UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

TEMA:

DOCUMENTOS DIGITALES COMO MEDIO DE PRUEBA EN LA LEGISLACIÓN ECUATORIANA

AUTOR:

Roca Villón, Vicente Javier

Trabajo de titulación previo a la obtención del grado de ABOGADO DE LOS TRIBUNALES Y JUZGADOS DE LA REPÚBLICA DEL ECUADOR

TUTOR:

Paredes Cavero, Ángela María

Guayaquil, Ecuador

27 de Agosto del 2016

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación, fue realizado en su totalidad por **Roca Villón, Vicente Javier**, como requerimiento para la obtención del Título de **Abogado de los Tribunales y Juzgados de la República del Ecuador**.

TUTOR (A)

_____

Paredes Cavero, Ángela María

DIRECTOR DE LA CARRERA

_____

Lynch Fernández, María Isabel

Guayaquil, a los 27 del mes de Agosto del año 2016

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Roca Villón, Vicente Javier**

DECLARO QUE:

El Trabajo de Titulación, **Documentos digitales como medio de prueba en la legislación ecuatoriana** previo a la obtención del Título de **Abogado de los Tribunales y Juzgados de la República del Ecuador** ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 27 del mes de Agosto del año 2016

EL AUTOR

_____

Roca Villón, Vicente Javier

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

AUTORIZACIÓN

Yo, **Roca Villón, Vicente Javier**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación, **Documentos digitales como medio de prueba en la legislación ecuatoriana,** cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 27 del mes de Agosto del año 2016

EL AUTOR:

_____

Roca Villón, Vicente Javier

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLÍTICAS

CARRERA DE DERECHO

TRIBUNAL DE SUSTENTACIÓN

_____

Ángela María Paredes Cavero

TUTOR

_____

María Isabel Lynch Fernández

DECANO O DIRECTOR DE CARRERA

_____

Paola Toscanini Sequeira

COORDINADOR DEL ÁREA O DOCENTE DE LA CARRERA

URKUND

Urkund Analysis Result

Analysed Document: Articulo Academico A 2016 Vicente Roca Villon.docx (D21459713)
Submitted: 2016-08-21 23:20:00
Submitted By: amparedescavero@gmail.com
Significance: 5 %

Sources included in the report:

TESIS - PRUEBA ELECTRONICA - UCSG.docx (D15914489)
trabajos.docx (D15082550)
tarea para el doctor orly delgado.docx (D16039607)

Instances where selected sources appear:

5

AGRADECIMIENTO

Agradezco a Dios por brindarme esta vida y por sus bendiciones, a mi madre Rossi, pilar inquebrantable y fundamental en mi vida, a mi padre Vicente, por ser mi modelo a seguir y apoyarme en mis anhelos de superación, a mi hermana Viviana por confiar en mí, sin ellos jamás habría llegado a donde estoy, razón por la cual son mi tesoro más valioso en este mundo.

Agradeciéndoles siempre, Vicente.

ÍNDICE

RESUMEN (ABSTRACT)

El presente estudio aborda el tema de los documentos electrónicos y las complejidades sociales negativas o de utilización errónea que estos conllevan como el crimen digital. Para contrarrestar aquello se ha desarrollado la informática forense, el cual inicia por el peritaje digital luego de recabar la evidencia digital y archivo digital bajo ciertos parámetros de manejo de evidencia. Así mismo se observa el uso del correo electrónico, firma digital, mensajes de texto, páginas web y finaliza con la normativa digital en el Ecuador y normativa en otros países.

PALABRAS CLAVE: documentos digitales, ciber crimen, legislación digital

ABSTRACT

This study addresses the issue of electronic documents and its negative social complexities or misuses involving digital crime. In order to counteract it has been developed computer forensics, which starts by the digital expertise after collecting digital evidence and digital record under certain evidence handling parameters. Likewise, the use of email, digital signature, text messages, web pages. It ends with the digital legal standards in Ecuador and other countries.

KEY WORDS: digital documents, cybercrime, digital forensics, digital law

INTRODUCCIÓN

El papel como elemento físico ha sido reemplazado por el soporte de medios electrónicos o documentos electrónicos. Un documento electrónico es un documento que siempre se encuentra almacenado en un soporte electromagnético y su contenido o información está registrada mediante un código bit. Debido a las interacciones en sociedad, pudieran existir situaciones en las que unos toman ventaja o perjudican a otras.

