TESIS DOCTORAL

Título	**LA PRUEBA ELECTRÓNICA: SUS IMPLICACIONES EN LA SEGURIDAD DE LA EMPRESA**
Realizada por	**SONIA PUIG FAURA**
en el Centro	**FACULTAD DE DERECHO ESADE**
Departamento	**DERECHO CIVIL**
Dirigida por	**DR. MANUEL RICHARD GONZÁLEZ** **DR. XAVIER ABEL LLUCH**

C. Claravall, 1-3
08022 Barcelona
Tel. 93 602 22 00
Fax 93 602 22 49
a/e. info@url.edu
www.url.edu

* * *

INTRODUCCION

Esta tesis doctoral tiene por objeto la definición y estudio de la «prueba electrónica». La prueba electrónica no siempre se define y se explica bien. Probablemente la causa de esta dificultad se halle en la complejidad y multiplicidad de los fenómenos y actividades de carácter o naturaleza electrónicos frente a la multiplicidad de manifestaciones de los mismos en la vida cotidiana. Tras la lectura de la mayor parte de los estudios que existen hoy sobre prueba electrónica nos dimos cuenta que siempre se trataba sobre prueba electrónica directamente sin el debido análisis del hecho electrónico y sus implicaciones en el ámbito del proceso. Por ello decidimos analizarlo desglosando sus distintos aspectos desde un punto de vista social y empresarial y finalmente analizando su vertiente o dimensión jurídica. Y a partir de esta última dimensión jurídica definir qué entendemos por prueba electrónica. Una vez obtenido un concepto claro nos adentramos en el estudio de su regulación y los posibles errores o carencias en la misma.

Para llegar a entender y poder definir la prueba electrónica y estudiar si la vigente regulación es la adecuada, decidimos partir de la génesis del hecho electrónico, su concepto técnico-científico. Es decir, consideramos que es fundamental para llegar a entender la prueba electrónica comprender primero de un modo sencillo qué es un hecho electrónico y qué es la electrónica. Con carácter general podemos afirmar que el hecho electrónico se relaciona con los electrones que son una de las partículas que conforman la estructura atómica de la materia y al mismo tiempo con la electrónica entendida como el ámbito físico de actuación de electrones caracterizado principalmente por el movimiento. Hacemos en nuestra exposición especial mención a la necesidad de no confundir el concepto de lo electrónico con el concepto de lo informático, puesto que no siempre la informática implica electrónica. Y partimos inicialmente de un concepto amplio de hecho electrónico aún sin olvidar que en la actualidad es preponderante la importancia del hecho electrónico como un sistema codificado de información, del mismo modo que lo es el alfabeto y los símbolos que lo componen. Es decir, intentamos explicar de modo claro qué es un hecho electrónico y como se genera, así como el modo y los medios o soportes en que se conserva y los dispositivos de reproducción que necesita para ser perceptible por el hombre, intentando diferenciar bien estos conceptos. Nuestro esfuerzo se basa en intentar evitar cometer los errores, de ciertos autores en el estudio de la prueba electrónica y cometidos también por nuestra vigente Ley de Enjuiciamiento Civil, puestos de manifiesto en la terminología empleada y en una regulación confusa. Creemos que generalmente dichos errores obedecen al hecho de no entender de un modo claro la realidad del hecho electrónico.

Precisamente la falta de entendimiento del hecho electrónico es lo que, por ejemplo, ha llevado a muchos autores a definirlo con adjetivos como «volátil». El hecho electrónico al contrario de lo que suele predicarse se caracteriza por una mayor persistencia o perdurabilidad frente a otros hechos. Es por ello que debemos matizar entre la persistencia del «hecho electrónico» y la volatilidad de la «expresión del hecho electrónico». Un registro electrónico es mucho más persistente que incluso una huella en un papel, por lo tanto el hecho electrónico se caracteriza por su persistencia y no por su volatilidad. No podemos confundir el «hecho electrónico» en sí con «la expresión de ese hecho electrónico» como, por ejemplo, una muestra de datos en pantalla o un *bit* producido en un determinado momento, esa expresión del mismo sí se caracteriza por su volatilidad.

Tras el estudio técnico-científico analizamos cuál es su dimensión social-empresarial y finalmente su dimensión jurídico-procesal. Ello por cuanto la dimensión social del hecho electrónico es lo que le incardina en nuestra realidad y es lo que le convierte en objeto de interés para la contienda jurídica y la prueba en el proceso. Una vez nos adentramos en su dimensión jurídica, dentro ya del proceso, el hecho electrónico actúa en el proceso jurisdiccional como cualquier otro hecho. En definitiva el adjetivo electrónico no modifica los requisitos y exigencias legales que debe cumplir cualquier hecho para ser introducido y valorado en el proceso como prueba.

Desde una perspectiva social analizamos cómo está influyendo el hecho electrónico en la actualidad tanto a nivel de Estado como de empresa. Desde un punto de vista empresarial, dada la enorme cantidad de información que en la actualidad procesan las empresas, concluimos con la necesidad del establecimiento de una política empresarial de protección y de conservación de la información de que dispone la empresa como mecanismo de prevención de posibles quiebras de seguridad que puedan implicar sanciones, litigios o infracciones de los que pueda, eventualmente, responder la misma. Siendo indudable la necesidad empresarial de proveerse de un sistema de seguridad de los datos, así como de su conservación a fin de que puedan ser aportados, en caso de litigio, ante los tribunales, mejorando las perspectivas de una acción legal con éxito. Lo anterior no obsta a que cada empresa deba efectuar un análisis estratégico previo atendiendo a sus propias necesidades.

Previo a entrar en la prueba analizamos la investigación y pericia del hecho electrónico. El concepto de informática forense y sus fases de investigación (análisis preliminar, adquisición de datos y análisis forense). Partiendo de un punto de vista técnico-científico para individualizar, identificar, recuperar, reconstruir o analizar un hecho electrónico se requiere de principios y técnicas

específicos. Y si además se pretende que el hecho electrónico tenga valor como prueba en un proceso se necesitan para ello, por parte de los expertos, conocimientos legales (procesales y constitucionales). De ahí la importancia de la disciplina informático-forense que incardina todos esos conocimientos, es decir, método, herramientas, cadena de custodia, legalidad y legitimidad en su obtención y tratamiento.

El análisis pone de relieve determinadas deficiencias en la prueba pericial informática, como el hecho de que la mayor parte de las veces adolece de la debida transparencia y conocimiento público de los sistemas de análisis empleados para obtener las conclusiones. Así sucede, en tanto que los peritos suelen utilizar herramientas informáticas protegidas por derechos de propiedad. Esta situación deviene en una falta de información técnica que puede invalidar o hacer dudar de las conclusiones del dictamen a las que se habrá llegado por procedimientos no explicitados y por tanto que no son del pleno conocimiento de la comunidad científica.

Por otro lado, respecto a la preservación, el proceso de investigación digital garantizará mejores resultados si con carácter preventivo las organizaciones, ya sea dentro o fuera del entorno empresarial, disponen de protocolos detallados que aseguren la integridad de los hechos electrónicos objeto de estudio forense, de tal forma que se evite la manipulación de los mismos por los efectos de la modificación intencionada o «tampering», descargas electrostáticas, campos magnéticos o conexión accidental a redes inalámbricas. Para ello es importante manipularlos y almacenarlos en soportes y lugares adecuados para garantizar su integridad. De igual modo consideramos esencial la regulación del depósito de dispositivos electrónicos una vez acceden al proceso y una vez concluido éste, así como que la Administración facilite el lugar y medios idóneos para la conservación de los mismos con máximas garantías de conservación y preservación, de modo que pueda accederse a los mismos en cualquier momento con garantía suficiente. Una vez concluido el proceso es fundamental tener en cuenta la regulación sobre protección de datos de carácter personal a efectos de destrucción de la información confidencial.

El estudio de la investigación del hecho electrónico nos lleva ineludiblemente al estudio de los derechos constitucionales, en cuanto que la actividad de investigación y pericia en materia de prueba electrónica puede colisionar o afectar los derechos fundamentales de los ciudadanos. Así resulta de una simple descripción de su objeto que vendrá referido al examen de dispositivos electrónicos en los que se pueden contener datos, informes y cualquier otro hecho relativo o perteneciente a la esfera privada de los ciudadanos. En el estudio cobra especial relevancia la privacidad, ámbito protegido por la Constitución Española y que se amplía jurisprudencialmente en una sociedad

tecnológicamente avanzada. La investigación del hecho electrónico debe respetar los derechos constitucionales: derecho al secreto de comunicaciones, derecho fundamental a la intimidad, derecho a la protección de datos y derecho a la inviolabilidad del domicilio.

En el análisis de los derechos constitucionales destacan determinados ámbitos con peculiaridades propias como el laboral, en el que el empresario está facultado para efectuar controles de los instrumentos electrónicos facilitados a sus trabajadores, pudiendo efectuar registros informáticos y adoptar las medidas oportunas para vigilar el cumplimiento de las obligaciones laborales de sus empleados. Sin embargo, no puede hacerlo de un modo arbitrario, sino respetando la dignidad del trabajador y los derechos fundamentales relacionados con la misma. Equilibrio que debe obedecer a los principios de idoneidad, necesidad y proporcionalidad, que, en su caso, serán valorados por los Tribunales. Y siempre, previa comunicación a los trabajadores de los sistemas de control y consecuencias disciplinarias en caso de mal uso de los mismos, en aras al principio de buena fe.

Por otro lado, se plantea la posibilidad de legislar en vía civil sobre la solicitud de autorización judicial para injerencias en el ámbito privado ponderando los derechos o intereses concurrentes y apartándonos de este modo a la denegación automática a esta posibilidad tanto desde el punto de vista legislativo como judicial. Un ejemplo claro de ello lo hallamos en el derecho fundamental a la protección de datos, en el que legalmente solo se permite el acceso a datos periféricos o de tráfico cuanto de trate de conductas calificadas de delito grave, condenando irremisiblemente al fracaso cualquier demanda por infracciones y conductas que no merezcan la calificación de delito grave propiamente dicho, quedando éstas absolutamente impunes ante la imposibilidad de obtener prueba siendo denegadas automáticamente por los jueces.

La investigación y pericia nos plantea, pues, dos cuestiones fundamentales como son los límites a la investigación que suponen los derechos constitucionales y si se dispone en vía civil de medios procesales de investigación y acceso a las fuentes de prueba que se hallen en poder de terceros. Ello por cuanto la investigación y pericia del hecho electrónico implica en muchas ocasiones el acceso a información que pertenece a la esfera privada del individuo y/o que se halla en poder de terceros. Concluimos que frente a ello la ley no regula un procedimiento ni habilita supuestos o establece presupuestos en la LEC que permitan a la parte acudir al juez para solicitar autorización judicial y poder acceder a la esfera privada del sujeto en aquellos casos en que dicha inmisión resulta justificada, a salvo probablemente de las posibilidades que permiten las diligencias preliminares. Aunque, ciertamente se

trata de una regulación insuficiente a este fin. Lo anterior determina un ámbito de actuación más difuso por parte del experto que, en todo momento, deberá ser consciente de los límites existentes en orden a la obtención y análisis de datos para la elaboración de su dictamen pericial. El único modo en que tales injerencias puedan considerarse lícitas es que estén reguladas por la ley y sean apreciadas por el Juez, en cuyo caso no existiría afectación de derechos procesales ni fundamentales protegidos por la Constitución Española. Es de especial importancia que la obtención de las pruebas examinadas en la pericia electrónica se lleve a cabo respetando los derechos fundamentales, ya que ello afectará a la futura eficacia de tales informes que no tendrán valor probatorio cuando los hechos que contienen se hubiesen obtenido con violación de los derechos y libertades fundamentales previstos en el art. 18 CE.

Nuestra propuesta es que el anterior vacío legal se cubra a través de la reforma de la regulación vigente en la Ley de Enjuiciamiento Civil, mediante una regulación unitaria que aúne los mecanismos legales ya existentes y sea capaz de cubrir legalmente todos los supuestos planteables, estableciendo un procedimiento regulado y común, que permita incluso con anterioridad a la demanda asegurar la prueba electrónica, permitir el conocimiento de los hechos mediante una análisis informático-forense y/o practicar prueba pericial *in situ* de ser necesario. De ese modo la norma procesal proporcionaría una vía de «investigación» en el proceso civil que permitiría el acceso a hechos fundamento de posibles demandas. No circunscribiendo dicha posibilidad exclusivamente a supuestos de patentes o competencia desleal. Ello permitiría al juez ofrecer la tutela judicial efectiva de los derechos prevista en la Constitución Española. La previsión legal y la decisión judicial tras el procedimiento correspondiente garantizarían la no afectación de derechos procesales y derechos fundamentales. Concretamos dicha propuesta en la creación de un procedimiento que garantice los derechos procesales y los derechos constitucionales, asegurando una tutela judicial rápida y anticipada como la llamada «Justice of référes» o «procédure de référé» de Francia que legitime la investigación y permita en su caso practicar prueba pericial simultánea. La regulación de un procedimiento de tales características y fuera del tema que nos ocupa permitiría, además, incluir todos aquellos supuestos que de forma desordenada se recogen en la Ley de Enjuiciamiento Civil y que en realidad están procurando al ciudadano una tutela anticipatoria, como algunos de los que se encuentran regulados en los artículos 250 y 727 de la LEC mezclándose con el proceso declarativo o las medidas cautelares.

Finalmente, se analiza la prueba electrónica, entrando en la dimensión jurídico-procesal del hecho electrónico. La prueba electrónica no se diferencia, en esencia, del resto de medios de prueba, ya que tiene la misma y evidente finalidad que es la de probar en el proceso jurisdiccional la certeza de los

hechos sometidos a enjuiciamiento. La diferencia, por tanto, se hallaría, exclusivamente, en la fuente de la prueba que se hallaría en lo que viene en llamarse dispositivos electrónicos, informáticos y similares. Estos son máquinas modernas que tienen la particularidad de adquirir información y procesarla por medio de lenguajes propios no accesibles para el hombre común. De este modo, podemos decir que la prueba electrónica tiene su base y fundamento en la información procedente de los citados medios o dispositivos electrónicos. Así, probablemente toda la discusión sobre el concepto y naturaleza de la prueba electrónica deba basarse en un análisis del modo en el que la información contenida en los modernos aparatos electrónicos se documente y aporte al proceso para su debida valoración. Desde este punto de vista, cabe señalar que la discusión sobre el concepto y naturaleza de la prueba electrónica debe tener en cuenta esas dos distintas fases de generación del hecho electrónico y de su documentación y aportación al proceso. La primera fase tiene una base y fundamento netamente técnico; mientras que la segunda debe analizarse desde presupuestos básicamente jurídicos.

Por lo tanto, desde un punto de vista estrictamente jurídico lo que viene en llamarse prueba electrónica, su concepto si se quiere, viene referido a aquellos medios de prueba en los que se contiene y mediante los que se pretende probar en el proceso los hechos de naturaleza electrónica constitutivos de las pretensiones de las partes. Ahora bien, ello no significa que el jurista deba prescindir, absolutamente, de las cuestiones referidas a la naturaleza técnica del hecho electrónico, ya que, indudablemente, la debida valoración del hecho electrónico como prueba en el proceso debe tener en cuenta todos los factores relativos a su génesis, almacenamiento y documentación. Sólo así el tribunal podrá valorar debidamente y con todas las cautelas y garantías el hecho electrónico y las consecuencias que deba tener para la prueba y, en definitiva, para el otorgamiento de las tutelas pretendidas. Nótese que esta es la función y finalidad del sistema de justicia.

