LA EFICACIA DE LA PRUEBA DIGITAL EN EL PROCESO PENAL COLOMBIANO

DIANA MARÍA RENDÓN LÓPEZ

FUNDACION UNIVERSITARIA CATOLICA DEL NORTE
EN CONVENIO CON LA UNIVERSIDAD DE MEDELLIN
ESPECIALIZACION PROBATORIO PENAL
ARMENIA 2012

LA EFICACIA DE LA PRUEBA DIGITAL EN EL PROCESO PENAL COLOMBIANO

DIANA MARÍA RENDÓN LÓPEZ

Trabajo de Grado presentado como requisito para obtener el título de Especialización Derecho Probatorio Penal

Asesor de contenido:

Dr. CARLOS ALBERTO MOJICA ARANQUE

NOTA DE ACEPTACIÓN

Firma del presidente del jurado

Firma del jurado

Firma del jurado

DEDICATORIA

Este trabajo de grado lleva todo mi amor por el derecho y se lo dedico a mi hijo que es mi gran inspiración.

Diana María

AGRADECIMIENTOS

La Autora expresa su agradecimiento a:

Dios que fue mi mayor inspiración, que me dio la fortaleza para aguantar tantas noches de trasnocho, empleo para poder sobrellevar los gastos, y me dotó de una familia buena que no me abandonó en ningún momento.

Al Doctor Carlos Alberto Mojica Araque, Docente del Programa de Derecho, de la Fundación Universitaria Católica del Norte en Convenio con la Universidad de Medellín, quien siempre puso a mi disposición su conocimiento y sabiduría.

Así mismo a todas aquellas personas que con su grano de arena me apoyaron y permitieron que sacara adelante este seminario.

TABLA DE CONTENIDO

CAPÍTULO I.

1. EL PROBLEMA

1.1. SELECCIÓN DEL TEMA

LA EFICACIA DE LA PRUEBA DIGITAL EN EL PROCESO PENAL COLOMBIANO.

1.2. PLANTEAMIENTO DEL PROBLEMA

1.2.1. Enunciado.

Evaluar las dificultades que presentan la prueba digital en el proceso penal en cuanto al decreto, práctica y valoración dentro del sistema procesal colombiano.

1.2.2. Descripción.

El artículo 382. MEDIOS DE CONOCIMIENTO. Dice a la letra: “Son medios de conocimiento la prueba testimonial, la prueba pericial, la prueba documental, la prueba de inspección, los elementos materiales probatorios, evidencia física, o cualquier otro medio técnico o científico, que no viole el ordenamiento jurídico”.

1.2.3. Formulación del problema.

¿Qué dificultades presenta la prueba digital en el proceso penal en cuanto al decreto, práctica y valoración dentro del sistema procesal colombiano?

1.3. OBJETIVOS

1.3.1 Objetivo general.

Evaluar las dificultades que presentan la prueba digital en el proceso penal en cuanto al decreto, práctica y valoración dentro del sistema procesal colombiano

1.3.2. Objetivos Específicos

- Evaluar las dificultades que presenta la prueba digital en el proceso penal en cuanto al decreto de la prueba dentro del sistema procesal colombiano
- Evaluar las dificultades que presenta la prueba digital en el proceso penal en cuanto a la práctica de la prueba dentro del sistema procesal colombiano
- Evaluar las dificultades que presenta la prueba digital en el proceso penal en cuanto a la valoración de la prueba dentro del sistema procesal colombiano

1.4. JUSTIFICACIÓN

La computadora y el manejo del Internet son herramientas principales o el medio para cometer conductas delictivas designadas como "Delitos Informáticos"

Entre los delitos informáticos tenemos: los que incluyen los cometidos contra el sistema y los cometidos por medio de sistemas informáticos ligados con Telemática, o a los bienes jurídicos que se han relacionado con la información: datos, documentos electrónicos, dinero electrónico…entre ellos están: acceso no autorizado, destrucción de datos, infracción de los derechos de autor, distribución de música por Internet (mp3), intercepción de E-mail, estafas electrónicas, transferencias de fondos.
La evidencia digital recolectada debe proteger su integridad, por ello las personas que manejan y recolecten esta evidencia debe ser calificada; hay unos principios sacramentales para su recolección y son identidad, integridad,

preservación, seguridad, almacenamiento, continuidad, autenticidad y originalidad. La evidencia digital debe ser manejada conforme a un procedimiento legal, se debe asegurar que las evidencias tomadas, no se modifiquen, pues deben conservar su estado original, y la persona que la recolecte debe estar debidamente entrenada y calificada para este propósito, su obtención debe estar completamente documentadas, preservadas y disponibles para su revisión

1.5. DELIMITACIÓN DEL PROBLEMA

1.5.1. Conceptual.

Esta investigación está delimitada conceptualmente por las siguiente variable respecto de la línea jurisprudencial y la ley 906 de 2004.

