Tema 7. Dictámenes y peritajes Informáticos

si duo imperata inter se repugnantia simili tibi faciuntur, ambo sequere
Si recibes dos órdenes contradictorias, cumple las dos

De la instrucción en las legiones de la Roma imperial

La figura del perito informático puede parecer algo difusa, con una visión que desde fuera puede tener más de ficción que de realidad, gracias a las novelas, comics, pseudodocumentales, series de televisión y películas procedentes de Estados Unidos, que nos presentan al cyber forense como una mezcla de Sherlock Holmes y Bill Gates. No se termina de apreciar qué es lo que se hace en esta actividad profesional en concreto, uno de los híbridos más perfectos entre la disciplina jurídica y la informática.

Pero poco de ficción y mucho de realidad tiene esta salida profesional que se presenta a los egresados de la carrera de informática. Sin embargo, sus particularidades requieren de al menos esbozar unas líneas maestras que sirvan de cauce para lo que el rio de la experiencia vaya aportando.

A lo largo del presente tema se va a tratar de establecer ese cauce, o al menos una base para crearlo. Tras una breve introducción, donde asentaremos los conceptos básicos, haremos una clasificación de los tipos de trabajo, tipos de peritajes que se pueden encontrar más comúnmente: no sólo pensando en el mundo judicial, sino también en el de las relaciones entre empresas, para lo que recurriremos a fuentes procedentes básicamente del mundo anglosajón, pues allí está mucho más desarrollada esta vía profesional. Nos queda describir al perito en si mismo, a sus competencias necesarias y marco en el que juega, y, por supuesto, centrar el resultado que se plasma de su trabajo: el dictamen, de los que veremos algunos ejemplos.

Como en todos los temas, cerraremos con un apartado bibliográfico, del que cabe destacar de forma anticipada un conjunto de direcciones url donde encontrar herramientas de ayuda para el trabajo del perito.

1. Breve introducción. Conceptos

Cuando dos partes desean dirimir sus diferencias, desde los inicios de la humanidad civilizada, se termina recurriendo a una tercera parte que se asume por las dos litigantes como “buena”, esto es, justa. Aunque no siempre, como veremos en el tema, la figura de esa tercera parte, suele representarse por un/una juez. No nos es difícil imaginar que el/la juez no tiene porqué saberlo todo de todas las materias del conocimiento humano. La medicina forense, es un ejemplo de cómo un experto ayuda al “justo” que toma las decisiones.

Haciendo un poco de historia, siguiendo a Noblett (Noblett, 4-5), podemos remontarnos para encontrar referencias a la "medicina legal" al siglo VI, y de forma rutinaria en tribunales, desde el siglo XVI. Sin embargo, los orígenes de la moderna ciencia forense se cifran a mediados de 1800. Algunos de los primeros esfuerzos para definir la ciencia forense, siempre según Noblett, podrían ser:

• En 1844, el Dr. Mathieu J.B. Orfila, considerado el padre de la toxicología, publicó un tratado científico sobre la detección de venenos y sus efectos en animales.

• En 1855, el doctor Bergeret d'Arbois utiliza la infestación de insectos para estimar el tiempo de la muerte.

• En la década de 1890, Edward Henry y el trabajo pionero de Francis Galton llevó a los métodos para clasificar y ordenar las huellas dactilares.

• En el año 1900, Edmond Locard estudió probabilidades sobre balas que emparejan, pelos, y patrones de salpicaduras de sangre; y demostró que un delincuente puede ser conectado a una escena del crimen por partículas de polvo.

• En 1914, Leone Lattes desarrolló métodos para determinar los tipos de sangre de las manchas de sangre seca.

• En la década de 1920, Calvin Goddard perfeccionó las técnicas necesarias para determinar si una bala fue disparada desde un arma sospechosa.

A modo de anécdota, para centrarnos en el trabajo de un perito, recordemos una sucedida en 1978, momento que parece próximo en el tiempo, pero que queda lo suficientemente lejano para que las costumbres de nuestra sociedad hayan dado un giro copernicano, cuando se celebró un juicio en la Magistratura de Trabajo madrileña, donde la empresa demandada era el Gay Club, un local con un espectáculo a cargo de travestidos, algo que entonces tenía una emergente popularidad entre la oferta de ocio urbano, tanto por la novedad como por la transgresión que suponía a las costumbres de décadas pasadas, una vez eliminada esa absurda censura de formas arcaizantes que limitaba hasta los escotes de las cantantes, y además era algo que llamaba mucho la atención, requisito imprescindible para todo espectáculo de éxito, dado que se contemplaba como una singularidad considerando los usos y costumbres del momento, muy distintos de los actuales. Con su *animus jocandi* de fondo, y ese prisma antedicho debe ser entendido este texto, recogido en un anecdotario del momento, muy otro del actual.

El alguacil llamó a las partes para empezar la vista oral:

- ¡Fulgencio Suárez Villaplana!

Entró en la sala una en apariencia espléndida mujer, de poderoso busto, largas pestañas y caderas ondulantes, muy marcadas en la minifalda. Su Señoría preguntó con asombro:

- Pero usted ¿quién es?

- Fulgencio, para servirle

- *Que le reconozca el forense, porque yo no me lo creo*

En esta anécdota, obviamente imposible a día de hoy por esos cambios que mencionábamos en nuestra sociedad, tomada del libro citado en la bibliografía, de Vizcaíno, el forense, funcionario del estado, usa de sus conocimientos en la anatomía humana para determinar algo que al Juez se le escapa. Obviamente hoy una situación así sería irrepetible en un juzgado por no ampararla ni el marco legal ni la sociedad que sustenta a ese marco. Pero nos sirve como ejemplo más allá de toda intención: el juez no sabe de algo, se declara ignorante al respecto, y pide ayuda: pide un perito.

Recordemos que las leyes no cambian por gusto, sino porque se acomodan a una situación cambiante. Y, de igual forma que no sería posible repetir la anécdota en el momento actual sin que el juez recibiera un linchamiento mediático y social por su actitud homófoba, las TIC también han hecho cambiar la ley. Y con ella, las necesidades de los peritos. Pongamos otro ejemplo. Pensemos en un adolescente de los años 80. En las paredes de habitación podía tener posters de Cash, de películas de terror, de imágenes de montaña…. Papeles que conforme fue creciendo, desaparecieron. Un adolescente hoy no solo tiene las paredes de su habitación, sino los muros de sus redes sociales. Y esos posters no se eliminan tan fácilmente. Pueden en un momento dado ser tan persistentes que atentarían contra su privacidad. ¿Haría falta para el primero de los casos el empleo de un perito que midiese la exposición de su privacidad? No. Pero hoy, para el adolescente que puede verse expuesto, sí. Por el cambio de la tecnología, y también de los usos y costumbres de la sociedad, donde no hacía falta un perito informático, hoy si lo hace. Y aquí, es donde entramos nosotros.

Pero para poder entender de qué hablamos, necesitamos usar conceptos que relacionaremos a lo largo de todo el tema. Y ya que hemos traído a colación el término “forense”, empecemos con él.

El término forense puede ser definido como la aplicación de la ciencia a una cuestión de derecho. Y, en lo que a nosotros respecta, podríamos centrarnos en la ciencia forense digital, o informática forense: la informática forense sería la recolección, preservación, análisis, y presentación de pruebas electrónicas para su uso en el ámbito jurídico de forma que sea válida a efectos legales usando herramientas y prácticas de aceptación general. En concreto, análisis forense digital sería la aplicación de la tecnología informática a una cuestión de derecho en la que las pruebas incluyeran elementos creados por personas y elementos creados por la tecnología como resultado de la interacción con una persona. Por ejemplo, los datos creados por un proceso requiere una máquina que se pueda programar, que fue ejecutada por una persona o incluso por un proceso automático que en último término ejecutó una persona. (Daniel, 3)

Otra definición muy próxima la tomamos de López Manrique (López Manrique, 25-35), quien dice que la computación forense (evidentemente, dependiendo de las fuentes, términos como computación o informática se entremezclan sin dejar percibir diferencia aparente) es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. También se define como el proceso de identificar, preservar, analizar y presentar evidencia digital de tal forma que puede ser aceptada en la

solución de un caso donde está involucrada la tecnología digital para investigar un crimen tecnológico.

Pero para poder realizar ese proceso de análisis, hace falta tener “algo”. Y ese algo se llama pericia. Así, definimos pericia como experiencia, práctica o habilidad en un arte o una actividad concreta. Podemos pues considerar perito a la persona que posee un título o que es especialista en algo determinado. El Perito, siguiendo al DRAE, Diccionario de la Lengua Española, es “la persona que, poseyendo especiales conocimientos teóricos o prácticos, informa, bajo juramento, al juzgador sobre los puntos litigiosos en cuanto se relaciona con su especial saber o experiencia”. Según el diccionario jurídico sería la “Persona que posee un título. Especialista en algo determinado. Jurídicamente nos referimos al que informa en un procedimiento, bajo juramento, sobre cuestiones litigiosas relacionadas con su especialidad o experiencia” (del Peso Navarro, 2001).