El crimen digital se refiere cuando personas buscan delinquir utilizando la tecnología disponible cometiendo infracciones. Nace así la necesidad de que el derecho informático el cual debería ser integrado a la sociedad de una forma más radical. La informática forense ayuda en este cometido al de recobrar los registros y mensajes de datos existentes dentro de un dispositivo informático o electrónico.

Los principios básicos de manejo de evidencia digital son muy específicos al aconsejar el manejo de la evidencia digital al acudir al lugar de los hechos al menos dos personas; ninguna acción debe alterar la información recabada; el personal competente puede acceder a la información a ser investigada solo en casos excepcionales explicando el porqué; y se debe llevar una bitácora de actividades relacionadas al manejo de dicha evidencia.

Es necesario anotar que 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 que se trata de un mensaje de datos o en razón de no haber sido presentado en su forma original. Lo propio al identificar toda información con el usuario, es decir la persona física que redactó dicha información y poder asimilarlo a una identidad virtual. Respecto a la valoración de pruebas por lo general caen en alguna de estas categorías: sistema de prueba legal, sistema de prueba libre y sistema de la sana crítica.

El perito digital deberá ser objetivo en su accionar, conservando la autenticidad e integridad de los medios probatorios, cumpliendo con los requisitos establecidos en la ley para dicha actividad, utilizando medios probatorios auténticos, relevantes y suficientes para cada caso, utilizando una cadena de custodia, estableciendo por escrito todos los pasos dados en el proceso pericial. También se argumenta que si

existe la posibilidad de determinar no sólo la identidad de un archivo original, sino también de uno que haya sido copiado, mediante los códigos binarios identificadores.

También se señala que impresiones de correos electrónicos *no sirven como prueba directa* en un juicio, puesto que el contenido, remitente, hora y fecha son modificables, teniendo por supuesto los conocimientos y el equipamiento técnico. Sin embargo que dicha prueba puede ser sumada y considerada con otras complementarias.

DESARROLLO

1. DOCUMENTOS ELECTRÓNICOS

García (2013) manifiesta que el papel como elemento corpóreo ha sido reemplazado por el soporte material a través de medios electrónicos, o documentos electrónicos. También expresa que el derecho informático debería ser integrado a la sociedad, siendo un fenómeno que debería ser reglamentado puesto que la presencia de la informática en nuestra sociedad obedece a la necesidad de no sólo gestión de la información sino también el control de la misma. Finalmente, se refiere a que el documento electrónico es un documento que siempre se encuentra almacenado en un soporte electromagnético y su contenido o información está registrada mediante un código bit. Los bits son el alfabeto de los documentos electrónicos. Se tiene entonces que el lenguaje bit solo puede ser leído o reproducido mediante lectores de electromagnéticos (p.288).

Así mismo García (2013) argumenta que los documentos electrónicos utilizan un lenguaje binario que puede ser descifrable (decodificado) y se convierte en un lenguaje perceptible por el hombre a través de la vista. En efecto, una vez codificada la información, tales datos son incomprensibles para el ser humano, pues no son legibles directamente por el ojo humano y están expresados en lenguaje binario, el cual no puede ser comprendido sino es traducido (decodificado) informáticamente a otro lenguaje comprensible por el hombre, que puede referirse a un leguaje en particular (p. 294).

Por otro lado González (2003) divide los documentos electrónicos en cuatro categorías: documentos electrónicos que constituyen instrumentos públicos; documentos electrónicos que constituyen instrumentos privados suscritos con firma electrónica avanzada; documentos electrónicos que constituyen instrumentos privados suscritos con firma electrónica simple; y documentos electrónicos residuales. Por tanto, el valor de aquellos reposa en su autoría mediante el reconocimiento, la determinación de su valor probatorio en el juicio entregándose por completo a las reglas que se establecen en legislaciones actualizadas (pg. 1).

Jara (2010) indica que en el caso de legislación ecuatoriana el documento electrónico es un mensaje de datos, es decir, es toda información creada, generada, comunicada, enviada, recibida o procesada por cualquier medio electrónico y que puede ser intercambiada por cualquier medio (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Disposición General Novena). En sentido estricto sería entonces el documento electrónico es aquel que está en formato electrónico, una información electrónica o digital que se ha creado, generado, recibido, comunicado, enviado, recibido o procesado por cualquier medio electrónico (p. 16).