Lo que caracteriza a la prueba electrónica frente a los demás tipos de prueba es que su objeto es probar un hecho de naturaleza electrónica que tiene relación con la pretensión de la parte y que puede ser valorada por el juez. Los hechos de naturaleza electrónica pertenecen a la realidad y no pueden enumerarse son ilimitados, evolucionan con las tecnologías y se amplían en número con el tiempo. En el ámbito del derecho esos hechos de naturaleza electrónica pueden acceder al proceso mediante cualquier medio de prueba de los expresamente previstos por la ley, en cuanto los medios de prueba son tasados. Y si tales hechos de naturaleza electrónica pueden cumplir iguales funciones que otras instituciones jurídicas deben suponer iguales efectos.

Dedicamos un apartado especial a explicar cómo se documenta desde un punto de vista técnico el hecho electrónico. En el epígrafe sobre el soporte material de un hecho electrónico lo definimos como el sustrato o base en el que éste se contiene y que puede ser objeto de prueba en el proceso jurisdiccional. Estos soportes suelen ser dispositivos de almacenamiento de datos, documentos o de registro de sucesos, que dan cuenta de la actividad electrónica producida en un determinado tiempo. Ello sin perjuicio de poder realizar una pericia técnica en tiempo real del comportamiento de un determinado sistema informático. En cualquier caso, señalamos que es importante distinguir los dispositivos técnicos que realizan las actividades programadas para cada máquina, de los dispositivos terminales que ofrecen los resultados en forma de imagen o de documento escrito. Desde este punto de vista, debemos tener clara la diferencia entre la actividad electrónica que se produce mediante fenómenos físicos de esa naturaleza y los resultados ofrecidos en los terminales de salida de datos que se ofrecen, por ejemplo, en una imagen.

Analizamos cómo se documenta un hecho electrónico y cómo accede este al proceso. Concluyendo que el hecho electrónico como tal únicamente podrá acceder al proceso mediante una prueba pericial. Ahora bien, esto será así siempre que nos estemos refiriendo al hecho electrónico en su acepción más técnica, porque no cabe duda que la plasmación de hechos electrónicos en documentos o imágenes podrá acceder al proceso mediante una prueba documental. Más aún, también cabe dar cuenta de la manifestación de un hecho electrónico por medio de la declaración de un testigo que puede dar cuenta de haber visto en una pantalla un determinado correo electrónico o, por ejemplo, una determinada medida o lectura en cualquier dispositivo electrónico. Ahora bien, la clave consiste en distinguir entre el hecho electrónico tal cual es en su auténtica naturaleza y su manifestación en forma de documento o imagen aprehensible para los seres humanos. En este segundo caso no podemos, *estricto sensu*, hablar de hecho electrónico, sino de documentos electrónicos. Esta diferenciación se debe aplicar distinguiendo entre las manifestaciones del hecho electrónico que se podrán acreditar directamente mediante el art. 299.2 LEC, es decir, a través de los «*…medios de reproducción de la palabra, sonido y la imagen, así como a los instrumentos que permitan archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso*» y el mismo hecho electrónico que deberá acreditarse mediante la prueba pericial a través del dictamen de peritos (art. 299.1.4º).

Finalmente estudiamos la prueba pericial electrónica, su objeto, naturaleza jurídica y finalidad. Para a continuación adentrarnos en la figura del perito tecnológico y del dictamen pericial.

En cuanto a la prueba pericial electrónica es relevante que el hecho electrónico, en la mayoría de los casos, suele ser en realidad un medio de acreditar el hecho fundamental que se pretende probar en el juicio. Efectivamente, la prueba pericial electrónica persigue probar o acreditar hechos o una actividad de naturaleza electrónica que fundamenta o tiene relación con la tutela pretendida en el proceso jurisdiccional. Así, si bien existen supuestos en que la finalidad es acreditar un hecho electrónico en sí mismo, la mayor parte de las veces la finalidad perseguida con la aportación de la prueba pericial al proceso es la de acreditar o valorar la certeza de una actividad de naturaleza, origen o que produce efectos en el ámbito de la electrónica.

Por otro lado, ponemos de relieve la enorme dificultad que encuentran los jueces frente a la complejidad de la prueba tecnológica y por lo tanto la necesidad de que sean los expertos quienes faciliten reglas técnicas que les permitan formar su convicción. En este sentido el juez no tiene porqué convertirse en un experto técnico puesto que no es esa su función en el proceso, sino que al juez le corresponde efectuar una valoración mediante el razonamiento de los informes de expertos que son quienes deben aportar sus conocimientos y sus conclusiones. Por lo tanto, la solución en aquellos casos en que la prueba presentada por las partes no sea suficiente para que el juez pueda llevar a cabo su función debería pasar en nuestro ordenamiento, con carácter excepcional, por facilitar procesalmente al juez la posibilidad de acudir a la pericial en aquellos supuestos que necesite conocimientos técnicos, científicos o prácticos en la materia y las partes no los hayan aportado o de aportarlos no fueran suficientes para poder adoptar una resolución (supuestos, por ejemplo, de prueba pericial dirimente en el supuesto de dictámenes periciales contradictorias).

El estudio del perito tecnológico nos lleva a diferenciar figuras afines como aquellos supuestos incardinados dentro del testigo-perito, como es el caso de que se trate de trabajadores contratados como expertos informático-forenses en los departamentos de seguridad de las empresas. Por otro lado, el estudio del perito informático plantea cuestiones de especial importancia como la falta de regulación y titulación oficial unificada de la profesión informática. La falta de verdaderos expertos titulados universitarios oficiales en informática-forense y con experiencia acreditada conlleva la actuación en juicio como peritos de personas no cualificadas que pueden cometer graves errores en el tratamiento de la prueba informática por desconocimiento y que avocan a una prueba sin valor alguno por infracción de la legalidad vigente o bien por falta de conocimientos técnicos y prácticos suficientes. La informática forense es una disciplina que requiere no solo tener conocimientos técnicos y prácticos necesarios sino también conocimientos legales. Por ello concluimos que en España sería aconsejable la unificación de las titulaciones oficiales en un único

grado de ingeniería informática en todas las universidades y la existencia de especialización en «*informática forense*» cursando un master que daría lugar a un título oficial universitario. Este último título incluiría no sólo conocimientos técnicos sino también jurídicos. Siendo requisito indispensable para poder ejercer como perito la necesidad de contar con una experiencia acreditada de entre dos y cinco años.

Por otro lado, tras estudiar la pericial individual y la pericial corporativa en el ámbito de la evidencia electrónica resaltamos que se hace apenas uso de la pericial corporativa. Probablemente ello es debido a la falta de Institutos o Instituciones informático-forenses de estudio e investigación de carácter público o privado y de cátedras específicas universitarias. Lo que va íntimamente ligado a la falta y a la inminente necesidad de regulación de estudios y titulaciones universitarias oficiales en informática forense. Y por otro lado, tampoco existen grupos de estudio e investigación dentro de los colegios oficiales que pudieran emitir dichos dictámenes.

Analizamos como se confeccionan las listas de peritos. Tras dicho análisis llegamos a la conclusión que la principal deficiencia del sistema de listas de peritos es que éstas no garantizan la profesionalidad ni experiencia de quienes forman parte de las mismas. La tendencia política y legislativa actual es permitir que cualquier profesional, en los supuestos de profesiones de colegiación voluntaria, pueda apuntarse a las listas para poder ejercer de peritos judiciales sin acreditar requisito alguno lo cual ofrece pocas garantías. Por otro lado, el vigente sistema implica otras deficiencias graves como los problemas de designación de peritos en partidos judiciales pequeños, puesto que se permite que sean los propios peritos quienes elijan libremente el lugar en que quieren actuar lo que supone una nueva grieta en un sistema igualitario y con plenas garantías a las partes, principalmente en supuestos en que una de éstas carece de recursos.

Una vez tratados temas como la designación, aceptación, imparcialidad y derechos y deberes de los peritos tecnológicos llegamos al epígrafe sobre el dictamen pericial, en el que tratamos principalmente la forma que éste debe adoptar y la compatibilidad entre los dictámenes periciales. Dado que este segundo punto ya ha sido tratado doctrinalmente en repetidas ocasiones damos mayor relevancia a la forma que debe revestir el dictamen pericial en cuanto será uno de los elementos más importantes que determinará el valor que le dé el juez a dicha prueba.

Teniendo en cuenta que el dictamen pericial constituye un medio de prueba (art. 299 LEC) que será objeto de valoración por el juez resulta fundamental que emplee un lenguaje de fácil comprensión, que se estructure de una forma clara

y que contenga todos los elementos e información necesarios para que el juez pueda conocer y entender las operaciones y razonamientos llevados a cabo por el perito y a través de los cuales formula finalmente sus conclusiones. Lo anterior incluye tanto los exámenes, métodos, experimentos e investigaciones efectuadas por el perito como los fundamentos técnicos y científicos en que se basa. Será de igual importancia tanto en el dictamen pericial preprocesal como en el procesal la indicación de todos los elementos relacionados con la cadena de custodia.

El dictamen pericial tecnológico puede ser de parte o bien de designación judicial. En ambos casos, el dictamen deberá revestir igual forma y contenido, respetarse la cadena de custodia que garantiza la integridad, conservación e inalterabilidad de los hechos electrónicos. Ello incluye su obtención, custodia, transporte y presentación en los tribunales hasta su disposición final por orden judicial.

En cuanto a la forma del dictamen pericial efectuamos una propuesta en cuanto su estructura, desglosando cada uno de los apartados que deben componer cada epígrafe. Sin perjuicio de mayor detalle en el epígrafe correspondiente señalar que en primer lugar se distingue una parte inicial relativa al perito o peritos intervinientes. Es decir, a los datos identificativos (nombre, dirección etc.), los relativos a su profesión, experiencia y prestigio profesional (titulaciones, publicaciones etc.) y su obligación de actuar con objetividad (juramento, tachas, causas de abstención y recusación). Reseñados los datos identificativos del perito, los relativos a su profesión, experiencia y prestigio profesional, el juramento o promesa del artículo 335.2 LEC y las posibles causas de tacha o manifestación de no estar incurso en causa de abstención o recusación en la parte inicial del dictamen, no adentramos en el cuerpo del dictamen pericial y su contenido propiamente dicho que en todo caso debe empezar con una descripción detallada de cada uno de los extremos solicitados por el abogado de la parte. De tratarse de diversas cuestiones debieran numerarse y separarse solicitando con claridad y precisión lo que se pida. Se dejará constancia de la fecha de inicio y fin de los estudios. Y a continuación conforme al sistema de cadena de custodia se reseñarán e identificarán todas las fuentes de prueba recibidas y su estado así como se dejará constancia de las precauciones adoptadas para que no exista pérdida de datos. Se documentarán fotográfica o videográficamente el lugar y los soportes, medios o dispositivos sobre los que se ejercerá el estudio y/o componentes objeto de análisis.

Después se entrará en el cuerpo del informe pericial propiamente dicho que comprenderá todos los estudios efectuados sobre el hecho electrónico. Contendrá en su caso, captura de la información, copia y preservación (fase de adquisición de datos) y fase de análisis forense, es decir, clasificación,

identificación, individualización y asociación de la información o datos electrónicos obtenidos. Es fundamental la constancia de cada una de las diligencias practicadas, documentando e identificando las fuentes, identificando las personas que hayan intervenido, haciendo constar los métodos y herramientas utilizadas, así como las posibles incidencias que hayan ocurrido. Precisamente en cuanto a las técnicas y herramientas entendemos fundamental que exista un apartado en el dictamen pericial que no solo las identifique sino que informe sobre aquellos estudios y publicaciones que las validan científicamente.

El cuerpo del dictamen pericial finalizará con las conclusiones finales, obtenidas tras los estudios efectuados sobre los hechos electrónicos y los medios o soportes que los contienen y/o sobre los dispositivos a través de los cuales se manifiestan. Las conclusiones deben dar respuesta a los extremos solicitados por las partes o el juez. Es fundamental que sean claras, comprensibles, concisas y sin ambigüedades. Las conclusiones serán «*evaluativas*» y de acuerdo con el «*paradigma de la verosimilitud*» (probabilidad como grado de creencia no de arbitrariedad) y no el habitual «*paradigma de la individualización*» (infalibilidad de la prueba científica), al perito sólo le compete ilustrar sobre lo que dicen los datos resultantes de la prueba y éstos han de expresarse científicamente en términos de verosimilitud. Es decir, lo único que el perito puede (y debe) hacer es expresar los resultados de la prueba de un modo científicamente riguroso y que al mismo tiempo permita al juez comprender el alcance exacto de los mismos de cara a realizar su valoración ponderándolos con el resto de pruebas. Es por ello incorrecto el uso de las *escalas verbales de la probabilidad*, muy utilizadas, y que reproducen el *paradigma de la individualización* indicando no lo que dicen los datos sino lo que se debe creer.

La cadena de custodia obliga a que una vez finalizados los estudios por parte del perito se especifique el destino final que se dará a las evidencias una vez concluido su análisis, reseñando para todas ellas el medio utilizado para la puesta a disposición de la parte (organismo o entidad) solicitante de la pericial. Se remitirá a la parte solicitante del dictamen los equipos y soportes digitales estudiados, acompañados del correspondiente recibo o documento de control de evidencias. Dicho recibo debidamente cumplimentado, debe devolverse al organismo u empresa que lo emite, una vez haya llegado el informe y las muestras objeto de estudio al organismo o entidad que lo solicitó, dando así por finalizado la trazabilidad y el proceso de custodia de las evidencias objeto de análisis forense.

El informe pericial será firmado por los peritos y otros responsables del entorno de análisis forense que lo emiten, según el plan de calidad instaurado en el mismo, o bien, se puede firmar digitalmente por los mismos actores anteriores.

Anexados al dictamen pericial se acompañarán, de conformidad a lo previsto en el artículo 336.2 LEC, los documentos, instrumentos o materiales adecuados para exponer el parecer del perito sobre lo que haya sido objeto de la pericia. Lo cual ayudará notablemente la comprensión por las partes y el juez de los extremos que conforman el dictamen. Este artículo permite anexar, por ejemplo, al dictamen pericial informático-forense la copia de la información obtenida de un ordenador y efectuada en un CD con el correspondiente *hash* –soporte de los datos informáticos obtenidos- y que permitiría una contrapericia. En aquellos supuestos en que no fuese posible o conveniente aportar estos materiales e instrumentos, el escrito de dictamen contendrá sobre ellos las indicaciones suficientes. Podrán, asimismo, acompañarse al dictamen los documentos que se estimen adecuados para su más acertada valoración (336.2 LEC).

A continuación el trabajo trata sobre la práctica de la prueba del hecho electrónico distinguiendo la práctica de la prueba pericial, como prueba electrónica propiamente dicha, de la práctica de la prueba que versa sobre la manifestación del hecho electrónico. Dentro de este último epígrafe se atiende a la prueba documental, la prueba de interrogatorio de partes y testigos y la prueba de reconocimiento judicial.

La prueba pericial en general, y la prueba pericial electrónica en particular, constituyen una prueba compleja en la que la comparecencia de los peritos en el juicio resulta esencial para que el juez pueda comprender y efectuar una razonada valoración de la prueba pericial en sentencia. Destacar también que en la prueba pericial electrónica la contradicción o la impugnación crítica de la prueba pericial presentada de contrario versará principalmente sobre las herramientas y métodos empleados por el perito y/o sobre el respeto de la cadena de custodia, aunque la impugnación crítica de los letrados podrá versar también sobre otros criterios, tales como, como la falta de cualificación profesional, contradicciones, concurrencia de algún motivo de tacha etc. Es fundamental que el informe pericial sea completo y detallado. Especial relevancia cobra el apartado relativo a la descripción de los elementos integrantes del dictamen pericial que sirven para la validación científica de los métodos y herramientas seguidos por el perito forense en su análisis.

