sistemas informáticos. Según el legislador, con esta disposición se busca "sancionar el uso de software malicioso, conocido como *malware*, conducta que se ha generalizado en la red causando enormes daños a los usuarios; por eso se castiga a quien, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos".[16]

Un ejemplo de *software* malicioso es precisamente el "virus informático" que venimos padeciendo desde 1949 y el cual cada día se convierte en un instrumento generador de muchos perjuicios a los sistemas de información.[17]

[16] Informe de ponencia..., ídem..

[17] Un estudio detallado del tema puede consultarse en Palazzi, Pablo, "Análisis legal del accionar de un virus informático en el derecho penal argentino y comparado", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, núm. 2, Bogotá, Universidad de los Andes, 2006, pp. 61-94. Disponible en: http://derechoytics.uniandes.edu.co.

F. Delito de violación de datos personales

Consagrado por primera vez en nuestra legislación penal, en el artículo 269f. Desde la primera sentencia de la Corte Constitucional sobre el tema (T-414 del 16 de junio de 1992), dicha corporación precisó que la persona, y no el administrador del banco de datos, es el titular y propietario del dato personal.[18] Esta misma línea se mantiene en el literal a) del artículo 3° de la ley 1266 de 2008, según el cual el titular de la información es "la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de *hábeas data* y demás derechos y garantías a que se refiere la presente ley".

El operador es titular de un derecho de administración de la información. Como tal, tiene la protección que le confieren, entre otras, las normas de derechos de autor sobre bases de datos. La ley 1266 de 2008 también lo protege en la medida en que impone a los usuarios utilizar la información suministrada por el operador para los fines hacia los cuales les fue entregada. Ello significa que, entre otros, el usuario no puede, salvo autorización del operador, crear otras bases de datos o sistemas de información para ofrecerlas a terceros.

La expresión "dato personal" es definida en el literal e) del artículo 3° de la ley estatutaria 1266[19] de 2008 como "cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica". No obstante

[18] Sobre datos personales y delitos informáticos, consúltense las siguientes tesis doctorales: Gómez Navajas, Justa, "La protección penal de los datos personales: análisis típico del artículo 197.2 del Código Penal", Universidad de Granada, 2000, https://www.educacion.es/teseo/mostrarRef.do?ref=226884; Riascos Gómez, Libardo Orlando, "El derecho a la intimidad, la visión IUS informática y el delito de datos personales", Universidad de Lleida, España, 2007, http://dialnet.unirioja.es/servlet/tesis?codigo=7857.

[19] "Por la cual se dictan las disposiciones generales del *hábeas data* y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países, y se dictan otras disposiciones".

lo anterior, debe entenderse que esta definición sólo opera para el caso del dato comercial y financiero, pues la Corte Constitucional restringió su campo de aplicación. En efecto, mediante la sentencia C-1011 de 2008 la Corte Constitucional avaló la citada ley pero bajo varios entendidos, muchas aclaraciones, y declaratorias puntuales de inexequibilidad. Algunos se plasmaron en la parte resolutiva de la sentencia y otros en la motiva. Adicionalmente, mediante auto 159 del 21 de abril de 2009 la Corte Constitucional aclaró algunas partes[20] de la sentencia en comento. Un análisis de la ley debe realizarse conjuntamente con el fallo mencionado y el auto aclaratorio, pues valga la pena anticiparlo, éste modificó sustancialmente el texto de la ley.

Pese al encabezado de la ley, su objeto: "desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos" (art. 1°) y su ámbito: "La presente ley se aplica a todos los datos de información personal" (art. 2°), la Corte Constitucional aclaró a lo largo de sus considerandos que el proyecto era una regulación parcial y sectorial del derecho de hábeas data. Luego de plantear argumentos de carácter sistemático, teleológico e histórico, la Corte selló este aspecto en los siguientes términos:

> "Las consideraciones expuestas demuestran que el proyecto de ley tiene un propósito unívoco, dirigido a establecer las reglas para administración de datos de contenido financiero y crediticio"; "no puede considerarse como un régimen que regule, en su integridad, el derecho al hábeas data"; "el ámbito de protección del derecho fundamental del *hábeas data* en el proyecto de ley, se restringe a la administración de datos de índole comercial o financiera,

[20] Numerales 3.3.2 (particularmente lo atinente a los deberes de las fuentes de información [art. 8°]) y 3.6.2.

destinada al cálculo del riesgo crediticio [...] y la [información] proveniente de terceros países con idéntica naturaleza".

Tanto la Superintendencia Financiera[21] como la de Industria y Comercio[22] concluyeron en junio de 2009 que la ley 1266 de 2008 es una regulación parcial que sólo resulta aplicable a la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, es decir, a aquella concerniente al surgimiento, cumplimiento y extinción de obligaciones dinerarias necesaria para determinar el nivel de riesgo crediticio de una persona.

La ley 1273 de 2009 consagra varios delitos que guardan estrecha relación con los datos personales y resultan de interés para los operadores de bases de datos. Uno de ellos es el de la "violación de datos personales" y el otro el de "daño informático". El primero precisamente castiga a aquel que, sin estar facultado para ello, "obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes".

Anota el legislador que con esta normativa "se quiere salvaguardar el derecho protegido a la autodeterminación informativa en estrecho nexo con valores como la dignidad humana y el libre desarrollo de la personalidad, así como con otras libertades públicas como la ideológica o la de expresión".[23] Realmente no encontramos mayor relación entre los motivos de legislador y el texto aprobado, porque acá no se está protegiendo al titular del dato sino al operador de éste. Fijémonos que no se sanciona la captura ilegal del dato (sin autorización del titular

[21] Cfr. concepto 2009029082-002 del 4 de junio de 2009, de la Superintendencia Financiera.

[22] Cfr. concepto 9037876 del 12 de junio de 20089, de la Superintendencia de Industria y Comercio.

[23] Informe de ponencia..., ídem.

o de la ley) sino la toma de datos personales contenidos en archivos o bases de datos.

El legislador realiza un uso desacertado de la expresión "autodeterminación informática".[24] Ésta tiene una acepción concreta en materia de protección de datos personales. En efecto, la sentencia del Tribunal Constitucional de la República Federal de Alemania sobre la ley de censo de población, profesión y lugares de trabajo, de 1983,[25] representa un antecedente importante sobre el alcance del derecho a la "autodeterminación de la información o autodeterminación informativa".

La *autodeterminación* comprende la trilogía compuesta por la persona, sus datos personales y sus derechos constitucionales. Representa un derecho esencial que cada día cobra mayor relevancia frente al creciente uso de la información sobre las personas. Se concreta en la facultad de éstas de decidir cuándo y dentro de qué límites son públicos los asuntos de la vida personal, así como en controlar lo que sucede con sus datos personales. El libre desarrollo de la personalidad en una sociedad libre, dice la sentencia, presupone la protección de las personas frente a la ilimitada recolección, archivo, uso, retransmisión y "reciclaje" de sus datos personales.

Señala el prenombrado fallo que las condiciones actuales y futuras del procesamiento de datos ponen en peligro la autodeterminación, pues las tecnologías facilitan: 1) archivar ilimitadamente datos personales; 2) integrar dicha información con la contenida en otras bases de datos de cualquier parte del mundo; 3) revisar o consultar los datos personales en cuestión de segundos. Se suma a lo anterior la imposibilidad o dificultad de la persona para controlar tanto el uso de sus datos personales como la calidad de la información.

[24] Para la Corte Constitucional "la autodeterminación informática es la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales" (SU-82 de 1995).

[25] Ley de censo de 1983.

En Colombia esta expresión fue traída a colación por el magistrado Ciro Angarita Barón en la sentencia T-414 de 1992. Sobre el particular señaló la Corte en esa oportunidad:

> [...] la posibilidad de acumular informaciones en cantidad ilimitada, de confrontarlas y agregarlas entre sí, de hacerles un seguimiento en una memoria indefectible, de objetivizarlas y transmitirlas como mercancía en forma de cintas, rollos o discos magnéticos, por ejemplo, permite un nuevo poder de dominio social sobre el individuo, el denominado poder informático. || Como necesario contrapeso, este nuevo poder ha engendrado la *libertad informática*. Consiste ella en la facultad de disponer de la información, de preservar la propia identidad informática, es decir, de permitir, controlar o rectificar los datos concernientes a la personalidad del titular de los mismos y que, como tales, lo identifican e individualizan ante los demás. Es, como se ve, una nueva dimensión social de la libertad individual diversa, y por razón de las circunstancias que explican su aparición, de otras clásicas manifestaciones de la libertad[26] [cursivas de los autores].

G. Delito de suplantación de sitios webs para capturar datos personales

Incorporado en el artículo 269g. Para el legislador, este tipo penal sanciona el *phishing:*

> El tipo se consuma con el diseño de páginas falsas de la entidad atacada; el imputado debe registrar ese sitio falso, que en el medio se le denomina como "carnada", con un dominio similar al de la entidad. Logrado el registro del

[26] Esta jurisprudencia ha sido permanentemente ratificada por la Corte Constitucional. Recientemente lo hizo en la sentencia C-1011 de 2008, por medio de la cual se realizó control constitucional previo y automático a la ley estatutaria 1266 de 2008 (comúnmente conocida como Ley de hábeas data).

nombre de dominio se debe ubicar el alojamiento web *(hosting)*. Luego, el delincuente remite correo electrónico masivo que se conoce como *spam* (lanza la carnada) a una base de datos que seguramente ha adquirido en el mercado negro. Seguidamente, caen incautos que no diferencian fácilmente entre la página web legítima y la falsa; el afectado, ingenuamente, suministra su información e incluye datos de acceso y contraseñas bancarias que son capturados por el delincuente, quien procede a realizar las operaciones bancarias electrónicas correspondientes y ordena las transferencias a cuentas de tercero.

Estas transferencias, normalmente, las realiza mediante correos electrónicos a través de terceros que se les llaman "mulas", enviando correos de ofertas de trabajo. El objetivo es claro: captar intermediarios para recibir el dinero; y la actividad es la de recibir en su cuenta el dinero procedente de las víctimas, que luego envían al *phisher* (delincuente informático) según instrucciones.[27]

Aunque el artículo 269g se titula "Suplantación de sitios web para capturar datos personales", el tipo penal no menciona la expresión "dato personal" ni mucho menos el propósito de aprehenderlo a través de páginas electrónicas, enlaces o ventanas emergentes falsas. Realmente lo que sanciona dicha norma es su diseño, tráfico, venta, ejecución, programación y envío con fines ilícitos.

Esta disposición también castiga a quien mediante la manipulación de nombres de dominio haga ingresar a una persona a una página web diferente creyendo que está accediendo a su banco u otro sitio personal o de confianza.

Estas conductas, en últimas, se realizan en la práctica para capturar datos de las personas y utilizarlos con fines ilícitos, como cuando a alguien se le hace ingresar a la supuesta página web de su entidad

[27] Informe de ponencia..., ídem.

financiera para solicitarle actualizar sus datos o cambiar sus claves. El delincuente, luego de lo anterior, utilizará esa información obtenida ilegalmente para, entre otras, saquear las cuentas de ahorro de la persona o cargar a su tarjeta de crédito la adquisición de bienes o la prestación de servicios nunca requeridos por el verdadero titular.

H. Delito de hurto por medios informáticos y semejantes

El artículo 269i prevé un hurto especial consistente en el apoderamiento de cosa mueble ajena que se realiza superando medidas de seguridad informáticas; manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante; o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

Este delito pone de presente algo ya sabido: los mecanismos electrónicos también son utilizados para cometer infracciones penales. Acá, simplemente, se configura un tipo penal cuya especialidad radica en el medio utilizado para incurrir en hurto.

I. Delito de transferencia no consentida de activos

El artículo 269j prevé como infracción penal la realización de artificio o engaños a través de la manipulación informática con miras a lograr la transferencia no consentida de cualquier activo en perjuicio de un tercero. Igualmente, sanciona a quien *fabrique, introduzca, posea o facilite programa de computador* destinado a la realización de la conducta descrita.

Esta conducta se denomina "estafa informática"[28] en el artículo 8° de la Convención sobre Cibercriminalidad. Allí se sanciona la producción de

[28] Sobre fraudes y estafas en el contexto digital, véase: Galán Muñoz, Alfonso, *El fraude y la estafa mediante sistemas informáticos: análisis del artículo 248 C. P.*, Valencia, Tirant Lo Blanch, 2005.

un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de, entre otras, "cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero".

Según el legislador, este tipo penal "también es llamado estafa electrónica o informática en el derecho comparado, distinta, en todo caso, de la figura clásica de estafa que requiere, para su producción, de diversos elementos entre los que sobresalen la utilización de un engaño por parte del autor del delito y, por consiguiente, la producción de un error en la víctima del mismo (confróntese, artículo 246 del Código Penal". Se precisa en la exposición de motivos:

> Naturalmente, es casi imposible tipificar como una estafa clásica la conducta de quien utilizando el computador de su casa logra llevar a cabo una transferencia bancaria de la cuenta de un tercero a una de su titularidad. En este supuesto, obvio es decirlo, sí existe el ánimo de lucro, pues el estafador actúa guiado por ese afán de enriquecerse económicamente y, además, se configura el perjuicio a un tercero, puesto que se produce un detrimento económico a otra persona; no obstante, no aparecen los dos elementos anteriormente señalados: el engaño a tercero y el error, pues el autor del delito no utiliza ninguna treta ni artimaña para engañar a la víctima o para viciar la voluntad del tercero, puesto que la acción se ha producido a través de una máquina (el computador) y, como consecuencia de ello, por la misma razón, tampoco se ha producido un error.[29]

IV. Bibliografía

Congreso de la República de Colombia:

— *Gaceta del Congreso* 931, del 11 de diciembre de 2008.

— *Gaceta del Congreso* núm. 911, del 9 de diciembre de 2008.

[29] Informe de ponencia..., ídem.

GALÁN MUÑOZ, Alfonso, *El fraude y la estafa mediante sistemas informáticos: análisis del artículo 248 C. P.*, Valencia, Tirant Lo Blanch, 2005.

GÓMEZ NAVAJAS, Justa, "*La protección penal de los datos personales: análisis típico del artículo 197.2 del Código Penal*", tesis doctoral, Universidad de Granada, 2000.

ORIN S., Kerr, *Computer Crime Law*, 2ª edición, American Casebook Series, USA, WEST, 2009.

PALAZZI, Pablo, *Delitos informáticos*, Buenos Aires, AD-HOC, 2000.

—, "Análisis legal del accionar de un virus informático en el derecho penal argentino y comparado", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* núm. 2, Bogotá, Universidad de los Andes, 2006.

POSADA MAYA, Ricardo, "Aproximación a la criminalidad informática en Colombia", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* núm. 2, Bogotá, Universidad de los Andes, 2006.

REYNA, Luis, "El bien jurídico en el delito informático", en ALFA-REDI, 2007.

RIASCOS GÓMEZ, Libardo Orlando, "El derecho a la intimidad, la visión *ius* informática y el delito de datos personales", tesis doctoral, Universidad de Lleida, España, 2007.

SUPERINTENDENCIA FINANCIERA, concepto 2009029082-002 del 4 de junio de 2009.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO, concepto 9037876 del 12 de junio de 2009.

CAPÍTULO VII

EL CONCEPTO DE LA INFORMACIÓN ELECTRÓNICAMENTE ALMACENADA EN EL ORDENAMIENTO JURÍDICO COLOMBIANO: ANÁLISIS Y PROPUESTA PARA COLOMBIA

Luis Andrés Iregui Villamarín y Jeimy J. Cano M.

*Es mejor proponerse lo correcto, aunque fallemos, que proponerse lo incorrecto y acertar**

I. Introducción

El mundo vive una revolución que comenzó a mediados de los años ochenta del siglo pasado y que hoy sigue cobrando más fuerza. Ya incluso se puede decir que ha triunfado y cambiado completamente nuestras vidas en todos sus aspectos, pero a un costo que pocos reconocen. Estamos hablando de la revolución tecnológica, y el costo es el de la inseguridad jurídica que ella ha generado. Es de esperarse que una disciplina tan tradicional como el derecho no pueda evolucionar a la velocidad que han venido trayendo los cambios propios de esta revolución, pero

* Frase del Dr. Rusell Ackoff en su libro *Recreación de las corporaciones. Un diseño organizacional para el siglo XXI*, Oxford, Oxford Press, p. 10.

a medida que la tecnología se funde cada vez más íntimamente con nuestras vidas, se hace urgente que se dé esa evolución en nuestro país.

Una de las áreas más cruciales de la disciplina del derecho es la probatoria. La información delicada, crucial para establecer la realidad de los hechos, es cada día más digital que física, lo cual exige un cambio en la manera de manejar esta información y de la persona que debe manejarla. En las anteriores investigaciones se trataron ambos problemas como partes fundamentales para resolver el interrogante que ata las tres investigaciones: ¿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?[1]

La primera investigación dio una visión global de soluciones a esta pregunta y dejó claras las prácticas y estándares internacionales más avanzados e importantes que se deben exigir para que un peritaje sea considerado adecuado y aceptable al momento de ser considerado como una prueba pericial. El estudio giró alrededor de cuatro ejes caracterizados por sus avances jurídicos en el tema: la Unión Europea, Estados Unidos, Australia y Singapur.

En el caso de la Unión Europea, no hay unanimidad entre sus miembros sobre procedimientos, estándares, etc., en relación con la prueba electrónica y los métodos de recolección de ésta. Incluso en la actualidad se trata a la prueba electrónica en los Tribunales europeos de la misma manera que se hace con las pruebas tradicionales o físicas, algo inadecuado. Sin embargo, sí se encontró que la mayoría de los juristas europeos consideran que el individuo que obtiene la prueba electrónica es el elemento más importante para determinar la influencia que dicha

[1] Pimentel, Javier; Cano, Jeimy, "Consideraciones sobre el estado del arte del peritaje informático y los estándares de manipulación de pruebas electrónicas en el mundo", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, vol. III, Bogotá, Universidad de los Andes, 2007, p. 3.

prueba pueda tener en el proceso.[2] También se puede tomar como lección de la Unión Europea la importancia de que la obtención de la prueba sea hecha, o al menos supervisada, por un perito informático, al tiempo que se observen ciertas formalidades en la manera de obtener la evidencia.

Estados Unidos, por su parte, proporciona una gran cantidad de información con respecto a la paradoja entre la Cuarta Enmienda de su Constitución y la búsqueda y recolección de evidencia necesaria para adelantar la obtención de pruebas. A diferencia de Europa, Estados Unidos ha reconocido las diferencias inherentes a la prueba electrónica frente a la prueba física tradicional. Su jurisprudencia ha desarrollado conceptos como la expectativa razonable de privacidad en el mundo digital y la pérdida de control de información almacenada electrónicamente por parte del investigado.[3] Por otro lado, esta nación ha establecido ciertas buenas prácticas para la obtención de evidencia digital con el objeto de que se garanticen los derechos del investigado.

Australia hace un énfasis distinto al incluir a la víctima o afectado como un sujeto que influencia directamente en la validez de la prueba. La principal lección que deja esta nación consiste en que las organizaciones deben tener siempre buenos registros de su información electrónica para que constituyan más fácilmente una prueba válida a la luz del derecho. Además, de nuevo se pueden observar recomendaciones para llevar a cabo una recolección de evidencia electrónica exitosa.[4]

Finalmente, Singapur hace una propuesta legislativa que busca regular los archivos de computadora como evidencia. Comparativamente, esto se puede equiparar en Colombia a la ley 527 de 1999, la cual

[2] Ibídem, p. 12.

[3] Ibídem, pp. 14-15.

[4] Ibídem, p. 22.

buscaba regular este tema al darle a los documentos electrónicos la misma fuerza probatoria que los físicos.[5]

La segunda investigación entró a mirar el estado de la figura del perito informático y las calidades específicas que debe poseer. Para esta aproximación se investigó sobre: 1) los pronunciamientos y recomendaciones de organismos internacionales, 2) quién es considerado perito informático en los dos países que más han avanzado en el área (Estados Unidos y Australia) y en Colombia, y 3) cuál debe ser la formación de esta clase de peritos según Estados Unidos (de nuevo la nación que más ha avanzado en el tema) y la realidad de este asunto en el caso colombiano.[6]

La investigación encontró que varios organismos internacionales ya se han pronunciado específicamente sobre aspectos que debe obedecer quien ostente el título de perito informático. El primer tratado internacional sobre crímenes informáticos se firmó en Budapest, durante la Convención del Delito Cibernético, celebrada allí por el Consejo de Europa, en el año 2001. En su artículo 35 este convenio exige que haya un personal debidamente formado y capacitado disponible permanentemente para investigar este tipo de delitos.[7]

En ese mismo año, durante la Asamblea General de la ONU se aprobó la resolución 55/63 sobre la "lucha contra la utilización de la tecnología de la información con fines delictivos", donde se hizo mención a la necesidad de capacitar a aquellos individuos encargados de asistir a la justicia en informática y además de proveerlos con el equipo necesario para que puedan llevar a cabo sus funciones de manera adecuada. La misma ONU, a través de la resolución 56/121, pidió que los Estados

[5] Ídem.

[6] Ramírez, Ángela, "El estado del arte del peritaje informático en Colombia", segunda parte (trabajo de grado), Bogotá, Universidad de los Andes, 2008, p. 5.

[7] Ibídem, p. 6.

Miembros tomarán en cuenta lo dicho por organizaciones internacionales sobre delitos informáticos a la hora de crear políticas o leyes.[8]

De igual manera, después de las reuniones del G8 en 1996 se creó un equipo para "prevenir, investigar y procesar" crímenes directamente relacionados con la tecnología. La Interpol, durante su Sexta Conferencia Internacional sobre Ciberdelincuencia, aprobó una resolución que hace específica mención a la necesidad de una buena formación para quienes vayan a inferir directamente en la justicia cuando ésta entre en la órbita de la información digital.[9]

Considerados los desarrollos de organismos internacionales, la investigación revela que éstos son realmente vagos y carecen de precisión, razón que justifica enfocar la investigación en aquellos países que se encuentran a la vanguardia del peritaje informático, con particular énfasis en el perfil que ha de guiar a un perito informático.