La peritación podemos considerarla como la facultad de ser oído, en los casos que, por razón de sus conocimientos o profesión, venga a decidir los puntos dudosos por medio de su informe o dictamen, término éste que por su especial relevancia desarrollaremos en epígrafe aparte.

El dictamen, o, mejor, su acepción como peritaje, podemos interpretarla (DRAE) como un "Trabajo o estudio realizado por un perito o experto con la finalidad de corroborar determinadas circunstancias o hechos". O, siguiendo la jerga, sería como sacar una foto de una situación dada, documentando objetivamente lo que se analiza y generando un informe claro, conciso y expeditivo.

Queda hablar del objeto del trabajo del perito. Sobre lo que efectúa su estudio, sus análisis, donde va a operar: en las pruebas, o, por ser más preciso en los términos, en las evidencias (para nosotros, e-evidencias) (Volonino, 9),

Visitando de nuevo el DRAE, vemos que prueba se define como “razón, argumento, instrumento u otro medio con que se pretende mostrar y hacer patente la verdad o falsedad de algo”.

Si habláramos de un asunto convencional, no informático, podríamos hablar de, como en las películas de clase B, una pistola, una huella en un vaso… pero nosotros precisamos marcar una serie de diferencias.

Así, para Daniel:

Una evidencia digital toma muchas formas. Generalmente son datos electrónicos, ya sea en forma de una transacción, un documento, o algún tipo de medios de comunicación como una grabación de audio o de vídeo. Las transacciones pueden abarcar transacciones financieras creadas durante el proceso de hacer una compra, pagar una cuenta, retirar dinero en efectivo, e incluso escribir un cheque. Y es que si bien escribir un cheque podría parecer un método pasado de moda que no es digital o electrónico, el procesamiento de la verificación es electrónico y se almacena así en el banco. Casi cualquier tipo de transacción de hoy se digitaliza

en algún momento, convirtiéndose así en digital la evidencia: así, dejan rastro digital visitar el médico, obtener recetas, registrar un niño en la guardería, y aun vacunar a un perro contra la rabia.

En el mundo conectado de hoy, es casi imposible para nadie estar completamente "fuera de la red" de tal manera que sus actividades no generen algún tipo de registro electrónico.

La explosión de las redes sociales a su vez ha creado toda una nueva área de evidencias electrónicas a la vez penetrantes y persistentes. La gente hoy comparte su día a día, actividades, pensamientos, fotos personales, e incluso su ubicación a través de Twitter o Facebook entre otros. A esto debe añadirse la explosión de la blogosfera, donde los individuos actúan como periodistas. (Daniel, 4)

De forma más concisa, Volonino nos define evidencias, como la prueba de un hecho acerca de lo que hizo o dejó de suceder, material utilizado para persuadir al juez o al jurado de la verdad o falsedad de un hecho controvertido. (Volonino, 335). Profundiza para darle el apellido de digital, de la siguiente manera: evidencia electrónica, e-evidencia, o e-pruebas sería la evidencia en forma digital o electrónica, como los archivos de correo electrónico de ordenador, mensajes instantáneos, calendarios y PDA (Volonino, 335)

Una colección de definiciones más formales la podemos tomar de Carvajal: (Carvajal, 89)

Se le llama evidencia digital a cualquier registro generado o almacenado en un sistema de cómputo que pueda ser utilizado como evidencia en un proceso legal

Veamos algunas definiciones:

"Cualquier información, que sujeta a una intervención humana u otra semejante que ha sido extraída de un medio informático", HB:171 2003 Guidelines for the Managment of IT evidence.

"Una vez reconocida la evidencia digital debe ser preservada en su estado original. Se debe tener en mente que la ley requiere que la evidencia sea autentica y sin alteraciones". (Casey, Eoghan, "digital Evidence and computer crime", 2000)

Carvajal concluye, definiendo características de la evidencia digital, que resulta interesante destacar en este momento:

Es la materia prima de los investigadores, es volátil y anónima, es modificable, es decir se puede duplicar, borrar o alterar pero son parte fundamental de la escena del delito, si se compromete la evidencia se puede perder el caso administrativo o legal de la investigación forense. Es crítico recordar que la evidencia se puede duplicar y aun así esta copia es original respecto de los entornos digitales.

Son estas características que hacen atípicas las que a partir de ahora llamaremos e-evidencias para distinguirlas de las evidencias convencionales, las que hacen difícil el trabajo de un perito informático. Así, una mala actuación puede corromper una e-evidencia.

Siguiendo a (López Manrique, 25-35), precisamos que el aspecto más importante a la hora de recolectar evidencias, es la preservación de la integridad de ésta. Otras consideraciones interesantes del mismo autor, nos hacen reflexionar sobre qué cantidad de e-evidencias, cuando están basadas en soportes físicos, se deben tomar. ¿Nos llevamos un equipo completo, para no arriesgarnos a dejar piezas de información potencialmente relevantes? ¿Y si nos demandan por perjudicar la vida de una persona o de un negocio más allá de lo absolutamente necesario? ¿Cuál sería el mínimo necesario a incautar para efectuar una investigación? En último término, será la dureza del crimen investigado la que determine la forma de actuar. Por otra parte, es obvio, no es lo mismo investigar sobre una microsd que sobre un mainframe.

El mismo autor nos apunta algo obvio para nosotros: no todas las e-evidencias tienen soporte físico. Muchas, cada vez más, tienen presencia únicamente en las redes. Puede estar en ordenadores lejanos físicamente… o desconocidos, de forma que debe hacerse un esfuerzo explícito para capturarla (por ej., mediante el uso de sniffers). Caso interesante suponen las redes sociales, como Facebook, tema tratado por Hoog. (Hoog, 360).

¿Qué evidencias sirven? ¿Todas? La mejor manera de dar respuesta a este interrogante es de forma gráfica, en la siguiente imagen:

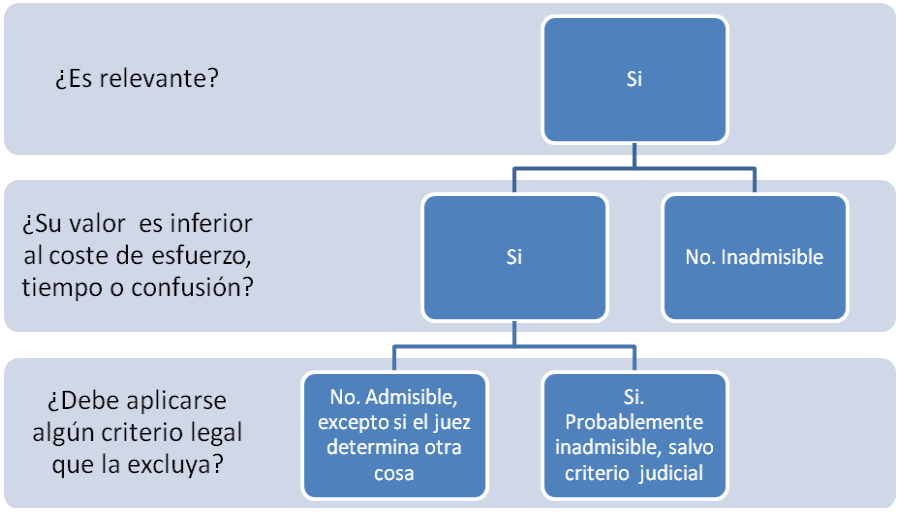

Ilustración 1 ¿Cuando una e-evidencia es admisible? Fuente: Adaptado de (Volonino, 25)

Algún otro concepto interesante que debemos empezar a considerar es bueno que no nos lo dejemos en el tintero en estos momentos iniciales, así, definamos, siguiendo a Volonino, una cadena de custodia. Sería el cuidado, control y rendición de cuentas de las pruebas a que se debe el perito en cada paso de una investigación, para verificar la integridad de la evidencia. El proceso de validación de cómo la e-evidencia fue recopilada, el seguimiento y protección en un tribunal de justicia. Si no existe, no existen pruebas. (Volonino, 332)

Dentro de las particularidades que pueden presentar las evidencias, se nos habla de evidencia demostrativa: un tipo de evidencia que se ofrece para explicar, o bien un resumen de otras

pruebas. No suelen ser admitidas en un juicio. Ejemplos: gráficos y mapas generados por ordenador. (Volonino, 333)

Cerrando el apartado de definiciones, no podemos dejar de escapar un término que a veces parece confuso: el de deposición, de uso habitual en los juzgados. Sería el testimonio bajo juramento ante la presencia de un tribunal (Volonino, 333)

Concluyendo, centrándonos en la prueba pericial, que sería la que nosotros crearíamos, podríamos definirla como el instrumento mediante el cual, expertos ajenos a las partes en litigio, con conocimientos relevantes en alguna ciencia, arte o profesión, recaban, analizan información y la pone en conocimiento de un juez, dando su opinión fundada sobre la interpretación y apreciación de la misma.