CAPÍTULO II.

2. MARCO REFERENCIAL

Cada día los infractores, tienen habilidades para el manejo de los sistemas informáticos, y sus víctimas pueden ser individuos, instituciones crediticias, gobiernos, empresas o personas, su fin es dañar en la mayoría de los casos el patrimonio de la víctima.

Razón por la que los operadores judiciales deben procurar una oportuna actualización de conocimientos para poder comprender el impacto que han provocado los avances tecnológicos en la sociedad y con ello el crecimiento sostenido que tendrán las nuevas fuentes de prueba digital. Se requiere un esfuerzo intelectual no solamente en cuestiones de derecho penal sustantivo, sino también en los aspectos de derecho penal adjetivo atinentes a la relación entre la investigación judicial y las nuevas tecnologías.

Profundizar en el tema, nos ayuda a tener un conjunto de ideas y/o conocimientos que tanto la Doctrinas, la Jurisprudencia y la Legislación referente a la prueba digital.

2.1. MARCO DE ANTECEDENTES

2.1.1 Antecedentes bibliográficos

- http://www.fiscalia.gov.co/moduloseeiccf/M8_ManejoPruebas200109.pdf
- http://www.corteconstitucional.gov.co/relatoria/2010/C-334-10.htm
- http://nisimblat.net/images/MEDIOS_DE_PRUEBA_UNIDAD_II_NATTAN_NISIMBLAT.pdf
- http://www.secretariasenado.gov.co/senado/basedoc/ley/2004/ley_09060_204a_pr009.html
- http://blogs.politicadigital.com.mx/firma-electronica/?p=212

- http://www.cej.org.co/component/docman/doc_view/377-evidencia-digital-en-colombia-una-reflexion-en-la-practica
- http://www.acis.org.co/index.php?id=856
- http://www.google.com.co/search?client=firefox-a&rls=org.mozilla%3Aes-ES%3Aofficial&channel=s&hl=es&source=hp&biw=1267&bih=654&q=Ley+prueba+digital&oq=
- http://www.revistajuridicaonline.com/index.php?option=com_content&task=view&id=155&Itemid=71

2.1.2 Antecedentes legales.

- Ley 906 de 2004
- Ley 599 de 2000
- Constitución Política de 1991
- Ley 527 de 1999

2.1.3 Antecedentes Jurisprudenciales.

- Sentencia C-334/10
- Sentencia C-144/10
- Sentencia No. C-662 de Junio 8 de 2000

2.2. MARCO CONCEPTUAL

2.2.1 Definición de términos básicos

- **DELITO INFORMATICO**. o crimen electrónico, es el término genérico para aquellas operaciones ilícitas realizadas por medio de Internet o que

tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

- **PRUEBA DIGITAL**. Es el examen y estudio que realiza un perito versado en una ciencia arte u oficio, cuyos servicios son utilizados por el juez para que lo ilustre en el esclarecimiento de un hecho que requiere de conocimientos especiales científicos o técnicos, para luego entregar su informe o dictamen pericial con sujeción a lo dispuesto por la ley.
-
- **TECNOLOGIA**. es el conjunto de conocimientos técnicos, ordenados científicamente, que permiten diseñar y crear bienes y servicios que facilitan la adaptación al medio ambiente y satisfacer tanto las necesidades esenciales como los deseos de las personas.

- **COMPUTADOR.** Llamado también ordenador, es una máquina electrónica que recibe y procesa datos para convertirlos en información útil.

2.3. MARCO TEÓRICO

Con el incremento del número de delitos informáticos presentados en todo el mundo, gran cantidad de países se han visto obligados a tener en cuenta este concepto en sus Legislaciones y a reglamentar la admisión de la evidencia digital en una corte. Colombia no es la excepción y, en consecuencia, los equipos nacionales de atención a incidentes informáticos deben trabajar con técnicas rigurosas que garanticen la admisibilidad legal de la evidencia digital en situaciones judiciales.

Dado que no existen investigaciones iguales, no es posible definir un procedimiento único para adelantar un análisis en Informática forense. Pero, si es posible definir una aproximación metodológica que permita el manejo adecuado de la evidencia digital, minimice la posibilidad de cometer errores en su manejo y que en alguna medida garantice la admisibilidad de la misma en situaciones jurídicas. Dicha aproximación incluye cinco etapas: planeación, recolección, aseguramiento, análisis y presentación de la Evidencia Digital.

CAPITULO III.

3. DISEÑO METODOLÓGICO

3.1. Tipo de Investigación.

El Tipo de Investigación que se viene utilizando en este trabajo, es de tipo cualitativo y documental porque es el que más se adapta al tema que estoy trabajando.

