El Peritaje en Tecnologías de Información

Expert Work in Information Technologies

Raúl Alvarado Rodríguez[1]

RESUMEN

En la sociedad actual, el uso de las tecnologías de la información está cada vez más ligado al quehacer humano. Desgraciadamente, el conocimiento puesto en manos equivocadas puede ser usado como medio para realizar actividades ilícitas o ser aplicado incorrectamente en lo que más importa: Vender por vender. Por tanto, en esta sociedad, metafóricamente denominada "sociedad de la información", se hace cada vez más necesaria la figura del **Perito en Tecnologías de la Información**. Su papel es fundamental, pues se constituye en garante de la verdad, la justicia, los derechos y libertades de las personas, en cuanto mejoren sus relaciones con las tecnologías de la información.

El título universitario de Ingeniero de Computación y Sistemas, Ingeniero de Sistemas, Ingeniero Informático o afín, garantiza la base intelectual requerida para complementarla con la formación de postgrado y prácticas necesarias, con el fin de poder desempeñar este importante papel con garantías plenas de éxito.

Palabras clave: Peritaje, sociedad de la información, tecnologías de la información.

ABSTRACT

In current society, the use of information technologies is getting linked more and more to human task. Unfortunately, knowledge in wrong hands can be used as a means to make illicit activities or applied incorrectly on what is more important: sell to sell. Therefore, in the present society, methaforicaly called “information society”, the figure of an Expert in Information Technologies is getting more and more important. His performance is fundamental, since he becomes a guarantor of the true, justice, rights, and people freedoms, in the sense of improving their relationships with information technologies.

Universities title of: Computing and System Engineer, System Engineer, Computer Science Engineer, or other compatible, guarantees the intellectual background required to be complemented with graduate studies and necessaries skills, in order to be able of carrying out this important task with a total success.

Key words: Expert work, information society, information technologies.

1 Ingeniero de Computación y Sistemas. Profesor de la Escuela de Ingeniería de Computación y Sistemas, UPAO. Consultor en Tecnologías de la Información.

INTRODUCCIÓN

En un mundo actual, interconectado y digital, las relaciones y operaciones entre las personas y las organizaciones cambian y adquieren nuevos matices que son parte de una naciente sociedad de la información.

Es innegable que el desarrollo tecnológico y, fundamentalmente, la modernización de los sistemas computarizados de gestión, almacenamiento y transmisión de información han permitido su masiva difusión. La utilidad de tales medios ha posibilitado su rápida inserción en actividades científicas, comerciales, académicas, militares, etc., sin perjuicio de coadyuvar, directa o indirectamente a la proliferación de nuevas modalidades delictivas.

En este contexto, al igual que en el mundo físico, las conductas criminales establecen un nuevo paradigma y reto, que exige la administración de la justicia, de la academia, del gobierno, de la industria y de la sociedad en general una respuesta coherente y formal que permita enfrentar la exigente ruta de la inseguridad de la información [CANO 2004] inherente a todos los sistemas informáticos y electrónicos.

El Peritaje en Tecnologías de la Información (TI) surge como respuesta natural de la evolución de la administración de justicia que busca avanzar y fortalecer sus estrategias para proveer los recursos técnicos, científicos y jurídicos que permitan al juzgador, alcanzar la verdad y asegurar el debido proceso en un ambiente de pruebas electrónicas.

El Peritaje en Tecnologías de Información

El Peritaje en TI es el estudio o trabajo sobre una materia concreta de las TI que realiza un experto o **Perito en TI**. En la dimensión del Derecho, el peritaje en TI tiene como fin informar, bajo juramento, al juzgador sobre puntos litigiosos en cuanto se relacionan con su especial saber o experiencia.

El peritaje en TI como tal es una actividad muy amplia de la profesión de Ingeniería de Computación y Sistemas o afín, que se puede definir como transversal y horizontal; ya que está íntimamente relacionada con la deontología profesional y afecta a cualquier materia informática. La deontología profesional define básicamente los deberes éticos que un profesional debe cumplir durante el desarrollo de sus funciones, lo que es aún más patente porque está en juego el honor profesional.

El hecho que el peritaje en TI sea una actividad horizontal no significa que cualquier Ingeniero pueda llevarla a cabo adecuadamente. Para ello, además de la ética profesional, se requiere ser muy buen conocedor de la materia de que se trate y saber demostrarlo. Este saber demostrarlo es fundamental en un peritaje en TI porque aunque de entrada se le supone la valía profesional al Perito, éste ha de saber fundamentar convenientemente las conclusiones de su estudio. Para ello, es necesario usar, en lo posible, métodos científicos contrastados y no dejarse influenciar por la subjetividad.