Inuca (2012) expresa que en el Ecuador es indispensable adaptar las leyes a los cambios tecnológicos, dando respuesta a las demandas de la sociedad dela información y de la práctica jurídica (pg. 54).

2. CRIMEN DIGITAL

Acurio (2010) ya se refirió al crimen digital, cuando personas que buscan delinquir al utilizando la tecnología disponible eludiendo a las autoridades empeñados en su cometimiento de infracciones. Así mismo Acurio (2010) enfatiza que la clave de toda investigación criminal por tanto se encuentra en la obtención de la información (elementos de convicción) en sus etapas más precisas: recolección, preservación y análisis de las evidencias digitales. Esto sucede cuando se confirma la existencia de la infracción y responsabilidad de quienes aparecen en un juicio como presuntos responsables y la misma tecnología servirá en el auxilio de perseguir al delito y al delincuente (pg. 1).

Bes (2014) se refiere a los *medios de prueba* y *fuentes de prueba* de origen digital y/o electrónico. Así, mismo menciona que determinar la autoría de documentos virtuales (digitales) es un problema complejo hoy en día puesto que cada vez es más difícil acreditar los medios tradicionales de prueba tales como papeles o testigos que han sido desplazados por e-mails o documentos virtuales. Bes (2014) argumenta que si no se brinda soluciones modernas los litigios que nacen por las nuevas formas de comunicación que no trae la tecnología, entonces el cuerpo de justicia no estaría cumpliendo su labor de búsqueda y construcción de una sociedad más justa e igualitaria (pg. 1).

3. INFORMATICA FORENSE

Nace entonces el concepto de informática forense (Acurio, 2010), cuyo objetivo primordial es el de recobrar los registros y mensajes de datos existentes dentro de un dispositivo informático o electrónico (computador o teléfono) de manera que dicha información pudiera ser utilizada como prueba ante un tribunal (pg. 2).

Pérez (2014) apunta a que es fundamental evidenciar que la prueba aportada al proceso corresponde en su identidad con el original, puesto que ello afecta al contenido de la impugnación, pudiéndose reclamar así mismo la exactitud y autenticidad de la prueba aportada al proceso judicial por falta de correspondencia con el original. La aportación de la prueba electrónica al proceso por tanto debe hacerse respetando garantías que están íntimamente asociadas a las herramientas forenses y a la utilización de protocolos que permitan garantizar que la evidencia goza de las garantías procesales para que sea admitida y valorada por el juzgador (pg. 7).

Pérez (2014) además adiciona que en la evidencia digital es raro que el delito no esté asociado a un mensaje de datos guardado y trasmitido por medios informáticos; (cámaras, computadores, Pendrive, CD, teléfonos móviles, etc.) y transmitido por los sistemas de comunicación (telecomunicaciones, Internet) a través de SMS, WhatsApp, Blogs, redes sociales, páginas web, sean imágenes, texto, o archivo (pg. 13).

4. EVIDENCIA DIGITAL

Los principios básicos de manejo de evidencia digital son muy específicos al aconsejar el manejo de la evidencia digital al acudir al lugar de los hechos al menos dos personas; ninguna acción debe alterar la información recabada; el personal competente puede accesar a la información a ser investigada solo en casos excepcionales explicando el porqué; y se debe llevar una bitácora de actividades relacionadas al manejo de dicha evidencia (Acurio 2010).

Parra (2006, pg. 7) menciona que 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 que se trata de un mensaje de datos o en razón de no haber sido presentado en su forma original. Así mismo expresa que el Capítulo VIII, del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil, el mismo que se refiere a la prueba documental, es decir, que se entienden incorporados a la legislación en el aspecto referenciado y se apreciarán teniendo en cuenta las disposiciones, plasmadas en los artículos 251 a 301 del C. de P. C

Carrasco (2015, pg. 5) indica que las evidencias digitales son todos aquellos datos e información almacenados en dispositivos electrónicos o transmitidos en formato digital que pueden tener valor probatorio en un procedimiento legal. Ejemplos de ellos son correos electrónicos, documentos, fotografías digitales, archivos de video o audio, logs de eventos o históricos son algunos ejemplos de lo que podría ser evidencias digitales.