Es de público conocimiento que el entorno de la tecnología de la información está cambiando rápida y radicalmente el modo en que las personas utilizan los sistemas de información, lo que ha hecho que los delitos informáticos cada día sean más apetecidos por los infractores, y en el mismo modo son complejos de investigar, hecho que ha generado que los peritos encargados de recolectar dichas pruebas cada día se tengan que actualizar, para elevar la calidad del servicio pericial, aunque el apoyo institucional no han sido los suficientes como ellos los esperan.

Es importante mencionar, que no se espera que toda la información que se examine y/o recolecte deba ser admisible como evidencia. Mucha de esta información será utilizada para, a través de ella, descubrir evidencia admisible.

3.2. Instrumentos para la recolección de la información.

Una vez localizados los rastros o documentos que van hacer objeto de investigación, el analista forense realiza:

- Exhaustiva labor de revisión, documentación e interpretación técnica de los resultados
- Informe Pericial
- Ratificación del informe
- La cantidad de información que se debe recolectar deber ser decidida por el investigador durante la etapa de planeación, teniendo en cuenta las hipótesis planteadas, las evidencias registradas y los elementos recolectados en los testimonios de los involucrados.

Es importante mencionar, que no se espera que toda la información que se examine y/o recolecte deba ser admisible como evidencia. Mucha de esta información será utilizada para, a través de ella, descubrir evidencia admisible [6].

La cantidad de información que se debe recolectar deber ser decidida por el investigador durante la etapa de planeación, teniendo en cuenta las hipótesis planteadas, las evidencias registradas y los elementos recolectados en los testimonios de los involucrados.

3.3. CRONOGRAMA DE ACTIVIDADES

ACTIVIDAD	NOV	DIC	ENE	FEB	MAR	MAYO
ELABORACIÓN DE OBJETIVOS						
REVISIÓN DE OBJETIVOS						
ELABORACIÓN MARCO CONCEPTUAL						
REVISIÓN MARCO CONCEPTUAL						
PROCESAMIENTO Y ANÁLISIS DE DATOS						
REVISIÓN DE JURADOS						
SUSTENTACIÓN						

CAPITULO IV.

4. APLICACIÓN DEL PROYECTO

4.1. ANÁLISIS DE DATOS.

El perito lo aplicará en los delitos informáticos, tenemos:

1. los cometidos contra el sistema y
2. los cometidos por medio de sistemas informáticos ligados con Telemática, o a los bienes jurídicos que se han relacionado con la información de:

- Datos
- Documentos electrónicos
- Dinero electrónico.
- Acceso no autorizado
- Destrucción de datos
- Infracción de los derechos de autor
- Distribución de música por Internet (mp3)
- Intercepción de E-mail
- Estafas electrónicas
- Transferencias de fondos.

EVIDENCIA DIGITAL Y MATERIAL[1]

La informática trabaja en dos escenarios sobre los cuales realizará el perito sus respectivos análisis, uno de ellos es el hardware (evidencia material) que se refiere a los componentes físicos de un sistema informático en particular tales como el monitor o pantalla, impresora, módems, reuters, entre otros y el otro se refiere al componente lógico es decir, a los programas computacionales, esto es, un conjunto de instrucciones para ser usadas por el ordenador con el objeto de obtener un determinado proceso o resultado.

Las personas que cometen delitos informáticos, son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, **los sujetos activos** poseen habilidades para el manejo de los sistemas

[1] José Custodio Chafloque

informáticos, generalmente por su situación laboral se encuentran en lugares estratégicos, donde se maneja información de carácter sensible; o bien son hábiles en el uso de los sistemas informatizados, aún cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Para referirse a los **sujetos pasivos**, se debe hacer una clara diferencia con las víctimas del delito, bueno pues, este último es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, en el caso de los delitos informáticos, las víctimas pueden ser individuos, instituciones crediticias, gobiernos u otros, quienes usan sistemas automatizados de información, generalmente conectados a otros. El sujeto pasivo del delito que en este caso nos ocupamos, es sumamente importante para el estudio de los delitos informáticos, ya que mediante el podemos conocer los diferentes ilícitos cometidos por los delincuentes informáticos, con la finalidad de prever las acciones pertinentes y, descubrir a tiempo el delito y, no de forma casual, debido al desconocimiento del modus operando de los sujetos activos. El bien jurídico penala tutelar, en el delito informático sería, "la información como valores económicos de la empresa", el mismo que no sólo constituye un interés social vital, sino que cumple con las exigencias de merecimiento de protección y necesidad de tutela concordante con la concepción de bien jurídico penal adoptada. La necesidad de tutela penal habrá de calificarse en atención a la eficacia de los medios de control social, en efecto, un interés social requerirá de protección en sede penal, cuando los demás medios con los que disponen las otras ramas del derecho hayan fracasado, pues como subraya **Berdugo , "**el Derecho Penal es sólo uno de los tantos instrumentos de control social existentes y posiblemente no sea el más importante de ellos..." Se puede decir que la informática y la información, como valor económico no tiene regulación específica en nuestro país, a diferencia de lo que ocurre en Derecho Comparado, no obstante, existen normas que de alguna u otra forma hacen referencia a ellas, así por ejemplo, la Ley de Derechos del Autor (D.L. Nº 822).