Estados Unidos es el país más avanzado en el tema de estudio, lo cual ha ocurrido como consecuencia de ser a su vez el más afectado por la delincuencia informática.[10] El desarrollo académico del perfil que requiere ostentar un perito informático se puede observar de la manera más elocuente y concreta en la tesis doctoral de Larry Jay Myers. Este escrito se hizo con el fin exclusivo de crear un modelo de investigador que goce de todas las herramientas y conocimientos necesarios para asistir válida, eficaz y legalmente a la justicia. El resultado consistió en unos criterios mínimos que debe obedecer un perito informático para logar detectar, investigar y perseguir el crimen informático. Estos criterios son producto de una comprensión adecuada de la naturaleza multidimensional que tiene un delito informático, puesto que éste se

[8] Ibídem, p. 6.

[9] Ibídem, p. 8.

[10] Ibídem, pp. 10-11.

desenvuelve en las áreas de justicia penal y criminología, principios de contabilidad y revisión, operaciones y tecnología.[11] El autor explica que el perito necesita conocer debidamente la justicia penal y la criminología de su país para evitar actuar de manera que éstas puedan sospechar de la prueba o de su interpretación pericial; saber de contabilidad y revisión para estar atento a las señales de que se ha perpetuado un fraude, y obviamente tener el entrenamiento técnico necesario, lo que implica ser un experto en informática, requisito del cual depende en gran medida su credibilidad como perito o experto.[12]

En Australia el tema se ha abordado de manera similar —no exacta— al caso estadounidense; se ha dejado clara la necesidad de un perito informático para aquellos casos en donde la tecnología sea un factor determinante. Sin embargo, a diferencia de los estadounidenses, Australia enfatiza particularmente sobre el trabajo en equipo y la cooperación entre los expertos y las autoridades para armonizar el proceso.[13] Hace hincapié en la importancia de que la cooperación no se limite a las autoridades y a los expertos, como también en que los jurados, jueces y abogados tomen interés y conozcan de temas informáticos para poder situarse en posición de colaboración.

En nuestro país el único desarrollo legal del peritaje informático se puede vislumbrar en tres artículos del Código de Procedimiento Civil. En el artículo 8° se establece lo que se entiende legalmente por auxiliar de la justicia (condición de la naturaleza de un perito), el artículo 233 se refiere a la procedencia de un peritaje, y el artículo 236 habla puntualmente de un caso en donde es necesaria la presencia de informáticos forenses para efectuar un peritaje.

[11] Ibídem, p. 12.

[12] Ibídem, pp. 12-14.

[13] Ibídem, p. 15.

La definición de perito en nuestro país consta de dos partes: perito de parte y perito de oficio. En ambos casos la persona es experta en alguna área de las tecnologías de información y comunicaciones, con la diferencia de que los de oficios son servidores públicos que hacen parte del aparato estatal y por lo tanto tienen una formación especializada, además de gozar de conocimientos jurídicos intrínsecos a sus labores. En Colombia son en especial importantes como peritos de oficio los miembros de la policía judicial expertos en informática.[14]

En cuanto a acciones legislativas, nuestro país ha visto dos proyectos de ley que han tratado el tema del peritaje informático. El 49 de 2007 es un proyecto que busca definir la actividad profesional de los tecnólogos en criminalística y ciencias forenses. Sin embargo, falla al momento de darle una aproximación tecnológica necesaria a esta disciplina. Por otro lado, la nueva ley 1273 de 2009 crea en nuestro ordenamiento un nuevo bien jurídico tutelado (denominado "De la protección de la información y de los datos"), y en general actualiza la legislación colombiana frente al tema del delito informático. Finalmente, el Gobierno colombiano ha implementado un agresivo plan para promover las tecnologías de la información y comunicación, dada la urgencia de que el país tenga profesionales preparados para enfrentar los retos venideros.[15]

Una investigación realizada por el profesor Cano ha ayudado a tener una mejor idea sobre las características fundamentales que deben existir en una persona para poder ser considerada perito informático: honestidad, experiencia, formación, imparcialidad y claridad de comunicación de resultados,[16] y también enumera siete elementos que deben ser considerados para mantener la idoneidad del procedimiento forense.

[14] Ibídem, p. 17.

[15] Ibídem, pp. 17-22.

[16] Ibídem, pp. 23-24.

En cuanto a la formación que debe recibir un perito informático, como hemos visto, el país más desarrollado en la materia es Estados Unidos. Después de varios estudios, esa nación ha llegado a cuatro pilares centrales alrededor de los cuales se debe educar al perito informático. La primera es la recolección de evidencia; la segunda, la preservación de evidencia; la tercera, la presentación de evidencia; y la última, la preparación forense.[17] Estos pilares han servido igualmente para construir programas académicos encaminados a capacitar en materia de informática forense, los cuales pueden ser carreras técnicas de dos años, carreras de pregrado de cuatro años, maestrías y programas profesionales de certificación. Cada una de ellos se diferencia de los otros por su núcleo, su diversidad, o simplemente su duración, pero la gran similitud es su enfoque en informática forense.[18]

Colombia no cuenta con el desarrollo que ha tenido Estados Unidos, incluso se puede afirmar que carece de un concepto institucional de peritaje informático. Como se evidenció en la investigación, tanto el CTI como la DIJIN (las agencias de inteligencia colombianas más desarrolladas en el tema) acreditan la idoneidad de sus investigadores con base en los conocimientos adquiridos en los estudios académicos y en la experiencia que tenga el individuo en la materia. Por otro lado, a nivel de posgrados varias universidades se centran apenas en auditoría, dejando a un lado aspectos fundamentales para un perito informático como el conocimiento técnico, por ejemplo. La Policía Nacional, por su parte ofrece programas de investigación criminal con diversas características y concentraciones, pero en ninguno confluyen todos los aspectos necesarios para la formación de un buen perito informático.[19] La investigación, además, constata que el mayor problema para crear

[17] Ibídem, p. 31.

[18] Ibídem, pp. 34-37.

[19] Ibídem, pp. 37-40.

un programa adecuado se puede deber a la falta de tipos penales con relación al delito informático. Sin embargo, como se dijo, la ley 1273 de 2009 establece el marco general para esta problemática.

La extensa investigación deja como resultado una comprensiva y educada propuesta con el objetivo de esgrimir en qué debe consistir una formación adecuada para un perito informático en Colombia. La propuesta es la de crear un posgrado el cual abarque todas las disciplinas que la investigación considera fundamentales. La pedagogía debe ser tanto práctica como teórica, y fomentar siempre los principios éticos propios de un perito informático.[20]

Habiendo hecho un recuento de las investigaciones que antecedieron la presente, es preciso comenzar a desarrollar ésta. En su primera parte encontramos que se resolvió el interrogante de cómo funcionan las buenas prácticas del peritaje en aquellas naciones que más han evolucionado esta disciplina; en la segunda, se respondió quién debe ser el perito que lleve a cabo una tarea tan delicada. Entonces, resueltas estas dos inquietudes, sólo resta solucionar qué debe evaluar el perito. Finalmente, aplicando lo investigado, es preciso encontrar la fórmula para incluir el peritaje informático dentro del ordenamiento jurídico colombiano.

Hecha tal reflexión, queda claro el problema jurídico de esta investigación: ¿qué es la información electrónicamente almacenada y cómo se debe incorporar el peritaje informático al ordenamiento jurídico colombiano?

Como se ha venido planteando, el tema del peritaje informático está directamente relacionado con la evidencia que se busca esclarecer por medio de él. Es alrededor de este tipo de evidencia, entonces, que debe girar este escrito. Los anteriores estudios han hecho referencia al concepto de información electrónicamente almacenada, pero no establecen

[20] Ibídem, pp. 41-43.

completamente la dimensión del concepto. Considerando que la finalidad de los tres análisis es implementar el peritaje informático, es fundamental comprender dicha pregunta.

Para insertar exitosamente la institución conocida como peritaje informático en nuestro ordenamiento, ella debe abarcar todas las ramas del derecho, una consecuencia propia de la influencia que tiene la tecnología sobre todos los aspectos de nuestras vidas. Así, el mejor lugar para insertar el peritaje informático es el Código de Procedimiento Civil (CPC), pues todos los demás se remiten a él como fuente de derecho complementaria. En este sentido, de incorporarse en dicho código el peritaje informático puede ser útil para muchas ramas del derecho y su aplicación en la solución de controversias ser visible en un espectro más amplio.

II. Concepto de la IÉA

A. Caso Estados Unidos

En el pasado, en Estados Unidos el concepto de evidencia se dividía en dos categorías: documentos y cosas. Sin embargo, con la reforma de diciembre 1° de 2006 a las Reglas Federales de Procedimiento Civil (*Federal Rules of Civil Procedure,* o FRCP, equivalente estadounidense al Código de Procedimiento Civil de Colombia) se creó una tercera categoría, completamente autónoma tanto filosófica como tecnológicamente de las otros dos: la información electrónicamente almacenada o IEA.[21]

Esto afectó directamente la regla 34,[22] pues dicha norma gobernaba la producción de documentos y cosas, pero ahora también gobierna la

[21] Paul, George; Nearon, Bruce, *The Discovery Revolution*, American Bar Association, 2006, p. 13.

[22] Esta regla establece las normas generales y el procedimiento para la obtención de pruebas por medio de documentos, la IEA, cosas tangibles, el acceso a propiedad o tierras para su inspección u otros motivos.

nueva categoría de la IEA. La regla nos proporciona un cimiento para entender el concepto de la IEA en EE. UU., definiéndola de la siguiente manera: cualquier tipo de escritos, dibujos, gráficos, listados, fotografías, grabaciones de sonido y otra data o compilación de data que pueda ser almacenada en cualquier tipo de medio que permita obtener la información directamente o, de ser necesario, después de transformar dicha información a una forma razonablemente utilizable.

Dado que se trata de un nuevo tipo de evidencia, es necesario complementar el concepto de la IEA con otras normas. Las reglas 26 y 37 hablan de "sistemas" de información electrónica, lo cual deja campo para interpretar la IEA como algo que hace parte de diversos sistemas. Al ser reconocido también el concepto de sistemas de información y casi que equipararlo legislativamente con el de la IEA establecido en la regla 34, la "razonabilidad" de adquisición de la IEA, su tratamiento y consecuentemente su validez como prueba jurídica van a depender del sistema del cual haga parte la información.[23] El cambio fundamental radica en que el concepto de la IEA en el ordenamiento jurídico expande la evidencia de lo físico a todo lo que pueda ser considerado información en el sentido más amplio de la palabra, algo que no sólo se adecúa a la realidad actual sino que tiene la visión de considerar que en el futuro nuevas formas de información y sistemas de ella pueden y probablemente van a surgir.

Un cambio de esta magnitud tiene implicaciones en el derecho, particularmente en el procesal. Como ocurre en el caso colombiano, en Estados Unidos hay normas que dictan las maneras idóneas para la obtención y evaluación de evidencia, de tal suerte que agregar una categoría nueva e independiente de evidencia suscita preocupaciones sobre los pasos procesales que la gobiernan. Esto generó controversia

[23] Ibídem, p. 14.

cuando se aprobó la enmienda al FRCP, pero la decisión fue explicada por el Comité de Consejeros en el año 2005 utilizando tres argumentos centrales.[24]

Primero, actualmente la mayoría de los documentos que existen tienen origen digital y es casi una certeza que con el tiempo la IEA va a desplazar por completo los documentos físicos. La creación de esta categoría como algo aparte de documentos es un progreso que obedece a la realidad de la sociedad. Segundo, muchos tipos de la IEA son difíciles de conceptualizar como documentos pero tienen un valor probatorio imposible de ignorar, como ocurre por ejemplo con las bases de datos. Finalmente, definir claramente la IEA como algo independiente permite crear reglas que se le apliquen en particular, pues pueden utilizar como punto de referencia la regla 34.[25]

Incluir un tipo nuevo de evidencia implicó adaptar las normas procedimentales del ordenamiento jurídico al nuevo concepto de la IEA. Hubo tres preguntas alrededor de este concepto. Primero, ¿en qué forma debe presentarse esta evidencia?; segundo, ¿cómo se debe adaptar el ordenamiento al problema de acceso a la IEA?; finalmente, ¿qué requisitos debe cumplir la IEA para ser una prueba válida y admisible en un proceso judicial?

El problema de la forma surge en la medida en que hay tantas formas de la IEA que cada una va a ser una especie particular. Incluso por la maleabilidad de este tipo de información, en muchos casos se puede transformar la forma original a una que sea más conveniente.[26] Un ejemplo problemático puede ser la información rescatada de un disco duro sumamente dañado y que por lo tanto está fragmentada

[24] Ibídem, p. 16.

[25] Ídem.

[26] Ibídem, p. 17.

y difícilmente puede ser interpretada por el juez sin la ayuda de un experto que la reconstruya. Pero si éste debe interpretar la IEA y no comprende la forma como fue recuperada o producida, es necesario que se presente de una manera especial. Por esta razón, la regla 34 (b) establece un nuevo procedimiento para el tipo de forma como debe hacerse.

La regla 34 (b) estipula que cuando una de las partes solicita la prueba, ésta puede (y en realidad debe hacerlo siempre) especificar la forma como pretende que se produzca la prueba. Frente a esto, la contraparte puede objetar la manera, argumentando por qué no considera ser la más adecuada, y además especificar aquella que considera más idónea. Consecuentemente, salvo una orden judicial o que haya un convenio entre las partes, la forma como se presenta la IEA debe ser, según reza la regla, la más común o "razonablemente utilizable".[27] Ocurre entonces que la parte puede presentar la IEA en una sola forma, lo cual ha de hacer con mucho cuidado, pues la presentación es fundamental a la hora de apreciar la prueba.[28]

El problema de recolectar la IEA es que ésta puede estar almacenada de maneras tan diferentes que la accesibilidad a ella se compromete. En lugar de tratarse de colecciones de objetos y otros elementos físicos, la IEA puede estar dispersa y su naturaleza no es física, lo cual conlleva a que accederla amerite un tratamiento especial dentro del ordenamiento.[29] Por ejemplo, una característica de la IEA es que puede ser muy simple, o muy complicado, acceder a ella (recordemos que hace parte de un sistema y éste puede ser de una complejidad que hace casi imposible recuperar la información) y producirla como prueba. En respuesta a ese

[27] Ídem.

[28] Ídem.

[29] Ibídem, p. 21.

problema, el legislador estadounidense separó la IEA específicamente en aquella que fuera "razonablemente accesible" o aquella que "no fuera razonablemente accesible".[30]

La primera de estas dos categorías, como lo indica su nombre, no presenta mayor problema, puesto que el descubrimiento de la IEA puede llevarse a cabo de manera relativamente fácil y económica. Sin embargo, aquella IEA que sea de difícil acceso sí puede presentar problemas, por ejemplo, altos costos o manipulación indebida que comprometa la validez de la prueba. Para solucionar la cuestión, el legislador estadounidense incluyó limitaciones específicas para la IEA en la regla 26 (b) 2) del FCRP. Esta norma deja en claro que las partes pueden escoger no presentar la IEA si ésta es de difícil o costoso acceso, pero además, que la Corte puede ordenar la producción de ésta, de oficio o por solicitud de la contraparte, si ella logra fundamentar lo suficiente la necesidad de obtención de la prueba.

Finalmente, para que sea considerada como prueba válida en un proceso judicial, la IEA debe cumplir con ciertos requisitos procesales, pero al considerar la complejidad y diferencia de la IEA comparada con las otras dos categorías de evidencia, de nuevo ésta exige tratarse de manera especial. Como consecuencia se genera una incertidumbre jurídica sobre qué normas deben aplicarse a la IEA y cuáles requisitos específicos son particulares a este tipo de prueba. Aunque la respuesta a ese interrogante puede ser muy difícil de encontrar en la ley, la jurisprudencia sobre el tema ha sido sumamente clara al especificar casi que en su totalidad los requisitos para ser válida la IEA como medio probatorio.

Aunque son muy pocos los pronunciamientos jurisprudenciales sobre los requisitos para que la IEA sea admisible en un proceso, en el caso

[30] Ídem.

Lorraine vs. Safavian el juez Grimm esbozó cinco reglas para que la IEA sea admisible en una Corte estadounidense:[31]

1) ¿Tiene la tendencia de hacer más o menos probable un hecho que tenga influencia en el proceso (en otras palabras, que cumpla con el requisito de relevancia encontrado en la regla 401 del FRCP)?
2) ¿Puede el proponente demostrar que la IEA es lo que dice ser (que sea auténtica, según la regla 901)?
3) Si la IEA es ofrecida por su sustantiva veracidad, ¿puede considerarse como rumor tal como éste es definido por la regla 801 y, de ser el caso, cabe dentro de algunas de las excepciones de las reglas 803, 804 y 807?
4) ¿Es la forma de la IEA la original o un duplicado según el marco de la regla de escrito original, y de no ser el caso, hay pruebas secundarias admisibles que prueben el contenido de la IEA (reglas 1001-1008)?
5) ¿Opaca el valor probatorio de la IEA el peligro de que exista un prejuicio injusto o cualquier otro factor identificado en la regla 403, de tal manera que deba ser excluida la prueba independientemente de su relevancia en el proceso?

Las anteriores preguntas son determinantes a la hora de atar el concepto de la IEA con la realidad y la práctica del derecho procesal estadounidense. Gracias a las instrucciones del juez Grimm, actualmente es más fácil entender y conceptualizar la IEA como una prueba especial dentro de un proceso judicial, algo fundamental a la hora de evaluar el concepto de la IEA que existe en Estados Unidos.

[31] Brady, Kevin, et al., "The Sedona Conference Commentary on ESI Evidence and Admissibility", The Sedona Conference Working Group Series, marzo de 2008, p. 2.

No obstante, la sentencia del juez Grimm le brindó al ordenamiento estadounidense otras disposiciones, incluido el pronunciamiento sobre la autenticidad de la IEA. Este tema es el más delicado cuando se trata de la IEA, pues su vulnerabilidad la hace de inmediato sujeto de sospecha por parte de un juez. Una sospecha merecida, que debe quedar esclarecida. Los medios para probar la autenticidad de la prueba varían dependiendo del ejemplo (se pueden encontrar: correo electrónico, comentarios en sitios de Internet, mensajes de texto, chats y datos almacenados en computadores), pero siempre incluyen como constante el testimonio de un experto.[32] Eso demuestra que un experto en la IEA puede llegar a ser un instrumento tan conveniente, oportuno y necesario en el proceso judicial, que está ligado directamente al concepto legal de la IEA.

Como hemos visto, existe un vasto desarrollo en esta materia en Estados Unidos comparado al de la gran mayoría de los países, pero eso no implica que los juristas estadounidenses hayan logrado una inclusión comprensiva e ideal de la IEA al ordenamiento jurídico de ese país. Es válido decir que allí el desarrollo legislativo ha sido en gran medida positivo por diversas razones, pero también es acertado afirmar que la aproximación utilizada por EE. UU. al concepto de la IEA genera inseguridades jurídicas cuyas implicaciones totales están aún por verse.

La gran ventaja de la solución estadounidense es igualmente la razón de ser de sus deficiencias. Lo más interesante de la aproximación de Estados Unidos es que decidió considerar a la IEA como algo completamente nuevo y distinto a lo que se venía tratando como evidencia. El principal beneficio de esto, como lo notó el Comité de Consejeros, consiste en que la información, su forma, su medio de almacenamiento, su presentación,

[32] Brady, Kevin, "Evidentiary Issues and electronically Stored Information (ESI)" [on line] CGOC Council, Estados Unidos, 2007 [citado en septiembre de 2008], pp. 4-5. Disponible en: <URL: http://cgoc. com/files/KevinBrady_ESI.pdf>.

y casi todo aspecto de ella, puede cambiar y probablemente va a hacerlo, como ha sucedido a través de los siglos. Es decir, darle una categoría de evidencia absolutamente nueva y hacerlo de una manera tan general como ocurre en la regla 34, permite que la categoría no se vuelva obsoleta fácilmente y por lo tanto genera seguridad jurídica a largo plazo. Otra razón por la cual este cambio es positivo es la de identificar a la IEA como un medio probatorio que puede presentar mayores dificultades a la hora de producir la evidencia para ser considerada dentro de un proceso. Al tomar esto en cuenta, el legislador atacó uno de los problemas más notorios, eje de la presente investigación. Ahora bien, que su aproximación sea la más acertada está aún por verse, pero al igual que la creación de la nueva categoría discutida, parece ser que se trata de una espada de doble filo.

Los detrimentos del modelo estadounidense pueden hallarse fácilmente. Primero, como lo vieron venir quienes objetaron o criticaron la reforma al FCRP, la creación de una nueva categoría de evidencia va a afectar la gran mayoría del ordenamiento jurídico de manera inmediata. Pero, sin modificar las normas actuales relacionadas con el tema lo suficiente como para generar claridad jurídica absoluta, el beneficio de crear una categoría de evidencia moderna se enfrenta a un obstáculo tradicional: la nueva categoría no se incluyó en todas las partes necesarias del ordenamiento, lo cual —gracias a su compleja y delicada naturaleza— ha generado problemas en el manejo y presentación de la evidencia frente a las Cortes. La dimensión del cambio ha generado una incertidumbre jurídica la cual ha hecho necesario que los jueces dicten los pasos a seguir para ser la IEA admisible en un proceso.

