XVI JORNADA NOTARIAL IBEROAMERICANA

La Habana, Cuba, 23 al 25 de noviembre de 2014

TEMA I

La función notarial y la aplicación de las nuevas tecnologías

La evidencia digital y el rol del notario

Esc. Gabriela Hormaizteguy

Coordinador nacional: Esc. Javier Wortman

50 años | 1964 2014 | Biblioteca "Prof. Esc. Julio R. Bardallo" Asociación de Escribanos del Uruguay

ASOCIACIÓN DE ESCRIBANOS DEL URUGUAY

ABSTRAC

El uso cada vez mayor de las TIC's ha llevado a que los medios de pruebas cambiaran al formato electrónico y a que se reporten en forma casi constante vulnerabilidades en los sistemas informáticos.

La informática forense, como disciplina auxiliar de la Justicia, nace para hacer frente a los desafíos ya sea que una evidencia digital no sea rechazada en juicio o "encontrar" a los culpables de delitos.-

Tanto la recolección como el almacenamiento o transferencia de evidencia digital debe documentarse en forma fehaciente.-

El Notario, en el ejercicio de la fe pública de que está investido, entendemos es el profesional indicado para labrar las actas de constatación de todo o parte del proceso.-

INTRODUCCIÓN

El 3er. Congreso Internacional del Notariado Latino definió al derecho notarial como el "conjunto de disposiciones legislativas, reglamentarias, usos, decisiones jurisprudenciales y doctrinas que rigen la función notarial y el instrumento público notarial".

El Notario, en ejercicio de esa función notarial, como profesional de alto nivel de competencia que es, colabora en el cumplimiento de las leyes y es sinónimo de seguridad, imparcialidad y confianza, es el más indicado para intervenir en el proceso de recolección de la evidencia digital.-

En el presente trabajo nos referiremos solamente al rol del notario respecto a su actuación en el análisis forense y la evidencia

digital, sin descartar la importancia de otras como la contratación electrónica, la firma electrónica avanzada, los documentos electrónicos, etc.-

El desarrollo de las nuevas tecnologías y sobretodo la modernización de los sistemas de almacenamiento y transmisión computarizados de la información, ha llevado a una difusión masiva, permitiendo grandes avances en la ciencia, la educación, el comercio.

Tanto en nuestras actividad personal como laboral utilizamos cada día mas los dispositivos informáticos y electrónicos, la información fluye de un lado para otro, en forma de correos electrónicos, SMS, mensajes de *"WhatsApp,"* discos duros externos, pendrives , etc.

Uruguay no está ajeno a los ataques informáticos ya sea a organismos públicos, empresas o a particulares, pero en menos medida que otros países.-

Según publicación del periódico uruguayo El País de fecha 16/12/2013 los virus más destacados son el "Trojan.JS.FBook.q" y el "Trojan-Spy.HTML.Fraud.iz", donde tenemos que "Estados Unidos en el primer lugar, y Rusia en el segundo, son los países que almacenaron la mayor cantidad de código malicioso en 2013. Uruguay ocupa el lugar 147 en el mundo (entre 200 países) y es el penúltimo de Latinoamérica que más virus almacena en sus propios servidores." "En otras palabras, Uruguay es el segundo país de esta región analizada que menos malware almacena en sus servidores."

Según informa CERTuy en su página web en el primer semestre del 2014 se registraron un total de 306 incidentes, considerando como tales cualquier intento exitoso o no de realizar un ataque informático.

Destacamos los siguientes datos: 54% de los ataques son de Phishing ,7% Falla mayor de HW/SW, 6% Robo de identidad, 5% Malware y 5% Malware.-

Por todo lo expuesto, llegamos a la conclusión que todos estamos siendo más vulnerables a manipulaciones por parte de "ciberdelincuentes" de diferentes maneras cometiéndose de esa manera diferentes tipo de delitos.-

Entre ellos podemos destacar: fraudes en internet, estafas, carding, redirección a falsas paginas (phising) , robos de datos, revelación de datos, robo de cuentas de e-mail, amenazas o injurias por medio de foros, mensajes, correos, manipulación de programas, pornografía infantil, difusión de material xenófobo o racista, sabotaje informático, piratería informática, fuga de datos, reproducción no autorizada de programas informáticos de protección legal, Scavenging, Piggybacking, Impersonation, etc, etc.

CIBERCRIMEN Y DELITOS INFORMÁTICOS

En los delitos cometidos en las TIC o a través de ellas existe un alto nivel de transnacionalidad, al involucrar normalmente mas de un país, donde por ejemplo se ideó, donde se llevó a cabo el mismo y el país donde se causó el daño penalmente sancionable.-

Es por tal motivo que se considera necesaria una coordinación a nivel internacional en la materia.-