Pero ¿Qué dice la ley? ¿Qué medios de prueba podremos emplear en un juicio?. Siguiendo el artículo 299 de la Ley de Enjuiciamiento Civil (Lec, Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil) serían:

- Interrogatorio de las partes.
- Documentos públicos.
- Documentos privados.
- Dictamen de peritos.
- Reconocimiento judicial.
- Interrogatorio de testigos.

Los temas que se abarcan desde un peritaje informático, pueden abarcar todas las áreas de la informática, e incluso algún área donde la relación con esta sea menor.

Ejemplos posibles: desde el desarrollo de sistemas al plagio entre aplicaciones, pasando por equipos, características de documentación como un manual de usuarios, …

Hay que dejar claro desde el primer momento que la prueba pericial es apreciada por Jueces o Tribunales en función de la *sana crítica*, por eso es de libre ponderación por el Tribunal.

Los dictámenes periciales, con toda la importancia que tienen en determinadas materias, son elementos de juicio, estimables en sus conclusiones, no solamente por la mera afirmación de estar emitidas por un técnico, sino por los razonamientos que a aquellas conducen, basados en las objetivas normas de la ciencia o de la técnica.

Todo ello, sin olvidar el principio rector de que *lo que no está en los autos, no existe legalmente*.

2. ¿Qué tipos de trabajo afronta un perito informático?

Una vez descritos los conceptos básicos, nuestro siguiente paso es clarificar el tipo de trabajo al que se puede enfrentar un perito informático. A priori podemos tener la impresión de que se resume en sus actuaciones ante los tribunales y poco más, y siempre centrado en delitos puramente tecnológicos, como robo de bases de datos o espionaje industrial, pero no es así. López Manrique nos indica con tino que (López Manrique, 25-35) la informática forense no es utilizada solo para investigar crímenes tecnológicos, como el acceso no autorizado a una red o la distribución de material ilegal, también es utilizada para investigar cualquier crimen donde un ordenador puede tener alguna evidencia almacenada (por ejemplo, un intercambio de correos electrónicos entre una víctima de violación y el violador). Así, entre los posibles campos de actuación, vemos que muchos provienen de la vida diaria, y no tienen que estar directamente relacionados con la informática, como por ejemplo buscar evidencias para "el mundo no digital", tal como divorcios, seguros, mobing…

Esto lleva a que el perito deba estudiar muchos métodos (Dube) y técnicas (Hoog, 196 y ss), pues la investigación puede llevar por distintas vías, desde el estudio de archivos en la nube (Lillard, 6), dispositivos móviles complejos, como smartphones (López Tarraella, 259), virus en sus distintas clasificaciones taxonómicas (Filiol, 81 y ss), o la captura de tráfico en la red (Lillard, 23).

Una primera aproximación a la clasificación de trabajos que puede enfrentar un perito informático, nos viene de la mano de Vacca (Vacca, 35 y ss), quien hace una división elemental, según el ámbito de trabajo:

- Ámbito militar. Carvajal (Carvajal, 86) sigue ésta vía al hablar de investigaciones sobre ciberterrorismo, y particularizándolo a los virus, podemos seguir a Filiol (Filiol, 338)
- Ámbito judicial/legal, que es el que típicamente se asume como el principal
- Ámbito empresarial, al que volveremos cuando hablemos de los arbitrajes.

El mismo Vacca (Vacca, 83) nos da una clasificación de tipos de trabajo, aplicables a cualquiera de los tres ámbitos:

- Análisis forense de sistemas informáticos:
- Sistemas de seguridad para Internet
- Sistemas de detección de intrusos
- Sistemas de seguridad basados en cortafuegos
- Seguridad para almacenamiento en red
- Sistemas de recuperación de desastres

- Sistemas de seguridad con clave pública
- Sistemas de seguridad de red inalámbrica
- Comunicaciones vía satélite encriptadas
- Mensajería instantánea
- Sistemas de privacidad de red
- Gestión de identidad
- Prevención de robo de identidad

No es el único que hace este tipo de categorización. Así, Daniel (Daniel, 18 y ss) nos facilita otra alternativa:

- Tipología en la informática forense
- Respuesta a incidentes
- Estudio de telefonía móvil
- Estudio de GPS
- Estudio de dispositivos de almacenamiento
- Análisis forense de medios sociales
- Vídeo digital y análisis forense de fotos y cámaras digitales
- Análisis forense de audio digital
- Estudio forense de juegos multijugador
- Estudio forense de consolas de videojuegos

Pero volvamos a los ámbitos de actuación. Los dos que nos ocupan principalmente son los que se desarrollan en torno a los tribunales o a la vida empresarial. Y puede que parezca que es algo lineal y simple. Nada más lejos de la realidad. Incluso en el mundo judicial, que parece menos complejo desde fuera que la inmensa variedad empresarial, la vida del perito puede volverse muy compleja. Así, podemos ver el ejemplo que nos ofrece Volonino.

Papel desempeñado	Tipo de caso	Condiciones de trabajo	Cuando está involucrado
Apoyo al demandante	Civil	Amistoso	Antes de toda actuación legal
Apoyo al demandado	Criminal	Neutral	Durante la e-investigación
Actuación como parte neutral	Empleo	Carencia de apoyo	Durante la captura de datos
Investigar para un particular/empresa	Divorcio	Hostil	Durante la revisión y análisis de los datos
Investigar para un particular/empresa	Fraude	Modo invisible	Justo antes del inicio del juicio

Adaptado de (Volonino, 121 y ss)

En ésta tabla podemos ver distintos papeles desempeñados en los tribunales, con evidentes diferencias. Entre esos factores que pueden influir en la investigación destacan las condiciones de trabajo. Volonino los describe como sigue:

- Ambiente hostil: Ejemplo: perito contratado por el abogado del demandante en un caso que implica el robo de planos de ingeniería por un ex empleado. Se sospecha que el empleado le dio copias a su nuevo jefe, sin más información relevante para el investigador. Intenta copiar ficheros y el correo electrónico del sospechoso en su antiguo PC de la oficina, así como los registros de la red para revisarlos. El personal de sistemas TI pone mala cara pues fueron los responsables de controlar el acceso a archivos confidenciales y filtrados de correo electrónico, donde fallaron evidentemente. Además, el abogado no se presenta, por lo que está allí solo, y la red se cayó hace una hora, así que no parece haber nadie tiene con tiempo para él.

- Modo invisible: El director de Recursos Humanos contrata al perito para inspeccionar un ordenador de un empleado para saber si está violando la política de la empresa viendo pornografía. Se necesita la investigación sin alertar al empleado o cualquier otra persona. Se trabaja después de las 10 pm, cuando la oficina está vacía, para crear copias de los ficheros.

- Ambiente neutral: el abogado de un acusado envía al perito un CD que contiene la imagen del ordenador su cliente. También recibe los detalles de las cookies y los archivos utilizados recientemente. El acusado está acusado de haber comprado a propósito o descargar pornografía infantil. La revisión y análisis demuestran la presencia de un pequeño número de posibles ficheros de imágenes, todas con tamaños de archivo más pequeño de 10 kilobytes (KB), la mayoría menor de 5K. Los

tamaños de archivo indican tamaño de las miniaturas las imágenes. No hay evidencia de los típicos indicadores de comportamiento pederasta (por ejemplo, los archivos de imágenes no estaban organizados, sin directorios, nombres de usuario, o cuentas de correo electrónico indicando su interés en ellos). La revisión muestra muchas visitas a sitios pornográficos para adultos (las miniaturas podrían haber sido descargadas sin saberlo)

- Entorno amistoso o carente de apoyo: Justo una semana antes de que comience el juicio, un fiscal pide a un perito que confirme que el sospechoso bajo custodia ha enviado por correo electrónico amenazas, que corroboran otros tipos de pruebas (cartas, faxes, y amenazas en persona). Se formulan al fiscal dos preguntas, "¿Cómo ligar esos correos al sospechoso? ¿Cómo saber que era él y no otra persona que envió el correo?". Nadie puede responder a eso. El análisis muestra que el correo había sido enviado desde una cuenta que el sospechoso usaba, pero se sigue sin poder vincular al sospechoso a los mensajes

Pero vamos por partes. En lo que respecta a las actuaciones fuera de los tribunales, mediando entre empresas, debemos centrarnos en la figura del arbitraje.

Se entiende por arbitraje la institución en que las personas físicas o jurídicas pueden someter previo convenio, a la decisión de uno o varios árbitros las cuestiones litigiosas surgidas o que puedan surgir en materia de su libre disposición conforme a derecho.

La ley a considerar es la Ley de Arbitraje (60/2003).