Aunque en principio esto puede parecer una solución viable (particularmente en un sistema jurídico anglosajón), no puede ser considerada de carácter integral o final puesto que cada juez puede interpretar de manera particular la ley dependiendo de la evidencia, mas no de la ley; unificar la jurisprudencia va a ser un reto considerable dada la diversidad

de IEA existentes, sus formas y su acceso, además de las del futuro. Así, a diferencia de las otras dos categorías de evidencia, la IEA en realidad está en una especie de limbo procesal que debe ser esclarecido por la misma ley mas no por los jueces. Por otro lado, el legislador fue vago en varios aspectos procesales, lo cual se suma a la inseguridad jurídica discutida. Por ejemplo, decidió dividir la IEA por la razonabilidad del acceso a ella, pero no deja claro un juicio de razonabilidad. ¿Quién decide y con base en qué criterios qué forma de información es razonablemente accesible?

En resumen, podemos ver que en Estados Unidos el concepto de la IEA es algo nuevo y diferente de las categorías de pruebas que existían antes de la reforma al FCRP del año 2006. Tomar este camino tiene tanto beneficios como perjuicios; por un lado, crea una categoría que cubre casi cualquier tipo de información y por lo tanto es más flexible a las innovaciones tecnológicas que seguro han de llegar, pero por otro, un tipo de prueba nuevo implicó cambios extensos al derecho procesal, los cuales no han sido fáciles de digerir para muchos jueces y abogados. Esto ha generado un desarrollo jurisprudencial inteligente y necesario pero sugiere que la incertidumbre jurídica alrededor de la IEA no ha sido del todo despejada.

B. Caso Australia

Otro país líder en legislación relacionada con el peritaje informático y la IEA es Australia, siendo su modelo distinto al de Estados Unidos. Es más, podría decirse que es el opuesto. A diferencia de sus contrapartes estadounidenses, los legisladores y jueces australianos entienden la IEA como un medio probatorio que cabe dentro del parámetro de la categoría de documento. No se creó una nueva categoría, y por consiguiente, en el caso australiano no existe formalmente el concepto de la IEA. Se

puede enmarcar dentro de la definición de documento que da la ley, pero la esencia electrónica de la información exige tratarle de manera especial, algo que, si bien no lo contempla el texto de la ley, ya ha sido desarrollado extensamente por la Corte Federal de Australia. Por lo anterior, para llegar a precisar el concepto de la IEA en el sistema jurídico australiano es necesario combinar lo que establece la jurisprudencia con el concepto general de documento estipulado en el *Evidence Act* de 1995.

Al igual que Estados Unidos, Australia actualizó su ordenamiento para que se adaptara a la era digital. Con el *Evidence Act* de 1995 Australia incorporó la evidencia digital en todas sus normas, pues en el diccionario de esta ley se define "documentos" como "cualquier registro de información, incluyendo: cualquier cosa en la que haya un escrito; cualquier cosa que tenga marcas, símbolos o perforaciones que tengan sentido para una persona cualificada para interpretarlos; cualquier cosa de la cual sonidos, imágenes o escritos puedan ser reproducidos con o sin la ayuda de otra cosa; un mapa, plano dibujo o fotografía".[33] Es importante el principio de la definición, donde se le da la calidad de documento a cualquier registro de información, así que la lista que compone la definición no es taxativa. Es decir, dentro de la categoría de documentos cae, literalmente, todo tipo de información, y no se le da tratamiento especial a ninguna, algo que dificulta precisar el concepto de la IEA en la ley australiana. Es acá donde juega un papel crucial la jurisprudencia.

Por ser más antigua esta adaptación legal que la estadounidense, su desarrollo en las Cortes ha sido más extenso, incluyendo a la Corte Federal de Australia, encargada de resolver en su mayoría casos civiles

[33] Australian Legal Information Institute [on line], "Diccionario del *Evidence Act* de Australia de 1995" [citado en septiembre de 2008]. Disponible en: <URL: http://www.austlii. edu.au/au/legis/nsw/consol_ act/ea199580/sch99.html>.

y comerciales. Esta alta Corte ha expedido una considerable cantidad de jurisprudencia al respecto. Por otro lado, tanto en el campo federal como en el estatal, los altos Tribunales de Australia han expresado, de varias maneras importantes conceptos jurídicos encaminados a establecer reglas básicas aplicables a la IEA dentro del sistema legal australiano. Se puede decir que la jurisprudencia es el complemento del *Evidence Act*, y define la diferencia entre la IEA y los demás tipos de documentos.

Inicialmente, el magistrado en jefe de la Corte Federal de Australia, Michael Eric John Black, comenzó a comprender la importancia de la IEA como medio probatorio y como un instrumento para agilizar el proceso judicial. En razón de esto, redactó la nota de práctica 17, en abril de 2000, titulada "Guía para el uso de la tecnología de información en litigios civiles de cualquier modo", la cual trataba aspectos básicos y de poca trascendencia conceptual, pues fue en su mayoría una nota de recomendaciones para que se compartiera información de manera electrónica entre las partes y la Corte.[34] No se trató de una jurisprudencia comprensiva que reglamentara el manejo de información electrónica dentro del proceso como una prueba. La nota no define a la IEA como un tipo de documento aparte. Se traduce el concepto de datos electrónicos como "información que puede ser utilizada en un computador",[35] pero no se establece claramente un concepto que comprenda la idea de la IEA.

Ocho años después, esta nota de práctica ha sido modificada por la Corte Federal de Australia. Después de varios meses los magistrados se pusieron de acuerdo y en julio de 2008 publicaron la extensamente modificada 7ª revisión de la nota de práctica 17, titulada: "Manejo de documentos, descubrimiento y el uso de la tecnología en la conducta

[34] Black, Michael Eric John, "Nota de práctica 17" [on line] [citada en septiembre de 2008]. Disponible en: <URL: http://www.fedcourt.gov.au/how/practice_notes_cj17.htm>.

[35] Black, Michael Eric John, "Nota de práctica 17", Anexo C [on line] [citada en septiembre de 2008]. Disponible en: <URL: http://www.fedcourt.gov.au/how/practice_notes_cj17_annexC. htm>.

del litigio". Esta nota es acompañada por cuatro documentos más que la complementan: 1) el protocolo de manejo de documentos, 2) el protocolo avanzado de manejo de documentos, 3) el glosario, y 4) la lista de control antes de descubrir. Juntos, estos documentos conforman lo que la Corte Federal de Australia llama el juego de herramientas para el manejo de documentos, juicios y descubrimiento.[36]

Este juego de herramientas es un salto cuántico en jurisprudencia sobre la IEA como medio probatorio. Es dentro de este paquete que podemos encontrar las piezas complementarias del rompecabezas jurídico para materializar un concepto legal de la IEA como prueba electrónica.

Dentro del glosario podemos ver que se define un tipo de documento especial, el electrónico,[37] como "un documento almacenado electrónicamente". Ahora tenemos una definición que habla de almacenar electrónicamente un documento, cosa que, combinada con la definición de documento del *Evidence Act*, nos da el concepto de la IEA.

En Australia la IEA se entiende como todo registro de información que sea almacenado electrónicamente, incluyendo: cualquier elemento en el que haya un escrito; cualquier elemento que tenga marcas, símbolos o perforaciones con sentido para una persona cualificada en interpretarlos; cualquier elemento del cual sonidos, imágenes o escritos puedan ser reproducidos con o sin la ayuda de herramientas; un mapa, plano, dibujo, o una fotografía.

Del concepto establecido se pueden sacar varias conclusiones. Primero, es un concepto infinito, no impone límites para lo que puede llegar a ser la IEA. Da varios ejemplos (muchos propios de documentos físicos, no

[36] Los cuatro escritos de este *eToolkit* están disponibles en: http://www.dev. azuredemoecourt. com/etoolkit/.

[37] Corte Federal de Australia, "Glosario de la Nota de práctica 17" [on line] [citado en septiembre de 2008]. Disponible en: <URL:http://www.dev.azuredemoecourt.com/etoolkit/eTrialToolkit/FileDownload.aspx?AttachmentID=49&FileName=20080630_Glossary_ FCA_v9.pdf.

electrónicos), pero afirma que cualquier registro de información almacenado electrónicamente cabe dentro de la definición. Consiguientemente, el concepto admite las peculiaridades propias de la IEA mencionadas en el caso estadounidense, por ejemplo, su facilidad de tomar varias formas y la vulnerabilidad a manipulación. Segundo, habla sobre registros de información, lo cual alude a la naturaleza sistemática de la IEA, como se vio en el caso de Estados Unidos. Tercero, el concepto es el resultado de la combinación de jurisprudencia y ley, de tal manera que no puede ser entendido sin apreciar ambas fuentes de manera integral. Por último, al ser una subcategoría de evidencia que cabe bajo la categoría de documentos, donde quiera que la ley o la jurisprudencia mencionen esta última se entiende, en principio, que cabe la IEA como prueba admisible.

Ahora, es necesario entrar en detalle y entender cómo se utiliza el concepto de la IEA dentro del ordenamiento jurídico australiano, pues sólo así es posible analizar el verdadero alcance de la IEA en el sistema legal de ese país. Como vimos en el caso de Estados Unidos, la IEA, independientemente de su concepto legal, afronta ciertos retos a la hora de poder presentarla en un proceso. El juego de herramientas publicado por la Corte Federal de Australia ayudó a establecer importantes pautas para el papel que juega la IEA en un proceso judicial. A su vez, existe otra nota de práctica de la Corte Federal Australiana, la número 24,[38] estableciendo los parámetros legales para la recolección de pruebas que consistan total o parcialmente de la IEA. Por otro lado, hay jurisprudencia adicional que habla de la credibilidad de la IEA como prueba. Finalmente, el *Evidence Act* tiene ciertas estipulaciones con referencia directa a formas de la IEA.

Como se mencionó, el juego de herramientas de la nota de práctica

[38] Corte Federal de Australia, "Nota de práctica 24" [on line] [citado en septiembre de 2008]. Disponible en: <URL: http://www.fedcourt.gov.au/how/practice_notes_cj24.html>.

17 consiste en varios escritos elaborados por la Corte Federal australiana que deben ser entendidos de manera comprensiva y unificada. El propósito de este juego de herramientas es el de organizar y clarificar el proceso de descubrimiento de pruebas que contienen la IEA. La nota de práctica es la guía para todo el proceso, mientras que los otros documentos son complementarios pero de todas maneras importantes, pues funcionan como material de apoyo para aquella. De particular interés son la lista de control antes de descubrir, el protocolo de manejo de documentos y el glosario. De este último ya se ha hablado, y el protocolo de manejo de documentos no es otra cosa que la directriz para el descubrimiento de entre 200 y 5000 documentos electrónicos; se trata de una ayuda para el manejo de un gran volumen de ellos con el fin de hacer más eficaz el proceso sin atentar contra la integridad probatoria. Por su parte, la lista de control antes de descubrimiento contiene aspectos más importantes y relevantes para entender la aproximación australiana al concepto de la IEA.

Esta lista es una directriz que debe ser utilizada durante la conferencia antes de descubrimiento. Durante ésta, las partes se ponen de acuerdo en todos los aspectos del proceso de descubrimiento. El proceso está dividido en doce pasos: 1) introducción, 2) participantes, 3) relevancia, 4) búsqueda razonable, 5) documentos electrónicos, 6) preservación de documentos, 7) dimensión del descubrimiento, 8) programación para el descubrimiento, 9) información privilegiada, 10) contrato con proveedores de servicio, 11) protocolo de manejo de documentos, 12) firmas.

De los anteriores pasos vale la pena resaltar ciertos aspectos de algunos. Las partes o la Corte pueden elegir un experto independiente que sea participante y asesore en la conferencia. Las partes deben intercambiar únicamente información relevante a asuntos del proceso, acordar estrategias para la búsqueda y descubrimiento de documentos y listar las fuentes y documentos que consideran han de ser excluidas de la lista.

También, desarrollar una estrategia de identificación, recolección, procesamiento, análisis, revisión e intercambio de documentos electrónicos, ponerse de acuerdo en la manera como van a preservar documentos y en cómo manejar información privilegiada accidentalmente descubierta; por último, utilizar el protocolo de manejo de documentos o uno propio que sea aprobado por la Corte.[39]

Se puede inferir que la participación, cooperación y voluntad de las partes es un componente clave para el proceso de descubrimiento. La reglamentación se limita a exigirles consensos a los participantes en relación con ciertas particularidades de un proceso que contenga material probatorio electrónico. En muchas ocasiones es probable que esta aproximación resulte más eficaz, menos onerosa y desgastante. Sin embargo, en caso de que las partes no puedan ponerse de acuerdo o existan disputas la nota de práctica 17 estipula que la Corte puede diferir a mediación de un tercero o adjudicar.[40]

Pero el concepto de la IEA se extiende más allá de la evidencia misma por sus propiedades técnicas, propiciando la necesidad de un experto para poder valorar la prueba. Como respuesta a esta necesidad se actualizó la nota de práctica 24, creando la figura de experto independiente en computadores (EIC). En la nota de práctica 24 se recomienda que siempre que se vayan a evaluar computadores como evidencia esté presente un EIC.[41] Incluso si se vislumbra la presencia de la IEA como prueba, es necesario que asista un EIC cuando se la recolecte.[42] El espí-

[39] Corte Federal de Australia, "Lista de descubrimiento de la nota de práctica 17" [on line] [citado en septiembre de 2008]. Disponible en: <URL:http://www.dev.azuredemoecourt. com/etoolkit/eTrialToolkit/FileDownload.aspx?AttachmentID=46&FileName=20080630_PDC_FCA_v4.pdf>.

[40] Corte Federal de Australia, "Nota de práctica 17" [on line] [citado en septiembre de 2008]. Disponible en: <URL:http://www.dev.azuredemoecourt. com/etoolkit/eTrialToolkit/FileDownload. aspx ?AttachmentID=45&FileName=20080630_PN_FCA_v7.pdf>

[41] Byrne, Seamus; Lambert, Geoffrey, *Okay Computer*, The Australian Corporate Lawyer, 2008, p. 14.

[42] Ob. cit., nota de práctica 24.

ritu de esta recomendación es el de que el experto se comporte como una especie de traductor tecnológico, por lo cual es implícito que su formación debe incluir educación legal, aun a nivel probatorio.[43] Sin embargo, los requisitos, conocimientos y características para ser un EIC no se han establecido hasta el momento en la legislación australiana o su jurisprudencia.

Incluso antes de darse la totalidad de la revolución electrónica, los jueces australianos ya habían tocado el concepto de la IEA. Por medio de jurisprudencia de los años ochenta se estableció que, si bien la información contenida dentro de un computador era susceptible a errores a causa de los procesos de la máquina, dichos errores son la excepción y no la regla, por lo cual la IEA contenida en un computador se presume verdadera, pero admite prueba en contrario.[44] Sobre esto vale la pena anotar que se habla específicamente de computadores, mas no de la IEA en general. Sin embargo, esta presunción sigue teniendo cabida dentro del concepto de la IEA, porque no convalidar una prueba que contiene o es la IEA exige la apreciación de un perito informático, lo cual supone un gasto económico sustancial. En el caso de la IEA, se debe presumir que la información es lo que dice ser, pero no más o menos de eso. Por ser electrónica, la información no debe ser tratada de manera preferente o de manera inferior, sino como una prueba con validez y relevancia específicas para el proceso que puede ser refutada.

Finalmente, el *Evidence Act* de 1995 contiene referencias precisas a la IEA, aunque en ocasiones toma una aproximación demasiado taxativa. Por ejemplo, aunque habla de manera general sobre documentos que puedan ser obtenidos porque un aparato los reproduce (verbigracia,

[43] Byrne, ob. cit., p. 16.

[44] Brereton, Paul Le Gay, "Evidence In Civil Proceedings: An Australian Perspective on Documentary and Electronic Evidence", Informe 26 de la Comisión de Reforma Legal de Australia, vol. 1. Disponible en: URL:http://www.lawlink.nsw.gov.au/lawlink/Supreme_ Court/ll_sc.nsf/pages/SCO_brereton0907>.

impresiones de registros electrónicos), en ocasiones se refiere al correo electrónico como si fuera la única manera de transmisión de datos electrónica, algo que resulta incongruente con la realidad.[45]

Con el concepto de la IEA en el ordenamiento jurídico australiano, sus alcances legales y el trato que se le ha dado, podemos entrar a analizar tanto los beneficios como los detrimentos del modelo australiano.

Las ventajas del modelo australiano son su generalización y su especificidad, aunque suene contradictorio. En general, podemos apreciar que en Australia la IEA es considerada dentro de una categoría de evidencia extensa y casi que sin límites, algo que, como se vio en el modelo estadounidense, es sumamente importante para que la legislación no quede obsoleta. De igual manera, al incluir la IEA dentro de una categoría existente y no crear otra de evidencia distinta, como ocurrió en el caso estadounidense, el papel de la IEA no debe ser de nuevo definido paso por paso, pues se entiende que cabe dentro de los parámetros normativos existentes. Así, genera mayor seguridad jurídica para un proceso donde se maneja la IEA, ya que los procedimientos deben ser especiales, más no conceptualmente diferentes. Por otro lado, ha logrado ser bastante específico, particularmente cuando de la jurisprudencia se trata.

A diferencia de Estados Unidos, Australia tiene una posición unificada y clara frente al tema de cómo manejar la IEA dentro de un proceso. La Corte Federal de Australia creó unas guías basadas en la cooperación de las partes, de tal manera que los litigantes se vigilan y agilizan el proceso de descubrimiento de pruebas, tomando siempre en cuenta las pautas establecidas por la Corte para que la evidencia no tenga problema cuando vaya a ser presentada en el proceso. Además, tenemos la presunción de validez de la información derivada de computadores, dejando claro

[45] Comisión de Reforma Legal de Australia, "Revisión del *Evidence Act* de 1995", Informe 28 [on line] [citado en octubre de 2008]. Disponible en: <URL: http://www.austlii.edu. au/au/other/alrc/publications/issues/28/>.

dónde debe recaer la carga probatoria cuando se ataque la veracidad o validez de una prueba. Otra nota positiva es el reconocimiento de la esencia técnica de la IEA. El modelo australiano no ignora la necesidad de un experto que interprete y sirva de traductor técnico de la IEA cuando ésta hace parte de un proceso judicial. Gracias a ese reconocimiento se creó la figura del EIC y, como vimos en la nota de práctica 24, esta figura no es meramente voluntaria, pues en casos que lo ameriten es necesaria.

Pero el modelo australiano no es perfecto y demuestra lo complicado que es para un ordenamiento jurídico tradicional, así sea de *common law*, asimilar la IEA como tipo de evidencia. En primer lugar, las notas de práctica son de carácter optativo y sirven como guías conceptuales, pero depende de la voluntad de las partes para que la parte procesal se desarrolle de acuerdo a lo estipulado en ellas. Esto es así en la medida en que, si se aprecian los procedimientos propuestos en las notas de práctica, es notable que la mayoría requiere de un consenso entre las partes. Por otro lado, las mismas notas de práctica son un avance jurisprudencial y sugestivo, mas no normativo e imperativo. Es decir, consideran de manera integral varios atributos de la IEA y proponen reglas especiales para este tipo de evidencia —por lo que seguir esas recomendaciones facilita la validez de la prueba— pero no seguirlas no acarrea sanción alguna. Si bien es una solución viable, también es vulnerable a estrategias legales de las partes que tropiecen en el proceso, particularmente si existe fuerte animosidad entre ellas. Por otro lado, la nota de práctica 24 ata al perito informático (en la forma de un EIC) al concepto de la IEA de manera jurídica, pero no lo hace con suficientes criterios. Dicha nota habla de la participación activa e importante de un EIC, pero no define qué requisitos debe cumplir este experto; se puede presumir que debe tener un nivel de entrenamiento técnico y legal propio de su tarea, mas al no dejar estipulados los requisitos o el perfil específico que ha de cum-

plir, su funcionalidad peligra, pues la definición de EIC es muy abstracta. Finalmente, la ley australiana puede llegar a ser demasiado específica en el trato de la IEA en algunas ocasiones. Es posible que esto sea a causa de una falta de comprensión técnica o un simple descuido por parte del legislador, pero en ocasiones la ley hace referencias incompletas a formas de la IEA.

En conclusión, podemos apreciar que en Australia el desarrollo del concepto de la IEA se ha llevado a cabo utilizando varios instrumentos y, particularmente, se le ha dado un papel importante a la jurisprudencia para guiar al mundo jurídico en cuanto al manejo y definiciones de la IEA. Vale la pena resaltar que la aproximación está muy centrada en la cooperación de las partes, en su mutuo acuerdo para agilizar el proceso y en que ellos mismos decidan cómo van a manejar la IEA dentro del proceso, algo que debe ser ratificado por el juez. Lo que acontece es que, si se da el acuerdo, la IEA va a gozar de una credibilidad y eficacia probatoria que las partes y el juez ya han aceptado y por lo tanto la controversia sobre la IEA se minimiza o desaparece. Sin embargo, no se propone claramente un procedimiento para el manejo de la prueba electrónica en el caso de no haber un acuerdo entre las partes. Esto es, se trata de una situación bipolar, en la cual si existe acuerdo entre las partes no hay problema (al menos en esa instancia del proceso, pues también puede ocurrir que las partes acuerden un manejo de la IEA indebido y se comprometa la validez de la prueba), pero si no hay acuerdo se abre campo la inseguridad jurídica. Por otro lado, en Australia ya se incluyó el papel de un experto perito en el concepto de la IEA; sin embargo, no se hace de manera integral, no hay claridad sobre lo que debe saber y las experticias que debe poseer una persona para ser considerada EIC.

C. Concepto de la IEA y sus elementos

Ahora que hay dos puntos de referencia específicos, cada uno con elementos particulares, podemos utilizar sus beneficios y desventajas para crear una lista de elementos del concepto de la IEA y a partir de éstos producir uno más completo que case las benevolencias de los modelos estudiados al tiempo que aprenda de sus fallas e intente resolverlas. Comencemos con una breve lista de los elementos comunes a ambos modelos.

En los dos casos tenemos un elemento de alcance de la IEA cuyo eje es la generalidad. Tanto el concepto estadounidense como el australiano buscan ser lo más amplios posible para quedar blindados frente a nuevos desarrollos tecnológicos. Por lo tanto, el crear un concepto de la IEA tiene que tomar en cuenta el largo alcance que ambos modelos legales proponen. La manera en que lo dicen es distinto, pues los estadounidenses han creado una definición nueva, mientras que los australianos echan mano de su muy amplia definición de documento.