Una vez tratada la práctica de la prueba sobre el hecho electrónico destinamos un epígrafe a la valoración de la prueba del hecho electrónico donde prima el estudio sobre la prueba pericial electrónica. Entendemos que la función crítica por parte del juez en sentencia del dictamen del perito debe pasar por una crítica razonada del dictamen pericial. Ello implica que el juez al efectuar la valoración del dictamen pericial no puede basarse únicamente en criterios como la cualificación del perito (competencia profesional, especialización, curriculum

profesional etc.), la solvencia o prestigio de la institución que lo emite de tratarse de pericial corporativa, o el criterio mayoritario de los dictámenes que concurren puesto que dichos criterios son evidentemente insuficientes y pueden llevar a una dejación por parte del juez en dicha función crítica. Tampoco puede el juez dar valor concluyente a una prueba científica automáticamente sin valoración crítica alguna ya que la prueba científica no es irrefutable. De ahí la importancia de que se emitan dictámenes periciales completos en los que consten todos los datos y diligencias practicadas, cadena de custodia, métodos y herramientas empleados y criterios de validación científica de los mismos. Y que para poder llevar a cabo una correcta valoración de la prueba pericial en el ámbito de la evidencia electrónica, así como en cualquier otro ámbito técnico o científico, los jueces reciban formación en epistemología y en metodología científica, no siendo suficientes a tal efecto conocimientos culturales medios.

Termina la tesis con una breve referencia a la impugnación del dictamen pericial.

Mi agradecimiento a mis directores de este trabajo de tesis doctoral Dr. Manuel Richard González y Dr. Xavier Abel Lluch quienes me han dedicado su tiempo y junto a los que he compartido reflexiones que han contribuido a hacerlo posible. Ambos un ejemplo a seguir como juristas y escritores.

* * *

CAPÍTULO I.- LAS NUEVAS TECNOLOGÍAS

1.1 La nueva era digital

La revolución de las tecnologías de la información y comunicación ha supuesto avances en su día inimaginables creando un entorno social nuevo basado en la movilidad y facilidad en las comunicaciones que permite relaciones globales de larga distancia y con una rapidez inmediata. Efectivamente, estamos experimentando una nueva realidad, la de un mundo en que todos estamos conectados digitalmente, un mundo impulsado por la tecnología, en el que las tecnologías de la información y comunicación engloban y afectan a todo nuestro entorno. Dichos avances tecnológicos están conllevando la reorganización de la realidad de personas, Estados y empresas.

Nos encontramos en la era de la desmaterialización del documento, incrementándose la actuación a través de medios electrónicos y la progresiva desaparición del papel. Las personas descargan, crean, intercambian información e interactúan en la red. Se habla de la generación de los llamados «nativos digitales», una nueva generación que ha convertido el uso de la información de minoritario a extensivo y global. Convivimos a diario con las TIC las cuales se utilizan con fines sociales, lúdicos, educativos y organizativos. Desde un punto de vista social utilizamos las TIC para relacionarnos, nos comunicamos a través de las mismas y compartimos información (fotografías, datos, grabaciones etc.). Utilizamos chats, correos electrónicos, plataformas como Facebook, Twiter o Dropbox etc. Y nos comunicamos verbal y visualmente a través de plataformas como Skype. Es tal el enorme poder de globalización de las TIC que a través de las mismas se es capaz de emprender revoluciones políticas, sociales y culturales, así como movimientos de apoyo o crítica en todo el mundo y en muy poco tiempo.

Por otro lado, desde una perspectiva lúdica participamos individualmente o con otros individuos de cualquier parte del mundo en juegos electrónicos en la red que nos sumergen en mundos ficticios (por ejemplo Minecraft o Club Penguin para los pequeños). En dichos juegos, en los que se utilizan los datos personales para registrarse, se encarnan personajes ficticios, compramos «objetos virtuales» mediante transacciones electrónicas y mantenemos conversaciones con otros participantes. La red nos permite también descargar música y películas y visualizar los videos que se cuelgan en la red (youtube). Podemos también comprar libros y leerlos en dispositivos electrónicos.

En cuando a la formación las TIC han llegado también al mundo educativo, los niños trabajan con recursos y plataformas electrónicas en los colegios, acceden

a material colgado en la nube por sus profesores o elaboran proyectos con información procedente de la red, juegan aprendiendo con juegos educativos que hacen referencia a los materiales objetos de estudio, y se comunican con profesores y compañeros a través de redes de comunicación electrónica internas. Los padres o tutores acceden a las notas de los menores e intercambian información y comunicaciones con sus profesores (por ej. en la plataforma Alexia). Y en las páginas web de los distintos colegios se cuelgan fotografías de los alumnos cuando realizan las actividades del centro.

En nuestra vida cotidiana efectuamos compras mediante transacciones electrónicas (ropa, comida, entradas para espectáculos etc.), operaciones bancarias mediante páginas web (transferencias, consultas de datos, renovaciones de tarjetas de crédito etc.) y archivamos gran parte de información privada en nuestros dispositivos electrónicos (fotografías, cuentas, videos, documentos etc.). Cada vez operamos y guardamos más información electrónicamente. De igual modo las personas jurídicas actúan, se gestionan y se organizan a través de las TIC. Comunicaciones, transacciones, publicidad, contabilidad, listas de clientes y proveedores etc. se gestionan y efectúan a través de TICS que dotan de agilidad y eficacia al mundo empresarial.

El Estado promueve la sociedad de la información y la aplicación de las nuevas tecnologías a la Administración e intenta organizarse para utilizar las tecnologías, ofertas de redes, servicios y aplicaciones digitales, de una forma más intensa y eficaz, contribuyendo a la mejora de la competitividad de las empresas, la generación de empleo de mayor calidad y a la prestación más eficiente y eficaz de los servicios públicos. A ese fin se establecen procedimientos de gestión administrativa a través de la red, mediante procedimientos informáticos, telemáticos o electrónicos de los ciudadanos con diversas Administraciones y entre las Administraciones entre sí.

Estamos hiperconectados y evolucionamos hacia los ámbitos Smart (smart-homes[1], smart-vehicles[2], smart-offices[3], smart-services[4], smarth-health[5], smart

[1] *Smart-homes*: La evolución del concepto de «domótica» que ya venimos utilizando desde hace años. Las casas del futuro serán más inteligentes porque actuarán tomando decisiones por nosotros para procurarnos un mayor bienestar, para aumentar la eficiencia en el uso de los recursos del hogar, o para ayudarnos a realizar tareas rutinarias. Podemos imaginar cientos de aplicaciones concretas que contribuirán a aumentar la inteligencia de nuestro hogar en frigoríficos, dispositivos de limpieza, robots que monitoricen nuestra dieta o la iluminación. Las Tecnologías de la Información en la empresa Española 2012, ESADE – Penteo, pág. 28. Información disponible en la página web http://www.penteo.com.

[2] *Smart-vehicles*: la capacidad que tendrán nuestros coches y motos en el futuro cercano para comunicarse con otros vehículos, autoridades o interactuar con la vía y el mobiliario urbano, tomando decisiones de conducción y se seguridad. Ya estamos viendo las primeras pruebas de conducción automatizada realizadas por Google (con sus vehículos automáticos). Nuestros

metering, smart grid[6], smart cities[7]). La tendencia es evolucionar en los próximos años hacia un Internet convertido en la infraestructura de comunicación del

---

vehículos podrán ser eléctricos y conocer dónde repostar batería (como el proyecto *A better place* desarrollado en Israel) y van a transformarse pronto tomando gran parte de las decisiones de la conducción en el día a día. Las Tecnologías de la Información en la empresa Española 2012, ESADE – Penteo, pág. 28. Información disponible en la página web http://www.penteo.com.

[3] *Smart-offices*: La hiperconectivad tendrá enormes implicaciones en nuestra relación con nuestro empleador y en la propia composición del despacho. Las oficinas serán más inteligentes, y nuestra casa se convertirá, cada vez en más casos, en nuestra oficina. La mayoría de los servicios basados en conocimiento pueden ser prestados online sin necesidad de acudir al trabajo con las implicaciones temporales, de conciliación y medioambientales que esto supone. Las Tecnologías de la Información en la empresa Española 2012, ESADE – Penteo, pág. 28. Información disponible en la página web http://www.penteo.com.

[4] *Smart-services*: La sensorización y la hiperconectividad van a crear infinitos modelos de negocio emergentes, la mayoría de ellos servicios avanzados que harán nuestra vida más fácil y por los que estaremos dispuestos a pagar un precio: desde optimización de rutas automatizadas, monitorización de dependientes, etc. La economía se hará más digital, por la cantidad de valor añadido y de negocio presente en este ámbito. Información disponible en la página web http://www.penteo.com.

[5] Smart-health: El concepto smart no sólo va a hacer nuestra vida más cómoda, también va a introducirse en el cuidado de nuestra salud. Monitorización de nuestras constantes y variables vitales, intervenciones a distancia, implantes que comunicarán los datos obtenidos y actuarán variando nuestra medicación en tiempo real. Todas estas innovaciones reducirán los tiempos de estancia hospitalaria y servirán para prevenir enfermedades o atenderlas de manera temprana. Las Tecnologías de la Información en la empresa Española 2012, ESADE – Penteo, pág. 28. Información disponible en la página web http://www.penteo.com.

[6] *Smart metering* y *Smart grid*: Un contador inteligente (smart meter) es un dispositivo que registra el consumo de un bien (electricidad, agua, gas) y comunica periódicamente al proveedor esta información, usualmente con el objetivo de facilitar la facturación por el consumo, pero también con el propósito de actuar proactivamente sobre las redes al conocer de manera inmediata los patrones de consumo. La relación entre el contador inteligente y el proveedor es bi-direccional, lo que permite emprender acciones en la instalación de manera automatiza como resultado de las lecturas y de las condiciones de cada momento. En 2008 había instalados en Europa más de 39 millones de contadores inteligentes, y sólo en el primer cuatrimeste de 2012 se instalaron en el mundo más de 17 millones. Una Smart grid es una red de distribución inteligente de energía eléctrica. Inteligente porque utiliza la información de contadores inteligentes para optimizar la producción y distribución de energía eléctrica. En España estamos asistiendo al despliegue, por ley, de medidores inteligentes. A finales de 2010 terminó la primera fase con el 30 de despliegue de contadores eléctricos inteligentes. A finales del 2018 este despliegue será total, cumpliendo con la Directiva comunitaria 2006/32/CE. Las Tecnologías de la Información en la empresa Española 2012, ESADE – Penteo, pág.28-29. Información disponible en la página web http://www.penteo.com.

[7] *Smart cities*: Se acepta que una ciudad es conocida como "smart" cuando ha alcanzado un desarrollo relevante de sus infraestructuras de transporte y comunicaciones, dispone de un elevado nivel de vida, gestiona inteligemente sus recursos naturales y se gobierna de manera

mundo que nos vinculará a todos con los objetos cotidianos, con caudales de acceso virtualmente ilimitados sobre fibras ópticas e infraestructuras inalámbricas[8].

Los datos, algunos sensibles o que incluyen información personal, fluyen a través de la red y trascienden los límites y fronteras, se comparten entre empresas, gobiernos y particulares a través de computadoras ubicadas en diversos países. Las fronteras desparecen en la red y los servicios suelen subcontratarse para un mayor ahorro de costos y mejora del servicio. Es decir, aumenta la práctica por medio de la cual se contrata un proveedor externo para que lleve a cabo un programa o para que proporcione un servicio, como por ejemplo la administración de una base de datos. Y ese proveedor externo puede estar en cualquier país del mundo.

El hombre ha cambiado social y culturalmente y se organiza y actúa de forma distinta. Es necesario que dicha transformación social venga arropada por normativa jurídica, es decir, el cambio requiere de un ordenamiento jurídico evolucionado y acorde con la actual realidad tecnológica. Para ello se replantean conceptos tradicionales como puede ser el concepto de «privacidad» y se crean y regulan conceptos jurídicos nuevos. Y finalmente, por otro lado, la nueva realidad reabre debates como el de libertad y seguridad, y cómo pueden justificarse las restricciones que implica la seguridad frente a la libertad. En este sentido movimientos como el «criptoanarquismo» y la «negación plausible» promueven el derecho a la libertad plena sin control ni restricción alguna[9].

---

participativa. Giffinger propone 6 ejes bajo los que una Smart-city es evaluada: a smarteconomy; smart mobility; smart environment; smart people; smart living; y, finalmente, smart governance. Lo que denominanos Smart-city hace referencia a lo que en realidad debería llamarse Digital City. Una ciudad digital es aquella comunidad en la que se aúnan conectividad de banda ancha, infraestructuras públicas de acceso y existencia de servicios ciudadanos electrónicos con un alto nivel de interoperabilidad. El concepto Smart city es por tanto una entidad social y política, no sólo tecnológica. Las Tecnologías de la Información en la empresa Española 2012, ESADE – Penteo, pág.28-29. Información disponible en la página web http://www.penteo.com.

[8] *Las Tecnologías de la Información en la empresa Española 2012*, Informe ESADE – Penteo, pág. 27. Información disponible en la página web http://www.penteo.com.

[9] El criptoanarquismo es una ideología o estrategia que se muestra a favor de la utilización de la criptografía asimétrica para hacer cumplir la privacidad y la libertad individual en las comunicaciones efectuadas a través de la red. Término popularizado por Timothy C. May, es descrito por Vernor Vinge como la realización ciberespacial del anarcocapitalismo. Los criptoanarquistas apuntan al objetivo de crear software criptográfico que se pueda utilizar para eludir la persecución judicial y el acoso al enviar y recibir información en redes de computadoras. Con el uso de estos programas informáticos, la conexión entre la identidad de un usuario o una organización y el seudónimo que usan es casi totalmente indemostrable, a menos que el usuario revele la conexión. La ubicación de un determinado usuario sería desconocida. En cierto sentido, el cifrado de redes anónimas (el «ciberespacio», textualmente

1.2 Derecho y evolución tecnológica

El mundo de las Tecnologías de la Información y Comunicación (TIC) es un mundo global y nuevo tanto conceptual como funcionalmente. Desde un punto de vista funcional la plataforma a través de la que actualmente se accede a la cultura, a las relaciones sociales, a las relaciones jurídicas ha cambiado. Todo se desarrolla a través de la red: visionamos, contratamos, nos comunicamos, informamos, archivamos y creamos a través de la red. Y las empresas publicitan, compran y venden en la misma (internet 1.0[10], internet 2.0[11], internet 3.0[12]). Un ejemplo de ello lo es la Web 3.0 a través de la cual se

---

«espaciocifrado» o «criptoespacio») puede considerarse como un territorio independiente, sin ley pública. Sin embargo, los participantes pueden, en teoría, voluntariamente crear leyes privadas o utilizar contratos o protocolos, o si el usuario es un seudónimo anónimo, depender de la reputación en línea. El criptoanarquismo depende en gran medida de «negación plausible» para evitar la censura. Los criptoanarquistas crean esta negación mediante el envío de mensajes cifrados a proxies interconectados en las redes de computadoras. Con el mensaje una carga útil de la información se incluye en la ruta. El mensaje es cifrado para cada uno de los proxies y el receptor los criptogramas asimétricos. Cada nodo sólo puede descifrar su propia parte del mensaje, y sólo puede obtener la información destinada para sí mismo. Es decir, que cada uno es el próximo de la cadena. Por lo tanto, es imposible para cualquier nodo de la cadena saber nada más que el anterior y el próximo o qué información se está transmitiendo al receptor final, dado que dicha información está cifrada. El receptor tampoco sabe quién es el remitente, excepto tal vez por otros destinos, la firma digital o algo similar. Quién envió la información y quién es el receptor es difícil de detectar. Definiciones obtenidas en Wikipedia con referencia bibliográfica a Vernor Vinge, James Frankel, True Names*: And the Opening of the Cyberspace Frontier* (2001), Tor Books, pág.44 y *Cyphernomicon* por Timothy C. May. Puede consultarse en la dirección electrónica http://goo.gl/ZJ0uA.