Hay una serie de cuestiones que quedan excluidas del arbitraje:

- Las cuestiones sobre las que haya recaído resolución judicial firme y definitiva.
- Las materias inseparablemente unidas a otra sobre las que las partes no tengan poder de disposición.
- Las cuestiones en que con arreglo a las Leyes debe intervenir el Ministerio Fiscal en representación y defensa de quienes, por carecer de capacidad de obrar o de representación legal no pueden actuar por sí mismos.
- Las cuestiones laborales.

En cuanto a los tipos de arbitrajes, podemos clasificarlos entre informales o formales.

El informal, es el realizado al margen de la Ley de Arbitraje y por el cual dos o más personas pactan la intervención dirimente de uno o más terceros y aceptan expresa o tácitamente su decisión después de emitida. Este acuerdo es válido y obligatorio para las partes si en él concurren los requisitos necesarios para la validez de un contrato.

En este caso es precisa la aceptación del tercero después de emitida produciendo los efectos de un vínculo contractual por lo que si no se cumple habrá que acudir a la vía judicial para conseguir el cumplimiento del contrato.

Los formales son aquellos que se realizan de acuerdo con lo dispuesto en la Ley de Arbitraje. Se distinguen dos tipos: arbitraje de derecho y arbitraje de equidad. El de derecho es aquel en el que los árbitros deben decidir sobre la cuestión, como si fueran jueces, conforme al derecho. Los árbitros tienen que ser abogados. En el de equidad los árbitros resuelven según su leal saber y entender y por tanto actúan sin estar sometidos al imperio de la Ley, como los jueces ordinarios.

Son las partes quienes tienen que elegir el tipo de arbitraje. En caso de no hacerlo, la Ley establece que los árbitros resolverán en equidad.

Para las empresas, recurrir a los arbitrajes tiene una serie de ventajas. Por ejemplo, la rapidez, porque se tramita en un corto espacio de tiempo, pudiendo establecer las partes el plazo máximo dentro del cual el laudo[1] debe ser dictado. Destaca así mismo la eficacia al poder escoger las partes a árbitros peritos en la materia por razón de su titulación o profesión.

Más ventajas, pasan por la ausencia de publicidad pues se pueden resolver las diferencias entre las partes de forma privada, de forma que no se generan esos juicios paralelos que los medios de comunicación acostumbran a generar, sobre todo cuando se trata de casos con cierto peso económico.

Por último cabe destacar la voluntariedad porque ambas partes se adhieren libremente al sistema para quedar vinculadas a las resoluciones, y la ejecutividad porque los laudos -resoluciones arbitrales- son de aplicación obligada.

Para cerrar el capítulo de los arbitrajes, nos queda hablar de la cláusula arbitral. La cláusula arbitral a incluir en los contratos es un elemento vital y clave para el caso de que surjan controversias y esté asegurado el cumplimiento de la voluntad de las partes de recurrir al arbitraje de la Corte. Esta cláusula tiene que expresar la voluntad inequívoca de las partes de someter la solución de todas las cuestiones litigiosas o de algunas de ellas surgidas o que puedan surgir de las relaciones jurídicas determinadas, sean o no contractuales, así como expresar la obligación de cumplir tal decisión. No es preciso que designe los árbitros pero puede hacerlo.

El modelo recomendado por la Corte de Arbitraje de la Cámara de Comercio de Madrid es el siguiente: Las partes intervinientes acuerdan que todo litigio, discrepancia, cuestión o reclamación resultantes de la ejecución o interpretación del presente contrato o relacionados con él, directa o indirectamente se resolverán definitivamente mediante arbitraje en el marco de la Corte de Arbitraje de la Cámara de Comercio e Industria de Madrid a la que se recomienda la admisión del arbitraje y la designación de los árbitros de acuerdo con su

[1] **laudo** (de laudar) 1. m. DER. Fallo de los árbitros o amigables componedores.

Reglamento y Estatutos. Igualmente las partes hacen constar expresamente su compromiso de cumplir el laudo arbitral que se dicte.

Y nos queda para cerrar este punto tratar de la actuación judicial del perito informático en sus distintos ámbitos. Siguiendo el Código Civil (CC) tendríamos la vía civil (Art. 12.6 CC). Para la mercantil el Código de Comercio.

Para que un perito pueda actuar como tal, tiene que ser nombrado por el Juez o Tribunal, a propuesta de las partes interesadas o del mismo Tribunal, a fin de que puedan ser recusados[2] o tachados por causas como el parentesco próximo, haber informado anteriormente en contra del recusante el vínculo profesional o de intereses con la otra parte, el interés en el juicio, la enemistad o la amistad manifiesta (Art. 124 LEC) (Ley de Enjuiciamiento Civil)

A ese respecto, en la misma LEC, nos encontramos artículos relativos al cuándo se debe hacer la recusación (Art. 125 LEC), el cómo (Art. 126 LEC), la posibilidad de que el perito no acepte la recusación (Art. 127 LEC), o la condena en costas por la recusación (Art. 128 LEC). Hay que dejar claro que un perito debe aceptar (o rechazar) explícitamente un peritaje si desea (o no desea) realizarlo (no sirve el refrán de quien calla otorga). Además de las causas expuestas, un perito debe rechazar el trabajo si el peritaje no corresponde al perfil de un Informático, y se le asigna por error. Son de interés al respecto los (Art. 100 y 105 LEC)

Puede el perito renunciar también si su nivel de conocimientos o experiencia no le facultan para dictaminar sobre la materia en cuestión, pero si no se da causa real, no debería rechazar un peritaje judicial, para evitar retrasos al proceso judicial.

En el caso de que la propuesta de designación sea por parte del Juez o Tribunal, se realizará bien a instancia de parte (Art 341 LEC) o sin instancia de parte, esto es, asignación de oficio, del perito por parte del tribunal. El nombramiento del perito viene también pautado por la LEC (Art. 342 LEC)

3. El perito. Su responsabilidad y sus derechos.

Hablemos ahora un poco sobre el perito en sí, dejando de lado su posible actividad como "cyberdetective" (Vacca, 155). Hemos tratado de su paso por tribunales, como un elemento probatorio más (artículo 3001.1 de la LEC

Artículo 300. Orden de práctica de los medios de prueba.

1. Salvo que el tribunal, de oficio o a instancia de parte, acuerde otro distinto, las pruebas se practicarán en el juicio o vista por el orden siguiente:

1.º Interrogatorio de las partes.

[2] . Según el DRAE, recusar es "poner tacha legítima al juez, al oficial, al perito que con carácter público interviene en un procedimiento o juicio, para que no actúe en él."

2.º Interrogatorio de testigos.

3.º Declaraciones de peritos sobre sus dictámenes o presentación de éstos, cuando excepcionalmente se hayan de admitir en ese momento.

4.º Reconocimiento judicial, cuando no se haya de llevar a cabo fuera de la sede del tribunal.

5.º Reproducción ante el tribunal de palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación y otros semejantes.

A este respecto, cabe indicar que se dice explícitamente que la prueba por perito sólo se podrá utilizar *cuando sean necesarios conocimientos científicos, artísticos, técnicos o prácticos para valorar hechos o circunstancias relevantes en el asunto o adquirir certeza sobre ellos*. (artículo 335 LEC). Sobre sus conocimientos correspondientes, nos habla también el mismo artículo de la LEC. De su título nos habla el artículo 340: *Los peritos deberán poseer el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de éste. Si se tratare de materias que no estén comprendidas en títulos profesionales oficiales, habrán de ser nombrados entre personas entendidas en aquellas materias.*

Evidentemente, las actuaciones ante los tribunales son cosa muy seria, y una mala actuación puede conllevar fuertes sanciones Durante el desempeño de sus actos, se puede incurrir en responsabilidades en los ámbitos civil, penal y profesional, bien por ser el culpable o por ser el causante, aun de forma indirecta, del daño causado.

Sobre la responsabilidad civil, cabe señalar que el mero incumplimiento, por dolo o negligencia es una posibilidad muy cierta. Es importante, pues cuando por culpa o negligencia, se causa daño a alguien, se está obligado a reparar el daño causado. Hay tres clases de responsabilidad civil: contractual (artículo 1101 CC), extracontractual, por culpa o negligencia (artículos 1902 y ss CC) y la delictual, originada por un acto delictivo tipificado, en el Código Penal (artículos 440, 459 y ss del Código Penal). Es importante recordar algo que se vio en la parte de profesionalismo: la importancia de tener un seguro de responsabilidad civil, que cubra las posibles implicaciones civiles en que pueda incurrir un perito informático en el ejercicio de su actividad profesional.

En cuanto a la responsabilidad penal, a diferencia del caso anterior, aquí es necesaria la voluntariedad. Se incluye el falso testimonio, el cohecho (recibir algo para "mirar a otro lado" o la falta de cumplimiento.