El extenso alcance del anterior elemento promueve la necesidad de que el ordenamiento jurídico comprenda su dimensión. Para lograrlo, se debe considerar la heterogeneidad de formas que puede tomar la IEA. Entender esa necesidad en Colombia puede lograrse haciendo referencia al caso de Singapur, que se encuentra en una de las investigaciones complementarias a la presente.

Ahora pasemos al elemento categórico, es decir, en qué categoría de evidencia cabe la IEA dentro del ordenamiento jurídico. La diferencia de raíz más importante entre los dos conceptos es que para los estadounidenses la IEA es tan diferente a los otros tipos de prueba, que amerita su propio grupo de evidencia. mientras que los australianos consideran que la IEA es una prueba documental pero requiere de disposiciones especiales por su naturaleza electrónica. La ventaja del primer modelo

es que se reconoce la especialidad de la prueba y exige la creación de procedimientos especiales para la IEA, de tal suerte que el desarrollo es de ceros y le permite al legislador crear algo, concebido teniendo en cuenta las características de la IEA. En el caso australiano, el elemento categórico de la IEA es especial mas no enteramente nuevo, pues la IEA pertenece a una categoría de evidencia existente. El beneficio radica en que, al no crear una nueva categoría, no es necesario entrar a adaptar el ordenamiento jurídico completo. La dicotomía se puede resumir de la siguiente manera: el elemento categórico en el concepto estadounidense exige que el ordenamiento sea adaptado al concepto, mientras que en el caso australiano el concepto se acomoda al ordenamiento.

Para establecer cómo categorizar la IEA en el caso colombiano es necesario tomar en cuenta ambas posiciones desde la óptica de un ordenamiento jurídico civil-continental y no uno que sea de *common law*, como es el caso de los dos países estudiados. El concepto estadounidense parece, en principio, ser el más adecuado para el caso colombiano, por varias razones.

Primero, si en Colombia el concepto de la IEA se categoriza como una especie de prueba distinta a cualquier otra, el legislador puede crearlo con una visión legal más específica, de tal manera que se pueden escribir las leyes suplementarias necesarias (como procedimientos especiales, la obligación de que participe un EIC, etc.), así como modificar leyes existentes. La ventaja es que se retoca la modernidad del ordenamiento por medio de leyes especiales, permitiendo atender la especialidad de la IEA con una fuerza legal indiscutible.

Segundo, adoptar la conceptualización australiana llevaría a que en algún momento las leyes antiguas creadas para evidencia distinta a la electrónica no puedan acomodarse a las particularidades de la IEA, causando sorpresas normativas que, si bien pueden ser resueltas de manera más eficiente en sistemas anglosajones, donde la jurisprudencia crea un

precedente legal, en nuestro sistema no pueden ser igualmente resueltas por la jurisprudencia. Cada una de dichas sorpresas requeriría una intervención directa del legislador, algo que resulta impráctico y demasiado lento.

Dicho lo anterior, sería inconveniente continuar sin mencionar que es importante seguir el ejemplo estadounidense tomando en cuenta sus deficiencias. Como se recalcó en su momento, el ordenamiento estadounidense carece de la suficiente claridad normativa para que funcione adecuadamente su concepto de la IEA. Además, llevar la nueva categoría al extremo de ser tratada como algo casi "fuera de este mundo" llevaría a que la cantidad de legislación nueva necesaria sea abrumadora, lo cual hace imposible el proyecto desde una perspectiva pragmática en un sistema civilista como el colombiano.

Esto nos presenta un problema paradójico: la IEA debe categorizarse como algo totalmente nuevo por sus características, pero debe también poder ser entendida dentro del sistema legal colombiano existente. En consecuencia, la mejor aproximación ha de ser una mixta. Tomando en cuenta el caso australiano y sus beneficios, es posible lograr que el concepto de la IEA sea una categoría nueva pero complementaria. Es decir, se limita a darle un estatus especial a la IEA como prueba (por especial no debe entenderse de ningún modo preferencial) al tiempo que se apropia de normas para otros tipos de evidencia (en particular la prueba documental) para lograr la máxima asociación posible entre lo nuevo y lo viejo.

Una mejor conceptualización del elemento categórico de la IEA puede ser la de verla como un tipo nuevo de evidencia pero atada a las normas vigentes para otras categorías de ésta. Si bien su complejidad y susceptibilidad a manipulación indebida exige crearse nuevas normas y una solución específica al problema, no hay que ser radical y dejar de lado todo el ordenamiento jurídico colombiano.

Comprender el elemento categórico utilizando una aproximación mixta permite, además, que sea más fácil casar el peritaje informático con la IEA, pues ésta requiere una legislación particular, diseñada o enmendada para atender los obstáculos que surgen durante su producción, descubrimiento y manipulación. Ocurre entonces que se pueden escribir normas basadas en los elementos de la IEA y en el papel desempeñado por el peritaje informático, además de poder hacerse alusión a normas existentes que pueden aplicarse a ella.

Tenemos también el elemento procesal. Hay dos aproximaciones, una que depende de la participación cooperativa de las partes y otra que exige regulación normativa. En ambos conceptos las partes tienen un papel diferente. Mientras que en el caso estadounidense se entiende que el juez se encarga de llevar el proceso de la mano, en Australia las partes juegan un papel fundamental.

La ventaja de que sean los directamente interesados quienes impulsen el manejo de la IEA en el proceso es la de haber mayor confianza y menos controversia probatoria, lo cual agiliza el proceso. Aunque esto puede ser cierto para cualquier tipo de prueba, si se trata de la IEA un consenso de las partes puede evitar un desgaste económico y significaría una reducción considerable en la duración del proceso. Sin embargo, pensar que ese va a ser siempre el caso es ingenuo, pues si existe un conflicto entre las partes es posible que haya animosidad y desconfianza, lo que complicaría un arreglo para manejar la IEA. En Australia no se deja claro qué ocurre cuando no hay consenso, por lo cual la IEA queda relegada a las mismas normas de las otras pruebas documentales, derrotando el trato especial que se le da.

Es importante que el elemento procesal incluya tanto una posibilidad activa de los interesados para fomentar la celeridad del litigio, como una clara estipulación sobre lo que ocurre si las partes no llegan a un arreglo. No obstante, si el elemento procesal se basa en la aplicación

de normas, no se debe caer en el error estadounidense: un juez no debe verse obligado a dar una guía basada en interrogantes para que los abogados, e incluso otros jueces, entiendan cómo aplicarle las normas procesales a la IEA.

En virtud de encontrarnos en un país de tradición civilista, el elemento procesal dentro del concepto de la IEA ha de ser uno que se rija por la aplicación de otras normas, mas no por la cooperación de las partes. Dicho esto, la cooperación de las partes tampoco puede ser ignorada.

Las normas que rijan al manejo de la IEA dentro de un proceso requieren encontrarse en parte basadas en los principios y las buenas prácticas del peritaje informático, pues de lo contrario no podrían sustentar el trato especial que se le da a este tipo de evidencia. Incluso dentro de un proceso judicial, con funcionarios estatales imparciales haciendo de responsables del manejo de la información, es necesario considerar guías de manipulación de evidencia que consista total o parcialmente de la IEA.

Un elemento adicional del concepto de la IEA es la carga probatoria. Ésta, en los dos países estudiados, recae sobre quien quiera desvirtuarla. Los australianos lo dejan tajantemente claro en la jurisprudencia, y en el caso estadounidense podemos ver que se aborda el problema desde la perspectiva de la accesibilidad, lo cual de por sí puede llegar a ser problemático, como se discutirá cuando se trate ese elemento. En este caso parecería más apropiado adoptar la perspectiva australiana para él, ya que si la carga probatoria recae sobre quien aporta las pruebas se obstaculiza en razón de su medio, mas no de la relevancia con los hechos. Es decir, se daría una especie de discriminación legal de la IEA frente a otros tipos de evidencia. También podemos hacer alusión a los argumentos de la Corte Federal de Australia en donde se establece que resulta más congruente con la realidad y más eficiente para el proceso

(tanto en tiempo como en dinero) que la prueba derivada de un almacenaje electrónico se presuma como verdadera.

Esta estrategia lleva a depender más del peritaje informático para que la IEA sea exitosamente asimilada por la ley colombiana. Para desvirtuar una prueba que contenga o sea completamente la IEA, se convierte en requisito la intervención de un perito experto, pues por su esencia técnica es muy complicado determinar la absoluta veracidad de una prueba basada en la IEA sin su intervención. Así, en cuanto a la carga de la prueba, quien decida atacarla es quien debe probar, utilizando un EIC, que no es idónea.

Finalmente, tenemos dos elementos íntimamente ligados el uno con el otro: el EIC y la accesibilidad. Debido a su naturaleza técnica y virtual, la accesibilidad a la IEA para poder producirla en un proceso como prueba es un tema delicado. De acuerdo con el modelo australiano, tan delicado que amerita el estar presente un EIC. Los estadounidenses reconocen el problema de accesibilidad, el cual puede ser razonable o no. Lo complicado es que no se definió un juicio de razonabilidad y, peor aún, no queda claro quién deba hacerlo. Es aquí donde juega un papel central el elemento de un EIC, presente en la jurisprudencia australiana. Un EIC bien entrenado, con los conocimientos suficientes, puede ser el individuo idóneo para solucionar el problema que presenta el elemento de accesibilidad.

En este orden de ideas, confluiría el elemento de accesibilidad con el de EIC, pues el efecto que pueda tener el primero sobre el proceso queda sujeto a lo que el segundo encuentre en un peritaje o dando su opinión como experto. Encontramos entonces un punto de encuentro entre el concepto de la IEA y una figura externa que debe entrar a jugar un papel importante en validar la IEA como prueba. Es por eso indispensable que una figura parecida al EIC se dé en Colombia para lograr abordar adecuadamente los retos probatorios propuestos por la IEA. Esta figura se puede denominar perito informático.

Tomando en cuenta todo lo anterior, y particularmente que el concepto de la IEA que busca producir el presente escrito está encaminado a ser utilizado en un sistema jurídico como el colombiano, ha llegado el momento de proponer puntualmente cómo deberían ser implementados los elementos mencionados con el fin de crear un concepto de la IEA para el caso de Colombia.

Primero, el elemento del alcance de la IEA debe buscar blindarse contra nuevas tecnologías que se desarrollan todos los días y que producirán a su vez nuevos e imprevisibles tipos de la IEA; es decir, tener un alcance amplio, flexible, para no quedar obsoleto. Por esto la IEA ha de tener el alcance de ser cualquier elemento que pueda ser almacenado electrónicamente, lo cual a su vez causa un problema por su generalidad. Es frustrante y demasiado usual encontrar que las normas son demasiado generales y, aunque en este caso el rasgo abstracto es necesario, éste puede ser ejemplificado para encontrar un tipo de equilibrio.

Segundo, el elemento categórico debe incluir las bondades de los modelos estudiados y tomar en cuenta sus deficiencias. Por lo tanto, es necesario entenderlo como una categoría de evidencia nueva, pero que eso no implique no poder interpretar normas antiguas para la nueva categoría. No es impensable que ciertas disposiciones, procesos y consideraciones que le son aplicables a otros tipos de evidencia lo sean también para la IEA. Sin embargo, la naturaleza técnica y especial de ésta amerita una nueva categoría de evidencia, pues sólo así se puede blindar el legislador contra el futuro.

Tercero, el elemento procesal requiere ser establecido por medio de nuevas normas; no obstante, en lo posible, puede utilizar normas ya existentes. La idea es que no haya lugar a dudas sobre cómo manejar pruebas basadas en la IEA, pero que esto no se dé a costo de un trauma al ordenamiento en general, de tal suerte que minimice la cantidad de

legislación creada, modificada o derogada. La cooperación de las partes es algo bienvenido y recompensado, mas no el principal motor procesal.

Cuarto, la carga de la prueba ha de estar siempre a cargo de la parte que quiere desafiar la veracidad de la prueba. De lo contrario, el obstáculo de la parte que desea aportar la prueba puede resultar muy difícil de superar y costoso. De igual manera, se debe enfatizar la necesidad de un perito informático como requisito para refutar la validez de la prueba.

Finalmente, debido al sensible elemento de la accesibilidad a la IEA, es imprescindible incorporar un elemento subjetivo en la persona de un EIC, el cual puede ser denominado perito informático, quien debe tener conocimientos especiales y formación técnica. Este individuo asesora al juez y actúa como traductor técnico durante el proceso para que él siempre tome decisiones con base en la mejor información disponible, no sólo en la que pueda entender inmediatamente.

Ahora, decidido el modelo que debe seguir cada elemento, es posible redactar un concepto específico de la IEA para Colombia.

La IEA es cualquier información almacenada electrónicamente, pero cuando entra en el mundo de lo jurídico es distinta a los otros tipos de evidencia por su compleja naturaleza técnica y sus singulares características. Para lidiar con los retos que presenta se requiere desarrollar una nueva aproximación procesal, sea por la creación, modificación o derogación de normas, pero ésta debe darle campo al consenso de las partes sobre cómo manejar la IEA en un proceso. La carga probatoria para refutar una prueba que sea la IEA recae sobre quien la ataca y su veracidad sólo puede ser establecida por un perito informático. En cualquier caso, la IEA es útil para el proceso únicamente cuando es comprendida por todos los sujetos procesales, por lo cual es indispensable que un perito informático esté presente siempre que haya manipulación de la IEA como prueba. Dicho perito debe considerarse como algo intrínseco de la IEA y por lo tanto sus

características, conocimientos y formación precisan de estar claramente dictaminadas en algún lugar del ordenamiento jurídico.

III. El peritaje informático desde la óptica del concepto de la IEA

Para lograr adaptar el concepto de la IEA y sus elementos al ordenamiento colombiano, antes debemos enmarcarlo en el mundo del peritaje informático, para que ambos se complementen y funcionen en armonía. Utilizando esta estrategia, se incorpora el elemento técnico (el peritaje informático) al concepto legal abstracto (el concepto de la IEA). Una estrategia adecuada para cumplir dicha meta es diseccionar una vez más el concepto de la IEA, elemento por elemento, y aplicarle lo aprendido sobre peritaje informático según la investigación hecha por Cano y Pimentel anteriormente citada, titulada: "Consideraciones del estado del arte del peritaje informático y los estándares de manipulación de las pruebas digitales del mundo".

Comencemos entonces por el elemento del alcance. En el concepto establecido, uno de los propósitos era el de que quedara blindado contra la rápida evolución tecnológica, lo que se tradujo en un alcance amplio y general. Incluso demasiado, pues genera incertidumbre jurídica para muchos que no estén del todo familiarizadas con la IEA. Además, cuando se tiene en cuenta al peritaje informático, es más importante aún dar alguna indicación, aunque sea enunciativa, toda vez que "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".[46] Por eso mismo es necesario guiar de alguna manera a los sujetos procesales y al mismo juez.

[46] Cano, Jeimy, *Evidencia digital: conceptos y retos*. GECTI, Bogotá, Legis, 2005, p. 186.

Una posible solución puede apreciarse en las recomendaciones de la Academia de Leyes de Singapur, citadas por Cano y Pimentel, donde se sugiere crear una lista meramente enunciativa de los casos más frecuentes de la IEA para que sean indudablemente admisibles.[47] Es importante mencionar que dicha lista no puede ceñirse a la IEA presente en computadores, pues si bien es común, existe un sinfín de posibilidades, ahora y en el futuro, que no los incluyen. Ésta es la lógica que lleva a obedecer el principio de neutralidad tecnológica expuesto en Singapur. Dicho principio establece que el legislador ha de abstenerse de favorecer una tecnología sobre las otras,[48] de tal suerte que la fuerza probatoria de alguna sea mayor que las otras, incluso mayor a documentos o cosas tradicionales.

En consecuencia, para que el concepto de la IEA pueda ser digerido más fácilmente, la norma debe incluir una lista que aprecie varias tecnologías y sirva de ejemplo para los casos más comunes, siempre dejando claro que se trata de una lista meramente enunciativa. La selección de dichas tecnologías debe ser hecha exclusivamente por el legislador después de estudios adecuados, y en todo momento teniendo presente el principio de neutralidad tecnológica. También es fundamental que tenga visión al elegir las tecnologías, con una visión del futuro a corto, mediano y largo plazo. Sin embargo, al final de esta investigación se dará una sugerencia sobre la posible redacción de una norma que defina precisamente qué es la IEA dentro del Código de Procedimiento Civil y sugiera los tipos de la IEA más comunes como medio probatorio.

Esto nos lleva al segundo elemento, el categórico. Adaptarlo a las buenas prácticas del peritaje informático resulta congruente con el proceso utilizado para el elemento de alcance. Es decir, al ser una categoría nueva,

[47] Pimentel, ob. cit., p. 19.

[48] Ídem.

son necesarios nuevas normas que dejen claros los pasos del procedimiento requeridos por dicha prueba. No obstante, como estamos buscando una aproximación que mezcla la nueva categoría con las viejas normas, la regla no debe ser redactar nuevas normas. Por el contrario, sin sacrificar la compleja esencia de la IEA como prueba, se debe intentar utilizar lo que ya está escrito. Ésta es la parte más difícil del proceso, pues exige adaptar el peritaje informático al caso colombiano basándose en un concepto de la IEA que de por sí es ajeno a la ley. Afortunadamente, podemos utilizar la investigación citada para establecer cómo el concepto de la IEA es compatible con el peritaje informático.

Según Cano y Pimentel, "la mayoría de los estándares revisados buscan dictar ciertas pautas a los investigadores y peritos para que logren maximizar la posibilidad de éxito de sus búsquedas y para que logren la admisibilidad del material probatorio recolectado". Por lo tanto, las normas que complementen el concepto de la IEA deben dejar como obligatorios los estándares que se ha comprobado aportan a la credibilidad de la IEA en un proceso judicial. Además, utilizando lo establecido en la investigación realizada por Ramírez es posible llegar a redactar una propuesta de artículo que describa los requisitos exigidos a un individuo para ser considerado perito informático.

Lo anterior está íntimamente ligado al elemento procesal, pues lograr unos textos que, por un lado, propongan ciertas pautas básicas para el peritaje y, por el otro, unos mínimos para poder considerar a un individuo perito informático, ataca dos problemas claves en el ámbito procesal. Éstos son los dos pasos procesales más importantes, pues es él quien hace que el abstracto y general concepto de la IEA pueda ser puntualizado en la realidad y así otorgarle un verdadero valor probatorio a la compleja prueba.

Entender el elemento de la carga de la prueba desde la óptica del peritaje informático se puede ver como una reacción legal a las reali-

dades de la IEA. La presunción de que ésta es lo que dice ser, es una reacción a la influencia del peritaje informático; es en parte consecuencia de la obligación de no darle una ventaja procesal considerable a quien objete la prueba. Como lo anotó la Corte Federal australiana, si aquel que presenta la IEA se ve obligado a probar su veracidad cuando la contraparte la cuestione, entonces quien presente una prueba con base en la IEA deberá asumir la responsabilidad de probarla, en lugar de ser el retador quien se vea en la obligación de desvirtuar la evidencia.[49]

Por ejemplo, si una persona puede probar la hora y fecha de una comunicación utilizando un correo electrónico, éste sería atacado por la contraparte para generarle costos, lo cual constituye una ventaja procesal sin sentido. Como consecuencia, el requerimiento de un peritaje informático afecta la carga de la prueba en el caso de la IEA, pues la dimensión del obstáculo que esto puede llegar a ser es suficiente motivo para que la contraparte ataque su veracidad, bien sea porque en realidad sospecha de la IEA, o porque sabe que puede perjudicar a su contrincante.

Lo anterior de ninguna manera se ajusta al espíritu de justicia con base en los hechos y la realidad que se promueve en casi todo sistema legal del planeta, pues se trata apenas de una ventaja procesal explotable sin justificación. Es apenas lógico entonces establecer que la carga de la prueba esté en manos del retador y éste debe ser quien asuma los costos.

Finalmente, tenemos el elemento del EIC (cuyo propósito, como se mencionó con anterioridad, es comprender el complejo elemento de accesibilidad que caracteriza a la IEA), lo que de nuevo hace alusión a la figura del perito informático. Para lograr que un EIC sea un perito debemos primero resaltar que si bien la figura es importante, es demasiado limitada.

[49] Brereton, ob. cit.

Que el experto sea independiente está bien, pero que sea sólo experto en computadores, no. Muchas veces el perito informático será un experto en computadores, pero habrá otras ocasiones, previsibles e imposibles de imaginar, que van a requerir de un experto en tecnologías distintas a éstos. Es clave volver a enfatizar lo importante de entender que la IEA es más que datos digitales en un computador y puede tomar muchas formas.

Como lo propone el profesor Cano, el perito informático "debe ser 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".[50] O sea que la figura de EIC debe ser traducida a un perito informático independiente (PII), el cual puede ser un experto especialista en una área relevante a la IEA, no un experto general. Para ponerlo de otra manera, el PII debe ser el género y el EIC la especie; se trata de un perito informático independiente especializado en temas de tecnologías de información. También, haber un perito informático experto en temas como redes, equipos inalámbricos, sistemas operativos, los cuales son otras especies de PII. Utilizando esta lógica para la nueva institución jurídica, se deriva el haber armonía con el elemento de alcance, tan importante para el concepto que estamos desarrollando.

IV. La IEA en el Código de Procedimiento Civil de Colombia

La razón de ser del presente escrito es establecer dónde enmarcar adecuadamente el peritaje informático, y en consecuencia la IEA, en el Código de Procedimiento Civil (CPC), pues se entiende que el concepto no existe en este contexto. Eso no implica que el ordenamiento de nues-

[50] Cano, Jeimy, "Estado del arte del peritaje informático en Latinoamérica", en *Alfa-Redi* [citado en octubre de 2008]. Disponible en: <URL: www.alfa-redi.org>.

tro país esté completamente atrasado en materia de evidencia de índole electrónica, pues existe normatividad explícitamente encaminada a resolver el problema de la evidencia electrónica en procesos civiles. Pero ese desarrollo es sumamente frágil, y en general se puede afirmar que la columna vertebral de él es la ley 527 de 1999.