Bes (2014) apunta a que es necesario identificar toda información con el usuario, es decir la persona física que redactó dicha información y poder asimilarlo a una identidad virtual (i.e. relacionar el autor humano de un correo electrónico con determinado usuario de dicho correo). Adicionalmente especifica la distinción que se efectúa en Derecho Procesal sobre la *fuente de prueba* y *medios de prueba*. La *fuente* determina aquello que existe en la realidad, independientemente de la existencia de un proceso; mientras que el *medio* es un concepto que se explica como aquellas fuentes de prueba que se logran introducir eficazmente dentro del proceso (pg. 2).

Carrasco (2015, pg. 16) expresó que empresas y organizaciones recurren con mayor frecuencia al uso de tecnologías de información y comunicación (TICs) como recurso integrado en las actividades de la empresa. Es por ello que es posible acceder a dichos recursos y utilizarlos como medio de prueba de requerirlo, sin embargo presentan cierta dificultad el analizar estas evidencias digitales en los conflictos laborales.

Insa (2015, pg. 139) reconoce que los empresarios enfrentan problemas laborales con respecto al uso incorrecto y abuso de recursos corporativos electrónicos cometidos por parte de su personal; así como a problemas de seguridad de los datos, ordenadores y servidores. También se consideran fraudes bancarios y delitos sobre propiedad intelectual, además de los derivados del comercio electrónico. Sin embargo, la mayoría de empresarios no dispone de un protocolo que regule el uso del material informático a disposición de sus empleados.

Así mismo, Riofrio (2010, pg. 165) respecto a la valoración de pruebas dice que por lo general caen en alguna de estas categorías: sistema de prueba legal, sistema de prueba libre y sistema de la sana crítica. El sistema de prueba legal cataloga las pruebas una por una, las examina, les confiere a cada una valor respectivo y le impone ese criterio al juzgador. El sistema de prueba libre permite al juez estudiar las pruebas conociendo los hechos y conjeturando según su mejor criterio, sin que quede obligado a expresar una sentencia previa. Finalmente, el sistema de prueba crítica, otorga al juez facultades para apreciar la prueba, sin embargo le impone el deber de establecer los hechos a través de un razonamiento lógico a partir de las pruebas rendidas, debiendo expresar en la sentencia un proceso lógico por el cual ha llegado a su final resolución o decisión.

Jara (2010) concuerda que en caso de que alguna de las partes niegue la validez de un mensaje de datos, deberá probar, conforme a la ley, que éste adolece de uno o varios vicios que la invalidan; o que el protocolo de seguridad no pueda ser reconocido técnicamente válido. Cualquier duda sobre la validez de dicha prueba podrá ser objeto de comprobación técnica (p. 29).

También Jara (2010) aclara que la impugnación a este tipo de documentos será en razón de que carezca de seguridades, como por vicios que lo invalidan, los mismos que deben ser probados por quien los alega; sin embargo, será necesario cuidar la integridad del mensaje, para lo cual se deberá contar con un sistema que proteja de cualquier alteración al mensaje original y de esta forma manteniéndolo completo, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación, requisito denominado de originalidad, establecido en el Art. 7 de la mencionada ley (p. 29).

En este aspecto será más fácil si se trata de un documento suscrito con una firma electrónica o digital que posea un certificado emitido por la entidad correspondiente y esté protegido con un código hash que es un software que utiliza métodos criptográficos y es usado para detectar cambios en el mismo. En caso de no tener estos aspectos, será necesario solicitar conjuntamente la intervención de un perito informático y una inspección para comprobar su integridad y originalidad.

5. PERITAJE DIGITAL

Según Acurio (2010) el perito digital deberá ser objetivo en su accionar, conservando la autenticidad e integridad de los medios probatorios, cumpliendo con los requisitos establecidos en la ley para dicha actividad, utilizando medios probatorios auténticos, relevantes y suficientes para cada caso, utilizando una cadena de custodia, estableciendo por escrito todos los pasos dados en el proceso pericial (pg. 3)

Adicionalmente, Acurio (2010, pg. 3) expresa la necesidad de establecer el rol que tiene un sistema informático dentro del camino del delito (*iter criminis*). Dicho rol será muy distinto en el caso probatorio de una investigación por un cometimiento de homicidio o por un fraude informático. También es necesario hacer una distinción respecto de evidencias electrónicas (sistema informático o hardware) versus evidencias digitales (datos, programas o información almacenada).