Aspectos clave a tener en cuenta en un caso informático[2]

A continuación, detallo algunos puntos importantes a tener en cuenta ante un caso que requiera análisis de información en computadora:

1. Tomar precauciones en el transporte y/o almacenamiento de la evidencia en computadora. La evidencia electrónica en muy frágil. El calor, polvo y campos magnéticos pueden destruir o alterarla en un periodo muy corto de tiempo. Se deben mantener todos los elementos de computación en lugares apropiados y sertrasladados con extremada precaución.

[2] Actuaciones en Delitos Informáticos, Autor: Lic. Sebastián Gómez, Perito Informático Oficial, Tribunal Superior de Justicia del Neuquén

*2. No encender u operar la computadora a inspeccionar.*La información de la computadora debe ser resguardada usando algún procedimiento de backup a nivel de bit stream (imagen completa del disco). Cuando la computadora esta en uso, existen riesgos potenciales de sobreescribir información almacenada en áreas de almacenamiento temporales que pueden
ser una importante fuente para la evidencia.

3. No solicitar la asistencia del "experto" en computación local. Sin el entrenamiento apropiado, cualquier persona con conocimientos de computación puede realizar procedimientos incorrectos. El Perito Informático, normalmente recibe la solicitud de intervención después de que ha sucedido el hecho. En muchos casos, evidencia informática valiosa se pierde porque alguna persona ha intentado realizar algún proceso en busca de información. Por estas razones, se debe requerir la asistencia del Perito Informático antes de encender la computadora. Actuaciones en Delitos Informáticos Lic. Sebastián Gómez

4. No ejecutar Windows para ver archivos gráficos y examinar archivos. El área de swap de Windows, puede ser una fuente invaluable de fragmentos de datos, contraseñas y claves para accesos a red. La ejecución de Windows puede destruir evidencia que existe en el archivo de swap. Además, ejecutando browsers como NetScape o Internet Explorer, puede destruirse o modificarse la evidencia almacenada en bookmarks, archivos gráficos y/o archivos de caché. Muchas veces, Windows es necesario para visualizar algunos archivos gráficos específicos y otros tipos de archivo. Sin embargo, la ejecución de Windows no debería llevarse a cabo hasta no haber hecho un backup a nivel de bit stream y haber analizado el área de swap en busca de evidencia potencial en forma de fragmentos de datos.

5. No chequear las computadoras que contienen la posible evidencia con antivirus. La evidencia podría alterarse o perderse si es afectada por un virus. Además sin los procedimientos adecuados se corren riesgos de aumentar la infección de
archivos o computadoras.

*6. No evaluar los e-mail de los empleados de una empresa, a menos que esto este autorizado.*Existen leyes de privacidad electrónica que protegen estos medios de comunicación. Antes de utilizar alguna herramienta para analizar este tipo de información, se debe chequear que no existan restricciones legales.

Función del Perito Informático en causas civiles y penales

La evidencia técnica ha comenzado a ser muy importante para la prueba de casos civiles y penales. Esta importancia se debe, en parte a los avances en la ciencia y en tecnología de computación. Durante la búsqueda de evidencia, es probable que puedan realizarse alteraciones en la información, y que esto lleve a planteos de nulidades. Vemos que es extremadamente importante que el procesamiento de evidencia en computadora sea realizado correctamente en casos delictivos. El

Perito Informático adquiere vital importancia para defender técnicamente estas búsquedas. Actuaciones en Delitos Informáticos
Lic. Sebastián Gómez

EL CONCEPTO DE DELITO INFORMÁTICO Y RELACIÓN CON OTRAS FIGURAS DELICTIVAS[3]

No existe un concepto unánimemente aceptado de lo que sea el delito informático debido a que la delincuencia informática comprende una serie de comportamientos difícilmente reducibles o agrupables en una sola definición.

De manera general, se puede definir el delito informático como aquél en el que, para su comisión, se emplea un sistema automático de procesamiento de datos o de transmisión de datos[ii].

En nuestra legislación esta figura se encuentra descrita en el artículo 186°, inciso 3, segundo párrafo, del Código Penal. Este hecho merece ser resaltado puesto que en otros países se habla de delito informático en sentido de lege ferenda ya que carecen de una tipificación expresa de estos comportamientos.

La aparición de estas nuevas conductas merece, no obstante, determinar si las figuras delictivas tradicionales contenidas en el Código Penal son suficientes para dar acogida al delito informático.