Lo más característico de la ley 527 de 1999 es que regula el valor probatorio de los mensajes de datos. Se trata de la primera aproximación seria del ordenamiento jurídico colombiano a la evidencia electrónica en casos civiles o comerciales. Este último tipo de casos se consideró como la verdadera raíz de la ley, pues,

> [...] sigue los lineamientos del proyecto tipo de la Ley modelo sobre comercio electrónico, de la Comisión de las Naciones Unidas para el Desarrollo del Derecho Mercantil Internacional —CNUDMI—, y la intención de esta Comisión fue la de promover la gestación de un proyecto de ley tipo en materia de comercio electrónico, inspirada en la convicción de que al dotársele de fundamento y respaldo jurídicos, se estimularía el uso de los mensajes de datos y del correo electrónico para el comercio, al hacerlos confiables y seguros, repercutiendo así necesariamente en la expansión del comercio internacional ya que trae consigo ventajas comparativas por su velocidad y acercamiento de las relaciones entre comerciantes y usuarios de bienes y servicios.[51]

Incluso la jurisprudencia establece que esta ley fue, en principio, de índole comercial, como lo estipuló el magistrado Fabio Morón Díaz en la sentencia C-662 de 2000, donde opina que la ley 527, obedece a la necesidad de que existiese en la legislación colombiana un régimen jurídico consonante con las nuevas realidades en que se desarrollan las comunicaciones

[51] Certain, Andrés; Cano, Jeimy; González, José, "Evidencia digital: contexto, situación e implicaciones nacionales", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, vol. I, Bogotá, Universidad de los Andes, 2005, p. 183.

y el comercio, de modo que las herramientas jurídicas y técnicas dieran un fundamento sólido y seguro a las relaciones y transacciones que se llevan a cabo por vía electrónica y telemática, al hacer confiable, seguro y válido el intercambio electrónico de informaciones.[52]

Un análisis de la ley 527 de 1999 a la luz de la doctrina y la jurisprudencia refuerza estos argumentos, pues la ley se limita a hablar de mensajes de datos como un tipo de documento. Esto plantea dos complicaciones para la IEA. Primero, está tomando en cuenta apenas un tipo de la IEA que, si bien es uno de los más comunes y especial en el comercio electrónico, no logra abarcar la totalidad del concepto de la IEA. Segundo, utiliza un equivalente funcional para darle la misma fuerza probatoria a los mensajes de datos que se le da a los otros tipos de documentos, cosa que, aunque acertada en varias ocasiones, no lo es en otras.

El mensaje de datos se encuentra definido en el artículo 2° de la ley 527 como "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), la Internet, el correo electrónico, el telegrama, el télex o el telefax". Aunque a primera vista es muy similar al concepto de la IEA establecido, hay varios factores cruciales que debemos analizar.

La citada definición habla de mensaje de datos. Al emplear la palabra "mensaje", la connotación de la definición es comunicativa, por lo cual implícitamente asume un intercambio de información. Si bien se dice expresamente que incluye información almacenada, el lenguaje, los ejemplos y las raíces comerciales de la norma apuntan a tratarse de legislación diseñada precisamente para mensajes de datos, no todo tipo de la IEA. Esto se hace sin reparo a la necesaria reflexión sobre la infinita cantidad

[52] Colombia, Corte Constitucional (2000), "Sentencia C-662", M. P.: Morón Díaz, F.

de finalidades, formas y sistemas que va a utilizar la IEA en el futuro, algo incongruente con una definición que parte de mensajes de datos.

Considerando lo anterior, es difícil ver de qué manera resultaría práctico considerar que todo tipo de la IEA es un mensaje de datos. Esta limitación no es apropiada para complacer el elemento de alcance que se viene proponiendo y en esa medida no satisface lo que busca este escrito: proponer un concepto de la IEA especial para el ordenamiento jurídico colombiano.

Quizás el elemento más importante del mensaje de datos, el cual podría ser tanto adecuado como errado en el caso de la IEA, es el equivalente funcional que se le da al mensaje de datos frente a otros tipos de documentos. Como quedó claro cuando se propuso el elemento categórico que mezclara el modelo estadounidense con el australiano, es necesario utilizar lo ya escrito antes de escribir nuevas normas. El equivalente funcional consagrado en la ley 527 a los mensajes de datos es el instrumento idóneo para llevar a cabo tal labor.

El Dr. Andrés Felipe Umaña Chaux explica de manera sucinta y clara lo que es y lo que implica el equivalente funcional:

> La palabra "equivalencia" del concepto da lugar, a la equiparación de la función probatoria de un mensaje de datos a la función que cumple un documento físico o tradicional. Los medios tradicionales de prueba cumplen con unas funciones específicas, y prueban unos hechos particulares; algunos prueban quién creó un documento, otros cuándo se creó, o con qué información se ha comprometido el creador del documento. El principio del equivalente funcional establece que un mensaje de datos que cumpla con esta misma función específica, tendrá los mismos efectos jurídicos que estos medios tradicionales.[53]

[53] Umaña Chaux, Andrés Felipe, "Algunos comentarios sobre el principio del equivalente funcional en la ley 527 de 1999", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, vol. I, Bogotá, Universidad de los Andes, 2005, p. 79.

La jurisprudencia desarrolló aún más el concepto de equivalencia funcional en la ley 527, pues la Corte Constitucional consideró que dicho concepto, al ser aplicado a los mensajes de datos de los cuales habla la norma, obligan a entenderse que se usa en todos los ámbitos del derecho, no sólo el comercial. Esto se puede observar en la sentencia C-831 de 2001: "ha de entenderse que la ley 527 de 1999 no se restringe a las operaciones comerciales sino que hace referencia en forma genérica al acceso y uso de los mensajes de datos, lo que obliga a una comprensión sistemática de sus disposiciones con el conjunto de normas que se refieren a este tema dentro de nuestro ordenamiento jurídico...".[54]

La equivalencia funcional es una herramienta de vital importancia para lograr asimilar el concepto de la IEA correctamente en el mundo jurídico de Colombia. Utilizar este instrumento nos permite armonizar el concepto de la IEA con una enorme cantidad de normas que se le aplican a otras pruebas o incluso otras instituciones jurídicas. Pero en este orden de ideas, categóricamente la distinción entre las pruebas documentales tradicionales y los mensajes de datos es mínima. Es más, la diferencia que se le da a los mensajes de datos frente a las pruebas documentales es sólo la que se establece en la ley 527, por ejemplo la integridad de un mensaje de datos (art. 9) y el criterio para valorar probatoriamente un mensaje de datos (art. 11).

Es en este momento cuando vale la pena recordar el razonamiento detrás de elegir un concepto de la IEA que unifique lo aprendido del caso estadounidense con lo del caso australiano. En el caso australiano se le otorgó un equivalente funcional a la IEA ante los documentos tal como se plantea en el caso de los mensajes de datos en la ley 527, pero la jurisprudencia entró a jugar un papel muy importante al momento de poner en práctica la equivalencia funcional probatoria, pues las

[54] Colombia, Corte Constitucional (2001), "Sentencia C-831", M. P.: Tafur Galvis, Á.

diferencias entre la IEA y los documentos tradicionales exigieron dicha intervención. La manera como se va a descubrir la información, la carga de la prueba, la participación de un perito informático y el intercambio de información entre las partes y el Despacho, entre otros, han sido reglamentados por la jurisprudencia.

En nuestro país es muy difícil que una jurisprudencia pueda tener un impacto semejante, lo cual acarrea la consecuencia de que la ley sea la que deba dar claridad sobre ciertos aspectos. Por lo anterior, resulta razonable afirmar que si bien la ley 527 de 1999 fue un avance hacia incorporar la IEA en el ordenamiento colombiano, no lo logró en la medida que incorporó apenas un tipo de la IEA, pero sí estableció el antecedente necesario para que una propuesta como la presente se pueda llevar a cabo. No hay razón para pensar que el equivalente funcional, particularmente el escrito y el de original (establecidos en los artículos 6° y 8°, respectivamente) no sirvan para introducir la IEA a Colombia. Es más, como se verá en el capítulo siguiente, son herramientas sin las cuales sería necesario reescribir todas las leyes para acomodar la IEA o dejarla a la suerte de cualquier otro documento.

Tomando en cuenta que la meta es incorporar tanto la IEA como el peritaje informático en la ley colombiana, sería insensato no hacer ciertas observaciones sobre el peritaje informático en la ley 527, y la consecuencia del equivalente funcional sobre la apreciación de la prueba. Al ser el primer intento en nuestro país de asimilar la revolución informática de las últimas tres décadas, hay mucho que podemos aprender de lo dicho en esta ley, pero en el caso del peritaje informático, es igual de importante notar lo que no se mencionó o consideró en ella.

Como se ha discutido, la ley en cuestión le reconoce cierta especialidad a los mensajes de datos por su naturaleza electrónica, es decir, por ser un tipo de la IEA, pero no a todos. Mucho se podrá escribir, y se ha escrito, sobre esta ley, pero lo más importante para lograr nuestro

objetivo es comprender en dónde se quedaría corta la ley 527 si fuera a aplicársele a todo tipo de la IEA.

Si bien el equivalente funcional es una herramienta vital para armonizar la IEA con el ordenamiento jurídico colombiano, también puede serlo para introducir el peritaje informático. Ésta es la limitación más evidente de la ley 527, porque, aunque logra con cierto grado de éxito introducir un concepto de prueba electrónica, no hace referencia específica al perito informático, ni menciona la íntima relación que hay entre comprender el valor probatorio de la IEA y la presencia de un perito informático. Por medio del equivalente funcional y de los tajantes enunciados estableciendo que los mensajes de datos no pueden ser descartados por el solo hecho de ser un mensaje de datos,[55] se le dio la importancia necesaria a todo mensaje de datos. Pero faltó darles el estatus especial necesario. Éstos son un tipo de la IEA, y consecuentemente sufren los mismos riesgos que la caracterizan como su vulnerabilidad a manipulación inadecuada o el problema de la accesibilidad. Faltó incorporar el perito informático a la ecuación legal de la prueba electrónica.

Para citar apenas un ejemplo de lo necesario que es el perito informático, aun cuando se aplica el equivalente funcional, podemos referirnos al artículo 261 del Código de Procedimiento Civil. Esta norma le da la facultad al juez de apreciar un documento roto o alterado de acuerdo a las reglas de la sana crítica.[56] Si el juez se encuentra frente a una prueba documental en forma de mensaje de datos o de cualquier otro tipo de la IEA, ¿cómo va a saber si está roto o alterado? La respuesta es la de que un

[55] Ley 527 de 1999, artículo 5°. *Reconocimiento jurídico de los mensajes de datos*. No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos.

[56] Código de Procedimiento Civil, artículo 261. *Documentos rotos o alterados*. Los documentos rotos, raspados o parcialmente destruidos, se apreciarán de acuerdo a las reglas de la sana crítica; las partes enmendadas o interlineadas se desecharán, a menos que las hubiere salvado bajo su firma quien suscribió o autorizó el documento.

juez promedio, con conocimientos ceñidos al derecho, su profesión, no va a lograr notar esa diferencia. Es necesario que alguien le explique frente a qué está abocado. Sin implementar un perito informático, aplicarle el equivalente funcional a este artículo podría tener consecuencias desastrosas.

Utilizando lo aprendido sobre el equivalente funcional y leyendo la ley 527, se puede apreciar que para comprender el estado probatorio de la IEA (en su forma de mensaje de datos, pues es la única que admite el ordenamiento jurídico) debemos referirnos a los documentos. Éstos son considerados como un medio probatorio de acuerdo con el artículo 175 del Código de Procedimiento Civil, pero en esa categoría de evidencia no existen disposiciones especiales para mensajes de datos. Ocurre entonces que si el juez debe valorar la IEA y la entiende como mensaje de datos pero no encuentra cómo apreciarla dentro de la ley, puede acogerse al inciso 2° del citado artículo, el cual reza: "El juez practicará las pruebas no previstas en este código de acuerdo con las disposiciones que regulen medios semejantes o según su prudente juicio".

Al ser el mensaje de datos una especie de la IEA, es fácil ver cómo un juez podría asimilar cualquier tipo de la IEA al mensaje de datos, ya que, al final, todo tipo de la IEA tiene como base un medio electrónico. Es decir, son semejantes. Sin embargo, también les podría aplicar su prudente juicio, como lo permite el artículo. En cualquier caso, no existiría la participación de un perito informático. Si el juez utiliza su prudente juicio, o si se ciñe a lo establecido en la ley 527 de 1999 para los mensajes de datos, es posible, e incluso probable, que no se percate de todas las realidades que puede descubrir u ocultar una prueba basada en la IEA. Es por esto que, "Será necesario un peritaje para complementar o apoyar la prueba documental, para determinar la autenticidad de la prueba, cuando se tache su autenticidad, o para determinar elementos claves como su fecha de emisión o recepción si

el mensaje fue abierto, para descifrar el documento, comprobar firmas electrónicas, etcétera".[57]

Consecuentemente, se puede afirmar que el ordenamiento jurídico colombiano ha comenzado a asimilar la IEA por medio de la ley 527 y el equivalente funcional que ésta instauró. Gracias a este avance es más fácil visualizar cómo insertar la IEA en el sistema legal colombiano, pues permite que se le apliquen normas que ya existen y pueden ser perfectamente aptas para ella (como lo son la mayoría de las disposiciones para documentos). Por otro lado, no se ha establecido la institución de peritaje informático como algo que se deba ver en conjunto con la IEA. Es decir, que no se ha completado el concepto de la IEA, pues carece del elemento del PII mencionado.

Lo dicho conlleva a no poder entenderse que sólo con cambiar las palabras "mensajes de datos" por "información electrónicamente almacenada" la IEA quedará implementada jurídicamente en Colombia. El equivalente funcional no puede ser llevado al extremo, como sucedió en Australia. Es necesario crear una categoría de prueba independiente, que sea fácil de puntualizar e individualizar en la ley, para a su vez crear legislación específicamente diseñada para ella.

Con el fin de retornar al objetivo del escrito, el presente capítulo nos permite ver que una aproximación mixta es solución viable y particularmente amigable en el caso de Colombia. Mientras que el equivalente funcional establecido en la ley 527 permite equiparar el nuevo concepto de la IEA a otras pruebas cuando sea posible, crear una nueva categoría de evidencia otorga darle la dimensión especial a la IEA que exige. De esta forma, es más clara la unión que se hace con el peritaje informático y se le atribuye una fuerza jurídica especial, pues lo ata directamente a un tipo de evidencia.

[57] Certain et ál., ob. cit., p. 191.

V. Propuesta

En aras de lograr implementar la IEA y en consecuencia el peritaje informático en Colombia, nos valdremos de todo lo aprendido en la presente investigación y aquellas que la anteceden. Por ello, es válido puntualizar lo que se ha propuesto esporádicamente a lo largo de la generalidad de escritos para el caso colombiano. Esto, sin embargo, debe hacerse de manera integral, por lo cual tratar cada investigación individualmente es inapropiado. Por el contrario, se debe puntualizar todo en conjunto, pues sólo así es posible generar una verdadera unidad que dé el resultado propuesto en esta investigación.

Como se planteó, es idóneo un modelo que mezcle lo existente en Colombia y lo normado tanto en Australia como en Estados Unidos con relación a la IEA, esto es, un modelo mixto. Eso nos permite crear una propuesta con aspectos utilizados en las más avanzadas legislaciones en materia de la IEA y fundirlos con la normatividad colombiana, de tal suerte que resulta una propuesta más comprensiva y que no se desentiende de la realidad legislativa del país.

Las herramientas desarrolladas permiten proponer un texto legal que debe ser similar a la ley 527 de 1999 en su finalidad (actualizar al ordenamiento jurídico colombiano para que se puedan entender mejor las pruebas que consistan de la IEA), pero al tiempo que hace uso de los atributos positivos de la ley 527, debe lograr sanar los aspectos de ésta que no se ajusten del todo a la realidad o al futuro de la IEA. El objetivo se puede lograr tomando cada elemento del concepto de la IEA al cual se ha llegado y puntualmente exponer cómo y por qué éste cabe dentro del marco legal colombiano.

Lo anterior, como se verá, lleva a la necesidad de incorporar el peritaje informático al ordenamiento jurídico colombiano. Tomando eso en cuenta, y en especial lo aprendido en la investigación de Pimentel

y Cano, la propuesta debe incluir una definición específica e indiscutible del perito informático, su función como auxiliar de la justicia y su papel en la validez judicial de pruebas que consistan en la IEA. Dicha norma ha de exigir que el perito cumpla ciertos requisitos, los cuales podremos establecer haciendo uso de la propuesta sugerida por Ángela Ramírez.

Para finalizar, se redactará una conclusión sobre lo más importante del presente escrito y sobre los nuevos interrogantes surgidos a raíz de él.

A. Definición de la IEA

Esta investigación ha propuesto que el concepto de la IEA en Colombia sea uno en consonancia con la realidad de este tipo de información, pero además, que esté preparado para cuanto ha de venir. Como respuesta a dicha demanda, es necesario que la IEA tenga un alcance amplio, y así se entienda que mientras sea información almacenada electrónicamente, sin cuidado de cualquier otro aspecto, puede ser considerada material probatorio (la validez de esa prueba es otro asunto, que se tratará en el acápite siguiente).

Ahora bien, como se estableció en su momento, es necesario casar la IEA con el peritaje informático, pues ningún otro individuo —de rango científico y técnico— es capaz de establecer más allá de la duda razonable que la IEA es lo que dice ser y se produjo de la manera como se propone. Ya mucho se ha dicho sobre lo técnica que es la naturaleza de la IEA, las variadas formas que puede tomar, y de que va a continuar evolucionando a una velocidad sorprendente. Cuanto incumbe al juez cuando se enfrente a una prueba consistente de la IEA es que ésta es más fácil de manipular indebidamente que documentos tradicionales y las pruebas de su autenticidad son más difíciles de entender que en el caso de éstos. Además, puede reproducir casi cualquier tipo de documento

de manera electrónica al tiempo que tomar formas completamente distintas a las de los documentos tradicionales.[58]

También quedó claro que, tanto en el caso estadounidense[59] como en el australiano,[60] la participación de un experto en el proceso, con el fin de validar la autenticidad e integridad de la prueba, es un medio idóneo para proteger el valor judicial de la IEA. No fue otra la razón por la cual se estudió el concepto de la IEA desde el punto de vista del peritaje informático, y teniendo en cuenta lo aprendido, la definición debe incluir una corta guía de los tipos de la IEA que más se presentan como pruebas. Una lista así sirve dos propósitos: deja explícitamente dicho que algunos de los más populares tipos de la IEA son admisibles en procesos judiciales, y además da unos ejemplos que se referencien como guía para aplicarle la definición a otros tipos de la IEA. Este listado puede ser establecido utilizando las formas explicadas por el juez Grimm[61] y las propuestas en la investigación de Pimentel y Cano.[62]

Ahora, para redactar el articulado, sería insensato no referirnos a la ley 527 de 1999, pues fue el primer intento del legislador colombiano por actualizar el ordenamiento del país para que dentro de él se comprendiera todo tipo de prueba electrónica. Además, como se demostró en el capítulo anterior, el equivalente funcional que propone la norma debe ser utilizado para lograr implementar el modelo mixto. Sin embargo, al leer la norma, ésta se limita a definir mensaje de datos, algo que resulta particularmente restrictivo. En virtud de esto, se hará uso de las definiciones establecidas en los otros países para redactar el articulado.

[58] Nearon, Paul, ob. cit., p.13.

[59] Brady, "Evidentiary Issues with ESI", pp. 4-5.

[60] Ob. cit., Nota de práctica 17.

[61] Brady, ídem.

[62] Pimentel, ob. cit., p. 9.

Como se comentó, el caso estadounidense establece una categoría completamente nueva de prueba, mientras que los australianos simplemente le aplicaron la definición de documento. En nuestra definición, ambas aproximaciones han de tener lugar, toda vez que se trata de un modelo mixto el cual debe permitir identificar nueva evidencia con normas hechas para pruebas en medios físicos. El alcance de la definición en ambos países es supremamente amplio y faculta para que todo tipo de información quepa dentro de la definición de la IEA. Ambas, también, nos dan una lista corta de tipos de información que pueden constituir la IEA. Esta lista es importante para nuestro caso, pues permite ligar la IEA a la prueba documental, el tratarse del tipo de información que más se manifiesta en forma documental.

Tomando en cuenta lo anterior, se propone el siguiente texto como definición legal de la IEA:

> La información electrónicamente almacenada (IEA), es cualquier forma de registro de información y cualquier tipo de escritos, dibujos, gráficos, listados, fotografías, grabaciones de sonido y otra data o compilación de datos, que pueda ser almacenada en cualquier tipo de medio que permita obtener la información directamente o, de ser necesario, con la ayuda de un perito informático. La siguiente es una lista meramente enunciativa de tipos y formas de la IEA:
>
> 1) Contenidos de archivo
> 2) Correo electrónico
> 3) Mensajes de texto/datos
> 4) Chat electrónico
> 5) Metadata
> 6) Datos de directorio
> 7) Datos de configuración

8) Datos de *logging*
9) Material forense recuperado
10) Interpretaciones de expertos

La anterior definición incluye todos los puntos claves que se han discutido a lo largo de las investigaciones: crea una nueva categoría de prueba, anudada a la vieja categoría de prueba documental, e introduce indiscutiblemente el perito informático en el concepto de la IEA, para que a su vez pueda hacer parte intrínseca del ordenamiento colombiano. También de importancia es la neutralidad tecnológica que se observa, pues se está hablando de tipos de la IEA, mas no se favorece ninguna tecnología.