La Asamblea General de la Organización de las Naciones Unidas en diciembre de 2011 manifestó que "observando que la dependencia de la tecnología de la información, aunque puede variar de un Estado a otro, ha dado lugar a un considerable aumento de la cooperación y coordinación a nivel mundial, en razón de lo cual la utilización de esa tecnología con fines delictivos puede tener graves consecuencias para todos los Estados," por resolución 56/121 invitó "…a los Estados Miembros a que, al elaborar leyes y políticas nacionales y al adoptar prácticas para luchar contra la utilización de la tecnología de la información con fines delictivos, tengan en cuenta, según proceda, la labor y los logros de la Comisión de Prevención del Delito y Justicia Penal y de otras organizaciones internacionales y regionales;"…

En tal sentido resulta interesante referenciar el acuerdo no jurisdiccional del Tribunal Supremo (España) de fecha 3/2/2005 estableciendo el principio de ubicuidad, por tanto para evitar la discusión sobre que tribunal es competente, tenemos que, el delito informático, de tracto mutante e itinerante y que establece sus efectos en múltiples sitios geográficos "se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. en consecuencia, el juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para la instrucción de la causa".-

En países latinoamericanos como por ejemplo Argentina, Chile, Bolivia, Costa Rica, México y Uruguay han modificado o se

encuentran en vías de modificar el ordenamiento jurídico para adaptarlo a los delitos cometidos usando las nuevas tecnologías.-

Pero solo las modificaciones normativas o la creación de figuras delictivas no es suficiente, ya en casi todos los países se está implementando otro tipo de medidas como la creación de unidades especializadas en la temática, tanto a nivel policial, judicial y empresarial.-

Hace ya varios años que Interpol tiene oficinas y personal especializado en delitos informáticos, la Unión Europea cuenta con la Europol que dentro de sus funciones se encuentra la facilitación del análisis de información para combatir el cibercrimen.

En Uruguay a nivel policial existe una División de Delitos Informáticos del Departamento de Delitos Complejos dependiente de la Dirección de Investigaciones de la Jefatura de Policía, que fue creada por Decreto 254/2003 y comenzó sus funciones en 2005.

Es sumamente importante estudiar los "ciberdelitos" ya que los mismos dependen en gran medida del conocimiento en lo que sucede dentro de un sistema informatizado y como es la estructura del mismo y generalmente se benefician de algún vacío legal.

Respecto a los delitos informáticos, la tendencia es entender que la protección a los bienes jurídicos, se haga desde la perspectiva de delitos ya tipificados tradicionalmente, con una re-interpretación especial a los efectos de llenar las lagunas originadas por los nuevos comportamientos delictivos.

Tendríamos entonces que básicamente los bienes jurídicos protegidos serían el patrimonio (fraudes informáticos,

manipulaciones de datos) el derecho a la intimidad a la protección de los datos personales, derecho de propiedad ya sea de elementos físicos de un sistema informático como de la información contenida en el mismo, a la seguridad (falsificaciones de documentos o datos)

Marcelo Huerta y Claudio Líbano definen los delitos informáticos como "todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro"

Para Núñez Ponce los delitos informáticos son "todas aquellas conductas que son ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso antijurídica y culpables en que se tienen computadoras o ordenadores en las cuales se usan diversas técnicas y funciones; desempeñando así un papel ya sea como método, medio o como instrumento o fin",

Los Dres. Enrique Moller y Ana Brian citando a María de la Luz Lima afirman que delito informático "en un sentido amplio es cualquier conducta criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en sentido estricto, el delito informático es cualquier acto ilícito penal

en el que las computadoras, sus técnicas o funciones desempeñan un papel ya sea como método, medio o fin".

El ordenamiento positivo uruguayo no contempla el "delito informático", no está tipificado como tal y tampoco como atenuante o agravante de un tipo legal ya existente

Bergstein hace referencia que en Uruguay existen tres posiciones respecto a si es necesario o no la creación de los delitos informáticos.

Los que sostienen la primera posición entienden que no sería necesario crear delitos específicos ya que “una adecuada aplicación de figuras delictivas como peculado, hurto, estafa, apropiación indebida, daño, reproducción no autorizada de fonogramas y videogramas, etc., abarcaría razonablemente las diferentes hipótesis delictivas, sin necesidad de crear nuevos delitos”

De acuerdo a la segunda posición el delito convencional solamente se vuelve complejo debido al medio utilizado.-

Y para los seguidores de la tercera posición “la tecnificación de los instrumentos delictivos y su singular potencialidad dañosa incide en la formulación de un bien jurídico que no puede ser encasillado en los bienes jurídicos tradicionales”.

Coincidiendo con el profesor Bauzá entendemos que hay varias figuras delictivas que de acuerdo al derecho penal uruguayo y hasta la sanción de ley específica, serían las aplicables, a los cibercrimenes,. De esa normativa destacamos las siguientes:

a) Establecidas en nuestro Código penal: Art 347 Estafa, Art 217 Atentado contra la regularidad de las comunicaciones, Arts. 236 y ss. Falsificación documentaria, Arts. 132.3, 163, 296 y ss Penal, Revelación de secretos, violación de correspondencia escrita, interceptación de noticia telegráfica o telefónica. Art 290 Amenazas, Art 358 Daño.

b) Establecidas en otras leyes: Art 697 Ley 16.736, Delitos contra la propiedad intelectual contenidos en las leyes 17.011 y 17.616 y Art 4 inc 2 de la Ley 18.600

A la fecha, se encuentra en el Parlamento un proyecto de ley sobre delitos informáticos, en su artículo primero efectúa varias definiciones y posteriormente establece

Art 2 se penalizará el acceso no autorizado a todo o parte de un sistema informático,

Art 3 penaliza al que sin autorización dañe, borre, altere, deteriore o suprima datos o sistemas informáticos, o inutilice, obstaculice o distorsione el funcionamiento de éstos.