2.1 Delito de Estafa

Entre las conductas defraudatorias cometidas mediante computadora y las defraudaciones en general, -dentro de las cuales se encuentra la estafa- existe una afinidad o proximidad en los conceptos. Pero al examinar más exhaustivamente los elementos típicos de la estafa, se acaba concluyendo que el fraude informático y el delito de estafa prácticamente sólo tienen en común el perjuicio patrimonial que provocan[iii].

Dentro de las manipulaciones informáticas se distingue:

a) La fase input o entrada de datos en la cual se introducen datos falsos o se modifican los reales añadiendo otros, o bien se omiten o suprimen datos.
b) Las manipulaciones en el programa que contiene las órdenes precisas para el tratamiento informático.
c) La fase output o salida de datos, donde no se afecta el tratamiento informático, sino la salida de los datos procesados al exterior, cuando van a ser visualizados en la pantalla, se van a imprimir o registrar.

[3] DELITOS INFORMÁTICOS,, Dr. Luis Alberto Bramont-Arias Torres,Publicado en Revista Peruana de Derecho de la Empresa, "DERECHO INFORMATICO Y TELEINFORMÁTICA JURÍDICA" N° 51

d) Las manipulaciones a distancia, en las cuales se opera desde una computadora fuera de las instalaciones informáticas afectadas, a las que se accede tecleando el código secreto de acceso, con la ayuda de un modem y de las líneas telefónicas.

El punto medular de la delincuencia informática es la manipulación de la computadora. La conducta consiste en modificaciones de datos, practicados especialmente por empleados de las empresas perjudicadas, con el fin de obtener un enriquecimiento personal, por ejemplo, el pago de sueldos, pagos injustificados de subsidios, manipulaciones en el balance, etc.
El delito de estafa, previsto en el art. 196° CP, se define como el perjuicio patrimonial ajeno, causado mediante engaño, astucia, ardid u otra forma fraudulenta, induciendo o manteniendo prendida por el delito de estafa.

En primer lugar, y en cuanto al engaño que se requiere en la estafa, éste se refiere de manera directa a una persona física, aunque últimamente algunos autores indican que puede estar dirigido a una persona jurídica. Sin embargo, el problema principal estriba en si la introducción de datos falsos en una máquina equivale al engaño sobre una persona. La opinión unánime de la doctrina, -y a la que nos adherimos-, rechaza tal identificación, puesto que, mientras en un extremo se encuentra el delincuente informático, en el otro existe una computadora. En realidad, para que exista engaño, es requisito la participación de dos personas.

Es indudable que en algunas conductas de manipulación fraudulenta sí se podrá configurar el delito de estafa, por ejemplo, cuando el delincuente informático engaña mediante una computadora a otra persona que se encuentra en el otro terminal; en este caso, al haber dos personas, podrá sustentarse el engaño, en donde el medio empleado para conseguirlo es una computadora.

También en la actualidad se puede plantear el engaño a una persona jurídica, como en el caso en que se solicita un préstamo al banco, falseando la situación económica real, o en el que ante una compañía de seguros se miente sobre el verdadero estado de salud de la persona.

Desde el punto de vista del Derecho Penal, se niega la posibilidad de engañar a una máquina. En este sentido, la computadora es sólo una máquina, un instrumento creado por el hombre.

En cuanto al error, como elemento de la estafa, se requiere la concurrencia de dos personas, lo cual se deduce de la descripción del tipo en el art. 196° CP, donde se indica “induciendo o manteniendo en error al agraviado mediante engaño”. Además, el error es entendido como el estado psíquico que padece el agraviado como consecuencia del engaño. Por estas razones es que en la manipulación de computadoras, tal y como está concebida y establecida en el Código Penal, no es posible sustentar que existe un engaño. De otro lado, no puede sostenerse que la

computadora incurre en un error, dado que actúa conforme a los madatos o datos de las instrucciones manipuladas[iv].

Por tanto, no hay estafa en los casos de manipulación de máquinas automáticas, pues no se puede hablar ni de error ni de engaño; sólo podrá plantearse hurto en el caso que se obtenga un bien mueble, pero será un hecho impune cuando se trata de prestación de servicios. Un problema semejante tiene lugar con la manipulación de computadoras a través de la introducción y alteración de programas[v].

En referencia al acto de disposición patrimonial en el delito de estafa, éste ha de realizarlo la persona engañada, quien se encuentra en una situación de error, de ahí que siempre se entienda en la estafa que el acto de disposición es un acto humano, es decir, realizado por una persona. En el caso de las manipulaciones informáticas fraudulentas el acto de disposición lo realiza la computadora, con lo cual se rompe el esquema planteado en el delito de estafa.