Sobre la responsabilidad profesional, refrescando los temas ya vistos de profesionalismo, baste decir que en ésta responsabilidad entra la ética, ya que hay que considerar que podemos perjudicar a otras partes (clientes, la sociedad…)

No podemos dejar pasar un asunto: los honorarios. Lo que un perito debe cobrar y cuando. Si se trata de algo extrajudicial, entra en el día a día de lo que llamamos eufemísticamente "mercado laboral". Pero cuando se trata de una actuación ante los tribunales, dada por una

parte la aureola de rigor que rodea a la Justicia, y por otra, a su sempiterna lentitud, incluso en los pagos, hay que hacer una serie de consideraciones:

Así, los que presten informe como peritos por orden judicial, tendrán derecho a reclamar los honorarios o indemnizaciones que sean justos. Éstos pueden ser impugnados por el juez o la sala de considerarlos excesivos, y oyendo el dictamen de la Academia, Colegio o Gremio al que pertenezcan, aprobará la tasación o mandará hacer en ella las alteraciones que considere justas, y a costa de quien proceda. Los honorarios se reclamarán mediante una minuta detallada y firmada. ¿Cómo valorar esa minuta?. Lo cierto es que no hay una norma única, depende de factores tan diversos como el tiempo empleado, la complejidad del trabajo, y gastos asociados (todos con sus justificantes) como desplazamientos, por ejemplo.

Dada esa lentitud a la que antes aludíamos, es tremendamente recomendable es pedir una provisión de fondos para atender los gastos que puedan producirse y al menos preverse. Muchas veces esa provisión será el único dinero que el perito vea, lamentablemente

Hay que recordar por último, que ésta es una actividad profesional, lo que la sujeta al Impuesto sobre Actividades Económicas.

Cabe recomendar una visita al artículo 1967 del CC donde se alude al a prescripción del pago a peritos.

4.Los dictámenes e informes periciales

Llega el momento de definir el resultado del trabajo, ese informe que se entrega para su estudio y que pasa a convertirse en una prueba, y que el perito tendrá que exponer (deponer) respondiendo a preguntas que sobre el mismo le hagan el juez y las partes.

Por sus características muy particulares, nos centraremos en la Justicia española. Para interesados en el mundo anglosajón resulta interesante el capítulo 5 del libro de Philips (Philipp, 358), autor que en páginas precedentes se ocupa de catalogar los dictámenes (Philipp, 343), definiéndolos grosso modo como internos, para la organización o empresa que los solicita, pero que no van a ver ser divulgados de ninguna forma, públicos (o declaración), a modo de auditoría que puede ser difundida incluso usando medios de comunicación y externo (en un tribunal), que sería los que ahora nos ocuparían.

Entremos en materia. Un dictamen es un informe escrito sobre una determinada materia, que debidamente motivado y razonado, es emitido por un profesional versado en la materia. Debe ser claro, conciso, fundamentado y justificado.

Los criterios para elaborar dictámenes e informes periciales están descritos en una norma de más que aconsejable consulta: UNE 197001 "Criterios generales para la elaboración de informes y dictámenes periciales". Se aconseja vivamente su empleo de cara a la elaboración de un trabajo de esta índole.

Dictamen, que acabamos de definir como informe, viene de dictaminar. Parece que estamos mezclando palabras, términos, lo que no nos deja más remedio que acudir de nuevo a la Real Academia de la Lengua Española, y comprobar que básicamente hablamos de lo mismo, de ramas del mismo tronco. Dictaminar aparece como "dar opinión y juicio que se forma o emite sobre una cosa" e Informar como "dictaminar un cuerpo consultivo, un funcionario o cualquier persona perita, un asunto de respectiva competencia."

Siempre que sea posible, se ha de contrastar con otros expertos (garantizando la confidencialidad de sus contenidos); esto es, personas que, a partir de la documentación que le entreguemos puedan determinar si, a su juicio, las conclusiones son adecuadas y están debidamente sustentadas. El motivo de que exista ésta posibilidad es obvio: podemos ser expertos en nuestro campo de actuación, pero nadie lo sabe todo jamás, siempre pueden aparecer lagunas que no lograremos subsanar ni mediante la bibliografía ni gastando horas y horas en hacer pruebas quemándonos las córneas delante de un monitor. En esos casos se hace imprescindible consultar con otras personas que nos puedan iluminar en nuestra oscuridad.

No olvidemos que con el peritaje pretendemos ayudar a quienes, por no tener los conocimientos técnicos necesarios, no pueden responder por si solos a algunas preguntas que les van surgiendo, preguntas que nos trasladan y que serán el grueso de esa prueba en que deviene el informe en sí mismo, motivo por el que debe ser escrito pensando en su lector, exponiendo las conclusiones de manera razonada y comprensible a los legos en la materia.

El informe, como vemos, debe ser escrito y cubrir el objetivo: responder a esas preguntas. Debe entregarse exclusivamente a quien lo pidió, quien decidirá si entrega copias, a quiénes y bajo qué condiciones.

Muchas veces se complementa con algún anexo que contenga documentación técnica o ampliaciones a las respuestas, que por lo breve que debe ser algo orientado a alguien que no sea experto, pueden parecer pobres argumentalmente. Con éste documento se busca el "cubrirse las espaldas" de cara a posibles revisiones por otros peritos, encargadas por alguna de las partes. Obviamente, no pueden contradecir el cuerpo principal del dictamen.

Más documentos que se suelen adjuntar pueden ser

- Una relación de los elementos no relevantes que se devuelven: ordenadores portátiles, cámaras, etc., y los que sí resultan relevantes. El perito no debe conservar ningún elemento intervenido al finalizar la investigación pericial

- Una relación de ficheros, cuentas de correo, etc. Con una breve descripción que explica el contenido que le hace relevante

Respecto al contenido del informe, no existen reglas exactas, una receta de cocina que nos dé el pastel perfecto. Por ejemplo, un índice sólo sería preciso si el tamaño del dictamen así lo sugiere. La bibliografía, las fuentes consultadas son siempre precisas, así como las limitaciones

encontradas (si se nos ha sido vetado el acceso a algún sitio, no hemos podido entrevistarnos con alguien, si se ha descubierto que cierta información que podría haber sido relevante para la investigación ha sido borrada, etc.)

A modo de esquema orientativo, podríamos decir que un modelo de informe podría tener las siguientes partes:

- **Consulta:** se expone brevemente la consulta que nos hacen. Si la realiza un juzgado, deben plasmarse los datos del juzgado, número de autos, clases de juicio y nombre y apellidos del demandado

- **Antecedentes:** Se detallan de forma clara y concisa.

- **Limitaciones**: Se indicará si se ha podido o no contar con determinada información, si se ha podido o no entrevistar a una persona clave, obtención de pruebas…

- **Alegaciones y consideraciones**: En función de todo lo anterior, se harán las alegaciones de carácter técnico, científico y jurídico. Tendrán una base práctica (basada en propia experiencia) y otra teórica (basada en textos, manuales, etc.).

- **Conclusiones:** Se terminara el dictamen con la opinión que a nosotros nos merece el asunto. En ellas debemos tratar de no incluir términos técnicos, que pueden aparecer si son necesarios, en otros anexos, para evitar que, p.e. un juez interprete de forma equivocada nuestra opinión.

- **Observaciones:** Destinadas a los posibles lectores desconocedores de la materia.

- **Firmado:** Preferentemente en todas las hojas.

Una vez visto qué es el dictamen, tendremos que siquiera sobrevolar el cómo es, aun más: el cómo se hace.

Vacca (Vacca, 191 y ss) propone una serie de pasos muy simples:

1. Recuperación de Datos

2. Recolección de evidencias y confiscación de datos

3. Duplicación y preservación de la evidencia digital

4. Verificación y autenticación de imágenes digitales

Quizá el punto principal sea el primero, el de la recogida de datos. Debemos tratar de obtener la información necesaria para cubrir los objetivos del trabajo a realizar. No disponer de ella puede llevarnos a rechazar el encargo. Y no solo hablamos, aunque es la más importante, de la información tomada como evidencia, sino de aquella que nos pueda servir de apoyo para

nuestra investigación, proceda ésta del uso generalizado (que puede no tener valor para un Juez en un momento determinado) o bibliográfico.