El peritaje en TI, como todo proyecto, consiste en una serie de fases que han de planificarse de acuerdo a la complejidad del asunto. De manera global, las fases son las siguientes:

1) Definición de la consulta y viabilidad

   El objetivo de esta fase es definir lo que el cliente quiere averiguar y el ámbito que abarcará para así hacer un estudio de viabilidad.

   En esta primera fase está presente la ética profesional del Perito, pues no ha de proseguir si estima que no va a ser capaz de resolver lo que le piden por no ser experto en esa materia concreta.

   Otra tarea que ha de realizarse en esta fase es -aunque parezca precipitada- la de solicitar por adelanto el importe estimado de los honorarios; esto nos evitará más de una desagradable sorpresa.

2) Estudio de antecedentes y toma de datos adicionales

   En esta fase, se recopila toda la documentación existente sobre el caso a fin de dar respuesta a lo que se está averiguando. Si con esto es suficiente, se confirma con la siguiente fase; de lo contrario, será necesario realizar un reconocimiento pericial, es decir, someter a la revisión técnica los elementos informáticos para obtener determinados datos de comportamiento o detalles técnicos imprescindibles.

   Esta tarea puede convertirse en la más delicada de todo el peritaje, pues es necesario tener en cuenta detalles como: una adecuada metodología de trabajo o tener experiencia en TI judicial (por ejemplo, para no destruir pruebas, o realizar simulaciones en un entorno lo más real posible, etc.), en todo caso, es muy importante que el cliente sea informado cuanto antes del costo que puede suponer lo que pide, o incluso la imposibilidad de averiguar algo.

3) Estudio de datos y hechos observados

En esta fase se buscan las relaciones entre los datos adquiridos para llegar a conclusiones intermedias que permitan construir los fundamentos del estudio.

4) Elaboración y entrega del informe pericial

Es común subestimar la dificultad de la elaboración del informe; al contrario de lo que se piensa, suele representar cierta complejidad. La razón, frecuentemente, invierte gran esfuerzo por sintetizar las conclusiones que al mismo tiempo no deben incluir términos demasiado técnicos, teniendo en cuenta que el cliente no es experto en la materia.

5) Defensa del informe

Esta fase tiene por objeto ratificar y afianzar el trabajo realizado. Para ello, el Perito comparece y oralmente aclara las conclusiones obtenidas y los métodos empleados para conseguirlas.

Es común que durante la defensa surjan nuevas preguntas nada triviales, a las que por desconocimiento del solicitante, espere respuestas en vivo y en directo. Ahí, desde luego, es preferible estudiar a fondo la cuestión antes de responder.

En el caso de un peritaje judicial, esta última fase es muy relevante, pues un buen trabajo mal defendido es lo peor que puede suceder y lo mejor para aquellos a los que sus conclusiones les perjudica. La preparación de la defensa es, en muchos casos, algo que no se debe descuidar. Lo ideal es reunirse con el solicitante del peritaje para fines de aclaración.

La Materia Informática

Antes de comenzar a discernir la modalidad de trabajo del Perito en TI o la eficacia probatoria de este tipo de medios es menester establecer el objeto, si se quiere, el sustrato material con el que se trabaja.

A los fines prácticos del peritaje en TI el objeto es, ni más ni menos que un conjunto de datos almacenados, administrados o transmitidos mediante sistemas informáticos, extendiendo también el concepto a los dispositivos o equipamientos que permitan el tratamiento automatizado de los mismos.

En este entorno serán objeto de examen para el Perito en TI, tanto el hardware como el software, toda vez que ambos caerían dentro del ámbito de conocimiento en la ciencia informática. Entendemos pues, al conocimiento relacionado con diversos factores pero, esencialmente identificado con la ciencia y con la experiencia.

En informática resulta sumamente difícil delimitar este conocimiento ya que los límites de la ciencia no están definidos. Partamos pues, de la base de sostener que el conocimiento del Perito debe sustentarse en un sistema verificable ordenado sobre pautas o hechos. Existe la generalizada creencia de que este sistema, entendido como un conjunto único y ordenado cuyos componentes son coherentes y solidarios entre sí es, a su vez, falible, pues al basarse en razonamientos inductivos que no abarcan la generalidad de los casos los resultados son, en esencia, falibles; no obstante, la base técnica de análisis es tan confiable como la de otras disciplinas criminalísticas.