Art 4 tipifica el delito de estafa informática para el que mediante el uso de tecnologías, se valiere de cualquier manipulación engañosa de sistemas informáticos o de información en ellos contenida, para procurarse a sí mismo o a un tercero un provecho injusto en daño de otro,

Art 5 El que, mediante la utilización de tecnologías, suplante la identidad de una persona física, aún fallecida, con la finalidad de cometer una actividad penada por la Ley, o de la cual resulte un

perjuicio injustificado, cometerá delito de suplantación de identidad.

Art 6 finalmente se establece que quien efectué cualquier tipo de tratamiento de datos personales a través de medio engañoso, abusivo o extorsivo será castigado con pena de tres meses de prisión a seis años de penitenciaría

Art 7 se fijan una serie de circunstancias agravantes.-

Para el presente trabajo no es relevante si se trata de un delito nuevo o no, sino que nos referiremos a la prueba del mismo y mas concretamente a la función que cumpliría un Notario en el momento de recabar la misma para que no sea cuestionada en juicio.

En la actualidad nos encontramos inmersos en un cambio de los paradigmas, hay nuevas formas de almacenar, transmitir y obtener información pero estas lamentablemente se ven ligadas a acciones delictivas todo lo que tiene relación con la seguridad informática, y es en estos casos donde cobra relevancia la informática forense.-

LA INFORMATICA FORENSE

La informática forense extrae, analiza y documenta la evidencia de un sistema informático o red, la mayoría de los casos como medida previa a iniciar un juicio penal o civil

Una vez que se constata que el dispositivo electrónico fue atacado, la informática forense intenta reconstruir ese ataque para

lograr ver el daño que se causó, donde se inició el mismo y por supuesto los autores.-

La evidencia digital es frágil y puede fácilmente ser modificada y perder autenticidad al ser presentada por ejemplo en un juicio. Por lo tanto se deben establecer normas de procedimiento y cadena de custodia.-

Los peritos coinciden que los procedimientos llevados a cabo mediante la informática forense tienen que cumplir las siguientes etapas:

- Adquisición: Lo primero que debe hacerse es copiar el contenido de toda la información del dispositivo a analizar ya que luego se trabajará sobre esta copia de tal manera que la información original quede intacta.-

Es interesante destacar que el simple arranque de una computadora altera algunos archivos, fechas o contenidos por lo que siempre se aconseja que esta labor se efectúe accediendo a los volúmenes en modo de "solo lectura"

- Validación y preservación de los datos adquiridos: Se calcula por medio matemáticos un código único que corresponde a esa combinación única de bytes que forma la totalidad del medio en análisis.- El mismo deberá ser complejo para impedir que sea generado en forma reversa con fines dolosos, y así solo personal legalmente autorizado pueda manipular así establecer una cadena de custodia consistente.-

- Análisis y descubrimiento de evidencia: en esta etapa realizan todas las pruebas que se consideren necesarias siempre sobre la copia que fue validada, y dependerá de caso concreto.-

Se puede buscar, por ejemplo, archivos creados, borrados o modificados entre tal o cual fecha, mensajes de correo, imágenes, videos, los archivos que fueron alterados respecto a su formato original, palabras claves como nombres, ciudades, números telefónicos, actividad en la web, etc formando así un perfil del usuario.-

Una vez localizadas todas las partes del sistema, se recomienda fotografiar todo el sistema así como su ubicación y los dispositivos de almacenamiento.

- Informe: se presenta un informe por escrito que no solo debe reflejar todas las evidencias recogidas, indicios y pruebas sino que debe ser redactado con un lenguaje técnico pero de tal manera que sea claro y sencillo y pueda ser leído por personas no expertas en la materia como magistrados, abogados, etc.-

Para López Delgado este informe deberá contener al menos los siguientes puntos:

- Antecedentes del incidente,
- Recolección de los datos,
- Descripción de la evidencia.
- Entorno del análisis.
- Descripción de las herramientas.

- Análisis de la evidencia.
- Información del sistema analizado.
- Descripción de los hallazgos.
- Cronología de la intrusión.
- Conclusiones.
- Recomendaciones específicas.
- Referencias.

El informe que efectúa el especialista en la materia sería tratado como un dictamen pericial .

Código General del Proceso uruguayo establece que "Son medios de prueba los documentos, la declaración de parte, la de testigos, **el dictamen pericial**, el examen judicial y las reproducciones de hechos…."