Sobre el segundo punto, la recolección de evidencias, cabe indicar que no toda evidencia tiene el mismo peso, como vimos al principio de éste tema. La imagen siguiente nos lo muestra de forma gráfica (Volonino, 89):

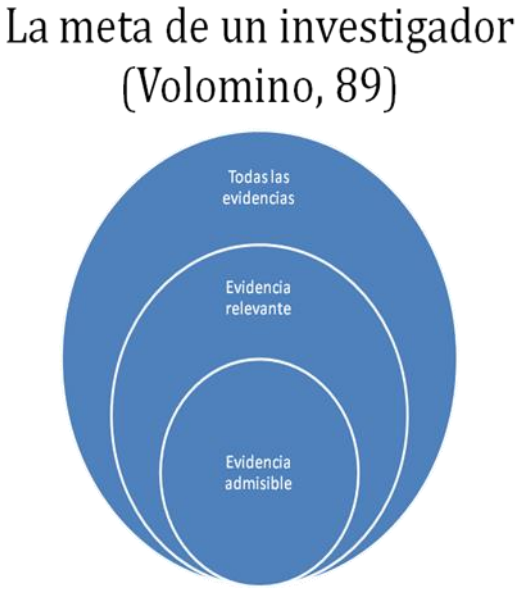

Ilustración 2 La meta de un investigador (tomado de Volonino, 89)

La tercera y cuarta fase, entrarían dentro de lo que podríamos catalogar como métodos y técnicas, que, como puede entenderse, son lo suficientemente amplios y diversos como para no profundizar en ellos en éste momento. Efectivamente, dependiendo del objetivo del peritaje y el entorno en el que trabajemos, pueden ir del mero estudio de la documentación que recibamos al estudio de variaciones en el código fuente de algunos programas, pasando por entrevistas, estudios estenográficos o cualquier alternativa imaginable: crear scripts que se ejecuten de forma automática, simular datos ficticios de un proveedor, cliente, etc., tomas de memoria, inclusión de rutinas en los programas que se ejecutan para poder hacer estudios sin afectar a los resultados reales, simulaciones en paralelo, trazado de ejecuciones (como el usado en el desarrollo para depurar errores)…

Antes de empezar a trabajar debemos tener claro que contamos con toda la documentación y fuentes de información necesarias para cubrir los objetivos del trabajo a realizar; algo que de no suceder así tendrá que reflejarse en el apartado de limitaciones, y en casos extremos, llevarnos a rechazar el encargo exponiendo los motivos.

Es obvio que, conforme el perito realiza su estudio, puede encontrar nuevos hallazgos, nuevas evidencias, que deberá reflejar en su informe.

Podría ser necesario realizar alguna actuación sin aviso previo, por lo que siempre previa autorización judicial, con coordinación con la policía judicial, la información vendría de forma directa. Esto conlleva un problema adicional: la precisión con la que pueda trabajarse en ese momento de prisas y bullicio, con los empleados de cara a la pared y con una mezcla de sorpresa e indignación ven como el perito husmea en sus ordenadores, y el secretario judicial rondando siempre por el local, añadiendo cierta zozobra al perito. Los datos obtenidos deben conservar la calidad precisa para que el trabajo no se desvirtúe.

Con todo esto, un dictamen tendrá que ser claro y bien explicado, incluso para profanos en la materia, conciso (no quiere decir que deba ser breve: puede ser todo lo extenso que se desee, pero muy concreto en sus conclusiones), fundamentado (apoyado no en abstracciones y consideraciones subjetivas), justificado, de forma que no deje espacio para la duda al lector posible y, en la medida de lo posible, con una presentación agradable.

Incluyamos una precisión en éste punto. Pueden darse dos casos de dictámenes judiciales de este tipo: por la vía civil, bien aportados con la demanda (Art 336.2 LEC), bien nombrados por el tribunal (Art 346 LEC), o bien por la vía penal (Art 346 y 348 LEC). En este último caso, la norma si indica algo sobre la composición del dictamen. Concretamente dice que:

El informe pericial ha de estar compuesto por los siguientes puntos:

Descripción de la persona o cosa que sea objeto del mismo, en el estado o del modo en que se halle.

Relación detallada de todas las operaciones practicadas por los peritos y su resultado.

Las conclusiones que en vista de tales datos formulen los peritos, conforme a los principios y reglas de su ciencia o arte.

Una vez entregado el trabajo, queda su valoración. Ésta es de libre ponderación por el tribunal, que puede rechazar por diversas razones, como por ejemplo que considere que el perito no posee la adecuada titulación a la naturaleza de la prueba solicitada o no es el idóneo para el caso. El perito no prueba en sí nada, solo suministra una base científica, técnica, artística o práctica para juzgar sobre aquello a que se refiere el dictamen. O, como dice el viejo dicho “no somos nadie”.

Las partes y sus defensores podrán concluir el acto de reconocimiento pericial y hacer a los peritos las observaciones que estimen oportunas, para esclarecer las causas que han conducido a las conclusiones del informe. Y cuando han intervenido varios, enfrentar sus resultados, motivo por el que sería ventajoso obtener de manera anticipada los dictámenes de los peritos de las otras partes. Si es un caso complejo (recordemos, por ejemplo, el 11-M) donde trabajan varios peritos y estuvieran de acuerdo todos o algunos de ellos, darán o extenderán su dictamen en una única declaración firmada por todos, ahorrando así un montón de tiempo en el proceso judicial.

No podemos cerrar éste hilo argumental sin citar el principio rector que reza “lo que no está en los Autos no existe legalmente” ya que podría generar indefensión el sustentar decisiones sobre información no existente. Esto obliga a prescindir totalmente de la prueba pericial que no fuera practicada con todas las garantías procesales.

Entregado el informe, queda efectuar la defensa en la sala del mismo. Si hay otras periciales practicadas, sería interesante disponer con antelación de ellos para analizarlos y encontrar argumentos adecuados, aunque puede imaginarse que ésta situación no es la habitual. Lo que sí ha de llevar consigo el perito es todo el material necesario para defender sus conclusiones: una de las partes, o el juez, puede pedir explicaciones al perito respecto a sus fundamentos, por lo que se hace necesario tener a mano toda la documentación posible, si es preciso ordenada cronológicamente, e incluso con otros índices auxiliares que permitan al perito localizar algo en un plazo de tiempo breve y razonable.

Cerramos éste apartado con una adaptación de una figura de Volonino (Volonino, 296) donde se nos muestra el paso del conjunto de habilidades que debe tener el perito para ejercer su trabajo, al dictamen en sí, considerado de forma amplia.

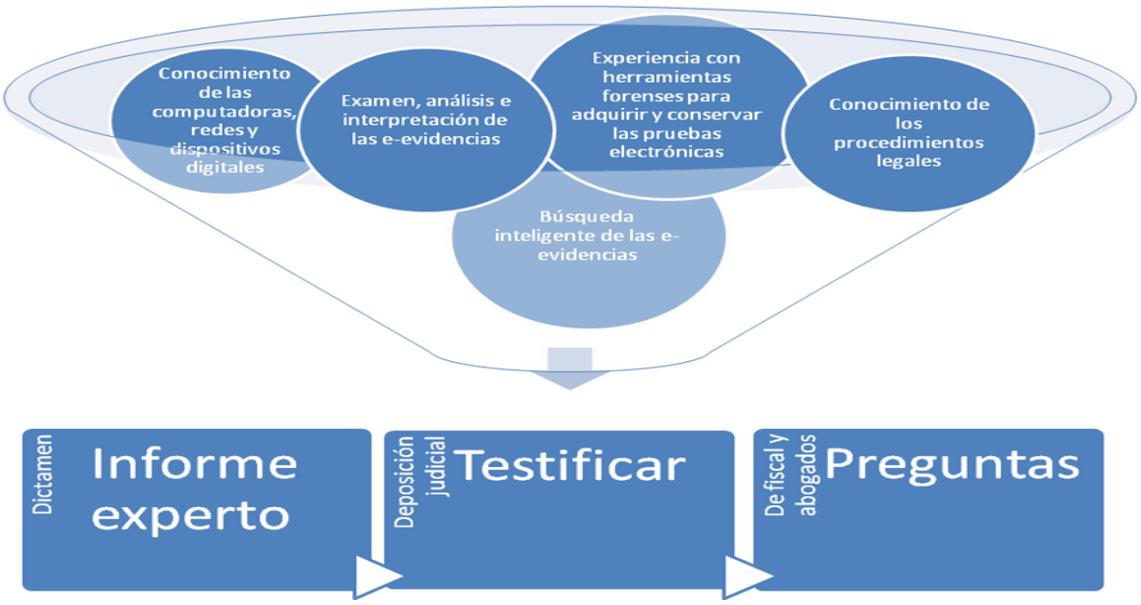

Ilustración 3 De las habilidades al trabajo del perito. Adaptado de (Volonino, 296)

5. Ejemplos

Un tema como éste quedaría cojo si no añadimos algún ejemplo. Obviamente, por cuestiones de tamaño, se han simplificado en lo posible, dejando reducidos al máximo los dictámenes, y,

claro, substituyendo los datos que pudieran relacionar a personas reales con otros ficticios. Que nadie se sienta identificado y, si lo hace, que quede entre él y su conciencia.

Primer ejemplo: Posible robo de datos. Unos empleados descontentos se van de la empresa con, supuestamente, una colección de datos de clientes con los que poder empezar de nuevo, lejos de sus jefes anteriores.