Finalmente, en cuanto al perjuicio en el delito de estafa, éste no ofrece mayor problema para comprenderlo dentro de la manipulación de una computadora, puesto que en ambos casos normalmente se causa un perjuicio a la persona.

En conclusión, en la legislación peruana, la casi totalidad de supuestos de manipulación de computadoras no puede acogerse dentro del delito de estafa. La única manera sería creando un tipo especial defraudatorio donde se prescinda de los elementos básicos de la estafa, -el engaño a una persona y la subsiguiente provocación del error-, tal como sucedió en Alemania con la creación del parágrafo 263 a) del Código Penal alemán.

2.2 El delito de Daños

El delito de daños se encuentra tipificado en el art. 205° CP. El comportamiento consiste en dañar, destruir o inutilizar un bien.

En el sistema informático, el delito de daños existirá si usuarios, carentes de autorización, alteran o destruyen archivos o bancos de datos a propósito.
Es importante precisar que, si los daños se producen de manera negligente, quedarán impunes dado que el delito de daños sólo puede cometerse de manera dolosa.
Estos hechos se conocen como “sabotaje”, hechos que resultan ser favorecidos gracias a la concentración de información en un mínimo espacio. La destrucción total de programas y datos puede poner en peligro la estabilidad de una empresa e incluso de la economía nacional[vi].
El modus operandi de estos actos se viene perfeccionando con el tiempo[vii]; en primer lugar, se realizaban con la causación de incendios, posteriormente, con la

introducción de los denominados “programas crasch”, virus, time bombs (la actividad destructiva comienza luego de un plazo), cancer roudtine (los programas destructivos tienen la particularidad de que se reproducen por sí mismos), que borran grandes cantidades de datos en un cortísimo espacio de tiempo.
Es indudable que estos comportamientos producen un daño en el patrimonio de las personas, por lo que no hay inconveniente en sancionar penalmente dichas conductas. Pero
es necesario indicar que con el delito de daños sólo se protege un determinado grupo de conductas que están comprendidas en el delito informático, quedando fuera otras, como por ejemplo, el acceso a una información reservada sin dañar la base de datos. De ahí que el delito de daños será de aplicación siempre que la conducta del autor del hecho limite la capacidad de funcionamiento de la base de datos.

2.3 El delito de falsedad documental

El delito de falsedad documental se encuentra tipificado en el art. 427° CP. La conducta consiste en hacer, en todo o en parte, un documento falso o adulterar uno verdadero que pueda dar origen a derecho u obligación o servir para probar un hecho.
El objeto material del delito es el documento. Se entiende por documento toda declaración materializada procedente de una persona que figura como su autor, cuyo contenido tiene eficacia probatoria en el ámbito del tráfico jurídico.
Para que exista documento, por tanto, es preciso la materialización de un pensamiento humano, entendida como la existencia de un soporte corporal estable, reconocible visualmente, atribuible a una persona e individualizable en cuanto su autor. Esto sí se puede predicar de los datos y programas de las computadoras[viii], en tanto la información se encuentre contenida en discos, siempre y cuando sea posible tener acceso a ésta. De ahí que el documento informático goce, al igual que el documento tradicional, de suficiente capacidad como medio probatorio, característica principal en función de la cual se justifica la tipificación de conductas tales como la falsedad documental[ix]. Al respecto, es necesario indicar que el art. 234° del Código Procesal Civil expresamente reconoce como documento las microformas tanto en la modalidad de microfilm como en la modalidad de soportes informáticos, haciendo referencia a la telemática en general, siempre y cuando recojan, contengan o representen algún hecho, o una actividad humana o su resultado.
Sin embargo, desde el punto de vista práctico, plantea problemas la posibilidad de determinar al autor del documento informático, dado que se exige normalmente que el documento sea la expresión de un pensamiento humano, situación que a veces es difícil reconocer por cuanto incluso existen computadoras capaces de crear nuevos mensajes a partir de los datos introducidos por el sujeto. En estos casos, la cuestión sería determinar hasta dónde llega la autonomía de la máquina para crear su propia fuente de información.

Por tanto, esta modalidad delictiva puede aplicarse al delincuente informático siempre y cuando se supere la concepción tradicional de documento que mantiene la legislación penal peruana, anclada básicamente en un papel escrito, y que se acepten nuevas formas de expresión documental, sobre la base de disquetes, CD, discos duros, en cuanto sistemas actuales de expresión de información.