B. Incorporación de elementos de la IEA

En el capítulo dos de la presente investigación se propusieron cinco elementos para entender el concepto de la IEA de acuerdo con lo aprendido de los casos estadounidense y australiano. Estos elementos son: el alcance, el categórico, el procesal, la carga probatoria y la accesibilidad, este último elemento siendo el lugar donde cabe el perito informático, como se explicó. Para incorporar la IEA a la normatividad colombiana como se ha entendido en este escrito, es preciso encajar cada elemento dentro del ordenamiento vigente, al tiempo que se sustenta la propuesta acorde a lo establecido en las investigaciones.

1. Elemento del alcance

Este elemento se puede definir como lo que establece la dimensión donde se abarca el concepto de la IEA. Por eso mismo, la definición en gran medida refleja este elemento, pues dentro de ella se buscó determinar lo

que es la IEA por medio de fijar su alcance. Aunque una de las principales razones para que el alcance sea extenso es a causa de la impredecible evolución de la tecnología, la otra razón puede encontrarse en que, al tener un alcance amplio, se tiene consonancia con lo ya establecido en la ley colombiana.

La definición propuesta explica en gran medida el elemento de alcance y la necesidad de que dicho elemento se caracterice por ser amplio. Sin embargo, al unísono se logra que la definición no se pierda en lo abstracto al enunciar ciertos tipos de la IEA que suelen ser los más comunes en procesos judiciales. De esta manera se obedece tanto la necesidad de prevenir contra el futuro, como los estándares del peritaje informático; se prevé que pueden surgir cientos de miles de nuevas posibilidades para este tipo de evidencia, pero también se guía y se sienta un punto de comparación que expone a las tecnologías más frecuentes en procesos judiciales.

La necesidad de comprender un gran espectro de tecnologías se reconoció en la ley 527, pero sólo para el caso de mensaje de datos. Como lo expresó el magistrado Álvaro Tafur Galvis, la ley 527 de 1999 buscó incorporar en la totalidad del ordenamiento jurídico los mensajes de datos utilizando el equivalente funcional.[63] Si el concepto de la IEA ha de adaptarse a lo existente en Colombia, el elemento de alcance debe reflejar la posibilidad de aplicar el equivalente funcional. Es apenas lógico inspirarse en la primera ley que intentó fusionar la IEA al ordenamiento colombiano para lograr una propuesta que sí logra incorporar el concepto en su totalidad en él.

Entonces, si se incorpora el elemento de alcance como se hace en la definición, ésta se asemeja mucho a lo que se buscó en la ley 527. Tal similitud no puede ser subestimada, pues no es accidental y tampoco inútil. Lograr

[63] Colombia, Corte Constitucional (2001), "Sentencia C-831", M. P.: Tafur Galvis, Á.

ese tipo de conexión con la ley 527 nos permite despejar dudas sobre la aplicabilidad del equivalente funcional a las normas que se proponen, algo necesario para crear el modelo mixto buscado. Si el equivalente funcional puede ser aplicado para mensajes de datos —un tipo de la IEA— su uso en un concepto amplio de la IEA no demuestra inconvenientes y se convierte entonces en el reflejo normativo de la evolución tecnológica.

2. Elemento categórico

Encajar el elemento de alcance de la manera propuesta nos brinda una herramienta crucial para el modelo mixto: el equivalente funcional. La ley 527 establece que los mensajes de datos se deben entender como prueba documental. Es decir, no se trata de un nuevo tipo de evidencia, sino de una prueba documental en un medio distinto al físico. Si bien esto puede ser una solución en muchas instancias, también podría convertirse en el mayor factor en contra de la seguridad jurídica de la prueba electrónica, como lo demostró el caso australiano. La solución es entender la IEA como un nuevo tipo de prueba por sus características especiales pero que puede tomar formas a las cuales se les apliquen las normas establecidas para otro tipo de pruebas.

Para mirarlo de una manera crítica, cabe la pregunta: ¿por qué una categoría nueva que puede ser aplicada a las leyes existentes y no usar otra existente que pueda ser complementada por leyes nuevas? La razón es sencilla pero multifacética. En primer lugar, tenemos la naturaleza misma de la IEA, de lo cual se deriva la necesidad de tener disposiciones especiales para este tipo de evidencia. Además, se entiende que es la evidencia del futuro, pues no es ningún secreto que todos los días hay más información en forma electrónica que física.

Estamos enfrentándonos a una prueba que puede tomar muchas formas; susceptible de ser modificada, manipulada o destruida fácilmente

y es en general sumamente vulnerable; que es de un nivel técnico y científico tan alto que las personas capaces de comprenderla en su totalidad son pocas. Además, la evolución es impredecible, lo cual hace aún más cuestionable dejar que este tipo de pruebas recorran exactamente el mismo camino legal que las documentales. Si hoy en día el Código de Procedimiento Civil no se adapta a la IEA y genera inseguridad jurídica (como se vio en el caso de los artículos 261 y 175), es difícil argumentar en contra del Comité de Consejeros de Estados Unidos[64] cuando afirma que las nuevas e impredecibles formas de la IEA por venir implica que se alejen de lo escrito para las pruebas físicas.

Crear una nueva categoría para la IEA permite que, por su amplio y comprensivo alcance, las innovaciones tecnológicas no se le escapen al derecho. La realidad de lo distintas que llegan a ser las formas de la IEA es atendida por esta aproximación. Más significativo aún es lograr enmarcar dentro de una sola categoría especial a toda la información electrónicamente almacenada, pues le da ese eje jurídico que encuentran los cuadros, las cartas, los archivos de papel, los videos y los mapas, entre otros, en la categoría de documentos. La IEA es la categoría de evidencia del siglo XXI. Como ocurrió en la realidad, es la evolución del documento físico; por eso tienen similitudes y por eso deben diferenciarse.

Por otro lado, el que se implemente una nueva categoría de evidencia permite incorporar adecuadamente la figura del perito informático. A través de las investigaciones se ha afirmado que ésta está muy cruda en Colombia y es necesaria para poder comprobar la validez jurídica de la IEA. Este estudio ha propuesto que el perito sea una parte integral del concepto de la IEA, algo más conveniente de lograr si se comprende el peritaje dentro de la categoría, lo cual va de la mano con el eje que crea

[64] Paul, ob. cit., p. 16.

una nueva categoría de la IEA, pues se entiende que el perito informático es un elemento que no se puede ignorar cuando se trata la IEA en un proceso judicial, independientemente de la forma que ésta tome.

Dicho esto, recordemos que se busca un modelo mixto. La estrategia no es gratuita, pues también es el modelo más conveniente en el caso del elemento categórico. Si bien se establece que la IEA requiere ser una categoría de prueba diferente por el futuro, debemos también pensar en el presente. De ahí que toma importancia la aproximación colombiana y australiana. La ley 527 de 1999 incorpora un tipo de la IEA a la ley colombiana como prueba documental, mientras que en Australia se entiende toda la IEA como tal. La gran ventaja de este modelo es la de introducir la IEA al ordenamiento pero no hay que reescribir nada, pues es tratada como una prueba documental.

Sin olvidar las características que hacen tan única a la IEA, también se deben considerar los aspectos similares a las pruebas tradicionales, particularmente —como lo exponen los casos colombiano y el australiano— las documentales. Para aprovechar este aspecto, vamos a utilizar el equivalente funcional. En virtud de que lo encontrado en la ley 527 es la voluntad del legislador, y alude a una ley que trata un tipo de la IEA, además de que ya se estableció la similitud entre esta ley y el elemento de alcance, dicha norma debe ser la columna vertebral de la IEA en el ordenamiento jurídico colombiano, pero sólo provisionalmente.

Los cambios que vendrán exigirán legislación específica para la IEA (incluso para tipos específicos de ella), razón por la cual es necesaria una nueva categoría. Ocurre entonces que se generarán conflictos entre aplicar el equivalente funcional o la nueva norma. Por ejemplo, si una nueva norma sale reglamentando los criterios para considerar auténtica una conversación por chat, ¿se le debe aplicar esa norma o el equivalente funcional, de acuerdo a la ley 527? En el caso de que algo así ocurra, es necesario que predomine la nueva ley siempre, pues se entiende ser

legislación que actualiza el ordenamiento jurídico para ponerlo al día con la realidad. Ésta es otra razón para que exista una categoría independiente de la IEA: ayuda a crear legislación específicamente diseñada para la IEA sin tener que incurrir en ambigüedades y permite una actualización más adecuada del ordenamiento.

Considerando lo anterior, podemos llegar a redactar un artículo que le permita al juez interpretar la IEA como una prueba documental utilizando el equivalente funcional establecido por el legislador en la ley 527, pero que se subroga a normas aplicadas a la IEA.

El texto que se propone para solucionar este asunto es el siguiente:

"La IEA podrá ser sujeto del equivalente funcional establecido para mensajes de datos en la ley 527 de 1999. La aplicación del equivalente funcional se subrogará a normas especiales para la IEA".

El siguiente reto en redacción legislativa es individualizar la IEA frente a las demás pruebas. El artículo 175 del Código de Procedimiento Civil establece cuáles son los medios de prueba. La propuesta es modificar este texto, para que el primer inciso rece de la siguiente manera (las *cursivas* marcan la modificación): *Sirven como pruebas, la declaración de parte, el juramento, el testimonio de terceros, el dictamen pericial, la inspección judicial, los documentos, los indicios, la* IEA *y cualesquiera otros medios que sean útiles para la formación del convencimiento del juez.*

Esta modificación hace que la IEA esté prevista dentro del código, de tal suerte que no se le aplica el segundo inciso del mismo artículo. Así, se genera una división importante entre la IEA y el resto de las pruebas, además de evitar que el juez practique pruebas de la IEA según su prudente juicio, algo que si bien ocasionalmente puede resultar bien, es demasiado arriesgado darle tanta libertad a un juez para apreciar una prueba tan especial. Hay campo para la sana crítica del juez, por supuesto, pero en el caso de la IEA en ocasiones es prudente limitarla, como se verá más adelante.

3. Elemento procesal

Desde el punto de vista de esta investigación, es decir, usando una comparación entre el concepto de la IEA de Estados Unidos y de Australia, el elemento procesal debe ser de nuevo mixto, pero dado nuestro sistema de ley continental o civilista, la jurisprudencia no es el mecanismo ideal para establecer el aspecto procesal de la IEA. Como se mencionó, esto se ha de establecer a nivel de norma para que tenga el respaldo de ser una fuente de derecho contundente.

El costo de un proceso que involucra la IEA puede llegar a ser considerable, particularmente cuando se entra a controvertir su autenticidad o validez probatoria. No obstante, en los procesos en donde no se controvierten las pruebas de la IEA, pueden surgir problemas de admisibilidad que podrían haber sido evitados si existiera una comunicación entre las partes. Si éstas se logran poner de acuerdo en aspectos como la recolección, presentación e intercambio de la IEA en un proceso judicial, como lo demostró el caso australiano, se pueden marcar pautas básicas para que las partes lleguen a acuerdos que resulten en un proceso más ameno, eficiente y económico para todos los interesados, incluyendo al Estado.

Esto sin perjuicio de que el juez pueda divagar del plan expuesto por las partes si lo considera apropiado. Las guías y procedimientos que se consideren idóneos para sugerirle a las partes, en aras de hacer menos traumático incluir la IEA como prueba en un proceso, pueden inspirarse en lo establecido en la nota de práctica 17 y sus anexos. Una propuesta específica y concreta de un proceso idóneo que lleven a cabo las partes desborda los límites del objetivo del presente escrito.

También es importante tomar en cuenta que se trata de una controversia, por lo cual la probabilidad de encontrar una pronunciada animosidad entre las partes es significativa. Es entonces ingenuo no

establecer el procedimiento a seguir en el caso de no llegarse a un acuerdo entre las partes para manejar la IEA dentro del proceso. Así, nos encontramos de nuevo frente a una nueva oportunidad para hacer uso inteligente del equivalente funcional.

Al estar frente a un tipo de evidencia que requiere un manejo especial y se caracteriza por su vulnerabilidad, cuando no se logre un acuerdo se debe tener mucho cuidado en cómo se manejará la IEA dentro del proceso. Sin embargo, el modelo mixto nos permite tener ese cuidado por medio de normas puntuales que resalten las necesidades de la IEA o de tipos específicos de ella, al tiempo que las normas que se le aplican procedimentalmente a los documentos puedan ser aplicadas a la IEA. Así, mientras se especifica, por ejemplo, que un perito es necesario para analizar la IEA en forma de metadata, se puede entender que otros documentos más parecidos a los físicos, como los generados por procesadores de palabras (v. gr. *Microsoft Word*) o las fotografías digitales, no requieren de un perito, sino cuando se pone en duda la validez o veracidad de la prueba.

4. Elemento de la carga probatoria

Para el cuarto elemento vamos a utilizar casi que exclusivamente el equivalente funcional con las pruebas documentales. No obstante, a causa de las características de la IEA, es importante hacer ciertas clarificaciones al respecto. Si bien se puede utilizar el equivalente funcional, éste no comprende el elevado costo económico del peritaje informático, cosa que, como se mencionó en la jurisprudencia australiana,[65] puede llegar a tener un valor tan grande que incita a ser utilizado abusivamente por una parte contra la otra.

[65] Brereton, ob. cit.

Este aspecto económico del peritaje informático es crítico para nuestro caso, pues se está atando directamente el peritaje informática a la IEA, algo que implica establecer una política de implementación del peritaje electrónico agresiva. Esto en virtud de que su íntima relación con la IEA hace del peritaje informático uno de los pilares de la evidencia electrónica en nuestra propuesta. Sería inconsecuente con lo establecido en las anteriores investigaciones y la presente no buscar una implementación agresiva del peritaje informático en aras de garantizar la autenticidad y validez de una prueba que conste de la IEA.

Para aplicar el equivalente funcional a la carga probatoria tan sólo hay que hacer referencia al artículo 252 del Código de Procedimiento Civil, el cual establece la presunción de autenticidad a favor de "los documentos privados presentados por las partes para ser incorporados a un expediente judicial con fines probatorios...".[66] Pues bien, en principio no hay razón para que el equivalente funcional frente a documentos se aplique también para la IEA. Es decir, se considera auténtica en un proceso judicial. Es cierto que admite prueba en contrario, pero como se planteará más adelante, la prueba idónea puede ser un peritaje informático.

Con relación a la cuestión económica inherente a los peritajes informáticos, se puede proponer, con base en lo aprendido del caso australiano y en el desarrollo de esta investigación, que en el caso de la IEA quien controvierta la prueba debe ser quien asuma los costos para desvirtuarla. La excepción a dicha obligación se da cuando el juez condena en costos a la contraparte.

Tomando en cuenta lo anterior, se propone el siguiente texto como articulado para establecer la carga de la prueba en la IEA: "La IEA se presumirá auténtica cuando sea incorporada a un expediente judicial

[66] Código de Procedimiento Civil de Colombia, artículo 252.

con fines probatorios. Desvirtuar la prueba y los costos derivados de los argumentos con que se ataca a la misma, son asumidos en su totalidad por la parte retadora, sin perjuicio de qué parte sea condenada en costos".

5. Elemento de accesibilidad/PII

El elemento de accesibilidad es uno de los más delicados para el valor probatorio de la IEA. La compleja naturaleza técnica de este medio de prueba hace que comprender la dificultad de su accesibilidad sea algo que sólo pueda lograr un perito informático adecuadamente entrenado. Como se vio en la investigación de Ángela Ramírez, el perfil para dicho individuo no es claro en Colombia, y no existe formalmente su figura legal en el país. Establecer específicamente qué es un perito informático, su labor y su incidencia sobre una prueba en forma de la IEA, es de vital importancia para poder traducir el complejo y técnico elemento de accesibilidad a la realidad legal de un proceso judicial.

En vista de que la propuesta para la definición de la IEA incluye, muy intencionalmente, la figura del perito informático, es adecuado aclarar a nivel legal qué es un perito informático. Redactar una definición legal se puede lograr a través de la doctrina, utilizando algunas referencias de este escrito. Específicamente, podemos utilizar la definición expuesta por el Dr. Cano, la cual define al perito informático como "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".[67]

Enseguida se hace necesario definir la labor que ha de cumplir el perito. De manera sencilla, éste debe elaborar un "dictamen técnico y científico sobre el objeto de análisis en el cual cuenta con la experiencia y

[67] Cano, ob. cit., p. 8.

conocimiento requerido, con el fin de que a través de fuentes de información y análisis exhaustivo llegue a conclusiones que pueda sustentar".[68] Ahora bien, cuando se entra en detalle sobre las implicaciones de dicho dictamen y su idoneidad para establecer la autenticidad de la IEA (según se entendió de la jurisprudencia del juez Grimm y las notas de práctica 17 y 24 de la Corte Federal australiana), la opinión de este experto toma la importancia legal propia de estar incluida dentro de la definición de la IEA.

Utilizando lo aprendido en los dos países estudiados, se propone crear la figura de perito informático independiente (PII). Como se vio, el perito debe ser utilizado en procesos judiciales para aclararle al juez dudas sobre la IEA. Se reitera, debe servir de traductor para el juez y las mismas partes sobre lo que es la IEA, lo cual implica su forma especial y si se ha comprometido de alguna manera la validez de la información. Ahora bien, esto da campo para que el examen pericial sea una influencia muy fuerte sobre la decisión del juez, de manera que el perito requiere ceñirse a responder las dudas del juez y aclarar apenas los aspectos técnicos de la información, no entrar a valorarlas.

Para insertar al perito informático dentro del ordenamiento colombiano, es posible aplicar el equivalente funcional. No hay razón para pensar que las labores del perito informático y el medio probatorio del peritaje tradicional no puedan trasladársele a él. Si bien estas normas fueron escritas considerando peritos tradicionales, el perito informático no se diferencia en gran medida de ellos desde un punto de vista legal, pues se trata de un auxiliar de la justicia que rinde un concepto técnico, el cual cabe perfectamente dentro de las normas establecidas en el capítulo v del título XIII del libro segundo del Código de Procedimiento Civil. Sin embargo, de nuevo ocurre lo acontecido con la categoría de la

[68] Ídem.

IEA: crear específicamente el peritaje informático le permite al legislador atar esa definición que establece al individuo ideal para comprobar la validez de una prueba consistente en la IEA.

Seguidamente pasamos a definir el rol del perito informático en un proceso que contenga la IEA. De nuevo haciendo alusión a lo aprendido de los casos estudiados, es claro que el papel del perito informático llega a ser de una importancia vital. Sin embargo, también acarrea unos sacrificios económicos considerables, que pueden o no ser ineludibles. Por lo tanto, hacer obligatoria la participación de un perito informático —algo necesario para poder atacar agresivamente el problema de autenticidad y validez de la IEA— debe ser un ejercicio cauteloso. La necesidad de requerirlo debe ser lo más limitada posible, pues de no ser imprescindible no se entiende la necesidad de que se incurra en esos costos. Esto es además congruente con lo que se buscó en el momento de establecer la carga de la prueba, ya que el problema de los costos puede ser un inconveniente real.

Sin embargo, en ocasiones, para asegurar la mayor seguridad jurídica posible, es inevitable la participación de un perito informático, bien sea para practicar un peritaje, servir al juez como traductor técnico, o cualquier papel auxiliar que pueda llegar a desempeñar. De lo visto, se pueden reconocer dos instancias en donde la ayuda de un perito informático es indispensable para garantizar la seguridad jurídica de la prueba que consista en la IEA. Dichos momentos son: cuando exista una controversia centrada en la autenticidad de la IEA o de su validez, y en el evento de que se debe recuperar la IEA cuando se practica una prueba.

En el primer caso la participación del perito informático es el mejor medio para llegar a aseverar la autenticidad de una prueba de la IEA, al menos en la mayoría de los casos, pues existen instancias en que ésta no es recuperable, realidad que no le permite al perito asegurar científicamente la autenticidad de la información. Ahora bien, cuando se habla

de la autenticidad y validez de la información se trata de establecer que la procedencia y circunstancias técnicas referidas por una parte son verdad. Esto puede permitir o no establecer quién tiene la razón en el litigio, pero siempre que sea posible practicarlo el peritaje informático esclarecerá los aspectos técnicos que pueden incidir sobre la validez probatoria, como las buenas prácticas en la cadena de custodia de la misma, por ejemplo.

En el segundo caso, el perito informático debidamente entrenado casi garantiza que cuando se recupere una prueba basada en la IEA la producción de ésta esté hecha de manera adecuada, por lo cual se despeja la inseguridad jurídica que muchas veces sigue a los métodos utilizados para comprobar la prueba. Recordemos el caso de los computadores del guerrillero colombiano alias Raúl Reyes, donde tres países se enfrentaron —hasta el punto de movilizar tropas a la frontera— por la IEA, todos alegando que la autenticidad no se podía establecer y que ésta fue indebida o debidamente manipulada. Si en Colombia existieran estándares y una formación adecuada para el peritaje informático, obligar dentro del proceso la participación de un perito en los casos mencionados aportaría beneficios a la seguridad jurídica del país de manera contundente.

Pero para que sea obligatorio el peritaje, éste debe ser también serio. De nada sirve establecer como obligación la participación de peritos si ellos no hacen su labor correctamente, si no se aplican estándares como los establecidos en la investigación de Pimentel y Cano, ni se fortalecen las bases educativas para poder ostentar el título de perito informático, aspecto tratado en la investigación de Ramírez. Por lo tanto, utilizando lo aprendido y propuesto en estas dos investigaciones, es posible concretar un texto donde se establezcan los mínimos educativos para ser un perito informático y que éstos se rijan por los estándares y buenas prácticas internacionales, los cuales pueden hallarse en la investigación de Cano y Pimentel.