De aquí se distinguen algunas precisiones respecto al hardware; para Acurio (2010, pg. 4) el hardware o elemento físico se constituye como mercancía ilegal o *fruto del delito* cuando su posesión no está autorizada por la ley (ie. decodificadores de señal por cable no autorizados) o cuando es obtenido mediante robo, hurto, fraude u otra

clase de infracción. El hardware es un *instrumento del delito* cuando cumple un papel importante en el cometimiento del delito al ser utilizada como un arma o herramienta. (ie. Snifers utilizados para capturar tráfico en la red o interceptar comunicaciones). El hardware es *evidencia*, cuando es un elemento físico que se constituye como prueba de la comisión del delito; el cual no ha sido catalogado ni como mercancía ilegal ni como fruto del delito. (i.e. scanner utilizad en digitalizar pornografía infantil). Bes (2014) añade a los teléfonos inteligentes (smartphones) y también el soporte lógico (procesador de textos Word en el caso de computadores o el sistema Android en el caso de teléfonos). También hace la distinción respecto a la no similitud entre computadores sin embargo que pueden compartir un mismo software (Mobile Office).

Por otro lado, también Acurio (2010, pg. 4) distingue que la información es mercancía ilegal o *fruto del delito* cuando su posesión no está permitida por la ley (ie. copias pirateadas de programas de computador, secretos industriales robados, pornografía infantil). La información es un *instrumento del delito* o herramienta cuando es utilizada como medio para cometer una infracción penal (i.e. programas de ordenador utilizados para romper seguridades o accesos a sistemas informáticos y brindar acceso no autorizado). La información es *evidencia* cuando acciones dejan un rastro digital (i.e. transacciones, ISP, direcciones, etc.).

6. ARCHIVOS DIGITALES

Un documento digital es aquella representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. (Ley No. 25.506, art. 6 de la República Argentina). Bes (2014) argumenta que si existe la posibilidad de determinar no sólo la identidad de un archivo original, sino también de uno que haya sido copiado, mediante los códigos binarios identificadores HASH que son “1” o”0”, en una multiplicidad de combinaciones. Es por ello que si el código HASH permanece inalterado significa que el archivo es idéntico, validando fecha de creación, contenido y autor; poniendo en evidencia que se respetó la cadena de custodia de dicha prueba en relación a un juicio (BES, 2004 pg. 9).

7. CORREO ELECTRÓNICO

El e-mail o correo electrónico se denomina al sistema de mensajería desde el internet mediante el protocolo SMTP (en español: Protocolo Simple de Transferencia de Correo). Por medio de mensajes de correo se pueden enviar no solamente texto, sino también todo tipo de documentos digitales. Bes (2014, pg. 10) reconoce que los ordenadores "cliente de protocolo" se conectan mediante una red entre ellos, y obtienen las aplicaciones necesarias de los servidores ficheros, los cuales se conectan al internet mediante un router y utilizan servicios Web mediante el servidor y se protegen de ataques de virus con diversos firewalls instalados. Pero todo está controlado por el administrador, el cual cuenta con privilegios exclusivos de mantenimiento y operación de toda la red. Lo interesante aquí es que los correos enviados dejan rastros en forma bitácora o "logs" que se pueden encontrar en los ordenadores "clientes" o en el servidor. El administrador de Red entonces contaría con poderes mucho más discrecionales que el propio empresario o gerente.

Un e-mail permite saber quién lo emitió, es decir de que terminal u ordenador fue enviado y en cual fue recibido. El mensaje de un correo electrónico no es único, puesto que su creación es múltiple. Desde el momento que el usuario envía el mensaje, no solamente se han creado múltiples copias, sino que las mismas se encuentran diseminadas en todo el mundo, dependiendo del punto de partida y de llegada del mensaje (Municoy 2000, pg. 157).

Bes (2014) señala que impresiones de correos electrónicos *no sirven como prueba directa* en un juicio, puesto que el contenido, remitente, hora y fecha son modificables, teniendo por supuesto los conocimientos y el equipamiento técnico. Sin embargo que dicha prueba puede ser sumada y considerada con otras complementarias (pg. 12).

8. FIRMA DIGITAL

Bes (2014, pg. 14) expresa que la firma digital se entiende al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de

exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma (Ley No. 25.506; art. 2 de la República Argentina).