Como es un tema muy delicado, teniendo en cuenta la volatilidad de la prueba, a los efectos que la misma no sea refutada en ninguno de sus aspectos debe actuar en el proceso de pericia informática, un fedatario que repetimos, deberá ser un Notario.-

Es decir, para que la "cadena de custodia" sea considera valida el Notario debe constatar que la prueba no ha sido contaminada y que es la misma antes y después de efectuado el análisis forense.-

Cobra suma importancia la figura del perito informático que coincidiendo con Jeimy Cano debe tener una formación profesional hibrida que si bien su área de formación es la informática debe estar interiorizado en las disciplinas jurídicas y especialmente en las criminalísticas.-

LA PRUEBA ELECTRÓNICA

En todos los tiempos, la valoración de la prueba en un proceso judicial fue una cuestión importante, hoy dadas las circunstancias es una necesidad imperiosa incursionar en la valoración de la prueba electrónica.-

La prueba electrónica, tal como lo establece en el año 2007 la Certificación Europea sobre Cibercrimen y Prueba Electrónica (ECCE), tiene características únicas y especiales:

Altamente volátil: en algunos casos el solo hecho de una pérdida de energía eléctrica o la existencia de una sistema automatizado que borre cada tanto tiempo los archivos mas viejos a los efectos de liberar espacio hacen que la prueba electrónica que esté alojada en un dispositivo se elimine.-

Debe ser interpretada por un experto: generalmente las pruebas electrónicas están ubicadas donde solo un experto buscaría o son necesarias herramientas muy específicas como el microscopio electrónico de barrido.

Puede ser alterada o destruida mediante el uso normal: ya sea que el usuario modifique o destruya algún documento o prueba voluntariamente o porque automáticamente el sistema operativo así lo hace.-

Se puede copiar sin límites: es indefinido el número de veces que puede copiarse la información digital y será exactamente igual al original por lo que resulta beneficioso en el sentido que varios expertos podrían estudiar esa prueba a la vez.-

Existen principios internacionales sobre valoración de pruebas propuestos desde 1996 por la ONU en la Ley Modelo de la Comisión de las Naciones Unidas sobre Derecho Mercantil Internacional (CNUDMI) sobre Comercio Electrónico y que son:

1.- La Atribuibilidad.- la condición de validez consiste en que el datagrama o mensaje de datos pueda de manera fiable ser adjudicado al emisor.

2.- La Integridad.- la condición de validez consistente en que el datagrama o mensaje de datos haya permanecido completo e inalterado durante el proceso de su comunicación, archivo o presentación.

3.- La Conservación.- la condición de validez consistente en que el datagrama o mensaje de datos sea accesible para su ulterior consulta; y sea preservado con el formato en que se haya generado, enviado o recibido o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida.

En el ordenamiento jurídico uruguayo impera un sistema de prueba mixta, consagrado por el Art. 140 del Código General del Proceso "Las pruebas se apreciarán tomando en cuenta cada una de las producidas y en su conjunto, racionalmente, de acuerdo con las reglas de la **sana crítica ,** salvo texto legal que expresamente disponga una regla de apreciación diversa."

Entendemos que aplicar la "sana crítica" a una materia cuyas manifestaciones son, por ejemplo un correo electrónico, una pagina web, el volcado informático, entrar a una computadora, Tablet o teléfono celular, una pericia informática es un gran reto para los operadores jurídicos en un campo donde prevalecen las innovaciones tecnológicas.-

Los peritos informáticos se pueden basar en cualquiera de las guías de buenas practicas que existen, siendo las mas utilizadas:

- Guía Australiana, Manejo de Evidencias en IT,
- Guía Reino Unido, Buenas Prácticas para Evidencia Basada en Computadores,
- Guía Hong Kong, Computación Forense,
- IOCE,
- Guía para las Mejores Prácticas en el Examen Forense de Tecnología Digital,
- RFC 3227,Guía para Recolectar y Archivar Evidencias,

En todas ellas aconsejan establecer un detallado y riguroso registro escrito y/o fotográfico para identificar la evidencia, la detección, recolección, protección y traslado de la misma hasta el momento de ser presentada como prueba en la justicia y por lo tanto, consideramos imprescindible la presencia del Notario.-

Por ejemplo ,si el dispositivo electrónico que incautó la justicia fue encendido antes de proceder al análisis forense en

presencia del Notario esa prueba podría no ser considerada válida puesto que el sistema operativo fue modificado, por lo tanto para que estrictamente se mantenga la cadena de custodia el Notario debe intervenir desde el comienzo y en todas las etapas.-

La evidencia digital podría estar representada entre otros, por archivos, imágenes, videos, procesos en ejecución en el sistema, etc.-

A continuación haremos referencia ,a vía de ejemplo, de casos donde se puede y en los hechos se aplica la informática forense

La gran mayoría de los documentos contenidos en una computadora tienen datos que a simple vista no podemos detectar, que solo un experto en el tema logra encontrarlos ya sea con herramientas adecuadas o no, que son los llamados metadatos.-

Cuando imprimimos un archivo, por mas que luego de hacerlo lo eliminemos de nuestra computadora, un perito forense analizando los archivos de bobina puede especificar que fue lo que se imprimió y hasta de donde o en que momento se dio la orden de impresión

Cuando navegan por internet con frecuencia la gran mayoría utiliza aplicaciones como la web browsing que va almacenando todas las páginas y contenidos visitados a los efectos de facilitar un futura búsqueda, lo que en caso de una pericia forense podrían llegar a evidenciar los motivos de la persona que supuestamente cometió un delito.