El suscrito ALBERTO MARIA POPEYE EL MARINO, Graduado en Informática, designado perito para el Juzgado de Instrucción número 14 de Klow en las *PREVIAS 1674/2021 - A*, según su saber y entender, emite el siguiente

Dictamen

Consulta

Comprobar si los ficheros de datos que figuran en la empresa Melollevocalentito SL proceden de la empresa Soyuntiranobuenoyque SA

No se formula ninguna pregunta precisa como tal. Para alcanzar el objetivo expuesto, se realizó una inspección en los locales de la empresa Melollevocalentito SL durante la cual se realizó una copia de los ficheros de que componen la base de datos de la citada empresa. En la misma actuación, se recogieron unos documentos que posteriormente fueron, al igual que los ficheros citados, contrastados con la base de datos de la empresa Soyuntiranobuenoyque SA, buscando similitudes.

Antecedentes y Limitaciones

En lo que se refiere a la actuación in situ, la actitud hacia el perito fue de total colaboración por los socios presentes en la empresa Melollevocalentito SL.

Para el estudio posterior, fue facilitado por parte de Soyuntiranobuenoyque SA un CD de instalación con el software de gestión de base de datos (ambas empresas trabajan con el mismo software de gestión, “Gestión Desastrosa”, software basado en windows XP y comercializado por Aprendíaprogramarenunkiosko SL) preciso para el estudio detallado de los ficheros que obraban ya en poder del perito. De igual manera, se facilitó al perito un PC portatil con una copia de los datos de la empresa Soyuntiranobuenoyque SA, precisos para hacer las comparaciones pertinentes. Se hizo preciso contactar con la empresa distribuidora del software de gestión de base de datos. Una vez puesto en contacto con un técnico de la misma, que respondía al nombre de pila “Exuperancio”, se facilitó por el mismo las claves precisas para el funcionamiento de la aplicación.

Alegaciones y Consideraciones

Las dimensiones desparejas de las bases de datos hacían imposible una comparación "bit a bit", es decir, mecánica registro a registro. La base de datos de Soyuntiranobuenoyque SA, posee[3] 1856 registros, mientras que la de Melollevocalentito SL tan sólo 69.

El primer acercamiento a este estudio, fue por el método llamado en argot de "huellas digitales". Este método consiste en buscar, registro[4] a registro de la base de datos similitudes exactas, basados en que si ocurre una errata durante el tecleo por parte del operador de los datos, esta errata tiene escasa probabilidad de repetirse en un registro similar (que aluda a la misma "ficha" real) en otra base de datos, pudiendo decirse, caso de que se encuentre esta coincidencia en dos registros de distinta bases de datos, que tal registro de la base de datos ha sido transferido[5] de la otra base de datos.

Después de aplicar este método, tanto in situ en las instalaciones de la empresa, como posteriormente con más calma gracias a la copia de la base de datos que se realizó, no se han encontrado registros susceptibles de sospecha de haber sido transferidos automáticamente. Este método, por razones obvias, no implica que no se haya realizado ninguna copia, tan solo que si se ha hecho no ha sido automática. Un registro puede ser copiado de manera manuscrita a una ficha de papel y después ser introducido mediante el teclado en otra base de datos. Esto implicó una posterior búsqueda manual, en la que si se encontraron elementos coincidentes, que se detallan en el apartado siguiente.

Se solicitó posteriormente un cotejo de las fichas manuales que se habían recogido en la empresa Melollevocalentito SL con los registros de la empresa SOYUNTIRANOBUENOYQUE SA. Este queda reflejado también en el apartado siguiente

Estudio de los datos

Comparación de las bases de datos

En aras de una mayor claridad, nos referiremos a los registros por su orden secuencial en el fichero de datos. En el fichero de la empresa Melollevocalentito SL serán nominados con los números 1 a 69 (pues 69 es el número total de registros que compone dicha base de datos) y en el caso de la empresa SOYUNTIRANOBUENOYQUE SA con los números 1 a 1856, siempre conforme a su orden secuencial.

[3] Aquí conviene hacer una aclaración. En todo momento se va a hablar en presente de los contenidos de las bases de datos, a pesar de que por definición estas sean cambiantes en tanto en cuanto reflejan la vida de las empresas. Esto es así pues nosotros nos centramos en el estudio de una "foto fija" de esas bases de datos, o en otras palabras, del contenido de las mismas en un momento determinado, el momento en el cual se realiza la copia para el estudio de las mismas.

[4] Registro: En el mundo de las bases de datos, cada una de las fichas que componen una tabla. Tabla: un conjunto de fichas que tienen una cierta homogeneidad (por ejemplo, los datos de nuestros proveedores podrían estar almacenados en una misma tabla).

Para determinar que un registro coincide con otro, se han verificado los campos más relevantes para poder afirmar tal simultaneidad. Estos campos son la dirección, el número, la población, el propietario y si se trata de venta o alquiler. En la tabla 1 aparecen reflejadas estas coincidencias. A modo de interpretación de la misma, cuando vemos en la primera fila con datos un 11 en la columna "Registro Melollevocalentito SL " y en la segunda un 1421 en la columna "Registro SOYUNTIRANOBUENOYQUE SA", lo que significa es lo siguiente: *existe coincidencia al menos en los campos dirección, número, población, propietario y se trata de un inmueble destinado al mismo tipo de transacción -alquiler o venta- en ambas bases de datos.* Existe alguna excepción a esta norma general, reseñada cuando se dé en la columna "Observaciones". Hay que destacar que no se da una coincidencia total en ningún caso, pero siempre por detalles menores, como puede ser el texto del campo observaciones, la forma de escribir el nombre del propietario -nombre detrás o delante del apellido, abreviaturas...- o precio de venta -siempre variaciones porcentualmente mínimas-

En el anexo 1 figura copia impresa de aquellos registros duplicados, apareciendo siempre en primer lugar el registro perteneciente a la base de datos de la empresa Melollevocalentito SL y después el perteneciente a la base de datos de la empresa SOYUNTIRANOBUENOYQUE SA.

De los 12 registros que presentan coincidencias (en realidad uno más, pero simplemente porque el registro 68 y el 69 de la empresa Melollevocalentito SL resultan ser el mismo y este es uno de los encontrados coincidentes con la base de datos de la empresa SOYUNTIRANOBUENOYQUE SA) dos de ellos, tal y como se especifica en el campo "Observaciones" de la tabla 1, no cumplen esta norma general que hemos expuesto más arriba. Se trata en ambos casos de registros que hablan del mismo inmueble físico, pero con distintas modalidades (venta en lugar de alquiler y viceversa) y, en el segundo caso, con distinto nombre de propietario

Tabla 1 - Registros coincidentes

Número de registro en la base de datos de Melollevocalentito SL :	Número de registro en la base de datos de SOYUNTIRANOBUENOYQUE SA:	
Registro Melollevocalentito SL	**Registro SOYUNTIRANOBUENOYQUE SA**	**Observaciones**
11	1421	
13	485	

[5] Migrado o copiado

20	1702	
21	827	
24	1145	Aparece como alquiler en lugar de venta
26	1784	
27	1138	
33	1345	
61	1042	
63	1412	Aparece venta en lugar de alquiler y otro nombre de propietario
67	1376	
68 y 69 (duplicados)	722	

En lo referente a la segunda parte del estudio, cotejo de las fichas manuales que se habían recogido en la empresa Melollevocalentito SL con los registros de la empresa SOYUNTIRANOBUENOYQUE SA

Conclusiones

Por todo lo anteriormente expresado, y según la documentación objetiva analizada como la bibliografía consultada y la práctica informática generalizada, hemos de concluir que existe alguna coincidencia, que no nos atrevemos a cifrar de significativa pues para ello haría falta un conocimiento del sector inmobiliario del que carece el perito que suscribe. Por otra parte, por inexistentes, carece es imposible dar respuesta a las preguntas formuladas.

Todo ello salvo mejor opinión a la que nos sometemos.

Klow, a 31 de enero de 2020

Firmado:

Alberto María Popeye El Marino

D.N.I. 99.999.999

Segundo ejemplo: tras pasar una encuesta en una empresa se cree ver en ella el uso ilegal de software: se usan programas para los que no se han pagado las licencias oportunas. Presuntamente, claro. Éste ejemplo es una adaptación del magnífico libro de Del Peso, que puede verse en la bibliografía.

Consulta

Conclusiones que se pueden deducir respecto a la utilización de software ilegal de la encuesta sobre utilización de Software realizada a la empresa Informática Copiada S.A.

Dictamen

Antecedentes

El Jefe de Sistemas de Información de Informática Copiada S.A. contesta a una encuesta donde entre otras preguntas figuran:

- Número de estaciones de trabajo de la empresa

- Qué paquetes de Sw utiliza cada estación de trabajo

- Paquetes de Sw contratados por la empresa

- Importe total del Sw contratado

Alegaciones y consideraciones

En el presente dictamen, pretenderemos a través de la información recogida mediante una encuesta realizada por Informática Copiada S.A., determinar el uso y utilización del Sw (programas producto) que se viene haciendo en los ordenadores personales de la misma y asimismo constatar si se está infringiendo la Ley de Propiedad Intelectual respecto a los derechos de autor.