Así mismo, Bes (2014) apunta que estos sistemas encriptan los contenidos y generalmente suministran dos claves: una de escritura (que solo debe poseer el emisor, y que lo hará responsable de todo lo que salga validado con dicho algoritmo) y otra pública que permitirá la lectura de lo que se envía bajo este sistema. De esa manera si se puede dar certeza de que lo remitido salió de alguien que conoce la clave del usuario emisor (pg. 14).

9. MENSAJES DE TEXTO / SMS

Un mensaje de texto o SMS (Short Message Service) es servicio disponible en teléfonos móviles que permite el envío de mensajes cortos. Constituyen una cadena alfanumérica de hasta 140-160 caracteres de 7 bits, y cuyo encapsulado incluye una serie de parámetros. En principio, se emplean para enviar y recibir mensajes de texto normal, pero existen extensiones del protocolo básico que permiten incluir otros tipos de contenido, dar formato a los mensajes o encadenar varios mensajes de texto para permitir mayor longitud.

Bes (2014) establece la forma de probarlo los mensajes de texto en un juicio sea cual fuere el caso puesto que por definición en dicho mensaje queda alojado el remitente y la fecha y hora de envío, por lo que se tendría certeza de dichos datos. Pero ¿Cómo acreditarlo en un proceso judicial? Puesto que difícilmente se pueda acompañar el equipo en el que está alojado el mensaje, se puede solicitar a la compañía celular una suma informativa a la debiera tenerse por probado (pg. 16).

10. PÁGINAS WEB

Se entiende por páginas Web (sitios, páginas o portales) a aquel documento situado en una red informática, al que se accede mediante enlaces de hipertexto (Diccionario

On-line de la Real Academia Española). Dichas páginas Web están compuestas principalmente por información (texto o módulos multimedia) así como por hiperenlaces. Adicionalmente, puede contener o asociar datos de estilo para especificar cómo debe visualizarse, y también aplicaciones embebidas para hacerla interactiva. Bes (2014) indica que las páginas Web son escritas en un lenguaje de marcado que provea la capacidad de manejar e insertar hiperenlaces, generalmente HTML (Hyper Text Markup Language). El contenido de la página puede ser predeterminado (página Web estática) o generado al momento de visualizarla o solicitarla a un servidor Web (página Web dinámica).

Bes (2014) refiriéndose a las páginas Web en cuanto a su forma probatoria, expresa que resulta complejo adaptarse a todas las variables que pueden presentarse dentro de las *fuentes* de prueba dentro de un juicio. Sin embargo la impresión del documento Web que está a la vista (es decir llevar a papel lo que se está visualizando en el monitor) y acompañarlo como documental; luego tratar de validarlo a través de una prueba pericial informática que le de legitimidad a esa impresión. Si el perito determina como positivo el cotejo, resultará cierta la prueba y superará la negativa de la contraparte, pero las dificultades se presentarán teniendo en cuenta que es el empleador quien, generalmente, administra el sitio y puede en cualquier momento modificar (de mala fe) lo que en algún momento figuraba como contenido en ella (pg. 15).

11. NORMATIVA DIGITAL EN EL ECUADOR

Para Jara (2010) la existencia y utilización del documento electrónico entre los ecuatorianos y en distintos tipos de relaciones comerciales y sociales, generó la necesidad de su regulación, debido a ello se dictó la Ley No.67 de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Registro Oficial 557 del 17 de abril de 2002). En dicha ley se tipifican algunas infracciones informáticas y se regulan algunos aspectos, como el reconocimiento legal a mensajes de datos, los documentos electrónicos que se convierten en especies, y también se regulan las firmas electrónicas, entidades de certificación, servicios electrónicos, derechos de usuarios o consumidores, los instrumentos Públicos, la prueba y notificaciones electrónicas, y se incluyen varias reformas al Código Penal (pg. 16).

Jara (2010) también apunta sobre los mensajes de datos y documentos electrónicos. La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Art. 2 dispone que para que tenga eficacia, sea valorado y produzca efectos el documento electrónico, los cuales deben cumplir con los requisitos que establece la ley. El Art. 53 de la misma ley, establece la presunción sobre su validez. Así, mismo el Art. 54, ordena que en aquel documento electrónico, o sea un medio de prueba, será necesario que esté en soporte material (informático) sea trascrito en papel (impreso) y además es necesario proporcionar los elementos materiales electrónicos o informáticos necesarios para su lectura y verificación (pg. 17).