Otro dato de relevancia que obtienen los peritos son fechas y horas lo que es guardado en el sistema operativo para cada archivo y si lo cruza con los metadatos puede asi establecerse una secuencia de lo ocurrido.-

Es muy sencillo editar un correo electrónico solo con "cortar" y "pegar" el contenido del mismo y luego "armarlo" en un documento de texto Word simulando la apariencia de correo, luego se imprime con el fin de presentar como prueba.-

En sí mismo esta impresión no acredita que ese correo sea real ni puede ser aceptado como medio probatorio en juicio ya que como vimos el mismo pudo haber sido manipulado.

Es por tal razón que se deben tener en cuenta otros aspectos como la máquina que lo contiene, la información digital adicional que proporciona el propio correo, el programa en el que se encuentra alojado, los servidores de correos electrónicos que como sabemos registran las conexiones que establecen los clientes (IP, día y hora) tanto para enviar como para recibir mensajes.

Casos jurisprudenciales interesantes

1) Sentencia de la Audiencia Provincial de Barcelona de fecha 29/1/2008 en procedimiento abreviado 255/02

BB y CC condenados como autores penalmente responsables de un delito contra la propiedad intelectual apelan la sentencia del Juzgado Penal manifestando entre otras cosas falta de adecuada custodia del material informático intervenido que no fue sellado, ni precintado, ni identificado correctamente, existiendo discordancias

numéricas entre la relación de material obrante al folio 245 y las actas domiciliarias

Hubo una correctísima identificación de los efectos incautados en cada uno de los domicilios registrados, como es de ver en las diferentes actas en el que el Secretario Judicial hace constar las indicaciones que aparecen en la carátula de cada Cd o diskette, aunque sea de forma somera y si no tiene identificación también lo hace constar así, indicando en ese caso incluso el color de las cajas en que se guardan dichos elementos (folio 130).que como recuerda José Enrique Vocal de la Junta de Gobierno del Colegio Oficial de Ingenieros en Informática de la Comunidad Valenciana (COIICV) en su ponencia sobre la pericial informática, "el objetivo de un peritaje de este tipo es presentar el contenido de archivos que puedan tener relevancia jurídica, informando de su significado y características, teniendo en cuenta además que el peritaje ha de poder ser repetido, por lo que no se pueden alterar los elementos informáticos originales trabajándose siempre sobre copias clónicas".

Comentario: Vemos reflejado en esta sentencia la importancia del momento de recoger la prueba lo cual debe quedar claramente establecido en acta que a criterio de la autora debería llevarse a cabo por un Notario o en su caso por un Actuario judicial.

2)Sentencia N° 530/2009 de la Audiencia Provincial Santa Cruz de Tenerife en apelación de sentencia delito.-

En el proceso penal se condenó a FF como autor de un delito de abuso sexual y un delito de corrupción de menores, el mismo apeló la sentencia y uno de los fundamentos de dicho

recurso fue quebrantamiento de normas y garantías procesales en la aportación de la prueba electrónica al acto del juicio

Manifestó que el material habría -o podría haber sido- manipulado, que la cadena de custodia no estaba asegurada y que la falta de entrega inmediata de los soportes originales a la autoridad judicial no permite excluir se hubiera podido producir una manipulación

Ante esta afirmación el tribunal manifiesta "La prueba en soporte electrónico plantea una problemática muy especial: es altamente volátil, y es posible su eliminación o manipulación por el propio sospechoso de forma rápida y efectiva -si se utiliza el software adecuado-, por lo que es necesario un aseguramiento inmediato de la misma; y, en parte por las mismas razones, es fácilmente manipulable -si bien estas manipulaciones y alteraciones pueden ser habitualmente detectadas mediante un examen forense de los soportes-. Por esta razón es recomendable que se proceda a un clonado de los soportes intervenidos: se obtiene una copia idéntica del soporte original sobre la que -sin posibilidades de alteración- pueden trabajar los agentes investigadores; y se puede comprobar la identidad absoluta de las copias obteniendo la huella digital del original y de la copia, que deben ser coincidentes. Esta operación de clonado se llevó a cabo con relación al disco duro, si bien en el caso del resto de soportes se llevó a cabo un examen directo de los mismos por parte de los agentes encargado de la investigación. En este caso, al tratarse de datos grabados en CD y en DVD, una manipulación de los contenidos -si bien posible- es más dificultosa y fácilmente detectable."