En la parte educativa, Ramírez propone crear una especialización que comprenda los variados aspectos del peritaje informático y sea por lo tanto multidisciplinaria. Puntualmente, "un perito informático es aquél que debe tener conocimientos en aspectos técnico-legales, económicos, en administración, en principios de contabilidad y revisión, en justicia penal y criminología, en computación y seguridad informática, principios de auditoría y contabilidad ocupacional, conceptos financieros, operaciones de sistemas de procedimiento criminal y recolección de evidencia".[69]

Ramírez también hace alusión a la necesidad de que la educación tenga un contenido tanto teórico como práctico. Siguiendo lo investigado en Estados Unidos y en Australia, encontró que para lograr focalizar tantas diferentes disciplinas y unificarlas bajo la bandera del peritaje informático, la práctica es el mejor instrumento.[70] Solamente viendo confluir los conceptos teóricos en la práctica del peritaje informático puede prepararse adecuadamente a una persona para ser perito informático.

Ahora bien, Ramírez puntualmente dice que la aproximación por medio de una especialización es solución a corto plazo.[71] Si bien esto es cierto, las bases sobre las cuales se funda esa educación no tienen por qué ser distintas, así sea un programa de pregrado, una especialización, una maestría, un diplomado o un certificado académico. Claramente, es necesario avanzar en el programa educativo específicamente, pero eso es más fácil una vez se comprenden los fundamentos para la formación de un perito informático apto para ser auxiliar de la justicia.

La orientación de esta educación debe tener en cuenta los estándares del peritaje informático que han dado resultado en otros países.

[69] Ramírez, ob. cit., pp. 39-40.

[70] Ibídem, p. 40.

[71] Ídem.

Como estamos siguiendo los ejemplos estadounidense y australiano de guía, lo investigado en esos dos países es propicio para estableces estos estándares. Y al igual que ocurre en el concepto de la IEA, parece ser que el caso estadounidense se complementa bien con el australiano: el primero hace énfasis en las buenas prácticas de los peritos, mientras que el segundo trata de establecer buenas prácticas ciudadanas. Combinar ambos estándares resulta en una propuesta que contempla tanto estándares que sustentan las prácticas del perito, como estándares que hacen más fácil admitir la IEA en un proceso al ser bien llevada por una o ambas partes.

La investigación de Pimentel y Cano halló que en Estados Unidos se observan en general cuatro prácticas,[72] creadas con una mentalidad orientada a asuntos penales e investigaciones, pero igualmente se pueden aplicar ciertas recomendaciones.

La primera, "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".[73] En nuestro caso se eliminaría el componente preferencial para tornarlo obligatorio y se haría referencia a la figura de perito informático, que debe ser definida en una norma (como se propondrá más adelante).

La segunda recomendación consiste en estudiar con profundidad el medio donde se encuentra la IEA y las condiciones relevantes: "Establecer qué tipo de hardware, software, sistemas operativos y configuraciones de red usa el investigado en aras de vislumbrar en dónde puede estar localizada la información que se busca y cómo se

[72] Pimentel, ob. cit., p. 16.

[73] Ídem.

podría acceder eventualmente a ella".[74] Este estándar es totalmente aplicable en el caso colombiano, y como ha demostrado resultados en un país con mucha más experiencia que el nuestro, es importante incluirlo en el ordenamiento colombiano.

El tercer estándar indica que el perito debe establecer una estrategia utilizando lo aprendido en el estándar anterior, para tener los planes apropiados con los cuales poder entrar a hacer el peritaje. Debe considerar todos los aspectos del medio donde se almacena, incluyendo la locación.[75] Es decir, si se trata de la IEA que está en un medio en concreto (como una foto en un disco duro) o información dispersa en medios distintos (como una base de datos distribuida en varios servidores).

El último estándar es útil por su finalidad de darle participación al juez en el proceso del peritaje. Se dice ser necesario que "se le indiquen al juez los procedimientos que se pretenden seguir para la recolección y asimiento del material probatorio".[76] Esto, toda vez que la estrategia desarrollada en el estándar anterior permite vislumbrar qué permisos puede requerir el perito para llevar a cabo su labor de manera adecuada. Así, en caso de tener que acceder a diversos tipos de la IEA, puede consultar y pedirle la autorización pertinente al juez.

En el caso australiano encontramos cinco estándares más generales para ser considerados cuando se pretenda preparar a un perito informático. Específicamente, son los siguientes:[77]

[74] Ídem.

[75] Ídem.

[76] Ídem.

[77] Pimentel, ob. cit., p. 19, citado por Ghosh, Ajoy, "Guidelines for the Management of IT Evidence", Hong Kong, APEC Telecommunications and Information Working Group 29th Meeting (21-26 March, 2004), p. 12.

- "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 y la fecha y hora de la creación de éstos, sobre la identidad de su autor y, por último, sobre la fiabilidad del procedimiento para su custodia y manipulación."[78]
- "Recolectar información de forma adecuada desde una perspectiva forense".[79]
- "Establecer procedimientos para la custodia y retención seguras de la información obtenida".[80] Esto podría lograrse llevando registros de acceso y manipulación realizada a la información que se pretende usar como prueba.
- Determinar si se están manipulando registros originales o copias de éstos. Así mismo, sería pertinente documentar apropiadamente cualquier tipo de acción tomada sobre los registros de evidencia. En ese aspecto, el *paper* australiano hace hincapié en que la evidencia original debe permanecer inalterada y en el evento en que su alteración sea inevitable se requiere documentar dicha alteración debidamente.
- Por último, se hace énfasis 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".

Tomando estos dos estándares y llevándolos a la práctica, tenemos guías para esclarecer lineamientos preliminares las cuales establecen

[78] Ídem.

[79] Ídem.

[80] Ídem.

buenas prácticas que pueden ser estandarizadas en el país y de ellas derivar la educación necesaria para un perito informático, además de proporcionarle al juez un instrumento con el cual evaluar la labor del perito.

Pues bien, los estándares y la propuesta a donde llegaron Ramírez, Pimentel y Cano se pueden incorporar de manera legal, pero hacerlo a un nivel detallado y comprensivo resulta demasiado ambicioso para cubrirlo dentro del presente escrito. Los textos redactados en las páginas anteriores necesitan ser considerados e implementados, pues ilustran la ideología que se estableció en el concepto de la IEA.

En consecuencia, con el propósito de incorporar explícitamente al peritaje informático dentro del ordenamiento colombiano, y vincularlo a la IEA por medio de la figura del PII, es necesario definirlo. Se propone entonces el siguiente texto como definición legal de perito informático:

> Un perito informático independiente es un experto en el área de la IEA que, de acuerdo con el tema requerido, puede ser seleccionado según su competencia, educación, certificación o experiencia para una labor de análisis neutral y objetivo.
>
> Su actividad es la de realizar un dictamen técnico y científico sobre el tipo de la IEA 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 puramente técnicas y fácticas que pueda sustentar. Dicho informe se considerará según lo dispuesto para las pruebas periciales en el capítulo V del título XIII del libro segundo del Código de Procedimiento Civil.
>
> Debe servir como intérprete técnico del juez, mas no como intérprete probatorio. Se debe limitar a sus funciones técnicas y abstenerse de valorar probatoriamente circunstancias distintas a las que dicte el peritaje.
>
> Será obligatoria su participación cuando se ponga en duda, por las partes o por el juez, una prueba que consista total o parcialmente de la IEA. Si

la prueba es a petición de parte, aquel que la controvierta debe costear el proceso del peritaje, salvo que la providencia judicial del proceso objeto de la prueba o la ley dispongan lo contrario. Cuando se practique la prueba de oficio, el Estado responderá por los costos.

También será obligatoria su participación cuando sea necesario recuperar o producir una prueba que conste de la IEA en un proceso judicial para su apreciación.

VI. Conclusiones y reflexiones

Revisando lo comentado e investigado, existen tres conclusiones fundamentales. Primero, la IEA no puede ser siempre valorada en su totalidad por el juez. Si se cuestiona la IEA, aclarar los aspectos técnicos que tienen incidencia directa sobre la manera apropiada de apreciar la prueba es algo que sólo puede ser logrado por alguien con la adecuada formación profesional, es decir, por un perito informático. Segundo, si bien la IEA en Colombia no ha sido desarrollada del todo, utilizar una aproximación legislativa que mezcle el modelo estadounidense con el australiano arroja como resultado una propuesta clara y aprovechable de cómo incorporar el concepto de la IEA a la ley colombiana. Tercero, si se incorpora la IEA, es por lo tanto un requisito incorporar a su vez al peritaje informático, pues no se puede esperar que los jueces de la nación logren comprender los aspectos tecnológicos de este tipo de prueba. Además, la incorporación del perito informático debe ser tanto de rango legal como institucional, particularmente desde el punto de vista educativo.

Las lecciones que deja la investigación y la propuesta formulada toman diversas formas. Por un lado, se intentó hacer un ejercicio comparativo que le generaran un aporte y un cimiento investigativo al derecho informático colombiano, el cual —como se vio en las tres investigaciones— no goza de gran contenido legislativo, doctrinal o jurisprudencial.

Ahora bien, aunque es un intento académico y formal, sería temerario decir que es definitivo, pues requiere de otros elementos que deben ser atendidos para que la propuesta pueda volverse realmente viable.

Como se ha mencionado, la IEA exige un perito informático, pero los estándares y la formación de éste no se han establecido. Y aunque aquí se ha tratado el tema de manera parcial, es perentorio implementar de alguna manera, bien sea por los intelectuales, por los legisladores o por los mismos peritos, estándares en la formación y en las buenas prácticas de los peritos informáticos.

Por otro lado, es de notar el papel relevante que se le da al perito en la propuesta. Su concepto puede llevar tal peso, que sea básicamente lo que determina el sentido del fallo del juez, al menos en cuanto a la validez de la IEA como prueba. Por lo tanto, es necesario crear una formación especial para los jueces, que si bien no tiene que ser muy compleja o exigente, les permita obtener conocimientos básicos para poder apreciar con una mentalidad más sabia y educada los peritajes que les sean entregados.

Es necesario, por lo tanto, llegar a una propuesta similar a la presentada en este escrito, pero con un énfasis judicial. Es decir, si bien el perito informático es una herramienta importante para el juez, aquél desempeña el papel de auxiliar de la justicia, mientras que éste debe ser el juzgador. Sin un entrenamiento adecuado es probable que en ocasiones el juez no logre comprender en su totalidad el peritaje que se le entrega, implicando que, a raíz de su ignorancia, le dé un valor probatorio al peritaje demasiado alto o demasiado bajo.

VII. Bibliografía

Australian Legal Information Institute, "Diccionario del *Evidence Act* de Australia de 1995".

Black, Michael Eric John, "Nota de práctica 17, anexo C".

—, "Nota de práctica 17".

— Brady, Kevin, "Evidentiary Issues and electronically Stored Information (esi)", cgog Council, Estados Unidos.

Brady, Kevin et ál., "The Sedona Conference Commentary on esi Evidence and Admissibility", The Sedona Conference Working Group Series, 2008.

Brereton, Paul Le Gay, "Evidence In Civil Proceedings: An Australian Perspective on Documentary and Electronic Evidence", septiembre de 2007 [citando el Informe 26 de la Comisión de Reforma Legal de Australia, vol. 1].

Byrne, Seamus; Lambert, Geoffrey, "Okay Computer", The Australian Corporate Lawyer, 2008.

Cano, Jeimy, *Evidencia digital: conceptos y retos*. gecti, Bogotá, Legis, 2005.

—, "Estado del arte del peritaje informático en Latinoamérica", *Alfa-Redi*.

Certain, Andrés; Cano, Jeimy; González, José, "Evidencia digital: contexto, situación e implicaciones nacionales", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, vol. I, Bogotá, Universidad de los Andes, 2005.

Código de Procedimiento Civil de Colombia.

Comisión de Reforma Legal de Australia, Revisión del *Evidence Act* de 1995, Informe 28.

Corte Constitucional de Colombia (2000), "Sentencia C-662", M. P.: Morón Díaz, F.

—, (2001), "Sentencia C-831", M. P.: Tafur Galvis, Á.

Corte Federal de Australia, "Glosario de la nota de práctica 17".

—, "Lista de descubrimiento de la nota de práctica 17".

—, "Nota de práctica 17".

—, "Nota de práctica 24".

Evidence Act, Australia, 1995.

Ghosh, Ajoy, "Guidelines for the Management of IT Evidence", Hong Kong, apec Telecommunications and Information Working Group 29th Meeting, 2004.

Paul, George; Nearon, Bruce, "The Discovery Revolution", American Bar Association, 2006.

Pimentel, Javier; Cano, Jeimy, "Consideraciones sobre el estado del arte del peritaje informático y los estándares de manipulación de pruebas electrónicas en el mundo", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, vol. III, Bogotá, Universidad de los Andes, 2007.

Ramírez, Ángela, "El estado del arte del peritaje informático en Colombia", Bogotá, Universidad de los Andes, 2008.

República de Colombia, Ley 527 de 1999.

Umaña Chaux, Andrés Felipe, "Algunos comentarios sobre el principio del equivalente funcional en la ley 527 de 1999", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, vol. I, Bogotá, Universidad de los Andes, 2005.

United States of America Federal Rules of Civil Procedure (frcp).

CAPÍTULO VIII

ESTRATEGIAS ANTIFORENSES EN INFORMÁTICA: RETOS Y REFLEXIONES

Jeimy José Cano Martínez

Cuando la palabra "obvio" se usa junto a una aseveración,
NO significa que la validez de la aseveración sea tan evidente
que no necesite ser demostrada
Russell Ackoff*

I. Introducción

Bien decía Albert Einstein: "Es absurdo pensar que obtendré cosas novedosas, haciendo siempre lo mismo". Este mensaje convoca de manera inmediata a la imaginación y a la realidad, cuestiona nuestro pensar y nuestro actuar, nos hace ver que los modelos y buenas prácticas, si bien nos permiten armonizar las acciones en un contexto operacional, táctico y estratégico, también nos muestra que son parte integral de los lentes con los cuales observamos el mundo y, por tanto, nos limitan para ver más allá de los márgenes que ellos establecen. La realidad en la que nos movemos nos supera en variedad y, por tanto, considerar acciones

* *Cápsulas de Ackoff*, p. 128.

fuera de los conceptos establecidos puede ayudarnos a mover la línea del conocimiento hasta ese momento conocida.

En este contexto, las prácticas en computación forense han venido avanzando y armonizándose de tal forma que los profesionales de esta disciplina consiguen cada vez resultados más confiables y tecnologías más efectivas (Davis, C.; Philipp, A.; Cowen, D., 2005); sin embargo, la misma dinámica de las vulnerabilidades tecnológicas y la inseguridad informática propia de los sistemas computacionales hace que día a día los esfuerzos de homogeneización de dichas prácticas reciban mensajes nuevos, que exijan repensar nuevamente la manera de cómo se adelantan las investigaciones y los análisis (Cano, J., 2007).

En consecuencia, y parafraseando a Ackoff (Ackoff, R.; Addison, H., 2007), "nadie puede diseñar un sistema que alguien más no pueda comprometer o vulnerar". Esta frase nos advierte que las mejoras y acciones adelantadas con las herramientas forenses siempre estarán expuestas a nuevos desafíos y pruebas, permitiendo nuevos desarrollos y estrategias para enfrentar la inseguridad de la información y los exigentes requisitos legales, alrededor de la evidencia digital, que se demandan al participar en un proceso judicial.

La computación antiforense plantea una reflexión en el "lado oscuro" de las investigaciones forenses. Una realidad la cual nos invita a ver "lo que nosotros no vemos", a quitarnos la venda de nuestra propia experiencia, para observar cómo cuanto conocemos puede ser vulnerado, distorsionado, escondido o destruido, sin que muchas veces nos percatemos de estos hechos. El escenario descrito debe cuestionar al investigador para reformar su propia práctica, más allá del uso de las herramientas forenses disponibles, buscando comprender cómo el atacante o intruso explora el funcionamiento mismo de los sistemas de archivo o dispositivos por fuera de lo que se exhibe en la teoría o la implementación práctica.

II. Evolución técnica de los ataques: conociendo al enemigo

Reconocer que existe un dual en computación forense es mirar a través de la lente divergente de la creatividad técnica y el desaprendizaje. Los intrusos (y también los hackers, en el buen sentido de la palabra) saben que cuando se profundiza en los conceptos establecidos es posible encontrar fuentes de luz aún desconocidas que desestabilizan el *statu quo* (Honeynet Project, 2004; Kovacich, G.; Boni, W., 2000).

Si nos remontamos a 1988, cuando se materializó el primer gusano en Internet (Ruiu, D., 2006), diseñado por Robert Morris, quien aprovechándose de una falla en los sistemas de correo electrónico logró poner fuera de servicio más de 60.000 sistemas de correo electrónico en los Estados Unidos, podemos ver que la investigación subsiguiente del hecho debió demandar un análisis detallado del protocolo de correo SMTP,[1] largas horas de seguimiento a los mensajes entre los destinos y, sobre manera, el conocimiento de la funcionalidad del gusano creado. Para esa época probablemente las herramientas forenses disponibles no eran tan abundantes, lo que exigió de los investigadores participantes mucho ingenio, conocimiento técnico y habilidad para encontrar respuesta a los interrogantes planteados.

Con el paso del tiempo, durante los años noventa, las fallas de seguridad o vulnerabilidades se fueron especializando (Ruiu, D., 2006). El *buffer overflow* (o desbordamiento de variables en los entornos de ejecución), los programas denominados *shellcodes* (códigos que al inyectarse en la memoria de un dispositivo y ejecutarse obtienen interfaz de comandos con privilegios altos), el IP *Spoofing* (la suplantación de dirección IP), la manipulación de la pila de protocolos, particularmente de TCP/IP, y la inundación de redes o sistemas de comunicaciones con

[1] SMTP: Simple Mail Transfer Protocol.

altas cantidades de paquetes válidos e inválidos, fueron la constante que puso en alerta a todas las empresas y sus mecanismos de seguridad para identificar y contrarrestar dichas manifestaciones y tratar de mantener el *control* aparente del funcionamiento de sus infraestructuras de computación y comunicaciones.

Este panorama de los noventa fue un gran reto para los investigadores forenses; tuvieron que ajustar sus prácticas y procedimientos, generalmente orientados a máquinas o dispositivos específicos, y adaptarlos a escenarios en redes donde la diversidad de sistemas operacionales, operaciones y comportamientos eran parte inherente del escenario de análisis.

Finalizando esa década e iniciando el nuevo milenio, otras formas de ataques siguieron apareciendo. Los temas orientados a la web, la inyección de código SQL, la suplantación de sitios webs, el *pharming* (envenenamiento del *caché* del servicio de nombres de dominio), las fallas en las bases de datos, la manipulación de paquetes de comunicación (fragmentación patológica, paquetes malformados), la ingeniería inversa, como estrategia para superar medidas de seguridad y control (Eilam, E., 2005) y nuevos gusanos, ahora más elaborados y con capacidad de contagio y expansión más evidente gracias a las conexiones vía web y los códigos ejecutables embebidos en sus páginas, muestran un panorama más exigente y elaborado para adelantar investigaciones forenses en informática.

Las habilidades forenses de los investigadores de este momento no solamente debían estar alimentadas por su práctica normal de manejo de evidencia, sino por el conocimiento técnico y profundo de los ataques y sus implicaciones. Durante esta época las simulaciones en laboratorios y ejercicios controlados en dichas instalaciones debían ser la práctica habitual para poder detallar los hallazgos y elaborar las conclusiones de los trabajos realizados.

Conforme ocurría esto, durante el inicio del año 2000 los intrusos nuevamente comprenden que los investigadores les siguen la pista de cerca, adaptándose rápidamente a los desafíos de la inseguridad. Luego no bastaba con perpetrar un ataque o fraude con alta destreza técnica y delicada implementación, sino que era necesario demorar o confundir a los investigadores con el fin de tener más tiempo y espacio para continuar aprendiendo, mientras ellos (los investigadores) lograban comprender qué había ocurrido (Garfinkel, S., 2007; Garfinkel, S., 2003). En este sentido, se inicia un cambio y ajuste de estrategia de los atacantes para ocultar, distorsionar o destruir los rastros que pudiesen haber quedado luego de sus acciones en los sistemas.

Con esta nueva evolución, las investigaciones forenses hasta el momento conocidas deben tener un cambio y adaptación para no sólo comprender lo ocurrido, sino conocer con mayor detalle si las evidencias recabadas corresponden al incidente y si éstas no han sido manipuladas por el atacante con el fin de evadir la investigación. Esa realidad exige de los investigadores forenses reconocer en las pruebas de vulnerabilidades efectuadas por los especialistas de seguridad un paradigma para aplicar ahora sobre las herramientas que ellos utilizan, pues la confiabilidad de éstas una vez más se somete a nuevos escenarios que pueden impactar negativamente el desarrollo de las investigaciones (Pan, L.; Batten, L., 2005).

III. Conceptos y técnicas de las investigaciones forenses en informática

Las técnicas antiforenses a la fecha no cuentan con un marco de referencia compartido para su estudio o análisis, pero revisándolas desde la perspectiva de las vulnerabilidades informáticas podríamos ver una oportunidad para comprender mejor su funcionamiento. En este sentido, las técnicas antiforenses retan a los investigadores a hacer fallar las

herramientas forenses disponibles y afinarlas (adaptado de Schneier, B., 2003).

Si bien la madurez de las herramientas forenses disponibles a la fecha es tema de investigación actual, de igual forma y con mayor preocupación están las técnicas antiforenses como ese factor crítico de éxito para ajustar los procedimientos forenses que se adelanten en las investigaciones. Es claro que los procedimientos estándares que actualmente se tienen con el objeto de asegurar la escena del incidente podrían no tener cambios significativos, pero sí requieren ser repensados y analizados a la luz de la imaginación de los atacantes para disminuir la capacidad de identificación, recolección, análisis y presentación de evidencia en un proceso.