2.4 Los delitos contra la propiedad intelectual

Los delitos contra la propiedad intelectual están tipificados en el art. 216° CP. El comportamiento consiste en copiar, reproducir, exhibir o difundir al público, en todo o en parte, por impresión, grabación, fonograma, videograma, fijación u otro medio, una obra o producción literaria, artística, científica o técnica, sin la autorización escrita del autor o productor o titular de los derechos.
Según esto, el sujeto se aprovecha de la creación intelectual de una persona, reproduciéndola, por lo que se afecta tanto al derecho del autor sobre su obra, como a los posibles titulares de este derecho, si es que ha sido cedido a otra persona.
A esta conducta los autores asimilan lo que se conoce como "piratería de software" frente a la copia lícita. Estos hechos han alcanzado en la realidad una especial gravedad dada la frecuencia con la que abundan copias piratas de todo tipo de programas de computadoras. Inclusive, en nuestro país ello ha obligado a la creación de una fiscalía especializada en la persecución de todas las conductas relativas a la defraudación del derecho de autor. Estas conductas representan un considerable perjuicio económico al autor, quien deja de percibir sus correspondientes derechos por la información y venta del software, que es elaborado con un considerable esfuerzo, en el cual, a menudo, se encierra un valioso know how comercial[x].

Por tanto, el delito contra la propiedad intelectual sólo comprenderá un grupo de comportamientos incluidos en el delito informático, básicamente, los referidos a la defraudación del derecho de autor por su creación científica en el campo del software.

EL ALCANCE DE LA LEY 527 DE 1999 Y DE LOS PRINCIPIOS MEDULARES QUE INCORPORA.[4]

Sobre el particular, surge un gran interrogante: ¿Se puede, en el sistema jurídico colombiano, realizar todo tipo de negocios, operaciones y transacciones en un entorno netamente digital, o, en razón de determinados requisitos se "escapan" de dicho entorno una serie de contratos y relaciones?

[4] **LEONARDO ESPINOSA QUINTERO,** Director Departamento de Derecho Comercial, Director Grupo de Investigación Globalización y Derecho, Universidad Sergio Arboleda 15 de marzo de 2010.

En primer lugar, es pertinente, mencionar que el Art. 1 de la Ley 527 de 1999 establece que, sus disposiciones, serán aplicables a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos:

a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales; b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

Es preciso advertir que, para los casos mencionados en el Art. 1 citado, se requiere que la legislación incorpore o facilite en sus marcos normativos concretos, el empleo de los medios o vías electrónicas. Por lo tanto, la lectura final no es la de que las temáticas en mención no puedan ser abordadas por medios electrónicos, sino que para ello se requerirá que su legislación específica así lo permita, por ejemplo, mediante los respectivos cambios legales que aprovechen e incorporen el ámbito digital.

En este sentido, el ordenamiento jurídico colombiano ha incluido diversos mecanismos y normatividades orientados a la incorporación de los medios electrónicos a la contratación electrónica.

Desde otra perspectiva, y en el sentido de examinar el Art. 47 de la Ley 527 de 1999 y el empleo de los medios electrónicos en relación con las exigencias formales incluidas en los códigos colombianos, se plantean dos posiciones que se explican a continuación:

Una primera posición, que podemos considerar **moderada**, se orienta a interpretar que las formalidades incluidas en las normas civiles y mercantiles, seguirán existiendo razón por la cual, para dichos eventos, es imperativo acudir, en algún momento contractual, a las “vías tradicionales”, como lo son la Escritura Pública o el documento escrito, entre otras.

El desafío, en esta posición, está en conciliar al máximo dichas vías con la alternatividad ofrecida por los modernos y cambiantes medios de comunicación actuales. La “forma” de expresión de la voluntad encontrará, para su exteriorización o expresión, tantos medios o vías como la inteligencia lo permita.

La segunda posición, que podríamos denominar **extrema**, es aquella que entiende derogadas las normas que incluyen o consagran requisitos de forma, (como por ejemplo el artículo 1611 del Código Civil), en aplicación de lo señalado por el artículo 47 de la Ley 527 de 1999, por considerarse *“disposiciones contrarias”* a los principios fijados, en especial, por los artículos 6° y 7° de la Ley 527, esto es al «principio de equivalencia funcional», en tanto exige la presencia de una firma, de un documento, o de un escrito físico que le de existencia al contrato de que se trate

Esta segunda posición, se considera más acorde con la interpretación amplia del p*rincipio de consensualidad* expuesta con anterioridad, así como se propende en mejor forma por la “inmersión” del ordenamiento jurídico colombiano en los medios electrónicos.

5. CONCLUSIONES

De acuerdo al material recaudado, y a conversaciones que he sostenido con investigadores del CTI de Armenia, lugar donde laboro, la computadora y el manejo del Internet son las herramientas principales o el medio para cometer conductas delictivas designadas como "Delitos Informáticos".

Ahora. Por medio del Internet se pueden producir ataques, los cuales van dirigidos a un objetivo principal, y en este caso es la información que posee una persona sujeta a cualquier intromisión; el agresor puede violentar su confidencialidad o integridad, y en este caso el medio involucrado es el computador.