El condenado también recurrió el hecho que se había presentado en juicio fotografías impresas diciendo que son copias que no

pueden ser objeto de valoración en el juicio, que en realidad debió presentarse los documentos originales .La Audiencia provincial con acierto estableció en la sentencia "El documento electrónico -en su contenido original- solamente contiene ceros y unos, su examen solamente puede llevarse a cabo utilizando los equipos técnicos necesarios provistos del software adecuado, y la confirmación de la autenticidad del documento solamente puede comprobarse a través de otros medios de prueba (cfr. art. 382 LEC), en particular, mediante informes técnicos, pero también mediante la declaración de los funcionarios que examinaron su contenido y que explican al Tribunal el procedimiento de examen

Comentario: Sumamente importante en toda pericia informática es la llamada cadena de custodia para evitar que se manipule o que se alegue por los demandados o imputados una manipulación de la misma. Insistimos, la presencia del Notario labrando las actas respectivas diríamos que casi anula tan circunstancia

Asimismo se aclara una de las dificultades de la prueba electrónica, que la misma en algunos casos solo puede ser obtenida por medio de herramientas especificas y de técnicos especializados en la materia.

3) Sentencia de la Audiencia Provincial de Barcelona N° 164/2008 del 9/5)2008

En juicio civil FF S.L y GG S.L demandaron a HH, JJ, SS, TT S.L , RR S.L. WW S.L por competencia desleal de los cuales algunos fueron condenados a pagar una determinada suma de dinero por incumplimiento de clausula penal otros a resarcir daños y perjuicios y otros absueltos,

Quienes presentaron apelación a la sentencia manifestaron, en principio, que no se había protegido el derecho al secreto de las comunicaciones Respecto a este agravio el Tribunal expresa: "en este caso no era posible apreciar una vulneración de este derecho constitucional porque el perito informático no había interferido ningún proceso de comunicación ajeno. El perito lo que hizo fue una búsqueda ciega a través de una herramienta informática denominada ENCASE, que no conlleva la lectura de toda la información para detectar lo relevante para la empresa, sino la utilización de palabras clave que sólo permiten rescatar lo que interesa, si es que no hubiera sido borrado en la reinstalación. Como explicábamos en nuestro anterior auto, el borrado usual (pues existen otros de bajo nivel que sí eliminan la información), no hace desaparecer los datos, sino que elimina las entradas de los mismos y hace imposible acceder a ellos: al romperse el código de entrada en sistema binario, los datos permanecen, pero confundidos e indistinguibles en una enorme cantidad de ceros y unos, de modo que el programa empleado pretende detectar los patrones binarios de ciertas palabras, y una vez detectados, reinterpretar por encima y por debajo hasta reconstruir un texto".

También los demandados alegaron violación al derecho de intimidad pero el Tribunal rechazó tal afirmación diciendo que "…la localización informática antes descrita de los mensajes que incorpora el informe pericial no es contrario a la intimidad de los demandados: la búsqueda ciega discriminó desde el principio todo lo que pudiera tener alguna relación con ese ámbito, y con lo obtenido no se afecta a su vida íntima, a esa esfera personal y reservada que preserva la dignidad y la libertad individual, sino a

ciertos actos puntuales de relevancia estrictamente comercial o empresarial. No es, por tanto, que la indagación efectuada afectara al derecho fundamental a la intimidad personal pero que la misma resultara justificada por un fin legítimo, proporcional, idónea y necesaria, sino que dicha pericial se mantuvo al margen del ámbito constitucionalmente protegido"…

Comentario: Una pericia informática realizada en cumplimiento de los protocolos establecidos y llevada a cabo por los analistas expertos en la materia lleva a que la prueba presentada no sea dejada de lado alegando violación de derechos personales.-

LA FUNCIÓN DEL NOTARIO EN LA CADENA DE CUSTODIA

Hoy en día, intercambiar información en Internet, como red abierta que es, implica asumir riesgos, es relativamente sencillo crear una página web falsa, obtener o manipular correos electrónicos, el receptor puede desconocer el autor del mensaje o éste aparecer como persona diferente, el mensaje puede ser modificado o falso o leído por un tercero no deseado

La seguridad es un término que se encuentra unido, de manera indisoluble, al Derecho.

En el análisis forense es de suma importancia la cadena de custodia, que es uno de los protocolos de actuación que deben rigurosamente seguirse respecto a determinada prueba informática es decir cómo y dónde se obtuvo, como se analizó, quien lo hizo, para llegar luego a un informe al respecto.-

La aplicación de las nuevas tecnologías de Información y comunicación han modificado casi todas las actividades que el

hombre realiza en este siglo XXI. La actividad del Notario no ha quedado ajena a este fenómeno y poco a poco se inserta en el esquema de sociedad digital y así surge una nueva generación de actividades.-

Son muy pocos los que hoy no tienen un correo electrónico o un teléfono móvil para sus comunicaciones y es así que también comenzó a requerirse la actuación de un Notario a los efectos de comprobar, por ejemplo, la existencia y/o texto de tal o cual mensaje o mail.-

Ya en el año 1998 en un Informe de la Comisión de Informática y Seguridad Jurídica de la Unión Internacional del Notariado Latino, entre las aplicaciones que se citan destacamos …"Archivo y conservación del documento electrónico: la posibilidad para las partes de presentar en juicio una copia certificada compulsada por el notario, que conserva el original, con la misma fuerza probatoria del original mismo, indudablemente permitirá atribuir mayor confidencialidad a documentos que son, en muchos aspectos, incorporales";…

Para Couture la fe pública es la calidad propia que la intervención del Notario acuerda a los instrumentos expedidos en el ejercicio de su función, derivada de la suposición legal de que lo aseverado por él, es verdad.