Si bien este principio general es aplicable a la totalidad de la actividad pericial, la incidencia de la falibilidad en cuanto a la valoración jurisdiccional de los resultados adquiere especial relevancia por diversas razones:

Existe un generalizado desconocimiento respecto de las modificaciones tecnológicas.

La exposición de resultados, por su intangibilidad, elevado nivel de abstracción y terminología técnica, resulta sumamente dificultoso.

La inexistencia de apoyo jurisprudencial suficiente, que permite al juzgador moverse sobre bases más o menos seguras, fundadas en la experiencia judicial, tal como ocurre con otras disciplinas criminalísticas.

Es incuestionable que si se introducen errores en la computadora, ésta expedirá errores, y que en tal supuesto, la información obtenida no será confiable.

Asimismo, el hecho de que en su mayoría, los soportes de datos pueden ser adulterados, ocultando total o parcialmente cualquier indicio de alteración, no brinda garantías de credibilidad.

Durante mucho tiempo y aún hoy, el problema de los medios probatorios indelebles genera conflictos, llegándose a sostener en algunos trabajos doctrinarios que si los soportes respectivos son indelebles, puede ser prueba en favor de su dueño si existe control de terceros de los datos teleprocesados entre equipos de distintos usuarios.

El excepticismo y la falta de credibilidad existente, no respecto de la idoneidad del experto, sino sobre la materia pericial en si misma, atentan severamente sobre la labor pericial, imponiendo mayores exigencias desde el momento mismo del allanamiento para la obtención y aseguramiento de la prueba.

Los Peritos en Tecnologías de Información

Los Peritos en TI son los profesionales encargados de proporcionar consultaría y evaluación de productos y/o servicios, así como observar las disposiciones para el desarrollo, instalación y seguridad de sistemas circunscritos dentro de las TI a organizaciones públicas y privadas.

En nuestro país, el Perito en TI debe tener título de Ingeniero de Computación y Sistemas, Ingeniero de Sistemas, Ingeniero Informático o afín, además de contar con la Colegiatura y Constancia de Habilidad del Colegio de Ingenieros del Perú.

Si es necesario, a petición de parte o de oficio, un juez podrá requerir opinión a universidades, corporaciones y entidades públicas o privadas de carácter científico o técnico, cuando el dictamen pericial requiriese operaciones o conocimientos de alta especialización.

Un Perito en TI debe ser un profesional preparado, idóneo en varias disciplinas, y sobre todo, eficaz Perito en la materia. Debe tenerse en cuenta, además, que es necesario, en ocasiones, conocer otros aspectos (mercado, realidad técnica, problemáticas, etc.), lo que no es fácil de encontrar en profesionales desactualizados.

Los Peritos en TI pueden tener intervención en áreas que involucran alguna de las siguientes especialidades [COL 02]:

a) Ingeniería de Software (Normalización, Estándares y Metodologías de Desarrollo de Sistemas).
b) Sistemas de Información (Teoría de la Información, Arquitectura de Sistemas, Administración de Proyectos; Sistemas de Información basados en tecnología de Internet).
c) Sistemas de Base de Datos (Multimedia, Bases de Datos Orientada a Objetos, Interoperabilidad de Sistemas Heterogéneos).
d) Cómputo Paralelo.
e) Automatización, Robótica e Inteligencia Artificial.
f) Auditoria, Gestión y Seguridad de Redes Locales de Datos y de Sistemas de Información.
g) Telemática (Comunicaciones de computadoras por medios alámbricos/ inalámbricos, Redes).
h) Datos de cobertura local y amplia.
i) Sistemas Especiales y tecnologías emergentes.

Estas especialidades se relacionan de manera directa con tres grandes campos de la labor pericial que podrían definirse como:

1) Pericias de autenticidad

En este caso hay la necesidad de disponer del patrón material de comparación, de hardware o de software, entendido como indubitable, que permita el análisis comparativo determinante de la autenticidad o no del elemento sospechado.

2) Pericias de contenido, funcionamiento y recuperación de datos

El alcance es mucho más amplio, pues abarca diversos aspectos como: almacenamiento de datos, análisis y determinación de estructuras de diseño de sistemas, medios de comunicación y transferencia de datos, métodos de entrada, acceso, procesamiento y salidas, etc., que en su conjunto, requieren la colaboración interdisciplinaria de profesionales en la materia.

3) Pericias sobre internet

La investigación de ilícitos cometidos a través de la web o bien mediante redes privadas o públicas constituyen un constante desafío para el profesional en TI, que lo obliga a poseer y mantener permanentemente actualizadas las herramientas (software) más modernas para la detección de intrusiones en sistemas remotos, utilización indebida del correo electrónico, etc.