[10] Internet es una red de computadoras formada a su vez por muchas redes independientes, que se pueden comunicar unas con otras, intercambiar mensajes y compartir información en forma de archivos (correo electrónico (e-mail), listas de correos, World Wide Web (www), el uso de multimedios, transferencias de archivos (FTP), buscadores, news, conferencias (Chat services) y Talk, y otros servicios). En 1991 Tim Bereners Lee crea la World Wide Web (www) proponiendo un sistema de «hipertexto» para compartir documentos, Hyper Text M K LHT t Markup (html). Posteriormente dicho sistema evolucionó naciendo la Web 1.0, la Web 2.0 y la Web 3.0. La Web 1.0 («Web») es un sistema basado en hipertexto y gráficos, e incluye efectos multimedios, siendo considerado como el acceso más sencillo y comprensible al universo de la información disponible en internet. Dicho sistema enlaza páginas o documentos localizados en la red sin importar su ubicación física o geográfica. Sus protocolos son Http, que es un protocolo de transferencia de hipertexto (Hyper Text Transfer Protocol) y Html, formato hipertextual y hipergráfico para publicar documentos en la red, creado para codificar y visualizar documentos y que incluye formatos, layout y estructura de un documento web. La Web 1.0 se caracteriza por poca cantidad de productores de contenidos, muchos lectores de dichos contenidos, páginas estáticas, y falta de actualización periódica de los sitios. Se trata de sitios direccionales y no colaborativos, siendo los usuarios meros lectores consumidores, y existiendo una interacción mínima reducida a formularios de contacto, inscripción a boletines etc.

[11] La Web 2.0 («Web social») nace como una segunda generación de web basada en comunidades de usuarios. Se evoluciona pues de una web meramente informativa, creada por

pretende, en marketing empresarial, almacenar las preferencias de los usuarios (gustos, costumbres, conectividad, interactividad, uso, etc.) y al mismo tiempo, combinándolas con los contenidos existentes en redes sociales e internet móvil, entre otros, poder atender de forma más precisa las demandas de información y facilitar la accesibilidad a los contenidos digitales. Proporcionando con ello, una

---

expertos a una web social, donde cualquiera puede participar fácilmente. Aparecen aplicaciones web muy potentes y sencillas de manejar enfocadas al usuario final. La Web 2.0 basa su desarrollo en Sistemas de Gestión de Contenidos (CMS) o Content Management System que permiten la creación y administración de contenidos, principalmente en páginas web. Consiste en una interfaz que controla una o varias bases de datos donde aloja el contenido. Dicho sistema permite manejar de manera independiente el contenido y el diseño. Los Sistemas de Gestión de Contenidos han evolucionado desde las páginas estáticas (HTML) de edición a mano, difícil actualización y contenido y diseño unidos, a las páginas dinámicas (CGI) gestores complicados y de poca flexibilidad, a las páginas dinámica (PHP, ASP, Java) de gran flexibilidad, con un crecimiento de las comunicaciones del usuario y la separación total entre presentación y contenido. La Web 2.0 se caracteriza pues: por ser el usuario el protagonista quien crea y comparte; por la participación, pues el conocimiento de comparte en base a la suma de esfuerzos individuales, cuantos más usuarios comparten mayor utilidad del servicio; y por la facilidad de utilización de las herramientas (no son necesarios grandes conocimientos técnicos). La Web 2.0 no es ninguna tecnología ni lenguaje de programación, sino una técnica de desarrollo web que combina varias tecnologías y consigue una navegación más ágil y rápida, más dinámica. Utiliza las siguientes tecnologías: XHTML (o HTML) y CSS (presentación de datos); Document Object Model (DOM) Document, que permite mostrar e interactuar dinámicamente con la información; XML y XSLT que permiten intercambiar y manipular datos con el servidor web; XMLHttpRequest, recuperación y envío de datos de modo asíncrono; y JavaScript (nexo de unión). Son tecnologías de la Web 2.0: Los Blogs, espacios web donde los autores escriben cronológicamente artículos y los lectores dejan sus comentarios, se actualizan periódicamente que recopilan cronológicamente textos o artículos de uno o varios autores, pueden ser de tipo personal, periodístico, empresariales o corporativos etc.; los Wiki, que son colecciones de páginas hipertexto que pueden ser visitadas y editadas por cualquier persona en cualquier momento, son básicamente un editor de texto online que permite que sus contenidos sean escritos de forma colaborativa través de un navegador, utilizando una notación sencilla para dar formato, crear enlaces etc.; y Really Simple Sindication (RSS), con un formato que permite que unos programas llamados «agregadotes» presenten el contenido de una página web sin necesidad de visitarla, usando un agregador el internauta puede suscribirse a varias páginas web y recibir automáticamente todas las novedades de las páginas en un único sitio.

[12] La Web 3.0 «Web semántica» es una web estructurada con significados bien definidos. Utiliza tecnologías RDF, OWL, JENA, SESAME, SPARQL etc. Está basada en la representación del significado y conexión del conocimiento; añade metadatos semánticos a la información de la web a través de la utilización de ontologías; amplía la interoperabilidad entre los sistemas informáticos; reduce la mediación de operadores humanos necesaria y supone la creación colectiva y colaborativa de recursos. La Web 4.0 «Web ubicua» es un tipo de web inteligente que utiliza como tecnologías algoritmos se procesamiento de lenguaje natural. Se caracteriza por el desarrollo de agentes personales inteligentes, el desarrollo de comunidades semánticas y las aplicaciones de web ubicua podrán identificar recursos y gestionarlos dentro del contexto de sesiones temporales o duraderas. Véase sobre este tema: LÓPEZ CUMPA, James, *La evolución de la Web*. Puede consultarse este artículo en la dirección electrónica http://goo.gl/pMylT, página consultada en fecha 3.7.2013.

herramienta esencial para la aceptación, adopción, flujo y funcionalidad de la publicidad de la empresa con el objetivo de fidelizar al usuario con las marcas que se presentan en la red (HERNÁNDEZ y KÜSTER, 2012)[13]. Desde un punto de vista conceptual aparecen, por ejemplo, objetos contractuales nuevos y virtuales que se adquieren en la red y nuevas tipologías de contrato (contratos informáticos, contratos electrónicos etc.).

La nueva realidad creada por las Tecnologías de la Información y Comunicación (TIC) requiere de cobertura por parte del ordenamiento jurídico para que queden protegidos los derechos de los ciudadanos. El derecho necesita adaptarse para poder cumplir con la función social reguladora de la comunidad que le es propia. Ello implica nueva regulación y unificación legislativa en el ámbito nacional, no sólo en derecho sustantivo –nuevos conceptos jurídicos y formas de relación jurídica- sino también en derecho procesal –aportación del hecho electrónico al proceso y fijación de su régimen jurídico-, y requiere, asimismo, regulación y unificación o colaboración legislativa a nivel internacional de los diferentes Estados para poder ser eficaz. La regulación de la nueva realidad generada por las TIC, la unificación normativa a nivel nacional e internacional en la medida de lo posible y la cooperación entre países son tres ejes fundamentales para garantizar la seguridad jurídica en nuestro nuevo entorno dentro y fuera de la red.

Desde una perspectiva conceptual el derecho sustantivo va adaptándose a las nuevas necesidades jurídicas pero necesita dar cobertura en muchos nuevos ámbitos en los que o bien no existe regulación específica, o bien la existente no está unificada, aplicándose, en ocasiones, normativa que fue en su día diseñada para objetos y relaciones jurídicas diferentes. A modo de ejemplo en el ámbito civil/mercantil hallamos esa diversidad legislativa tanto en la regulación de la «contratación informática» como en la «contratación electrónica» ambas fruto de la implantación de las nuevas tecnologías. La primera, «contratación informática», incluye aquellos contratos cuyo objeto jurídico sean un bien o servicios informáticos o ambos, o que una de las prestaciones de las partes tenga por objeto ese bien o servicio informático. Dentro de su ámbito nacen nuevos contratos como: la compraventa informática, los contratos sobre software, el leasing informático, el contrato de mantenimiento informático, la auditoría informática, el contrato de *outsourcing* o *facilities management*, el

[13] Véase sobre este tema el artículo publicado por KÜSTER, Inés y HERNÁNDEZ, Asunción, *De la Web 2.0 a la Web 3.0: antecedentes y consecuencias de la actitud e intención del uso de las redes sociales en la web semántica*, Universia Business Review, primer trimestre 2013. Puede consultarse este artículo en la dirección electrónica http://goo.gl/05iV0, página consultada en fecha 3 de julio 2013.

contrato de *scrow*[14], el contrato llave en mano (*turn key Package*), el contrato de seguro informático, los contratos de acceso a internet, los contratos de alojamiento en sitios web (*web site hosting*), contratos de publicidad etc[15].

Los contratos informáticos no tienen tipicidad única o propia, por lo que resulta aplicable el Código Civil y, en su caso, de constituir acto de comercio, el Código de Comercio. En relación con los derechos de autor y los programas de ordenador les resulta aplicable también el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, así como la Ley 5/1998, de 6 de marzo, de incorporación al derecho español de la Directiva 96/9/CE, del parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos, cuando el objeto del contrato sea una base de datos, sin perjuicio además de las normas que sean de aplicación según el contenido de las mismas. Por otro lado, cuando una de las partes contractuales sea una Administración Pública resultará también de aplicación la normativa vigente en materia de contratos con las Administraciones públicas.

---

[14] Como consecuencia de los conflictos que van surgiendo en el ámbito de desarrollo de software se van instaurando contratos que en España eran jurídicamente desconocidos como el ESCROW, no exentos de problemas. En la línea de la protección de las creaciones intelectuales existe la posibilidad de pactar, entre la empresa que desarrolla un programa de ordenador y el cliente, que el primero depositará el código fuente de dicho programa ante un Notario o tercera parte confiable, en previsión de una serie de sucesos. Esto es lo que se conoce como «Escrow». El motivo que aconseja pactar este tipo de cláusulas o contratos es debido a los problemas que pueden derivarse, cuando una empresa adquiere una licencia de uso de software, por la desaparición de la empresa desarrolladora de dicho programa. En esos casos, la empresa licenciataria habrá adquirido el uso de un software que no podrá modificar ni actualizar porque no se le entrega el código fuente, sino lo que se conoce como código objeto, por lo que quedará, con el tiempo, obsoleto o bien no podrá ajustarse a aplicaciones nuevas. Lógicamente, no se está pensando ni en usuarios domésticos ni en programas genéricos, sino en empresas que han adquirido un software específico, a veces desarrollado a medida, que ha instalado en muchos de sus equipos y por el que ha pagado una buena suma de dinero. En la práctica, la empresa desarrolladora del software y la licenciataria establecerán, en el contrato de cesión de uso de software, una cláusula por la que la primera se comprometerá a depositar ante un tercero el código fuente del programa en cuestión. En realidad, lo que se deposita es un soporte informático (se aconsejan dos copias), ya que el código fuente, como bien inmaterial, no puede depositarse, así como otros manuales y documentación que no se haya entregado con el contrato de cesión de uso. PRENAFETA RODRÍGUEZ, Javier, *Sobre el contrato de Escrow: Naturaleza jurídica y algunos problemas, Noticias jurídicas, artículos doctrinales, derecho informático,* Marzo, 2002. Puede consultarse este artículo en la dirección electrónica http://goo.gl/C7Buk

[15] Sobre este particular véase el artículo publicado por GOTZONE MUGICA ARRIEN, *Los contratos Informático*s, Saberes, Revista de estudios jurídicos, económicos y sociales, Vol. I, 2003, separata. Universidad Alfonso X El Sabio. Puede consultarse este artículo en la dirección electrónica goo.gl/2Z2yH o www.uax.es/publicaciones/archivos/SABDER03_029.pdf. Página consultada el 19.07.12.

La «contratación electrónica»[16], entendida como la contratación realizada a través de la utilización de algún medio electrónico, se regula también por normativa diversa, y dado su posible carácter no sólo nacional sino también transfronterizo y extracomunitario le afectan aspectos fiscales, jurídico-internacionales, de propiedad industrial e intelectual, de protección a la intimidad personal de los contratantes, de seguridad pública y de competencia empresarial. Sin entrar en los anteriores aspectos, a la contratación electrónica le resulta de aplicación: El Código Civil (condiciones básicas para la contratación, principios de libertad y autonomía de la voluntad, exigencias mínimas de estructura del contrato como consentimiento (oferta y aceptación), objeto y causa, incluyéndose la forma cuando funciona en su vertiente «*ad solemnitatem*» (obligatoria); el Código de Comercio que contiene algunas normas preceptivas cuando se trata de contratación mercantil, entre comerciantes; el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, que contiene un marco normativo protector de esta clase de receptores de bienes o servicios, cuyas normas de obligado cumplimiento se destinan a la información del consumidor, redacción de las cláusulas en el contrato, régimen de garantías y responsabilidades y determinación de cláusulas abusivas, y es de aplicación plena a la contratación electrónica; la Ley 7/1998, de 14 de abril, de Condiciones Generales de la contratación, que establece el régimen jurídico de las cláusulas predispuestas en los contratos, denominados contratos de adhesión al imponerse por una de las partes a la otra, sin negociación; la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista, que establece el régimen general del comercio minorista, regulándose la venta a distancia, de especial aplicación en el comercio electrónico, en sede de B2C («*Business To Consumer*»), ya que no se contempla la modalidad B2B (de empresario a empresario); el Real Decreto Ley 14/1999, de 17 de septiembre, de firma electrónica, que establece y regula la validez de la firma electrónica en España, las condiciones para que sean efectivas jurídicamente y la regulación de las entidades que ofrecen tal soporte electrónico, como los servicios de certificación y verificación de la misma; la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico; y el Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, de condiciones generales de la contratación.

En el ámbito comunitario resulta de aplicación a la contratación electrónica: La Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil

[16] La «contratación informática», cuyo objeto es un bien o servicio informático, no debe confundirse con el concepto de «contratación electrónica» que es la que se realiza a través de medios informáticos y cuyo objeto pueden no ser bienes o servicios informáticos.

Internacional sobre Comercio Electrónico, Texto adoptado por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional en su 29º periodo de sesiones, de 28 de mayo a 14 de junio de 1996, en Nueva York; la Directiva 93/13/CEE, de 5 de abril de 1993, sobre Cláusulas Abusivas en Contratos Celebrados con Consumidores, que aproxima y armoniza las legislaciones de los Estados Miembros de la Unión Europea, de aplicación en cláusulas que no hayan sido negociadas individualmente (contratos de adhesión), estableciendo una norma general para la Unión, a la que se puede recurrir en caso de existir lagunas en el ordenamiento de alguno de los Estados Miembros; la Directiva 97/7, de 20 de mayo, de Protección de los Consumidores en Materia de Contratos a Distancia, cuyo objetivo es establecer un marco común en la UE, es decir, establece los requisitos mínimos que deben tener las transacciones a distancia, incluyendo Internet, regulándose la información previa, la confirmación escrita del mensaje, cumplimiento contractual, regulación del pago con tarjeta, y limitaciones del empleo de técnicas de comunicación como el fax; la Directiva 99/93, de 13 de diciembre, por el que se establece un Marco Comunitario para la Firma Electrónica, cuya finalidad es facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico, así como algunos servicios de certificación, su importancia radica en la equiparación de la firma electrónica a la manuscrita; y la Directiva 2000/31, de 8 de junio, de Aspectos Jurídicos de los Servicios de la Sociedad de la Información, en particular el Comercio Electrónico en el Mercado Interior, tratándose de servicios prestados normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios (libro digital, audio o video, catálogo en línea)[17].