Tenemos entonces que al notario la ley le atribuye la potestad de dotar de certeza los hechos que le constan por evidencia directa o conocimiento y que luego hace constar en documentos escritos con máxima eficacia probatoria.

Para Bardallo, “la fe pública es una de las grandes instituciones del mundo latino, porque contribuye eficazmente a la seguridad de las relaciones jurídicas, al poner en la base de las mismas, la verdad de los hechos sobre los cuales aquéllas se constituyen, modifican y extinguen”

El ejercicio de la fe pública notarial se desarrolla en tres etapas, la primera de percepción de los hechos, luego la representación de los mismo en el documento notarial que corresponda y la tercera de confirmación de lo acontecido, de esta manera asegura que la relación entre los hechos y lo que surge del documento sea correcta.

En la primera etapa el notario debe percibir inmediata y directamente los hechos por sus sentidos principalmente de vista y oído y comprender e interpretar esos hechos percibidos.

Posteriormente el Notario redacta el documento que corresponde, ya sea una escritura pública si estamos frente a un negocio juridico, un certificado cuando se refiera a hechos conocidos por el Notario o a documentación que tenga a la vista, o un acta para el caso de actos jurídicos no negociables y por ultimo al autorizarlo asevera que existe correspondencia y presume fidelidad de esa relación documental.-

El documento notarial es un medio de prueba documental, indirecta y principalmente de tipo legal ya que su valor probatorio lo impone la ley salvo que se demuestre la falta de veracidad de los extremos amparados por la fe pública.-

Preservando cuidadosamente estas cualidades, el Notario añade, ahora, la utilización vanguardista de las nuevas tecnologías

y como depositario de la fe pública y, garante de la seguridad jurídica cumple un rol estratégico en la sociedad de la información.

Siguiendo al Esc Wortman entendemos que “Uno de los aspectos importantes en la gestión de indicios y pruebas electrónicas para que éstas puedan ser consideradas evidencias es la adecuada preservación de su contenido, de forma que la información esté disponible para los peritos, sin que pueda cuestionarse su obtención o su custodia. Por otro lado, también es importante el propio análisis de la información existente, por parte de los expertos con profundos conocimientos informáticos, acompañados del escribano quien labrará el acta de comprobación respectiva de los procedimientos técnicos, observaciones y conclusiones a las que se arriben”

Por tanto, el rol del notario en toda esta actividad de recolección de evidencia digital, sería la de labrar todas las actas que se consideren necesarias como medio de prueba.-

Para Larraud el acta notarial es el "instrumento matriz autorizado por el Escribano fuera de su protocolo, para consignar circunstanciadamente y baje su fe un hecho cualquiera o un acto no constitutivo de otorgamiento, que presencia".

En el derecho positivo uruguayo el fundamento legal de las actas notarial, lo encontramos en la ley orgánica del Notariado del año 1878 en sus artículos 1º: “Escribano Público es la persona habilitada por autoridad competente para redactar, extender y autorizar bajo su fe y firma, todos los actos y contratos que deben celebrarse con su intervención entre los particulares o entre éstos y toda clase de personas jurídicas” y 60 : “Es deber de los Escribanos

autorizar todos los actos y contratos para que fuesen llamados, a no ser que tengan legítimo impedimento"

En cuanto al valor probatorio del documento notarial por es titulo autentico y como tal hace plena fe de haberse otorgado y su fecha mientras no se demuestre lo contrario mediante tacha de falsedad

. En vía judicial el Código General del Proceso Uruguayo reconoce la autenticidad del documento público, entre otros, en los siguientes artículos:

170.1 "El documento público se presume auténtico mientras no se demuestre lo contrario mediante tacha de falsedad; igual regla se aplicará al documento privado cuyas firmas se encuentren autenticadas por notario o autoridad competente."

172.1 "La parte que impugne de falsedad material de un documento público o un documento privado auténtico o tenido por auténtico, presentado por su adversario, deberá hacerlo en las oportunidades a que alude el artículo anterior, promoviendo demanda incidental con la que se formará pieza por separado, en cuyo procedimiento, además de la parte contraria, será oído el Ministerio Público. La falsedad ideológica o la nulidad del documento se argüirá como defensa en el propio proceso"

Aunque el Código Civil Uruguayo (art. 1574) indica que el instrumento público "es" un título auténtico, mientras el Código General del Proceso Uruguayo (art.170.1) refiere que "se presume" auténtico, en realidad las dos expresiones son equivalentes puesto que el ser o ser presumido solo caen frente a la sentencia judicial

que declare la falsedad material del documento en ambas normativas.