Puede solicitarse al experto: lectura del contenido de discos, verificación de copia y/o adulteración de sistemas y aplicaciones de software, impresión del material secuestrado, impresión del contenido de discos rígidos, establecer el uso indebido de marcas o la explicación de uso de utilitarios y/o sistemas de computación.

Puede requerirse la intervención del experto, con carácter previo a la realización de allanamientos y procedimientos varios, a fin de informar al magistrado requirente las medidas a adoptar, la disponibilidad de equipos y personal técnico en el momento de la diligencia y determinar si la labor pericial puede llevarse *in situ* (condición óptima), o bien cuáles serían las posibles consecuencias de diferir su tratamiento en cuanto a tiempo y lugar de realización.

Concretamente, el Perito no es más que un testigo que ha visto los resultados y examinado los rastros materiales: es la mirada del juez en esos rastros que requieren algún conocimiento especial propio de su ciencia, arte, profesión u oficio.

La Prueba Pericial en Tecnologías de Información

Es el medio de prueba, de suma importancia para cualquier actuación judicial y/o arbitraje que precisen conocimientos científicos o técnicos especializados.

La Prueba Pericial es admisible cuando la apreciación de los hechos controvertidos requiere conocimientos especiales en alguna ciencia, arte, industria o actividad técnica.

En lo que se refiere a peritajes en TI, hay que tener en cuenta que no siempre se relaciona con delitos en TI exclusivamente, es decir, no siempre las TI forman parte de un asunto judicial con motivo de un delito. La TI puede verse implicada:

Cuando es utilizada como medio de un delito.
Cuando es el objeto propio del delito (ejemplo, compra de software ilegal).
Cuando tiene lugar en el conflicto de forma colateral, en ocasiones, determinantes.
Cuando hay incumplimientos de contratos de programación y desarrollo.

El informe pericial

El dictamen del Perito debe contener una opinión fundada, exponiendo al juez los antecedentes de orden técnico que tuvo en cuenta, pues, como ya se dijo, su objeto es ilustrar el conocimiento al magistrado. La pericia, por definición no puede consistir en una mera opinión del experto, prescindiendo del necesario sustento científico.

En materia informática dicha tarea suele ser sumamente dificultosa. En primer término se discriminó, a los fines prácticos la posibilidad de realizar distintos tipos de trabajos periciales.

Cuando se trate de pericias tendientes a establecer la autenticidad de marcas o aplicaciones de software, así como también de unidades lógicas, u elementos electrónicos que integran un procesador y que normalmente caen dentro del la esfera de incumbencia del Perito en TI, el dictamen suele ser sencillo, en la medida en que se cuenta con los correspondientes patrones de comparación o indubitables. Allí podrá expresarse el experto con un alto grado de certeza sobre las características del material secuestrado, en su lineal comparación frente a su original, tal como se realiza normalmente en los casos de violación a la normativa que protege la propiedad intelectual. No obstante, debe, en consecuencia, tenerse en cuenta que este tipo de pericias informáticas no reposan sobre bases estrictamente científicas sino en simples operaciones de comparación; carecen de por sí del valor convincente que tienen los informes periciales de otro tipo, por tanto exige la concordancia con las demás pruebas y elementos de convicción que el proceso ostenta. Es por ello, ineficaz como solo dato a los fines de una condena pues carece de pleno valor demostrativo en nuestro sistema formal.

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, etc. Allí donde la prueba pierde su materialidad, para convertirse exclusivamente en dato, como 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.

El registro electrónico reviste carácter probatorio bajo ciertas condiciones de fidelidad, inalterabilidad y completitud, según reglas de la sana crítica racional y con salvedad de la prueba en contrario, las constancias de almacenamientos, registro, recuperación y reproducción indeleble obtenidas en los elaboradores electrónicos de datos, en cuanto fueran idóneos y pertinentes para acreditar los hechos.

La tarea pericial, en cuanto a su validez probatoria, se ve simplificada cuando el objeto de examen radica en sistemas de registro que poseen respaldo normativo, diversos aspectos informáticos autorizados y reglados en derecho tributario, etc.