La falta de unificación legislativa es evidente. Pero la necesidad de regulación y unificación también se hace patente en otros ámbitos como, por ejemplo, en la necesidad de que el ordenamiento jurídico dote de suficiente eficacia jurídica a la documental que se trasfiere por las redes, y que es de uso común en el tráfico mercantil por tratarse de una forma rápida y eficaz y suponer un ahorro de costes en recursos materiales y humanos para las empresas; o en ámbitos carentes de suficiente protección como la privacidad[18].

---

[17] Véase BERNING PRIETO, Antonio David, *Derecho de la contratación electrónica*, Noticias Jurídicas, Artículos Doctrinales: Derecho Informático, Junio 2008. Puede consultarse este artículo en la dirección electrónica http://goo.gl/55KCX (página consultada en fecha 2.7.2013).

[18] «Privacidad» entendida de un modo más global al concepto existente hasta el momento. Es decir entendida como aquella que constituye un «conjunto más amplio, más global de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre si, arrojan como precipitado un retrato de la personalidad del individuo que este tiene derecho a mantener reservado» (Exposición de Motivos de la LOPD).

En lo referente a la privacidad existe la necesidad de una regulación unitaria, global y clara de la protección de datos que proteja al usuario -escasamente formado en general- frente al oscurantismo existente en las redes. Una normativa basada en el consentimiento informado y transparente –regulación en supuestos como los rastreos con fines publicitarios a través de *cookies* asociadas a la publicidad comportamental y al comercio electrónico-, y que regule el «derecho al olvido» en Internet permitiendo al usuario suprimir información almacenada en la red[19]. A nivel europeo viene trabajándose en este sentido. En el ámbito de protección del derecho a la intimidad destacan Directivas como la 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de datos personales y a la protección a la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Y actualmente, se ha puesto en marcha uno de los proyectos de mayor entidad existente hasta el momento, el Proyecto de Reglamento para la protección de datos en la Unión europea (el 25 de enero de 2012, la Comisión propuso una reforma generalizada de las normas de protección de datos de la UE de 1995 con el fin de afianzar los derechos a la privacidad en Internet e impulsar la economía digital en Europa). Las redes y los servicios digitales deben ser respetuosos con la privacidad, ya que los individuos tienen derecho al control sobre el acceso y uso de sus datos personales.

Desde otra perspectiva jurídica más amplia, quizá debamos incluso plantearnos que la regulación en algunos ámbitos pueda ser diferente a la existente hasta ahora, no sólo en cuanto al concepto sino también en cuanto a los límites y objeto de protección. Es decir, quizá ha llegado el momento de dejar de querer encajar unos nuevos hechos y circunstancias en esquemas predeterminados que ya no tienen sentido en la actualidad. Un ejemplo de ello, en el ámbito de propiedad intelectual, lo sería la regulación de los derechos de autor. Teniendo en cuenta que la plataforma de acceso a la cultura ha cambiado y que, en principio, podemos acceder a la red y conseguir cualquier producto cultural sin la limitación impeditiva de las leyes protectoras de derechos de autor. Es evidente que procede una adaptación legal a un nuevo escenario social con la finalidad de crear leyes realmente más eficaces y adaptadas a la actual realidad[20].

[19] El Tribunal de Justicia de la Unión Europea ha dictado en fecha 13 de mayo de 2014 una sentencia en que se reconoce el «derecho al olvido». Dicha sentencia concluye que Google es responsable del tratamiento que aplique a los datos de carácter personal que aparecen en las páginas web publicadas por terceros y por tanto debe respetar la directiva comunitaria sobre protección de datos.

[20] En este sentido se pronunció LESSIG en el 1st Digital Law World Congress celebrado en el ICAB de Barcelona el 29 de junio 2012, en el ámbito de la normativa sobre propiedad intelectual en el que afirma que debemos «desregular» y centrar la normativa donde sea beneficioso,

En cuanto al aumento del uso de las TIC supone correlativamente el aumento de mayor número de conflictos relacionados con las mismas, abriéndose el camino al nacimiento de nuevas conductas ilícitas que han sido objeto de regulación legal y/o doctrina jurisprudencial. Así por ejemplo, en el ámbito penal, conductas ilícitas cometidas a través de ordenador o internet (injurias, calumnias, estafas informáticas[21], falsedades documentales, usurpaciones de estado civil, extorsión[22], hurto[23], apropiación indebida[24] etc.) o delitos contra la informática (daños a sistemas informáticos, a datos o vías telemáticas de comunicación, por ejemplo, bloqueando sistemas -ataques de denegación de servicios o Dos-, destruyendo programas, dañando dispositivos de almacenamiento o alterando datos (fraude), destruyéndolos (sabotaje[25]) o

---

creando una normativa realista. La regulación actual de derechos de autor no puede funcionar en la era digital porque sino nuestros hijos dejarán de crear (son chicos que crean videos, los versionan o modifican videos existentes y los cuelgan en Internet). Entiende que deben dejar de sancionarse en este ámbito aquellas conductas que no persiguen lucro o son realizadas por no profesionales y limitar la protección de los derechos de autor respecto a quienes viven de su obra, apuesta por los «fair use» americanos o «usos justos». Véase LESSIG LAWRENCE. Law professor Harvard University. Digital Law 1st world congress. 29 de junio 2012. ICAB. Puede consultarse este artículo en la dirección electrónica http://goo.gl/bbhTM. Página consultada el 24.02.13.

[21] Dentro de las estafas informáticas podemos destacar el abuso de tarjeta de crédito, la ficción de crédito y el uso de tarjeta caducada, cancelada, falsa o alterada (art. 248 CP)

[22] «Ransomware» es un tipo de malware, muchas veces distribuido mediante spam, que como diferentes técnicas secuestra documentos, discos o incluso equipos enteros, exigiendo al usuario un pago por el rescate. MARTÍNEZ DE CARVAJAL HEDRICH, Ernesto. *Informática Forense, 44 casos reales.* Julio 2012. pág. 99.

[23] En el hurto conductas tipificadas como la utilización de tarjeta ajena y apoderamiento de soportes informáticos (art. 234 CP).

[24] En la tipología de la apropiación indebida destacamos conductas como el librar dinero por error, o en cantidad superior a la solicitada por el cajero automático (art. 252 y 253 CP).

[25] Podemos definir el «sabotaje» como aquel acto que consiste en borrar, suprimir o modificar sin autorización funciones o datos de un sistema informático con intención de obstaculizar o impedir el funcionamiento normal del sistema. Esto puede hacerse de forma directa y manual o de forma remota o con programas diseñados al efecto, tales como virus, gusanos o bombas. El «Virus» es un programa capaz de incrustarse en otro o, incluso, sustituirlo para realizar acciones no deseadas en el ordenador afectado y sin conocimiento ni el consentimiento del propietario. Um virus no es capaz de replicarse a si mismo, pero si es capaz de infectar otros programas o sectores específicos de dispositivos de almacenamiento, ya sea del mismo equipo o de equipos remotos. Los programas infectados infectan a su vez otros programas y así sucesivamente. Una vía habitual de infección es la descarga desde internet de programas que han sido previamente infectados. También pueden entrar a través de un soporte físico, como por ejemplo una memoria USB, previamente conectada a un sistema informático. Los tipos de virus más difundidos son: Troyanos que una vez entran en un sistema abren una puerta de comunicaciones para permitir acceso a intrusos); Bombas lógicas, son programas o partes de

usándolos ilícitamente (piratería, espionaje), acceso a sistemas informáticos sin autorización, interceptación de datos[26], interceptación de comunicaciones, delitos contra la propiedad intelectual etc.). En el ámbito civil, infracciones como la vulneración de los derechos a la intimidad, el honor o la propia imagen cuando no sean conductas constitutivas de delito o la revelación de datos personales[27]. Y finalmente en el ámbito laboral cabe señalar las infracciones de los deberes del trabajador, en relación con el uso de las nuevas tecnologías de la empresa –correo electrónico, móvil etc.- para fines personales o incluso para la comisión de ilícitos como la sustracción de información confidencial de la empresa.

Frente a la comisión de ilícitos es aconsejable que los diferentes países tengan legislaciones homogéneas y/o establezcan protocolos de colaboración en todos

---

programa que se activan al producirse un determinado evento, como por ejemplo llegar una fecha; y Hoax, son pseudovirus que mediante engaño logran que el usuario colabore con su propagación o, incluso, en llevar a cabo el borrado de ficheros vitales –ej. El «osito» era un mensaje de correo absolutamente inocuo que avisaba de un riesgo en el ordenador y animaba al usuario a eliminar un fichero que en realidad era parte vital del sistema operativo.

Los «gusanos» a diferencia de los virus están formados por código Independiente que no se incorpora al código de otros programas, y son capaces de replicarse hasta llegar a consumir los recursos de los equipos infectados. Las «bombas lógicas» son programas diseñados para provocar daños en el sistema de forma retardada. Sueles confeccionarse mediante líneas de código insertadas en otros programas, que no alteran su funcionamiento normal, y activan la bomba al ocurrir un determinado evento (bomba lógica) o bien al llegar a una fecha (bomba cronológica). «Defacement» significa «desfiguración» en inglés, es el término con el que se conoce a la modificación no autorizada de una página web, para lo que debe lograrse acceder a los permisos de administrador al servidor que la contiene. Al autor del «defacement» se le denomina «defacer».Véase sobre el tema MARTÍNEZ DE CARVAJAL HEDRICH, Ernesto. *Informática Forense, 44 casos reales, j*Julio 2012. págs. 54-60

[26] Un «sniffer» es un programa capaz de interceptar los paquetes de información que circulan por internet para obtener claves y datos de otras personas. Basta un sniffer, que se puede descargar desde internet y una conexión no cifrada, para que los datos objeto de la transmisión puedan ser capturados. MARTÍNEZ DE CARVAJAL HEDRICH, Ernesto. *Informática Forense, 44 casos reales.* Julio 2012. págs. 77-78.

[27] ORTUÑO NAVALÓN señala como ejemplos frecuentes las reclamaciones judiciales por inclusión unilateral de los ciudadanos en ficheros de morosos (ASNEF y otros) por incumplimiento de obligaciones dinerarias (SAP Barcelona, sec. 16ª, núm. 26/2011, de 19 de enero, SAP Sevilla, sec. 6ª, núm. 78/2011 de 11 de marzo, o SAP Madrid, sec. 9ª, núm. 86/2011, de 11 de febrero), así como el acceso de terceros al contenido de tales ficheros (véase en este sentido STC 254/1993, de 20 de julio). Igualmente señala los supuestos de reproducción de obras impresas sin la debida autorización vulnerando los derechos de autor y aquellos supuestos en que se analiza si la música bajada directamente de Internet es o no música libre «copyleft» (SAP Valencia, sec. 9ª, núm. 372/2011, de 4 de octubre). ORTUÑO NAVALÓN, MC, *La prueba electrónica ante los Tribunales*, ed., Tirant Lo Blanc, Valencia, 2014.

los ámbitos. Principalmente en derecho penal en aras a una mayor facilidad en la persecución del delito. Las TIC facilitan la comisión de delitos que pueden afectar al territorio de diversos países. Una acción ilícita desde un ordenador fijo o móvil cuyo origen es ignorado que redirecciona a través de servidores ubicados en diferentes países y produce un resultado también en diferentes ubicaciones. La comisión de dichos delitos puede generar problemas de competencia entre tribunales[28], a las que se añaden dificultades de obtención de la prueba (comisiones rogatorias que suelen ser lentas y no siempre son bien cumplimentadas), y de validez en España de la prueba obtenida en el extranjero. Por parte de los Estados es importante garantizar la seguridad «ciberseguridad» centrada en la protección de servicios e infraestructuras críticas así como la protección frente a accesos no autorizados de la información. A nivel europeo se trabaja en este sentido. Un ejemplo de ello es la Convención sobre Delito Cibernético del Consejo de Europa, de 23 de noviembre de 2001 (Budapest), que entró en vigor el 1 de julio de 2004. Dicho Convenio establece una armonización de las definiciones de delitos cibernéticos, determina procedimientos para la recolección de la evidencia y garantías a nivel de distintas jurisdicciones internacionales.

Fuera de Europa, sin embargo, la coordinación o armonización resulta más difícil con algunos países como Estados Unidos, dadas las diferencias legislativas existentes. Estados Unidos, por ejemplo, sancionó, en fecha 24 de octubre de 2001, The Usa Patriot Act (Ley Patriota de los Estados Unidos) que, frente a las políticas de protección de datos europeas, permite en Estados Unidos que el Gobierno no sólo exija información a cualquier ciudadano americano (imagínense organizaciones americanas, tales como Microsoft), sino que además éstos tengan prohibido el hecho de revelar a los afectados que dicha información ha sido transferida al gobierno (art. 215 Patriot Act). El único requisito para emitir dicha orden judicial es que exista una investigación en curso sobre actividades terroristas o de inteligencia secreta, llevada a cabo bajo las directivas del Procurador General. Las autoridades americanas no tienen obligación de acreditar la existencia de causa probable (existencia de hechos específicos que conducen a la creencia de que se cometió un delito o que está a punto de cometerse). Lo único que es vinculante es que la información «pueda estar relacionada» a una investigación en curso relativa a actividades terroristas o de inteligencia secreta, no es necesario prueba de un nexo real. Además, de acuerdo a dicha ley, el particular o empresa que comunica la información al FBI

[28] En España el Tribunal Supremo aplica a los delitos informáticos «el principio de ubicuidad» con arreglo al cual son competentes cualquiera órganos territoriales de los lugares donde se cometieron actos ejecutivos del delito. SSTS de 17 de marzo de 2005 y de 12 de julio de 2009. Acuerdo no jurisdiccional del Pleno de la Sala 2ª del Tribunal Supremo de fecha 3 de febrero de 2005.

después de haberse emitido la orden judicial no puede ser objeto de demanda por daños y perjuicios. Esta controvertida ley se estableció como lucha contra el terrorismo (ahora ciberterrorismo). Ello provoca seria preocupación dada la posible vulnerabilidad de los derechos de privacidad de los ciudadanos y sociedades españolas. Imaginemos el supuesto de una empresa española que subcontrata servicios de un proveedor americano encontrándose las bases de datos en Estados Unidos, por ejemplo un banco[29].

Los supuestos son muchos, y no es la finalidad del presente trabajo detenernos en cada uno de ellos, aunque sí señalar que existe una nueva realidad jurídica creada por las Tecnologías de la Información y Comunicación (TIC) que ha hecho replantear conceptos, relaciones jurídicas y proceso y que requieren de una nueva perspectiva y regulación. Frente a ello en general la actividad legislativa avanza pero con lentitud frente a la rapidez de evolución de las TIC, y a veces la unificación y colaboración entre países no es fácil dadas las diferentes legislaciones existentes. La lentitud de los procesos de reforma legislativa y de colaboración entre países, su complejidad y procedimiento, ha supuesto que muchas voces apuesten por la autorregulación de los operadores y buenos usos, y sobre todo por una normativa no encorsetada.