CONCLUSIONES

1)Sin perjuicio que las nuevas tecnologías están presentes en nuestras vidas en todos los ámbitos y por tanto también lo vemos reflejado en un aumento considerable de procesos judiciales donde se presentan pruebas electrónicas, ésta continua siendo un instrumento desconocido para la gran mayoría de los operadores jurídicos.-

2) Entendemos que es necesario establecer modelos conceptuales desarrollados tanto por informáticos como por juristas para enfrentar el problema de un uso de las nuevas tecnologías en forma correcta en cada proceso judicial, que garanticen y resguarden la información.-

3) El notario cuando constata procesos tecnológicos, los dota de fe pública que no importa si es tradicional o informática sino que es ejercida con imparcialidad y legalidad y que los documentos que expide hacen prueba por si solos.-

4) Este avance tecnológico plantea muchos retos al Escribano quien debe analizarlos con serenidad y prudencia teniendo en cuenta que la informática no es un fin sino solo una herramienta más para desarrollar su actividad y recordando siempre que la certeza y la seguridad jurídica son los pilares de la misma.

4) Y finalizamos el presente trabajo con las palabras de una destacada profesora uruguaya la Notaria Julia Siri: “En el nuevo Derecho uruguayo, los nuevos medios tecnológicos son admitidos como medios probatorios. El escribano, como realizador del Derecho no debe autolimitarse sino procurar la inserción de los mismos dentro de su función autenticante en la medida en que la legislación vigente lo permita. Al mismo tiempo habrá de procurarse las soluciones legislativas que liberen a la función notarial del rigorismo formal que hoy la asfixia, incompatible con su: carácter de fedatario y con los nuevos tiempos”

BIBLIOGRAFIA

Bauzá, Marcelo. Criminalidad Informática: Reto crítico y abierto. Revista de Legislación Uruguaya 2012 (julio)

Bergstein, Nahúm. Derecho Penal e Informática. La Justicia Uruguaya Tomo 11

Montano Gómez, Pedro J. Los delitos informáticos. UY/DOC/325/2009

Delpiazzo, Carlos E. Derecho e informática.- La Justicia Uruguaya Tomo 88

Delpiazzo, Carlos E. "Perspectivas de la Informática jurídica en nuestro país", . Revista de Jurisprudencia y Doctrina, Año 1983,

Taruffo, Michele. Conocimiento Científico y estándares de prueba judicial. Boletín mexicano de derecho comparado. Nro 114.

Elizalde Martín Francisco, Modelo de administración de prueba digital. (e-Discovery)Un método para desarrollarlo en pequeñas y mediana empresas.-

López Del Carril, Gonzalo.-La prueba informática.LA LEY 09/06/2011,

Torres-González**.** Firmas Digitales y Autenticación de Evidencia Electrónica. **:**

Molina Quiroga, Eduardo Evidencia digital y prueba informática. LA LEY 04/06/2014.

Bender Agustín Peritaje Informático. No. 139 - Febrero del 2010.-La Validez en Juicio de la Prueba producida utilizando la Máquina del Tiempo de Internet.

López Delgado, Miguel "Análisis Forense Digital" Segunda Edición: junio 2007

Téllez Valdés, Julio, Para una sistematización del derecho penal de la informática véase: "Derecho Informático", México,

Autores varios Coordinación Abel Webke y Shaffer Burkhard. "Certificación Europea sobre Cibercrimen y Pruebas Electronicas"

Huerta Miranda, Marcelo y Líbano Manzur Claudio, Los Delitos Informáticos, Editorial Jurídica Cono Sur.

Cano Jeimy José , Remolina Nelson , Rueda Andrea, Pimentel Javier, Ramírez Angela, Segrera Marta, Iregui Luis El peritaje informático y la evidencia digital en Colombia. Conceptos, retos y propuestas.

Informe emitido en la II Reunión Plenaria de la Comisión de Asuntos Americanos celebrada en Santa Fe de Bogotá del 3 al 5 /12/98, citado por SIRI Julia "La incidencia del documento electrónico en el Derecho Notarial, ¿atenta o no contra sus principios?

Nuñez Ponce, Julio. Derecho Informático,

Wortman, Javier, El Derecho Informático y la intervención notarial Revista AEU N°93 año 2007

Larraud Rufino. Curso de derecho notarial.

Bardallo, Julio R. Fe pública notarial, Revista del Notariado Nº 769

Apat, Hugo y otros. El documento notarial. Su valor probatorio, Revista Notarial Nº 909,

Farini, Martha B. El documento notarial y la prueba preconstituida, revista notarial Nº 833,

Couture Eduardo J. El concepto de Fe publica

Lazaro Carmen y otros. Pruebas electrónicas ante los tribunales en la lucha contra la ceibercriminalidad. Un proyecto europeo.

http://www.alfa-redi.org/node/8931 (visitada 05/07/14)

http://www.todouruguay.net/que-es-la-informatica-forense/(visitada 05/07/14)

http://www.informaticaforense.com/criminalistica/ (visitada 07/07/14)

http://www.informaticaforense.com.ar/informatica_forense.htm(visitada 7/07/14)

http://www.youtube.com/watch?v=UhumXfZedM0 visitada 10/07/14

http://www.poderjudicial.es/ (visitada 10/07/14)

http://www.elpais.com.uy/vida-actual/uruguay-pais-menos-preferido-sudamerica.html (visitada 15/07/14)