Entre los delitos informáticos tenemos: los que incluyen los cometidos contra el sistema y los cometidos por medio de sistemas informáticos ligados con Telemática, o a los bienes jurídicos que se han relacionado con la información: datos, documentos electrónicos, dinero electrónico…entre ellos están: acceso no autorizado, destrucción de datos, infracción de los derechos de autor, distribución de música por Internet (mp3), intercepción de E-mail, estafas electrónicas, transferencias de fondos.

Estos hechos, pueden ser valorados por medio del peritaje, aunque poseen problemas de tiempo, costo, y probabilidad de éxito.

Es de sumo cuidado la prueba, ya que previo a su intervención debe requerirse la intervención del Juez de Control de Garantías, con el fin de no violentar derechos fundamentales como es el derecho a la intimidad.

La evidencia digital recolectada debe proteger su integridad, por ello las personas que manejan y recolecten esta evidencia debe ser calificada; hay unos principios sacramentales para su recolección y son identidad, integridad, preservación, seguridad, almacenamiento, continuidad, autenticidad y originalidad. La evidencia digital debe ser manejada conforme a un procedimiento legal, se debe asegurar que las evidencias tomadas, no se modifiquen, pues deben conservar su estado original, y la persona que la recolecte debe estar debidamente entrenada y calificada para este propósito, su obtención debe estar completamente documentadas, preservadas y disponibles para su revisión.

Estos delitos son cometidos por personas que poseen ciertas características que no es común de los delincuentes, esto es, usan sistemas automatizados de información, generalmente conectados a otros.

Los infractores, tienen habilidades para el manejo de los sistemas informáticos, y sus víctimas pueden ser individuos, instituciones crediticias, gobiernos, empresas o personas, su fin es dañar en la mayoría de los casos el patrimonio de la víctima.

La eficacia probatoria de los elementos informáticos, y su interpretación a través de los dictámenes periciales genera y, generará por bastante tiempo inconvenientes, cuando la prueba derivada de los procesadores de datos se haya obtenido de sistemas no implementados a la luz de previsiones legales o reglamentaciones específicas y resulta inevitable su cuestionamiento.

Distinto es el caso en que se someta a dictamen el modo de funcionamiento de un dispositivo, la obtención de información borrada o alterada en soportes magnéticos, la determinación de maniobras fraudulentas mediante el uso de aplicaciones informáticas, puertas falsas, contabilidades paralelas, intrusiones no autorizadas a sistemas de redes o bases de datos a través de internet, violación de la correspondencia electrónica. Es allí donde la prueba pierde su materialidad, para convertirse exclusivamente en "dato", en mera información traducida en desniveles de tensión eléctrica, la función del perito se vuelve compleja. Por un lado debe suplir las limitaciones técnicas que dificultan la obtención del resultado pretendido y, luego, realizar la traducción de dichos resultados, en la inteligencia de que serán interpretados por quienes no poseen su "visión tecnológica" y procederán a tener por acreditada o no la comisión de delitos.

“Sì se pretende que la evidencia digital sea válida y, en consecuencia, valorada por el juez en sus providencias, se debe recaudar teniendo en cuenta factores como: conocimiento, confirmación y verificación de la información; aseguramiento del lugar de los hechos; observación análisis y valoración del lugar de los hechos; fijación del lugar de los hechos; recolección embalaje y rotulado de los elementos materia de prueba; envío de los elementos materia de prueba al almacén de evidencias o al laboratorio especializado; documentación del sistema de cadena de custodia; entrega de los elementos”, Lo anterior, según el Plan nacional de capacitación, óp. cit., pp. 65-71.

6. RECOMENDACIONES

Es claro que la tecnología se ha propagado de manera masiva en nuestro país, lo que no se puede ocultar es la falta de confianza en el manejo de ella, pues le compete al estado, a las entidades bancarias, y a los empresarios fortalecer las estrategias con miras a generarla. Hoy día está presente en casi todos los campos de la vida moderna.

Si bien, el estado cuenta con normas constitucionales y legales para tramitar los procesos que se siguen en contra de los expertos infractores en informática; sí recomienda que las personas naturales, las compañías de mercado se preocupen por el debido manejo de la era informática.

Ahora, por seguridad los perititos en informática, manifiestan que cada vez el uso de la computación como medio para cometer delitos sea mayor, pues la pericia de éstos infractores es asombrosa porque son unos verdaderos especialistas de la red, cuentas de correos, datos bancarios, entre otros…

Indican, que esta clase de conductas reprochables en la mayoría de los casos quedan impunes, debido a la falta de conocimiento y preparación de los organismos de administración de justicia y los cuerpos policiales que no poseen las herramientas adecuadas para investigar y perseguir esta clase de infracciones, que han generado un impacto en la sociedad.

En este orden de ideas, debe tenerse cuidado con el almacenamiento de la información, y las técnicas empleadas para este sistema moderno computacional.