1.3 La administración y el desarrollo tecnológico

España inició en marzo de 2012 la elaboración de una Agenda Digital con el objetivo de establecer las líneas de actuación prioritarias en el sector de las tecnologías de la información y las Comunicaciones (TIC) para los próximos años. La finalidad es utilizar la oferta de redes, servicios y aplicaciones digitales de forma que contribuyan a la mejora de la competitividad de las empresas, a la generación de empleo de mayor calidad y a la prestación más eficiente y eficaz de los servicios públicos. En paralelo a este proceso de recepción de ideas y propuestas para la Agenda Digital para España, se constituyó el 22 de marzo de 2012, el Grupo de Expertos de Alto Nivel, formado por profesionales del sector con amplia experiencia y con capacidad de aportar una visión estratégica y a largo plazo y que emitió el 22 de junio de 2012 el «Informe de recomendaciones del Grupo de Expertos de Alto Nivel para la Agenda Digital para España»[30].

[29] Véase sobre este punto LECOURS, ALAIN P., *Usa Patriot Act. Efectos extraterritoriales de la Ley Patriota de los EEUU. Derechos de Privacidad de los ciudadanos norteamericanos*, La Crónica Jurídica. Puede consultarse en la dirección http//goo.gl/w24Xi.

[30] *Informe de recomendaciones del Grupo de Expertos de Alto Nivel para la Agenda Digital para España*. Ministerio de Industria, Energía y Turismo. Gobierno de España. Puede consultarse en la página electrónica goo.gl/aCg9C. Página visitada en fecha 19.07.12.

En el anterior informe se enumeran seis objetivos principales: 1. Fomentar el despliegue de redes y servicios para garantizar la conectividad digital; 2. Desarrollar la economía digital para el crecimiento, la competitividad y la internacionalización de la empresa española; 3. Mejorar la e-Administración y soluciones digitales para una prestación eficiente de los servicios públicos; 4. Garantizar la privacidad, confianza y seguridad en el ámbito digital; 5. Impulsar el Sistema de I+D+i en tecnologías de la Información y las Comunicaciones; y 6. Promover la capacitación para la inclusión digital y la formación de nuevos profesionales TIC.

La eficacia y eficiencia de las Administraciones Públicas incluye una adecuada utilización de las NTIC a través de las cuales se presten servicios públicos y sirvan como medio para relacionarse con ciudadanos y empresas. Se pretende con ello obtener una Administración más productiva y que sea más accesible a los ciudadanos. La Unión Europea en la nueva Agenda Digital para Europa ha establecido como objetivos para 2015 que, al menos, el 50% de los europeos usen la administración electrónica y el 25% envíen los formularios electrónicamente a la hora de realizar trámites con sus Administraciones. En España, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP), reconoció el derecho de los ciudadanos a relacionarse electrónicamente con las Administraciones, y en esta línea también las actuaciones del Plan Avanza ayudaron a introducir las TIC en servicios públicos como la Educación, la Sanidad y la Justicia. Estas últimas son áreas de la Administración Pública que han incorporado o están incorporando las NTIC de forma más reciente frente a otras como la Administración Tributaria o la Seguridad Social ya veteranas en el uso de estas tecnologías.

La Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP) tiene por finalidad promover el uso de las Tecnologías de la Información y las Comunicaciones en las relaciones entre la Administración Pública y los ciudadanos, y entre las diferentes Administraciones Públicas. En virtud de esta ley los ciudadanos podrán realizar todas sus gestiones administrativas por medios electrónicos, quedando las Administraciones Públicas obligadas a ofrecer sus servicios por Internet, dispositivos móviles, TDT o cualquier medio electrónico futuro. Quedan fuera de dicha Ley las empresas municipales respecto a las cuales no es de aplicación a (art.2.2 LAECSP).

La Guía Práctica de la Ley 11/1997, elaborada por la Comisión de Modernización y Calidad de la Federación Española de Provincias y Municipios (FEMP) [31], señala

[31] La información referente a la LAECSP se ha obtenido de la Guía Práctica de la Ley 11/1997, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP), Comisión de

que se trata de una ley que impone a las Administraciones las relaciones electrónicas, reconociendo el derecho por ley a los ciudadanos a poder relacionarse electrónicamente con las Administraciones Públicas (art. 1 LAECSP). Este reconocimiento explícito de nuevos derechos ciudadanos, se transforma, del lado de los Ayuntamientos y Administraciones Públicas en una declaración de deberes: éstos tienen la obligación de hacer efectivo este derecho. El sentido imperativo de la norma la diferencia de la Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJAP-PAC) que potestativamente dejaba en manos de las Administraciones Públicas determinar si los ciudadanos iban a poder de modo efectivo, o no, relacionarse con medios electrónicos con ellas, según que estas quisieran poner en pie los instrumentos necesarios para esa comunicación, es decir, que se limitó a abrir la posibilidad de establecer relaciones telemáticas con la Administración pero no las impuso. La LAECSP supone que las Administraciones Públicas son, a su vez, también sujetos de derechos, están obligadas a cooperar entre sí, y tienen derecho a que las otras administraciones cooperen. En este sentido, destaca el derecho de los ciudadanos a «*no aportar los datos y documentos que obren en poder de las administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información (…)*», garantizando el derecho de las administraciones a exigir entre si el suministro electrónico de dicha información.

El Real Decreto, de 27 de enero de 2009, Reglamento de la LAECSP, viene a desarrollarla, siendo el complemento necesario para conseguir la efectiva realización de los derechos regulados en la Ley de Acceso Electrónico, facilitándolos en la medida que lo permitan las nuevas tecnologías y garantizando que no resulten afectados derechos constitucionales, como la protección de datos[32], los derechos de acceso a la información administrativa o la preservación de intereses de terceros. Dicho Real Decreto establece un marco muy flexible para la implantación de las vías de comunicación de las administraciones con los ciudadanos, cuidando los niveles de seguridad y protección de derechos e intereses previstos tanto en la propia Ley 11/2007 como en la legislación administrativa en general. Asimismo, desarrolla la

Modernización y Calidad de la Federación Española de Provincias y Municipios (FEMP). Puede consultarse en la dirección electrónica http://goo.gl/l1MFCd.

[32] Véase al efecto la Recomendación 2/2008, de 25 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre publicación de datos personales en boletines y diarios oficiales en Internet, en sitios web institucionales y otros medios electrónicos y telemáticos; la Recomendación 3/2008, de 30 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre tratamiento de datos de carácter personal en servicios de administración electrónica; o la Recomendación 1/2008, de 15 de abril, elaborada por la Agencia Catalana de Protección de Datos.

identificación y firma electrónica, los registros, notificaciones y comunicaciones electrónicas y la regulación detallada de documentos y expedientes administrativos electrónicos, así como los elementos necesarios para evitar la solicitud a los ciudadanos de documentos que ya obran en poder de las administraciones públicas, entre otros aspectos.

En resumen, los ciudadanos tienen en relación con la utilización de los medios electrónicos en la actividad administrativa, y en los términos previstos en la Ley, un conjunto de derechos complementarios tales como: Acceso electrónico; elegir, entre aquellos que en cada momento se encuentren disponibles, el canal a través del cual relacionarse por medios electrónicos con las Administraciones Públicas; no aportar documentación que obre en poder de las Administraciones Públicas; la igualdad en el acceso electrónico a los servicios de las Administraciones Públicas; acceder por medios electrónicos a la información de los expedientes; obtener copias electrónicas; usar firma electrónica como medio de identificación y presentación de la documentación; la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas; calidad de los servicios públicos prestados por medios electrónicos; y a utilizar estándares abiertos para comunicarse con las Administraciones Públicas (art. 6 LAECSP).

Por otro lado, las Administraciones Públicas tienen en relación con la utilización de los medios electrónicos en la actividad administrativa, y en los términos previstos en la Ley, las siguientes obligaciones: Fomentar múltiples canales de acceso a la información; asegurar la inoperabilidad organizativa, semántica y técnica; validez documental y de gestión de la copia electrónica; herramientas de consulta del expediente electrónico; admitir el DNI-e y demás sistemas de firma electrónica; estrategia documental y repositorio unificado de documentos; cumplimiento de la LOPD; medir la calidad de los servicios prestados; disponibilidad 24x7; calidad de los servicios públicos prestados por medios electrónicos; y compatibilidad con los diferentes navegadores y formatos[33].

La Guía Práctica de la Ley 11/1997, desarrollada para el cumplimiento de la LAECSP, define diferentes áreas de actuación sobre las que se deben poner en marcha las medidas para adaptarse a la Ley, entre las que encontramos: Fomentar múltiples canales de acceso a la información; adaptación de los canales de comunicación, habilitando los medios necesarios para la prestación de Servicios Públicos Digitales a los ciudadanos (art. 8.1); adaptación de

[33] Guía Práctica de la Ley 11/1997, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP), la Comisión de Modernización y Calidad de la Federación Española de Provincias y Municipios (FEMP). Puede consultarse este artículo en la dirección electrónica http://goo.gl/l1MFCd, págs.16 a 22.

procedimientos administrativos a la tramitación electrónica, adaptación de los trámites de los procedimientos administrativos que se inician a instancia de parte y, que deben ser transformados en Servicios Públicos Electrónicos y facilitarse por medios telemáticos a los ciudadanos (art. 9 y 10 y Disposición Final Tercera); adaptación a la tecnología de Front- Office, entendido como la tecnología específica de soporte a los procesos internos de la Administración Electrónica y que deberá permitir la comunicación entre ciudadanos y Administración –sistemas informáticos para el soporte de páginas Web, registro telemático, consulta de expedientes, pago telemático etc. (art. 10); adaptación de la Tecnología de Back-Office o Sistema de Gestión Integral (SGI), adaptando la tecnología de soporte a los procesos internos de la Administración y su integración con el Front-Office, entendiendo por Back-Office todos aquellos sistemas internos que permitan la gestión informatizada de la actuación administrativa (sistemas de gestión de expedientes, contabilidad, bases de datos del padrón etc.); adaptación organizativa, incluyéndose en este punto aquellas medidas reflejadas en la Ley que afectan a la estructura organizativa de las entidades Locales, las cuales necesitan ser adaptadas a la hora de prestar servicios de Administración Electrónica a la ciudadanía (art. 22.3), por ejemplo, la institución obligada de un Registro de Funcionarios públicos habilitados para que dichos funcionarios puedan realizar válidamente, mediante el uso del sistema de firma electrónica del que hayan sido dotados, la identificación y autenticación de los ciudadanos que no dispongan de algunos de los instrumentos previstos en el artículo 13 de la LAECSP, para la realización de cualquier operación por medios electrónicos; y adaptación normativa, es decir, las Entidades Locales deberán instrumentar actuaciones de carácter reglamentario, normando las condiciones, las garantías, y los efectos jurídicos de los Servicios Públicos Electrónicos en las relaciones con los ciudadanos, dando de esta manera plena seguridad jurídica a estos servicios (art. 10.3)[34].

Las TIC deben incorporarse también para facilitar el desarrollo de la economía[35]. En el Informe de recomendaciones del Grupo de Expertos de Alto Nivel para la Agenda Digital para España se señala que para facilitar el funcionamiento ágil y dinámico de la economía se deberá impulsar la realización de actos mercantiles inmediatos entre empresas y ciudadanos. Para ello será necesario integrar en

[34] Puede consultarse la Guía Práctica de la Ley 11/1997, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP), la Comisión de Modernización y Calidad de la Federación Española de Provincias y Municipios (FEMP), pág. 23. Este artículo se halla disponible en la dirección electrónica http://goo.gl/l1MFCd.

[35] La estrategia «Europa20» de la Comisión europea incluye entre sus prioridades el desarrollo de una economía basada en el conocimiento y la innovación que haga un uso más eficaz de los recursos, siendo la digitalización y automatización de procesos administrativos un factor clave en la mejora de la productividad de la economía.

plataformas tecnológicas digitales en línea y tiempo real, los fedatarios públicos, el Registro Mercantil (unificado a nivel nacional), así como Hacienda. Se trata de permitir la incorporación de procesos inmediatos en la contratación entre personas físicas y jurídicas, con repercusión económica y que eviten trámites y demoras innecesarias e inaceptables. Las TIC pueden y deben permitir la eficacia manteniendo las necesidades jurídicas[36].

La Administración de Justicia tampoco ha quedado al margen de las TIC, elaborándose el Plan de Modernización de la Justicia 2009/2012, que recoge medidas organizativas, procedimentales y relacionadas con el uso de la tecnología y prevé el acceso a los profesionales de forma telemática a la información de los asuntos de la Oficina judicial de manera actualizada, personalizada y con un máximo nivel de seguridad. El Informe actual de expertos, sin embargo recomienda la corrección de desajustes detectados en su implementación. Podemos destacar el programa de actuación 4.1, cuyo objeto es continuar implementando el plan de transparencia judicial del Ministerio de Justicia, incrementando los niveles de acceso de los ciudadanos a la información. Se desarrollan para ello actuaciones encomendadas específicamente tanto a producir como a publicar información acerca de la actuación del Ministerio, así como a garantizar el acceso a los ciudadanos a toda la información relevante relativa a la Administración de Justicia.

En el ámbito judicial español se ha previsto el sistema Lexnet por Acuerdo de 28 de septiembre de 2005 del Pleno del Consejo General del Poder Judicial y regulado por RD 84/2007, de 26 de enero, BOE de 13 de febrero de 2007: «Sobre implantación en la Administración de Justicia del sistema informático de telecomunicaciones Lexnet para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos». Se define como «*una plataforma tecnológica que permite la remisión y recepción de escritos y documentos procesales, basada en un sistema de correo electrónico seguro, mediante el empleo de la firma electrónica reconocida*»[37]. Ahora bien son conocidas las dificultades de implantación de este sistema, en gran parte debido a la utilización de distintas sistemas técnicos en las CCAA y la falta de medios.

---

[36] Este tema puede consultarse en el «Informe de recomendaciones del Grupo de Expertos de Alto Nivel para la Agenda Digital para España». Ministerio de Industria, Energía y Turismo. Gobierno de España, pág. 42. Disponible en la dirección electrónica goo.gl/aCg9C. Página visitada el 19.07.12.

[37] Véase DE HOYOS SANCHO, M.*, Hacia un proceso civil más eficiente: Comunicaciones telemáticas. El sistema "Lexnet"*, en "Oralidad y escritura en un proceso civil eficiente", Vol. II, ob. cit., pág.94.

Entre las funcionalidades del sistema Lexnet, y según se recoge en el Anexo V del RD 84/2007, se encuentra la del traslado de copias de escritos y documentos, al órgano jurisdiccional y a los Procuradores personados, de tal manera que quede constancia en las misma copias de la fecha y hora en que se ha realizado el traslado. El sistema Lexnet ha sido creado y desarrollado por el Ministerio de Justicia y se implementa en las Oficinas Judiciales correspondientes al ámbito de actuación del Ministerio de Justicia, siquiera se han firmado también convenios de cooperación tecnológica entre el Ministerio de Justicia y las Comunidades Autónomas con competencias asumidas en materia de Justicia. En fecha 4 de octubre de 2005 con la Generalitat Valenciana (BOE núm. 278, de 21 de noviembre); en fecha 5 de mayo de 2006 con la Generalitat de Cataluña (BOE núm. 151, de 26 de junio) y en fecha 20 de diciembre con la Xunta de Galicia (BOE núm. 29, de 2 de febrero).

En último lugar, señalar que en aplicación del mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP), de imponer las relaciones electrónicas con los ciudadanos el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica estableció en su disposición adicional primera, el desarrollo de una serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas. Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad. Todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica. Dentro de este conjunto de Normas Técnicas de Interoperabilidad, las normas relativas al documento electrónico, al expediente electrónico, a la digitalización de documentos en soporte papel, a los procedimientos de copiado auténtico y conversión y a la política de gestión de documentos electrónicos responden a lo previsto en el citado Real Decreto 4/2010, de 8 de enero, sobre interoperabilidad, recuperación y conservación del documento electrónico, a la luz de la necesidad de garantizar todos estos aspectos para el documento electrónico a lo largo del tiempo.