Por otro lado Jara (2010) detalla la práctica de la prueba, la cual se practica de conformidad con lo previsto en el Código de Procedimiento Civil y observando las normas siguientes: a) al presentar un mensaje de datos dentro de un proceso judicial en los juzgados o tribunales del país, se deberá adjuntar el soporte informático y la transcripción en papel del documento electrónico, así como los elementos necesarios para su lectura y verificación; b) en el caso de impugnación del certificado o de la firma electrónica por cualesquiera de las partes, el juez o tribunal, a petición de parte, ordenará a la entidad de certificación de información correspondiente, remitir a ese despacho los certificados de firma electrónica y documentos en los que se basó la solicitud del firmante, debidamente certificados; c) el faxsímil, será admitido como medio de prueba, siempre y cuando haya sido enviado y recibido como mensaje de datos, mantenga su integridad, se conserve y cumpla con las exigencias contempladas en esta ley (pg. 28).

Actualmente tenemos en vigencia el Código Orgánico General de Procesos desde el 22 de mayo del 2016, donde se reconoce a los documentos digitales como: los documentos producidos electrónicamente con sus respectivos anexos, serán considerados originales para todos los efectos legales. Las reproducciones digitalizadas o escaneadas de documentos públicos o privados que se agreguen al expediente electrónico tienen la misma fuerza probatoria del original. Los documentos originales escaneados, serán conservados por la o el titular y presentados en la audiencia de juicio o cuando la o el juzgador lo solicite. (Art. 202 COGEP)

Por otro lado el Código Orgánico Integral Penal actualmente vigente desde el 10 de Agosto del 2014 expresa: El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí. (Art. 500 COIP)

12. NORMATIVA DIGITAL EN OTROS PAISES

Bes (2014) apuntó que España cuenta con dos leyes que admiten documentos electrónicos y obligan a conservar los datos de tráfico (información de usuario, etc.) por 12 meses (No.34 del 2002 y No. 25 del 2007). Por otro lado, Colombia estableció una ley que conceptualiza y establece la forma de acreditar documentos electrónicos (No. 527 de 1999). Sin embargo, en los Estados Unidos, los jueces están prevenidos que una dirección virtual IP no necesariamente corresponde a una persona específica (debido a hackeo de cuentas, etc.)

CONCLUSIONES

Partiendo del concepto de que prueba documental**, e**s todo documento público o privado que recoja, contenga o represente algún hecho o declare, constituya o incorpore un derecho, debo recalcar que el avance de la Tecnología ha provocado un cambio en la forma de entender las pruebas en un proceso. Las computadoras y demás instrumentos de informática han pasado de ser una herramienta opcional y se han convertido en una necesidad, las cuales en la actualidad son nuestras herramientas indispensables de trabajo y nos sirven para el desarrollo de nuestras tareas y actividades diarias, pues guardamos en estos sistemas una gran cantidad de información.

Con la introducción de este gran avance surgieron los documentos digitales y a nivel mundial las normas debieron adaptarse ante tal cambio y necesidad, los documentos digitales como medio probatorio están siendo un medio a través del cual se busca lograr que los juzgadores acierten jurídicamente al momento de dictar sentencias, pues anteriormente en la mayoría de casos se limitaba solamente a la percepción del documento probatorio a través del papel.

Analizando el Código Orgánico General de Procesos encontramos que se reconoce como prueba al documento digital, estableciendo así una gran responsabilidad para los profesionales del derecho, para los juzgadores y funcionarios judiciales el tratamiento de este tipo de documento probatorio en los procesos litigiosos.

Considero que los documentos digitales como medios de prueba son suficientes para que representen o prueben un hecho o incorporen un derecho, ya que en la actualidad no solamente realizamos tareas de trabajo, estudiantiles y comerciales con una computadora o laptop, también con los smartphones, tablets y cualquier otra herramienta informática.

REFERENCIAS (o BIBLIOGRAFÍA)

Acurio, S. (2009). Introducción a Informática Forense. Dirección de Tecnologías de Información. Fiscalía General del Estado, Ecuador

Acurio, S. (2010). Manual de Manejo de Evidencia Digitales y Entornos Informáticos, Versión 2.0. Dirección de Tecnologías de Información. Fiscalía General del Estado, Ecuador

Bes, E. (2014). Prueba Digital y su inclusión en el procedimiento laboral. Ponencia en VI Congreso de Derecho Laboral y Relaciones del Trabajo. Mar del Plata, Argentina.