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. De todos modos, ello obedece exclusivamente a la reticencia o retardo con que el Derecho enfrenta los avances tecnológicos pues, para desvirtuar la opinión de cualquier Perito es imprescindible valorar elementos que permitan advertir fehacientemente el error o el insuficiente empleo de datos científicos, que deben conocer por su profesión. En general no es la ausencia de método o fundamentos científicos

lo que pone en tela de juicio la eficacia probatoria de los dictámenes sino la tendencia a creer que todo aquello que escapa a la percepción directa de los sentidos y se requiere de un experto para dilucidar su existencia, es esencialmente falible; cuando en realidad, la pericia informática, como muchas otras, se funda en principios técnicos inobjetables y no existe prueba de igual significado procesal que le desvirtúe.

El futuro del Peritaje de TI como rol y profesión

El Peritaje en TI es un rol y una profesión al mismo tiempo, lo que establece un reto académico y personal para quien la selecciona como desarrollo profesional, pues sabe que como Perito en TI los niveles de exigencia y control que se le pedirán, irán más allá de lo que normalmente se tiene para los profesionales en su área.

A un Perito en TI como a cualquier otro profesional, se le exige actualización permanente en su área, en temas tecnológicos, sicológicos, legales, de seguridad, entre otras.

Un profesional en peritaje en TI integral, sin olvidar su formación base, está llamado a mantener un enfoque sistémico que le permita establecer relaciones entre las diferentes disciplinas que debe conocer para construir nuevas posibilidades y procedimientos que mejoren las técnicas para probar, reconstruir, verificar, analizar y presentar el resultado de su trabajo. En este sentido, el Perito en TI integral es un elemento valioso para la administración de justicia, en la medida que este el resultado de sus investigaciones y propuestas de mejora para ampliar el espectro de referentes científicos, legales y técnicos, a fin de que los jueces puedan resolver con mayor facilidad los temas en litigio.

Mientras la justicia no considere la formación de este profesional plural y criminalista digital, los delincuentes intrusos o agresores en el entorno digital estarán planeando nuevas estrategias y artimañas para poner en aprietos a la justicia que fallará posiblemente con pocos y limitados fuentes de información y análisis integrales.

El Perito en TI, que podemos contextualizar como criminalista digital, que es el resultado de la evolución natural de los instrumentos de la justicia para establecer un nuevo referente frente al rápido avance de las tecnologías de información. De tal manera que se puedan preparar y ajustar los instrumentos científicos, técnicos y legales, bajo la percepción de que los litigios y problemas en el entorno digital signifiquen retos y confrontaciones de la inseguridad informática con argumentos, técnicas y procedimientos que aseguren la transparencia y confianza de los procesos y sus resultados.

CONCLUSIONES

1. Analizando las dos caras del Peritaje en TI, se advierte que pese al efecto benefactor de la tecnología sobre la vida de las sociedades modernas, su inserción en el marco jurídico regulatorio no ha sido suficientemente veloz, generando vacíos legales, aparentemente insalvables, que colocan a infinidad de situaciones de hecho, transacciones comerciales o relaciones contractuales en un entorno de inseguridad jurídica.
2. En un sentido profundamente negativo, así como determinadas actividades lícitas aparecen como no reguladas o no regulables; la comisión de delitos que tienen por objeto a la información en si misma, tratada, almacenada o transmitida por sistemas electrónicos o computacionales, resultan, generalmente, impunes ante su atipicidad conforme los ordenamientos legales vigentes.
3. La administración de justicia debe desarrollar elementos técnicos, jurídicos y administrativos que le permitan confrontar, validar y asegurar un adecuado proceso ante situaciones litigiosas donde la evidencia en formato digital, electrónico o informático sea la protagonista.
4. La formación de personal especializado en estas temáticas, es un factor decisivo para el entrenamiento y actualización de los métodos tradicionales en ciencias penales, forenses y criminalísticas, que en un nuevo orden social de una sociedad digital, alcanzan niveles de pericia y especialización especiales.

REFERENCIAS BIBLIOGRÁFICAS

[RIO 05] RIOFRÍO, J. (2005). La Prueba Electrónica. Editorial Temis.

[CAN 04] CANO, J. (2004) Inseguridad informática. Un concepto dual en seguridad informática. Revista de Ingeniería. Universidad de Los Andes. Facultad de Ingeniería. Mayo. ISSN: 0121-4993.

[ESC 04] ESCUELA PRÁCTICA TECNOLÓGICA DE MURCIA (2004). Apuntes del "Curso de peritajes informáticos".

[COL 02] COLEGIO DE PROFESIONALES EN COMPUTACIÓN DE BAJA CALIFORNIA (2002). "Reglamento del Colegio", Capítulo V: De los Peritos.

[DEL 01] DEL PESO NAVARRO, Emilio. 2001. Peritajes Informáticos. Editorial Díaz de Santos. ISBN: 84-7978-497-0.