1.4 Tecnología y seguridad informática en la empresa

La inversión en tecnología por parte de las empresas y su conexión con los servicios tecnológicos que brinda internet las convierte en empresas más eficaces y con mejores resultados. Dicha inversión no solo implica dotar a las empresas de mayor eficacia, es decir, contar con una mejor gestión y organización, sino que también puede ir destinada a lograr crecimiento y expansión empresarial (por ejemplo inversión tecnológica basada en el cliente o exportación). La implantación de las TIC en el ámbito empresarial junto a las oportunidades que brinda internet implica la transformación del sistema productivo y la creación de nuevas formas de negocio. A nivel de mercado, las soluciones de Business Intelligence (BI), por ejemplo, se plantean en la actualidad como un proceso continuo de cambio de la cultura empresarial y no ya como un proyecto TIC. No obstante, la mediana y gran empresa española todavía es reacia a la implantación de este tipo de planteamientos empresariales. Algunas tendencias como Big Data o Social Analytics son todavía percibidas como algo lejano, y la proclividad a la inversión para estos propósitos es todavía baja[38].

El ahorro de costes es uno de los objetivos en tiempos de crisis que prima en la empresa española. En este sentido existe una tendencia al alza a la implantación de sistemas como, el «cloud computing» o «informática en la nube» que ofrece servicios de computación a través de la red pagando sólo por el consumo. La nube permite el uso de aplicaciones en un servidor web con acceso a Internet y facilita el acceso a documentos, correo electrónico, servicios telemáticos, desde cualquier lugar y plataforma. Es decir, la contratación por parte de las empresas de los servicios *cloud* significa que dichas empresas que tradicionalmente facturaban por licencias ahora lo harán por uso[39]. La contratación del *cloud* supondrá además ahorro de plantilla de profesionales en la empresa[40].

---

[38] Puede consultarse sobre este punto el informe elaborado por Penteo, analista independiente de TIC «Soluciones BI 2014». Información disponible en la página web http://www.penteo.com.

[39] Véase el *informe Cloud Computing en España 2013* elaborado por Penteo. Dicho informe analiza la situación de los servicios Cloud en España su adopción por parte de la empresa española y la oferta que existe actualmente de este tipo de servicios en nuestro país. Tras analizar las perspectivas de adopción de servicios Cloud de la mediana y gran empresa española, Penteo concluye que «*el mercado de Cloud computing en España se sitúa entre el primer y segundo estado del «ciclo de adopción tecnológica», con una demanda que comienza a considerar seriamente la inversión en esta tecnología. En concreto, el Cloud computing ha pasado a ocupar el cuarto lugar* –quinto lugar en el informe IT Spending & Priorities de Penteo de 2014 - *en las prioridades de gasto e inversión de los CIO (chief information officer o director de informática y sistemas) españoles. El estudio pone de manifiesto que el Cloud Computing ha empezado a abandonar su carácter de tecnología emergente, a medida que la oferta de servicios empieza a madurar y que la demanda comienza a considerarla entre sus prioridades de gasto e inversión. Todo ello a pesar de estar en un contexto*

Los recursos tecnológicos suponen muchas ventajas pero también inconvenientes que deben preverse por parte de las empresas. Así por ejemplo, en el caso del «cloud computing», si bien supone ventajas como servicios menos costosos, facilidad de integración y rapidez de las aplicaciones, también implica inconvenientes como mayor falta de seguridad y vulnerabilidad, en cuanto la información sensible de los negocios no se halla en las instalaciones de las empresas. La información de la empresa en la nube recorre diferentes nodos para llegar a su destino siendo cada uno de ellos y sus canales un foco de inseguridad, si se usan protocolos seguros como HTPPS la velocidad disminuye debido a la sobrecarga de los mismos. En el «cloud computing» los datos almacenados en la nube se encuentran físicamente en un servidor ubicado en cualquier punto del mundo. Es por ello recomendable que se elijan proveedores de servicios que cumplan las exigencias legales que a nivel nacional y europeo se establecen en protección de datos, así como acceder y conocer el tratamiento que el proveedor va a hacer de los mismos, revisando la jurisdicción y legislación a la que se somete el proveedor del servicio. El trabajo en la nube puede suponer una dificultad en orden a acceder y acreditar un hecho electrónico (una información) que pueda servir de prueba en el proceso. Por lo tanto, será necesario asegurarse de que se dispone de un buen proveedor de servicios que asegure el debido almacenamiento y seguridad de los datos al fin citado[41]. Todo ello, teniendo en cuenta la necesidad de

---

de reducción reiterada de los presupuestos TIC, pero en el que los proveedores llevan tres años de intensa comunicación de estos servicios. La Nube penetra lentamente en la empresa española, que busca agilidad y reducción de costes. El informe Penteo ha analizado también cuáles son las principales barreras de entrada, siendo la seguridad y la ubicación de los datos las que provocan más recelos. Surge también entre los CIO, en este sentido, la preocupación por las dificultades de integración». Información disponible en la página web http://www.penteo.com.

[40] Como indica el Informe «*Las Tecnologías de la Información en la empresa Española 2012*», elaborado por ESADE – Penteo, la contratación de tales servicios afecta también a los departamentos TIC de las empresas, «*La industria de TI bajo el modelo de Cloud Computing necesitará menos profesionales para proveer las tecnologías básicas. Nuestra visión es que, incluso en el contexto de crecimiento de las necesidades TIC, el incremento de la capacidad de los sistemas y la automatización de las tareas de administración y gestión, reducirán las plantillas de profesionales en los proveedores y los Departamentos de Sistemas de las empresas. La virtualización, que tanto éxito ha tenido en nuestros centros de datos, no ha tenido este efecto porque no ha eliminado la necesidad de personal con nuevos conocimientos y responsabilidades. Sin embargo, Cloud supone la automatización de tareas manuales. Así, las funciones de instalación, mantenimiento y administración de sistemas van a verse fuertemente afectados por la nube*». *Las Tecnologías de la Información en la empresa Española 2012*, ESADE – Penteo, págs.12-13. Información disponible en la página web http://www.penteo.com.

[41] Véase la valoración que se efectúa sobre *Cloud Computing* en *Opinion 05/2012 on Cloud Computing*, July 1st 2012. Article 29, Data Protection Working Party. 01037/12/EM WP 196. Disponible en http://goo.gl/ClBpg. Página visitada el 17.09.12.

garantizar los derechos de los ciudadanos respecto a la protección de datos y al deber de confidencialidad[42].

El anterior ejemplo del *cloud* no supone sino la advertencia de que las nuevas tecnologías en la empresa hacen que aparezca la necesidad empresarial de instrumentar sistemas preventivos de seguridad básicamente en dos ámbitos: en primer lugar, respecto a la seguridad de la información de la empresa o de la que dispone ésta (knowhouse, listas de clientes y proveedores, datos web 0.3 etc.) [43]; y en segundo lugar, respecto a la prevención de posibles infracciones, demandas o litigios.

En este mundo caracterizado por la hiperconectividad, es decir, en que todo está conectado, las organizaciones deben preparar su infraestructura con el fin de responder al crecimiento exponencial de conexiones a la par que garantizan su seguridad y la privacidad de sus datos.

---

[42] Es fundamental que empresas y profesionales, principalmente los vinculados al deber de confidencialidad, como por ejemplo los abogados, no incurran en la vulneración de la legislación sobre protección de datos al desarrollar su actividad empleando el sistema de *cloud computing*.

[43] Frente a al fenómeno que se produce con el incremento masivo en el almacenamiento y flujo de datos fruto de la era digital a nivel estructurado, no estructurado, procedente de redes sociales, imágenes, voz y vídeo se propone la tendencia Big Data. «*Big Data es una tendencia de una extraordinaria importancia, no sólo tecnológica, sino corporativa*». «*Según algunas estimaciones, el año 2011 rozamos los dos zettabytes (1 zettabyte = 10 21 bytes) de datos creados en el mundo. Empresas de servicios financieros, fabricantes de productos de consumo, cadenas de distribución e incluso gobiernos se enfrentan a una ola de datos que no pueden capturar, gestionar, ni analizar con las herramientas y plataformas de gestión de la información tradicionales (Business Intelligence, Datawarehouses, etc.). Big Data puede llegar a ser el activo más valioso de una organización siempre y cuando exista un modelo de captura y análisis de la información. Esto depende de las estrategias y soluciones que se pongan en marcha a corto plazo para afrontar el ingente crecimiento del volumen, la complejidad, la diversidad, y la velocidad de los datos, en particular por la proliferación de los datos procedentes de redes sociales. Durante el 2011 se crearon 1,8 zettabytes de datos (18 billones de gigabytes); en la próxima década el número de servidores que gestionan esos datos se multiplicará por 10; cada día se envían en el mundo 294.000 millones de emails; una compañía como Wal-Mart procesa más de un millón de transacciones cada hora y posee bases de datos con una capacidad estimada de 2,5 petabytes. Estos son algunos ejemplos de uno de los retos que espera a las organizaciones en los próximos años: el crecimiento exponencial de los datos corporativos. La era digital ha producido un salto brusco en el volumen, naturaleza y complejidad de los datos. Las redes sociales, los teléfonos inteligentes, el aumento imparable del comercio electrónico… son nuevas fuentes que producen interacciones e información constante que las compañías no se pueden permitir ignorar pero tampoco saben cómo gestionar*». Véase sobre ello *Las Tecnologías de la Información en la empresa Española 2012*, ESADE – Penteo, págs. 20-25. Información disponible en la página web http://www.penteo.com.

A ese fin se produce la necesidad de que las empresas cumplan con la normativa vigente relacionada con esta nueva realidad ya sea para su propia protección o para la de terceros. En este sentido, podemos destacar la normativa sobre protección de datos, normativa sobre contabilidad informática, la obligatoriedad de hacer copias de seguridad, la necesidad de contar con registros de acceso, las normas ISO etc. Por otro lado, la generación, almacenamiento, conservación y gestión de hechos electrónicos por parte de las organizaciones se convierte en objeto principal de regulación y control para aquellas personas jurídicas o entes que pretendan disponer de información con valor probatorio. Los hechos electrónicos deben ser preservados.

La enorme cantidad de información que en la actualidad procesan exige el establecimiento de una política empresarial de protección y de conservación de la información de que dispone la empresa como mecanismo de prevención de posibles quiebras de seguridad que puedan implicar sanciones, litigios o infracciones de los que pueda, eventualmente, responder la «empresa». Resulta indudable la necesidad empresarial de proveerse de un sistema de seguridad de los datos, así como de su conservación a fin de que puedan ser aportados, en caso de litigio, ante los tribunales, mejorando las perspectivas de una acción legal con éxito. Con base al conocimiento de dichos activos de información y el valor que suponen para la organización deberá diseñarse el sistema de seguridad de la misma, una planificación estratégica de los sistemas de información[44].

La contratación de los servicios «cloud computing», la virtualización y las redes sociales que han contribuido al aumento de la productividad también han desdibujado los límites de las organizaciones, que están obligadas, a replantearse sus políticas de seguridad, ya que aumenta el potencial de pérdida de datos y de sufrir un ataque dirigido, que es lo que más preocupa a las empresas. De hecho, los ataques son cada vez más selectivos y dirigidos hacia grupos concretos de usuarios para obtener datos financieros o propiedad intelectual. Actualmente los medios de control y seguridad ya no pueden ceñirse exclusivamente a los «firewalls» y las políticas internas definidas por cada compañía. Es recomendable que la seguridad abarque toda la infraestructura de red, la combinación de aplicaciones y el acceso a los datos- en un entorno cada vez más global. Cambiar las técnicas de protección tradicionales y apostar por una estrategia de defensa adaptativa e interactiva que combine la inteligencia de red con la gestión de políticas, minimizando los tiempos de respuesta frente a las amenazas y que esa respuesta esté

[44] Respecto a dichas políticas de prevención y detección véase ROWLINGSON, Robert, *A Ten Strep Process for Forensic Readiness,* International Journal od Digital Evidence, V.2 I. 3, 2004, disponible en la dirección electrónica www.ijde.org.

automatizada. Las soluciones de seguridad más indicadas son las que integran tres requisitos fundamentales: estrategia adaptativa, análisis de las amenazas global y en tiempo real y respuesta automatizada. Y todas ellas tienen un denominador común: la inteligencia de red. En lugar de intentar garantizar la seguridad a nivel de dispositivo, todos los objetos conectados a la red se beneficiarán de la seguridad inherente a la propia red. «*En un futuro más cercano de lo que pensamos, las redes programables contarán con funciones de detección de amenazas y mitigación automáticas que mejorarán la fiabilidad y seguridad de red como un todo, reemplazando a las arquitecturas tradicionales enfocadas en blindar dispositivos individuales como switches, routers, balanceadores de carga, firewalls de próxima generación o sistemas avanzados de prevención de intrusiones. El Internet of Everything es un fenómeno imparable, por lo que empresas y Administraciones deben empezar a adoptar hoy las tecnologías de seguridad del mañana, basadas en una red más inteligente, programable y automatizada*»[45].

Resulta indudable la necesidad de adoptar a nivel empresarial soluciones adecuadas a nivel preventivo que aseguren la prueba del hecho electrónico en el proceso en el supuesto de una demanda judicial, asegurando el menor coste económico como de imagen de la empresa (pérdida del litigio, paralización de la actividad por investigación forense, demandas en cascada, cotización en bolsa etc.). Sin embargo, es evidente que desde el punto de vista empresarial cada organización deberá valorar y ponderar los costes temporales y en dinero de la implantación de sistemas de seguridad de la información frente al coste de fallos de seguridad y probabilidad de que ocurran.

En todo caso debe existir una estrategia o análisis previo. Es recomendable que las empresas actúen con anterioridad a la producción de los hechos, es decir, con mayor responsabilidad y adecuadas políticas de prevención y detección, lo que garantiza que en caso de litigio se disponga de todos los medios de prueba necesarios y suficientes disponibles. A ese fin resulta necesaria la implantación de políticas de anticipación al proceso en el ámbito corporativo, individual y global, así como la implantación de un protocolo unificado de investigación forense que dé seguridad a las actuaciones.

Una labor preventiva por parte de la empresa junto a la existencia legal de una normativa procesal suficiente y dotada de claridad que regule la aportación y práctica de la prueba del hecho electrónico en el proceso, tanto a nivel nacional como internacional favorecerá la obtención de mayores y mejores resultados

[45] VARGAS, R. *Hacia un nuevo modelo de seguridad integrada en la red*, LOS EXPERTOS OPINAN, 26 de febrero de 2014. Puede consultarse tal información en la página web http.//ismsforum.es en la sección «noticias».

probatorios, facilitará la labor de los cuerpos y fuerzas de seguridad en el ámbito penal, a la vez que servirá de elemento disuasorio para quienes conozcan de la implantación de los mismos en el ámbito empresarial, principalmente los trabajadores. Se obtienen mayores beneficios empresariales en cuanto se puede minimizar la interrupción en la actividad de las empresas en supuestos de investigación digital, facilitando una investigación rápida y eficaz, y por lo tanto evita costes económicos[46].

En el ámbito anglosajón, se ha desarrollado un campo de conocimiento llamado «*Forensic Readiness*» o «política de anticipación al proceso», con el objeto de desarrollar medidas preventivas que disminuyan costes y mitiguen riesgos a las empresas antes de un potencial evento controvertido o litigio. Se trata del campo de conocimiento que reúne tanto principios de derecho procesal como de tecnología de la información. Todo ello ante el elevado coste de la «Investigación Digital Forense», las dificultades técnicas que pueden haber para recabar y aportar pruebas electrónicas que sean aceptadas en los tribunales como auténticas una vez transcurridos los hechos controvertidos, y las estrategias de las organizaciones para mitigar los riesgos de ser demandadas o denunciadas.