Carrasco, F. (2015). Ponencia: Valor probatorio de los documentos electrónicos en materia laboral: Caso México. Universidad Popular Autónoma del Estado de Puebla (UPAEP), México.

García, N. (2013). Valor Probatorio de los Documentos Digitales emitidos en el juicio en línea. Tribunal Federal de Justicia Fiscal y Administrativa. Colección de Estudios Jurídicos, tomo XXIV, México

González, F. (2003). La Prueba de las Obligaciones y la Firma Electrónica, Revista Chilena de Derecho Informático. No. 2, Chile.

Insa, F. (2015). Pruebas Electrónicas ante los Tribunales en la Lucha contra la Cibercriminalidad. Un Proyecto Europeo. Enlace: Revista Venezolana de Información, Tecnología y Conocimiento, Vol. 5, No. 02, Universidad de Zulia, Venezuela. p. 139

Inuca, L. (2012). Tesis de Grado "La Prueba y las tecnologías de la información y comunicación en el proceso penal". Universidad Técnica articular de Loja, Ecuador.

Jara, M. (2010). Tesis de Grado "La Prueba Electrónica Documental en el Código de Procedimiento Penal Ecuatoriano". Universidad de Cuenca. Ecuador

Municoy, M. (2000). El Internet y el Art. 18 de la Constitución Nacional. Cuadernos de Doctrina y Jurisprudencia Penal. Ed. Ad-Hoc Villela Editor. Año VI, No. 10, pág. 157

Parra, J. (2006). Ponencia "El Documento Electrónico y su alcance probatorio". I Convención de Derecho Informático. Universidad Externado de Colombia. Colombia

Pérez, J. (2014). La prueba electrónica: consideraciones. Prolex

Riofrio, J. (2010). Eficacia Probatoria de los Documentos Electrónicos", Revista Jurídica, Facultad de Jurisprudencia y Ciencias Sociales y Políticas, Universidad Católica de Santiago de Guayaquil, p. 165

DECLARACIÓN Y AUTORIZACIÓN

Yo, **ROCA VILLÓN, VICENTE JAVIER**, con C.C: # 0925722803 autor/a del trabajo de titulación: **Documentos digitales como medio de prueba en la legislación ecuatoriana** previo a la obtención del título de **Abogado de los Tribunales y Juzgados de la República del Ecuador** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 27 de Agosto de 2016

_____

Nombre: **Roca Villón, Vicente Javier**

C.C: **0925722803**

Presidencia de la República del Ecuador

Plan Nacional de Ciencia, Tecnología, Innovación y Saberes

SENESCYT
Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	**Documentos digitales como medio de prueba en la legislación ecuatoriana.**		
AUTOR(ES)	Vicente Javier, Roca Villón		
REVISOR(ES)/TUTOR(ES)	Ángela María, Paredes Cavero		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Jurisprudencia y Ciencias Sociales y Políticas		
CARRERA:	Derecho		
TITULO OBTENIDO:	Abogado de los tribunales y juzgados de la República del Ecuador		
FECHA DE PUBLICACIÓN:	27 de Agosto de 2016	**No. DE PÁGINAS:**	**(# 23 de páginas)**
ÁREAS TEMÁTICAS:	Derecho informático, criminología, derecho penal		
PALABRAS CLAVES/ KEYWORDS:	Documentos digitales, ciber crimen, legislación digital.		

RESUMEN/ABSTRACT (150-250 palabras):

El presente estudio aborda el tema de los documentos electrónicos y las complejidades sociales negativas o de utilización errónea que estos conllevan como el crimen digital. Para contrarrestar aquello se ha desarrollado la informática forense, el cual inicia por el peritaje digital luego de recabar la evidencia digital y archivo digital bajo ciertos parámetros de manejo de evidencia. Así mismo se observa el uso del correo electrónico, firma digital, mensajes de texto, páginas web y finaliza con la normativa digital en el Ecuador y normativa en otros países.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-4-2784338	E-mail: vicenterocav@hotmail.com
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre:** Toscanini Sequeira, Paola	
	Teléfono: +593-4-220439 ext: 2225	
	E-mail: paolats77@hotmail.com	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	