La encuesta analizada presenta los siguientes puntos de interés:

- La encuesta responde a una serie de preguntas de carácter inocuo consideradas aisladamente y pretende recabar información auténtica y veraz sobre la utilización de Sw (programas producto) sujeto a "licencia de uso" por los distintos suministradores, siendo en este caso bastante completo y acertado para sus fines.

- En la encuesta se identifica claramente a Informática Copiada, así como la persona que responde a la misma, cargo y áreas específicas de responsabilidad.

- Se observa que la persona encargada de contestar a la encuesta tiene responsabilidad real sobre: adquisición o aprobación para adquirir, definir los requisitos técnicos que precise y definir los estándares de uso, tanto para el hardware como para el software. Se deduce de ello que además del conocimiento del trabajo que tiene asignado por la compañía para la que trabaja tienen un perfecto y directo conocimiento de la situación de la microinformática de la empresa.

- Atendiendo a la adquisición y utilización de paquetes de Sw por la compañía, se observa que de ocho paquetes instalados sólo uno ha sido adquirido a un distribuidor. De los datos de la encuesta se puede deducir que más de un 90% de los programas instalados han sido reproducidos internamente de forma ilegal. Es importante resaltar que siendo 600 las copias existentes y en uso permanente en los ochenta ordenadores personales de la empresa, tan solo cuarenta han sido adquiridas a un distribuidor, siendo las restantes reproducciones internas y no disponiendo de las licencias de uso correspondientes.

- Otro punto que merece especial atención es el alto nivel de utilización de este tipo de software en la Compañía correspondiendo tanto al departamento de microinformatica como al resto de los departamentos de la Compañía que tienen ordenadores personales.

- Respecto al capítulo económico, existe una clara falta de correspondencia entre el número de copias utilizadas y el gasto correspondiente a esta partida en los brazos de la compañía. Seiscientas copias utilizadas y ochocientas mil reales de vellón de gasto.

Conclusiones

Del estudio se deduce claramente que en Informática Copiada se viene utilizando Sw de forma ilegal con clara infracción de la Ley de Propiedad Intelectual realizando con lo que coloquialmente se viene denominando piratería del Sw.

Todo ello salvo mejor opinión a la que nos sometemos.

Matalasparras a 9 de marzo de 2025

Firma.

Alberto María Popeye El Marino

DNI: 99.999.999

6. Bibliografía

El presente tema es una revisión más que profunda de otro presentado en su momento en

De Miguel Molina, María. y Oltra Gutiérrez, Juan V. (2007). “Deontología y Aspectos Legales de la Informática: cuestiones jurídicas, técnicas y éticas básicas”. Servicio de Publicaciones de la Universidad Politécnica de Valencia, Valencia.

Éste volumen, editado en su momento sin más ánimo que el puramente doméstico en lo docente, ha sido lo que podríamos llamar dentro de la modestia de la difusión de los textos universitarios un “top de ventas”, llegando a venderse ejemplares en tierras lejanas y remotas. Intentaremos dar con la música exacta, de nuevo, para esta canción.

Referencias básicas:

AENOR (2011). Norma UNE 197001 "Criterios generales para la elaboración de informes y dictámenes periciales"

Carvajal, Armando (2007). “Introducción a las técnicas de ataque e investigación forense, un enfoque pragmático”. Globalteksecurity, Colombia.

Daniel, Larry E. y Daniel, Lars E. (2012). “Digital Forensics for Legal Professionals. Understanding Digital Evidence From the Warrant to the Courtroom”. Syngress, EEUU.

Del Peso Navarro, Emilio. (2001). *Peritajes Informáticos.* Ediciones Diaz de Santos, Madrid. Existe un precedente, *Manual de dictámenes y peritajes informáticos: Análisis de casos prácticos.* Emilio del Peso Navarro. (1995)

Dube, Roger (2008). “Hardware-Based Computer Security Techniques to Defeat Hackers. From Biometrics to Quantum Cryptography”. Wiley, EEUU.

Filiol, Eric (2005). “Computer viruses: from theory to applications”. Springer. EE.UU.

Hoog, Andrew (2011). “Android Forensics”. Syngress, EE.UU.

Lillard, Terrence (2010). “Digital forensics for network, Internet, and cloud computing: a forensic evidence guide for moving targets and data”. Syngress, EEUU.

López Manrique, Yuri Vladimir (2006). “Computación forense: una forma de obtener evidencias para combatir y prevenir delitos informáticos”. Universidad de San Carlos. Guatemala.

López Tarraella, Aurelio (2012). “Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models”. Springer, Holanda.

Noblett, Michael y Feldman, Adam (1999). “Computer Forensics: Tools & Methodology. Critical Review & Technology. Assessment Report”. IATAL, EEUU.

Philipp, Aaron; Cowen, David y Davis, Chris (2010). “Hacking exposed computer forensics”. MC Graw Hill, EEUU.

Vacca, John R. (2005). “Computer Forensics: Computer Crime Scene Investigation”. Thomson. Boston, EEUU

Volonino, Linda y Anzaldua, Reynaldo (2008). “Computer Forensics For Dummies”. Wiley, EEUU.

Referencias útiles para saber más, o para complementar con anécdotas

Vizcaíno Casas, Fernando. (1997). “*Historias Puñeteras”.* Planeta, Madrid..

Boixo, Ignacio. (2003). “*Guía de buenas prácticas para el peritaje informático en recuperación de imágenes y documentos”*, http://www.infoperitos.com/guiaimagenes.pdf (julio de 2019)

Martos, Juan (2006). “*El perito informático, ese gran desconocido”,* http://www.recoverylabs.com/prensa/2006/10_06_peritaje.htm. (julio de 2019)

Oltra Gutiérrez, Juan V. (2008) “*Introducción a los Peritajes”,* http://riunet.upv.es/handle/10251/1493 Universitat Politècnica de València. Escuela Técnica Superior de Ingeniería Informática – ETSINF, UPV, Valencia (julio de 2019)

Farmer, Dan y Venema, Wietse (2005). “Forensics Discovery”. Addison-Wesley, EE.UU. http://www.porcupine.org/forensics/forensic-discovery/ (Julio de 2012). Éstos autores facilitan una colección de herramientas útiles para investigar en entornos UNIX, titulados genéricamente “The Coroner's Toolkit”, disponibles en http://www.porcupine.org/forensics/tct.html

Ram, Kylie (2008). “Introduction to Forensics". *Linux Journal* (enero 2008). Disponible en: http://www.linuxjournal.com/article/9922 (julio 2019)

Ram, Kylie (2011). “Introduction to forensics” (conferencia). http://greenfly.org/talks/security/forensics.html (julio 2019)

Normativa de interés:

Código Civil, http://www.ucm.es/info/civil/jgstorch/leyes/ccivil.htm (julio 2019)

Ley de Enjuiciamiento Civil, http://noticias.juridicas.com/base_datos/Privado/l1-2000.html a matizar con la Ley 13/2009, de 3 de noviembre, de reforma de la legislación procesal para la implantación de la nueva Oficina judicial http://civil.udg.es/normacivil/estatal/proceso/L13-2009.htm (julio 2019)

Ley de Enjuiciamiento Criminal, http://noticias.juridicas.com/base_datos/Penal/lecr.html (julio 2019)

Asociaciones profesionales:

Academia Americana de Ciencias Forenses http://www.aafs.org/ (julio 2019)

American Board of Criminalistics, http://www.criminalistics.com/ (julio 2019)

Forensic Expert Witness Association, http://www.forensic.org/ (julio 2019)

Herramientas útiles

Entorno Windows

Encase Forensic, http://www.guidancesoftware.com/ (julio 2019)

Herramientas open source, http://www2.opensourceforensics.org/tools/windows (julio 2019)

Entorno Linux

Penguin SLEUTH KIT (Knopix), http://www.sleuthkit.org/sleuthkit/desc.php; también http://penguinsleuth.org/index.php?option=com_frontpage&Itemid=1 (julio 2019)

Local Area Security Linux (Knopix) http://jascha.me/projects/local-area-security/ (julio 2019)

Helix (knoppix), http://www.e-fense.com/products.php (julio 2019). Interesante esta página en italiano: http://www.forlex.it/index.php

Knoppix STD http://s-t-d.org/ (julio 2019)

Otras páginas de interés:

Belgian Computer Forensic, http://www.lnx4n6.be/ (julio 2019)

El libro de Volonino trae unos interesantes complementos disponibles en: www.dummies.com/go/computerforensics (julio 2019)

Forensic and Incident Response Environment (FIRE) http://fire.dmzs.com/ (julio 2019)

Inside Security (INSERT), http://www.inside-security.de/insert_en.html (julio 2019)

IRItaly Live CD Project (**Gentoo** based), http://www.iritaly-livecd.org/ (julio 2019)

Índice