Las técnicas antiforenses genéricas (Peikari, C.; Chuvakin, A., 2004), como las forenses específicas en informática, evolucionan y se perfeccionan; en este sentido, los conceptos base para la comprensión de sistemas de archivo, sistemas de comunicaciones, sistemas inalámbricos, medios de almacenamiento, sistemas operacionales, protocolos de comunicaciones, manejo de dispositivos electrónicos recientes como los asociados con *Radio Frequency Identification* (RFID), se vuelven críticos en la formación y práctica de los investigadores forenses, pues sin un conocimiento claro de ellos habrá mayores oportunidades del atacante para confundir y distorsionar la realidad de los hechos. Es importante aclarar el no pretenderse que el investigador tenga un conocimiento total de todos los conceptos base presentados, sino la conciencia y experiencia requerida para que en el trabajo de campo futuro sepa qué hacer, qué no y dónde puede aportar, hasta reconocer posibles estrategias de evasión por parte de los intrusos.

Las técnicas forenses en este escenario de constante evolución requieren un protocolo diferente de estandarización y ajuste para estar tan cerca como las nuevas vulnerabilidades que se presenten tanto en sus

herramientas como en las infraestructuras de las empresas. En este contexto, los encargados del mejoramiento de las prácticas forenses (institutos internacionales, organismos gubernamentales, universidades e investigadores de campo) deben dedicar parte de su tiempo a mirar cómo los eventos del entorno son relevantes para la práctica de las investigaciones forenses. No solamente se trata de la regulación del ejercicio práctico y procedimental, necesaria para generar mayor confiabilidad de los resultados (Ieong, R., 2006), sino de la capacidad para desarrollar nuevas formas de fortalecer las herramientas y técnicas utilizadas en pro del avance de la disciplina como tal y por ende de la Administración de Justicia.

IV. Un marco conceptual de estrategias antiforenses

Para desarrollar un marco conceptual de análisis de las estrategias antiforenses revisaremos algunas definiciones disponibles sobre éstas (Harris, R., 2006):

1) [...] "métodos usados para prevenir (o actuar en contra de) la aplicación de la ciencia, por parte de las agencias de policía, como apoyo a las leyes penales y civiles en un sistema de Administración de Justicia".
2) [...] "limitar la identificación, recolección y validación de datos electrónicos [...]".
3) [...] "cualquier intento para limitar la cantidad y calidad de la evidencia forense".
4) [...] "cualquier intento para comprometer la disponibilidad o utilidad de la evidencia en un proceso forense [...]".

Revisando estas definiciones, observamos que cada una de ellas hace énfasis en diferentes realidades de las investigaciones forenses. La primera

está orientada al proceso formal en el cual se funda la criminalística y el ejercicio formal de los criminalistas para apoyar a la Administración de Justicia en su búsqueda de la verdad en cada uno de los procesos. La segunda y tercera están enfocadas al proceso de la investigación que procura la mejor evidencia posible para probar lo ocurrido. Finalmente, la cuarta, trata de cubrir todas las anteriores, combinando lo requerido en el proceso formal forense y la utilidad de la evidencia identificada, recuperada y analizada.

Si tratamos de modificar la cuarta definición, podríamos expandirla de tal forma que oriente a los investigadores forenses en la práctica. La propuesta sería: "Cualquier intento exitoso efectuado por un individuo o proceso que impacte de manera negativa la identificación, la disponibilidad, la confiabilidad y la relevancia de la evidencia digital en un proceso forense".

Considerando lo anterior, las estrategias antiforenses aplicadas en la escena del posible ilícito o incidente buscan, entre otros objetivos, los siguientes (Garfinkel, S., 2007):

- Limitar la detección de un evento que haya ocurrido.
- Distorsionar la información residente en el sitio.
- Incrementar el tiempo requerido para la investigación del caso.
- Generar dudas en el informe forense o en el testimonio que se presente.
- Engañar y limitar la operación de las herramientas forenses informáticas.
- Diseñar y ejecutar un ataque contra el investigador forense que realiza la pericia.
- Eliminar los rastros que pudiesen haber quedado luego de los hechos investigados.

En consecuencia, las estrategias antiforenses establecen un nuevo capítulo en las investigaciones científicas tanto en seguridad de la información como en las ciencias forenses, pues considerando los objetivos planteados, se requiere conocer detalladamente los procedimientos forenses establecidos a la fecha para desvirtuarlos uno a uno y así generar confusión e incertidumbre en todos los actores del proceso.

Si lo previamente planteado es correcto, se hace necesario profundizar en los métodos previstos para materializar dichas estrategias antiforenses. Investigaciones recientes (Harris, R., 2006) proponen la clasificación de métodos evasivos como: destrucción de la evidencia, eliminación de la fuente de la evidencia, ocultar la evidencia y falsificación de evidencia.

Destrucción de la evidencia (Cano, J., 2007b). Este método busca modificar físicamente el objeto que contiene la evidencia requerida, de tal forma que no sea posible conseguirla de manera confiable o real. Cuando se habla de *eliminar la fuente de la evidencia*, significa neutralizar el sistema o la técnica utilizada por el sistema para dejar los rastros (Hoglund, G.; Butler, J., 2006); al controlar esta técnica o proceso no existirá la evidencia y, por tanto, no habrá trazas que seguir en una investigación (Cano, J., 2007b).

Si el atacante no ha podido materializar los dos métodos anteriores puede optar por *esconder la evidencia* o *falsificarla*. En la primera, la evidencia se dispersa en el medio que la contiene, se oculta en él o en el sistema donde se encuentra, limitando los hallazgos del investigador en su proceso. En la segunda, crea o invalida la evidencia residente en el sistema para limitar las conclusiones y análisis que adelante el investigador (Cano, J., 2007b).

Complementando la propuesta efectuada por Harris, Garfinkel (Garfinkel, S., 2007) detalla algunas técnicas tradicionalmente utilizadas para materializar los métodos previamente presentados, entre los cuales

mencionamos la sobreescritura de datos y metadatos, así como la utilización de técnicas criptográficas y esteganográficas.

La sobreescritura de datos y metadatos está asociada con la modificación física de la información residente en los medios de almacenamiento y sus sistemas de archivo. Es una manera de dejar inconsistente una posible recuperación de información o una forma de construir entradas falsas en las tablas de asignación de archivos que generen la aparición de archivos inexistentes.

Las técnicas criptográficas son un desafío para los investigadores forenses (Casey, E., 2002), ya que identificar la evidencia cifrada (sin la llave de cifra) establece una barrera para continuar con los hallazgos y genera discontinuidad en los rastros requeridos para armar la cadena de los eventos. La criptografía actualmente ataca la efectividad de las herramientas forenses y los resultados asociados con los análisis realizados por éstas. De igual forma, la esteganografía, entendida como el arte de esconder la información, no solamente sobre imágenes, sino sobre sistemas de archivo o tráfico de red, amplía el espectro de análisis y cuidados que el investigador debe tener cuando de aplicar sus procedimientos se trata (Eckstein, K.; Jahnke, M.; 2005; Sieffer, M.; Forbe, R.; Green, C.; Popyack, L.; Blake, T., 2004).

A continuación, un resumen de las técnicas y algunos ejemplos:

	Destrucción de la evidencia	*Eliminar la fuente de la evidencia*	*Esconder la evidencia*	*Falsificar la evidencia*
Destrucción del medio físico que contiene la evidencia	X			
Sobreescritura de archivos y estructuras en los sistemas de archivo	X			X

CONTINÚA...

...CONTINUACIÓN

	Destrucción de la evidencia	*Eliminar la fuente de la evidencia*	*Esconder la evidencia*	*Falsificar la evidencia*
Deshabilitación de las bitácoras de eventos		X		
Ocultar archivos dentro de otros (esteganografía)			X	
Uso de programas para cifrar información (criptografía)			X	
Manipulación de las fechas de modificación, acceso y creación de los archivos				X

V. Retos emergentes para los investigadores forenses en informática

Junto con las técnicas antiforenses se presentan nuevos retos para los investigadores forenses en informática. Dichos retos representan todo un nuevo descubrimiento de posibilidades y actividades que demandan de los investigadores entender en profundidad las posibilidades de las tecnologías y la manera como los atacantes se aprovechan de los riesgos inherentes en ellas. Veamos dos tendencias que se advierten en informática forense, con el fin de establecer un referente básico de la realidad a la que pronto se deberán enfrentar estos investigadores.

A. Rastros en ambientes virtuales

El rápido incremento de las plataformas virtuales, la virtualización de servidores y del almacenamiento, nos muestra un futuro más demandante

de reflexiones y análisis para comprender ahora en un entorno dominado por la memoria y archivos residentes en disco, lo que significa un rastro en una infraestructura virtualizada.

Los entornos virtualizados son escenarios de alta volatilidad en el manejo de memoria, múltiples referencias a archivos en disco que soportan las operaciones en memoria dinámica, redefinición de lo que significa un sistema de archivos y, por tanto, los elementos de seguridad propios del acceso a sus objetos. Si bien la virtualización busca aislar un sistema operativo de otro en el contexto de la ejecución de su entorno en la máquina que lo contiene, es probable que comparta segmentos de memoria en conjunto con otras instancias de otros sistemas operativos en ejecución, lo cual puede hacer vulnerable a una falla generalizada en la máquina original que lo contiene. Esto es, la máquina real donde se instala la máquina virtual puede comprometerse y ser atacada desde la virtual, inhabilitando probablemente los rastros tanto en la máquina virtual como en la real.

En este escenario virtual encontrar los rastros de un ataque o incidente de seguridad exige del investigador forense comprender en detalle el funcionamiento de las máquinas virtuales, su utilización de la memoria y el disco, los archivos que ayudan al manejo de cada entorno y sus relaciones entre sí. Luego de esto, establecer qué tipo de rastros podrían haber quedado en las máquinas virtuales, la identificación de los usuarios y las posibles estrategias que ha utilizado el atacante para desvirtuar las trazas identificadas.

Los ambientes virtuales son a la fecha uno de los referentes más exigentes para la computación forense, pues la definición de lo que puede ser un rastro y su materialización en el contexto real de la máquina que lo contiene requiere mayor análisis e investigación.

B. Informática forense en bases de datos

A las bases de datos hoy por hoy las podríamos llamar las "joyas de la corona" informática. Allí residen los datos fundamentales de las organizaciones. Dichos datos, luego de su procesamiento, producen la información que genera uno de los principales activos de las empresas actuales. Las bases de datos, o mejor, los sistema manejadores de bases de datos, son un gran reto para la informática forense dado que las herramientas que se han de utilizar para su análisis (a la fecha) deben ser propias del fabricante de ellas, pues no se cuenta con herramientas generales que puedan revisar y analizar los datos o información residente dentro de éstas.

Los principios fundamentales para el análisis forense en bases de datos se encuentran fundados en (Fowler, K., 2009):

- Probar o no la ocurrencia de una brecha de seguridad en los datos.
- Determinar el alcance de la intrusión en la base de datos.
- Reconstruir las operaciones de *Data Manipulation Language* (DML) y *Data Definition Language* (DDL) efectuadas por un usuario.
- Identificar las transacciones pre y postintrusión.
- Recuperar (en la medida de lo posible) los datos borrados de la base de datos.

La informática forense en bases de datos se puede realizar existan o no previamente diseñados registros de auditoría (*logging*), dado que los sistemas manejadores de bases de datos (SMBD) dejan registros de sus actividades en sitios propios de su instalación, en el sistema operacional que lo contiene o en lugares que no son reportados directamente por el proveedor del SMBD. En este sentido, se hace necesario avanzar en nuevas

distinciones sobre el funcionamiento de las bases de datos para superar aquello que afirma Ackoff (2007): "la única cosa más difícil que iniciar algo nuevo en una organización, es detener algo viejo existente en ella".

Las bases de datos han sido consideradas el corazón de los datos corporativos, configurando uno de los activos más valiosos de las empresas modernas. Por lo tanto, las medidas de seguridad requeridas para su funcionamiento confiable exigen un entendimiento detallado de las condiciones en las cuales éstas operan a fin de comprender en profundidad lo que ocurre cuando algo anormal sucede. En este contexto, se abre un nuevo capítulo complementario a lo expuesto en el tema forense, el de las técnicas antiforenses en bases de datos, que no son otra cosa que lo previamente explicado en el esquema conceptual sobre técnicas antiforenses, aplicado al mundo de los SMBD.

VI. REPENSANDO LAS INVESTIGACIONES FORENSES EN INFORMÁTICA: APRENDIENDO CON EL ENEMIGO

Parafraseando a Ackoff, tenemos que "los problemas complejos (entendiendo éstos como la falta de variedad requerida por un observador para comprender el fenómeno en estudio) no tienen soluciones simples, sólo mentes simplistas que piensan que sí las tienen". En este contexto, la complejidad que exhiben las estrategias antiforenses exige de todos los participantes una reflexión profunda para avanzar en una integración de ellas en las prácticas forenses actuales.

Repensar la práctica de la computación forense exige altos compromisos de investigación y desarrollo tanto de la Academia como de la industria, que de manera conjunta utilicen lo mejor de sus recursos para afinar las herramientas forenses informáticas disponibles frente a los retos actuales e iniciar aplicaciones forenses que utilicen heurísticas semejantes a las disponibles en los sistemas antivirus, de manera que

permitan advertir posibles usos de métodos antiforenses en los medios investigados.

De igual forma, se requiere que la Administración de Justicia y los entes de policía judicial avancen de manera coordinada con el legislador para entrar en una dinámica de entrenamiento técnico y ajuste de las regulaciones que les facilite tanto a los investigadores de campo como a las organizaciones construir marcos de acción confiables y válidos tanto desde el punto de vista jurídico y tecnológico. Es importante anotar que la integración de la tecnología y el ordenamiento jurídico es un proceso que exige desaprender de cuanto conocemos, para abrir la mente hacia las posibilidades y limitaciones que brindan los nuevos desarrollos tecnológicos, así como aprovecharnos de lo expuesto en las regulaciones actuales para potenciar los procedimientos tecnológicos actuales y futuros.

Repensar las investigaciones forenses implica estudiar y analizar los vectores de ataques y tendencias en inseguridad informática presentes en las infraestructuras computacionales y aplicaciones, para seguirles la pista a los atacantes y sus estrategias, de tal forma que se puedan incorporar nuevas distinciones de análisis en los procesos forenses.

No podemos crecer en la práctica y en el mejoramiento de los informes de pericias forenses en informática sin evidenciar la fuente misma de las investigaciones: las fallas o problemas. Bien dice Ackoff (Ackoff, R.; Addison, H., 2007) que el futuro estará mejor fundado si lo consideramos en función de las posibilidades y no de las probabilidades.

VII. Reflexiones finales

Se dice que "la mejor forma de predecir el futuro es crearlo", y para ello se requiere del concurso de cada uno de nosotros. El futuro de las

investigaciones forenses está por escribirse y las estrategias antiforenses nos ayudan a pensar en las posibilidades que tenemos para desarrollar un buen futuro en esta disciplina.

Sabemos que tarde o temprano los atacantes o intrusos nos sorprenderán con estrategias evasivas que pondrán bajo revisión los procedimientos actuales en identificación, recolección, análisis y presentación de evidencia digital. No obstante, y sin perjuicio de los avances que se realicen para actualizar las prácticas forenses, se hace necesario un cambio de mentalidad de los investigadores: pasar de un pensamiento causal, a uno más sistémico y global, de tal manera que, considerando los nexos causales sugeridos por la evidencia, podamos construir un escenario de mayores variables y posibilidades que nos permita ir más allá de los hechos y recomendar a las organizaciones acciones que potencien su capacidad preventiva y reactiva ante los incidentes.

Las estrategias antiforenses son condiciones necesarias para ver a través de los ojos de los intrusos y aumentar la variedad de las acciones de los investigadores en sus procedimientos, y condición (no siempre) suficiente para ver las diversas alternativas que la imaginación de los investigadores e intrusos pueden lograr para intranquilizar a los peritos informáticos en el desarrollo de un proceso de investigación forense en informática.

Explorar el terreno de las estrategias antiforenses y sus métodos asociados es equivalente a recorrer los secretos de la creatividad: "suspender nuestras estrategias analíticas de pensamiento, para permitirnos encontrarnos, *sin prejuicios*, directamente con el sistema" (Senge, P.; Scharmer, C.; Jaworski, J.; Flowers, B., 2005) y, así, dejarnos sorprender por la riqueza de sus relaciones y posibilidades.

VIII. Bibliografía

Ackoff, R.; Addison, H., *Management F-law. How organizations really work*, Triarchy Press, 2007.

Akella, J.; Kanakamedala, K.; Roberts, R., "What's on CIO agendas in 2007: A McKinsey Survey", The McKensey Quarterly.

Cano, J., "Inseguridad informática y computación antiforense. Dos conceptos emergentes en seguridad informática", 2007.

—, "Administrando la confidencialidad de la información: algunas consideraciones sobre el saneamiento de medios de almacenamiento", 2007.

Casey, E., "Practical approaches to recovering encrypted digital evidence", Proceedings of Digital Forensic Research Workshop, 2005.

—, "Investigating Sophisticated security breaches", en *Communications of ACM*, vol. 49, núm. 2, pp. 48-54.

Davis, C.; Philipp, A.; Cowen, D., *Hacking Exposed. Computer Forensics*, McGraw-Hill, 2005.

Eckstein, K.; Jahnke, M., "Data hiding in journaling file systems", Proceedings of Digital Forensic Research Workshop, 2005.

Eilam, E., *Reversing. Secrets of reverse engineering*, John Wiley & Sons, 2005.

Fowler, K., *SQL Sever forensic analysis*, Addison Wesley, 2009.

Garfinkel, S., "Remembrance of Data Passed: A Study of Disk Sanitization Practices", en *IEEE Security & Privacy*.

—, "Anti-Forensics: Techniques, Detection and Countermeasures", Proceeding of The 2nd International Conference on i-Warfare and Security (ICIW), Naval Postgraduate School, Monterrey, CA.

— Garfinkel, T.; Rosenblum, M., "When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments", Department of Computer Science, Stanford University.

HARRIS, R., "Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem", *en Digital Investigation*, pp. 44-49.

HOGLUND, G.; BUTLER, J., *Subverting the windows kernel. Rootkits*, Addison Wesley, 2006.

HONEYNET PROJECT, *Know your enemy. Learning about security threads*, Addison Wesley, 2004.

IEONG, R., FORZA, "Digital Forensics Investigation Framework That Incorporate Legal Issues", Proceedings of Digital Forensic Research Workshop, 2006.

KOVACICH, G.; BONI, W., *High-technology crime investigator's handbook. Working in the global information environment*, Butterworth Heinemann, 2000.

PAN, L.; BATTEN, L., "Reproducibility of Digital Evidence in Forensic Investigations", Proceedings of Digital Forensic Research Workshop, 2005.

PEIKARI, C.; CHUVAKIN, A., *Security warrior*, O'Reilly, 2004.

RUIU, D., "Learning from information security history", en *IEEE Security & Privacy*, 2006.

SCHNEIER, B., *Beyond fear. Thinking sensible about security in an uncertain world*, Copernicus Books, 2003.

SENGE, P.; SCHARMER, C.; JAWORSKI, J.; FLOWERS, B., *Presence. Exploring profound change in people, organizations and society*, Currency Doubleday, 2005.

SIEFFER, M.; FORBE, R.; GREEN, C.; POPYACK, L.; BLAKE, T., "Stego intrusion detection system", Proceedings of Digital Forensic Research Workshop, 2004.

Este libro se terminó de imprimir en los talleres
de Editorial Kimpres ltda., en mayo de 2010,
año del Bicentenario de la Independencia
de la República de Colombia (20 de julio de 1810).

LABORE ET CONSTANTIA

BIBLIOTECA JURÍDICA UNIANDINA

Derecho procesal civil
María del Socorro Rueda (Coord.)

Introducción a las infracciones urbanísticas
Aída Elena Lemus Chois - Víctor David Lemus Chois

De las sociedades comerciales
Lisandro Peña Nossa

Arbitraje internacional en materia tributaria
Eleonora Lozano Rodríguez

Derecho de las obligaciones, tomo I
Marcela Castro de Cifuentes (Coord.)

Manual de derecho administrativo
Helena Alviar García (Coord.)

Derecho comercial. Actos de comercio, empresas, comerciantes y empresarios
Marcela Castro de Cifuentes

La propiedad intelectual en la era de las tecnologías
Wilson Rafael Ríos Ruiz

Restablecimiento de derechos de la infancia
Miguel Enrique Rojas Gómez

Temas de derecho penal
Ricardo Posada Maya (Coord.)

Fundamentos de la tributación
Eleonora Lozano Rodríguez (Coord.)

Portafolios de inversión: la norma y el negocio
Juan Carlos Varón Palomino

La culpa en el derecho sancionador
Daniel Fernando Jiménez J.

Derecho de las organizaciones internacionales
René Urueña

Derecho, desarrollo y feminismo en América Latina
Helena Alviar García

Derecho de las telecomunicaciones
GECTI

La construcción del derecho administrativo colombiano
Diego Isaías Peña Porras

La letra y el espíritu de la ley
Diego Eduardo López Medina

Arbitraje comercial internacional. Instituciones básicas y derecho aplicable
Santiago Talero Rueda

El peritaje informático y la evidencia digital en Colombia. Conceptos, retos y propuestas es el quinto libro publicado por el Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho de la Universidad de los Andes. Se trata de una obra, dirigida por el profesor Jeimy Cano Martínez, que reúne un conjunto de investigaciones especializadas sobre el peritaje informático y la evidencia digital.

El GECTI se ha propuesto aunar esfuerzos, compartir y difundir conocimientos para poner en marcha una articulación valiosa entre expertos de distintas disciplinas que le permita fomentar un trabajo multidisciplinario y establecer un puente entre la universidad y la sociedad con el fin de promover reflexiones y acciones en materia de Internet, la sociedad de la información, las telecomunicaciones y temas convergentes. En desarrollo de dicho objetivo, el profesor Cano se encargó de la definición temática y metodológica de los capítulos.

Universidad de los Andes

ISBN 978-958695492-1
9 789586 954921