La política de «anticipación al proceso» se fundamenta en el denominado «comportamiento proactivo», que determina la implantación en el ámbito empresarial de protocolos de seguridad tales como: archivos de «*mail*», de *sharepoint*, de clientes, de facturas, y ficheros y contratos catalogados y archivados; identificar a los propietarios de la información del riesgo o «*custodians*», servidores y ubicaciones de datos; recolección y procesamiento regular de datos, para comprobar que la información cumple con la regulación vigente y con las políticas de buena praxis empresarial; evaluación de cumplimiento de las nuevas regulaciones (monitoreo de datos, cumplimiento, políticas contractuales); aplicación de políticas de retención de archivos (no

[46] Existen normas que ayudan a las empresas en esas políticas de prevención y detección. Así en el Proyecto PNE 71505 sobre Tecnologías de La Información (TI), «Sistema de Gestión de Evidencias Electrónicas» (SGEE), tiene por objeto definir el Sistema de Gestión de Evidencias Electrónicas (SGEE), así como los formatos de intercambio y los mecanismos técnicos aplicables para el mantenimiento de confiabilidad (1). Esta norma está dividida en tres partes: Vocabulario y principios generales; buenas prácticas en la gestión de evidencias electrónicas; y formatos y mecanismos técnicos. Engloba: generación, gestión, seguridad, conservación y/o almacenamiento de la evidencia electrónica antes de la adquisición.

La administración de las evidencias electrónicas (o ciclo de vida) o Sistema de Gestión de Evidencias Electrónicas (SGEE), incluye el proceso de generación, almacenamiento, transmisión, recuperación (extracción y exportación), tratamiento (consolidación, agregación, correlación) y comunicación de las evidencias electrónicas. La norma 71505 adopta un enfoque por procesos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora del Sistema de Gestión de Evidencias Electrónicas de una organización.

debe procederse a su borrado en determinado plazo); aplicación de normativa de recursos humanos, propiedad intelectual, áreas de cumplimiento regulado como por ejemplo protección de datos; etiquetado de información y clasificación; cadena de custodia etc. [47].

Las políticas anticipatorias por parte de las empresas se componen, por lo tanto, de elementos «técnicos» y los que podríamos llamar «jurídicos». En primer lugar, dentro de los «elementos técnicos» se encontrarían, por ejemplo, los referidos a los dispositivos de detección, como los «*honeypots*» que pueden proporcionar un aviso de hecho sospechoso en el sistema -cuando se sufre un ataque o una intrusión efectiva toda la actividad queda registrada para poder llevar a cabo un posterior análisis-; o medidas a adoptar para determinar la autenticidad de los documentos electrónicos como la criptografía de sellado de tiempo junto con los productos de red de sincronización pueden ayudar a determinar los hechos ya que, por ejemplo, la fecha y hora de la creación o modificación de un archivo pueden ser fácilmente manipulados y además normalmente los relojes de los ordenadores son inexactos; o el uso de la firma electrónica.

En segundo lugar, hablamos de «elementos jurídicos», que suelen integrarse en los llamados programas de «*Corporate Compliance*» diseñados para cada tipo de negocio[48]. Permiten crear o integrar los protocolos de mecanismos de control ya existentes en cada empresa dándoles una correcta difusión mediante un plan de comunicación eficaz, establecer los mecanismos técnicos de control sobre los trabajadores exigidos por la ley para evitar la responsabilidad penal de las empresas mediante auditorías de sus departamentos, identificar riesgos o

[47] Véase sobre el tema RAMOS ROMEU, F. y CAÑABATE PÉREZ, J. *Los datos digitales en el proceso civil: prevención, producción y autenticación.*, Revista Jurídica de Catalunya. Núm.1-2011, págs.62-63; y PUYOL, DANIEL., *La importancia de estar preparados para cualquier litigio.* Conferencia Online sobre software y soluciones TIC para que los documentos electrónicos e e-mail mantengan valor probatorio. Puede consultarse esta última en la página web Demosdesoftware www, it-latino.net., goo.gl/dTnCn. Página visitada en fecha 19.07.12.

[48] No debemos olvidar que el «compliance» incluye varios niveles de la organización empresarial. En un primer nivel (CMS) se pretende la coordinación de las diferentes áreas de cumplimiento. A continuación en un segundo nivel se encuentran los sistemas específicos que pueden coexistir para diferentes ámbitos de cumplimiento (por ejemplo prevención penal) y, seguidamente, en un tercer nivel, se incluyen los especializados en apartados específicos (por ej. soborno dentro de la prevención penal).

Puede consultarse sobre «corporate compliance»: CASANOVAS YSLA, A., *Legal compliance. Principios de Cumplimiento generalmente aceptados*, ed. Dijusa, Madrid, 2012.

implementar soluciones como canales de denuncia, códigos de conducta o prevención de blanqueo de capitales[49].

En cuanto a la responsabilidad penal de las personas jurídicas debemos hacer hincapié en la relevancia de que las empresas se doten de efectivos sistemas hábiles para prevenir o detectar injustos penales y evitar ser declaradas responsables en un proceso penal conforme a lo previsto en el artículo 31 bis del Código Penal. El tradicional principio «*societas delinquere non potest*» ha dejado de tener aplicación en nuestro ordenamiento jurídico desde la reforma del Código Penal operada por la Ley Orgánica 5/2010, de 22 de junio (artículo 31 bis). El legislador español ha optado por imputar responsabilidad penal a las personas jurídicas desde una doble vertiente: 1. Cuando los delitos sean cometidos por sus representantes legales y administradores de hecho o de derecho; 2. Cuando los delitos sean cometidos por los trabajadores de la empresa, si ésta no ha ejercido sobre ellos el debido control. En ambos casos se requiere que el delito se cometa en nombre y por cuenta de la organización, en su provecho y en el ejercicio de sus actividades sociales[50].

Por otro lado, el pasado 20 de septiembre de 2013, el gobierno aprobó remitir a las Cortes Generales, para que inicie su tramitación parlamentaria el proyecto de ley orgánica por el que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, de fecha 4 de octubre de 2013. Dicho proyecto establece en el art. 31 bis CP como eximente de la responsabilidad penal la implantación de un modelo o sistema de prevención y detección de delitos si se

[49] Respecto a las normas ISO en materia de «compliance» ténganse en cuenta la próxima publicación en el año 2015 de: la norma ISO DIS 19600 CMS, cuyo contenido versa sobre las directrices para disponer de un sistema de gestión de cumplimiento (CMS) que facilite el cumplimiento de las obligaciones derivadas tanto de las normas como de los estándares voluntarios (industriales o sectoriales); y la norma ISO WD 37001 ABMS relativa a los requisitos de cumplimiento obligado para obtener una certificación de un sistema para la prevención y detección del soborno. Ambas normas contienen modelos de gestión aplicados al ámbito del cumplimiento.

[50] Véase sobre este tema la Circular de la Fiscalía del Estado 1/2011, relativa a la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica número 5/2010.

ha llevado a cabo con anterioridad a la comisión del delito[51]. En dicho precepto detalla también aquellas medidas de prevención y control que deben adoptarse

[51] El apartado vigésimo del proyecto de reforma modifica el artículo 31 bis, que queda redactado como sigue: «*1. En los supuestos previstos en este Código, las personas jurídicas serán penalmente responsables: a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma; b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso.*

2. Si el delito fuere cometido por las personas indicadas en la letra a) del apartado anterior, la persona jurídica quedará exenta de responsabilidad si se cumplen las siguientes condiciones: 1.ª) el órgano de administración ha adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza; 2.ª) la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado ha sido confiado a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control; 3.ª) los autores individuales han cometido el delito eludiendo fraudulentamente los modelos de organización y de prevención, y; 4.ª) no se ha producido una omisión o un ejercicio insuficiente de sus funciones de supervisión, vigilancia y control por parte del órgano al que se refiere la letra b). En los casos en los que las anteriores circunstancias solamente puedan ser objeto de acreditación parcial, esta circunstancia será valorada a los efectos de atenuación de la pena.

3. En las personas jurídicas de pequeñas dimensiones, las funciones de supervisión a que se refiere la condición 2ª del apartado 2 podrán ser asumidas directamente por el órgano de administración. A estos efectos, son personas jurídicas de pequeñas dimensiones aquéllas que, según la legislación aplicable, estén autorizadas a presentar cuenta de pérdidas y ganancias abreviada.

4. Si el delito fuera cometido por las personas indicadas en la letra b) del apartado 1, la persona jurídica quedará exenta de responsabilidad si, antes de la comisión del delito, ha adoptado y ejecutado eficazmente un modelo de organización y gestión que resulte adecuado para prevenir delitos de la naturaleza del que fue cometido. En este caso resultará igualmente aplicable lo dispuesto en el párrafo segundo del número 2 de este artículo.

para prevenir la comisión de comportamientos delictivos por parte de la empresa (o sus administradores, representantes o empleados). Asimismo, introduce un nuevo apartado seis en el artículo 286 CP en el que regula un nuevo delito castigando al representante legal o de hecho que omita la adopción de las medidas de vigilancia o control exigibles[52].

La empresa debe establecer mecanismos de prevención y detección eficaces y cumplir con la normativa existente a todos los niveles. Así, desde la referida a la protección de datos como a la que rige en orden a la reclamación judicial. A ese fin resultan imprescindibles las políticas de uso de los sistemas informáticos de la empresa incluyendo en este ámbito las normas sobre tratamiento de datos personales, sobre posibilidad de inspección de e-mail y sobre monitorización

---

5 .Los modelos de organización y gestión a que se refieren la condición 1ª del apartado 2 y el apartado anterior, deberán cumplir los siguientes requisitos: 1. Identificarán las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos (evaluación del riesgo*); 2. Establecerán los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos* (código ético o de comportamiento corporativo*); 3. Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos; 4. Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención (*whistle blowers*); 5. Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo. organización, así como el tipo de actividades que se llevan a cabo, garanticen el desarrollo de su actividad conforme a la Ley y permitan la detección rápida y prevención de situaciones de riesgo, y requerirá, en todo caso: a) de una verificación periódica del mismo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios; y b) de un sistema disciplinario que sancione adecuadamente las infracciones de las medidas de control y organización establecidas en el modelo de prevención.»*

[52] El proyecto de reforma del Código Penal introduce en su apartado centésimo octogésimo segundo dentro de la nueva sección cuarta bis del capítulo XI del título XIII, un nuevo artículo 286 seis, con la siguiente redacción: «*1. Será castigado con pena de prisión de tres meses a un año o multa de doce a veinticuatro meses, e inhabilitación especial para el ejercicio de la industria o comercio por tiempo de seis meses a dos años en todo caso, el representante legal o administrador de hecho o de derecho de cualquier persona jurídica o empresa, organización o entidad que carezca de personalidad jurídica, que omita la adopción de las medidas de vigilancia o control que resultan exigibles para evitar la infracción de deberes o conductas peligrosas tipificadas como delito, cuando se dé inicio a la ejecución de una de esas conductas ilícitas que habría sido evitada o, al menos, seriamente dificultada, si se hubiera empleado la diligencia debida. Dentro de estas medidas de vigilancia y control se incluye la contratación, selección cuidadosa y responsable, y vigilancia del personal de inspección y control y, en general, las expresadas en los apartados 2 y 3 del artículo 31 bis.//2. Si el delito hubiera sido cometido por imprudencia se impondrá la pena de multa de tres a seis meses.//3. No podrá imponerse una pena más grave que la prevista para el delito que debió haber sido impedido u obstaculizado por las medidas de vigilancia y control omitidas.»*

del PC e Internet[53] y la creación de Departamentos de Seguridad distintos del de Auditoria[54] que realicen los seguimientos y los documenten. A tal efecto resulta fundamental en la empresa la figura del responsable de cumplimiento normativo o *Chief Compliance Officer* (CCO) o de un órgano colegiado de cumplimiento normativo o *compliance committee*, si bien en las pequeñas empresas (esto es, las que estén autorizadas a presentar cuenta de pérdidas y ganancias abreviada) esta función la puede desempeñar el órgano de administración[55]. Dichos departamentos y protocolos asegurarán la exención de responsabilidad penal de la empresa y, en su caso, una prueba lícita en cualquier proceso y de menor coste para la empresa. Se producirá una detección inmediata del hecho siguiéndose los protocolos existentes y asegurando la prueba, lo cual evitará la necesidad de una costosa investigación forense, evitándose que debido a la volatilidad del hecho electrónico desaparezca la evidencia. Y de existir las normas de uso con información al trabajador, la empresa asegura la licitud de la prueba en el proceso[56].

La carencia de departamentos específicos de seguimiento y documentación y de normas empresariales de uso informático dificulta la intervención directa de

[53] Como veremos en el § 4.1.2.2 resulta fundamental para la licitud de la prueba obtenida a partir de tales procedimientos la información previa a los trabajadores sobre las políticas empresariales de uso de medios corporativos como el ordenador o móvil de empresa.

[54] *«En términos generales podemos definir la auditoría como un examen crítico y «preventivo» que se realiza con el fin de evaluar la eficacia, eficiencia o grado de cumplimiento respecto a un estándar, de un departamento, un organismo, una entidad etc. La auditoría informática es el examen y validación de los elementos, controles y procedimientos utilizados por el área informática, a fin de verificar: La garantía de continuidad de servicio; la confidencialidad de la información; la seguridad de la información; la integridad y coherencia de la información; el cumplimiento de la normativa vigente; el cumplimiento de la normativa interna; y la gestión eficaz de los recursos humanos y técnicos*». Su labor no es de «investigación» sino de «verificación» o «prevención». MARTÍNEZ DE CARVAJAL HEDRICH, Ernesto. *Informática Forense, 44 casos reales.* Julio 2012. págs. 17-19.

[55] Véase CASANOVAS ISLA, A., *Legal compliance,* ob. cit., págs. 203-219.

[56] Así la STC de 26 de septiembre de 2007 (Ponente: D. Aurelio Desdentado) establece que el control de los dispositivos electrónicos sólo será lícito si se ha informado previamente a los trabajadores de la política de uso de los elementos informáticos. Por ello, de no disponerse de protocolos deberá seguirse un proceso de máxima transparencia cumpliendo con todas las garantías de legalidad: efectuarse la intervención en presencia del trabajador, notario, técnico-perito y testigos, solicitar el consentimiento del trabajador, obtener el disco duro ante el notario y efectuarle entrega, depositar el ordenador del trabajador en la notaria o bajo precinto, depositar el disco duro en la notaría y trasladar la copia al laboratorio, garantizando en todo el proceso la cadena de custodia con todas las garantías de integridad.

dichos equipos para la obtención de copias del mailbox, de logs[57], de directorios del servidor o del PC del trabajador, cuando resulta necesaria en procesos judiciales tanto de ámbito laboral, civil o mercantil. Efectivamente, pueden darse problemas de dificultad probatoria del hecho electrónico en un supuesto de litigio. Así, por ejemplo, puede ser difícil probar una transacción comercial sin firma electrónica, sin copia archivada de una factura electrónica o listado electrónico de clientes, o sin copias de los archivos íntegros que acompañan un mail y guardado de todos los datos de encabezamiento de este último. Sin embargo, todavía existen muchas empresas en España que desconocen la tecnología forense en nuestro país, a pesar de que este procedimiento puede ser crucial para probar delitos como el fraude, la corrupción o el robo de información[58]. Tampoco existen protocolos unificados de investigación informática-forense, ni una regulación clara y completa que determine los requisitos necesarios para la presentación de evidencias electrónicas en los juzgados.

Frente a la política de anticipación al proceso, la empresa que no haya adoptado tales medidas de prevención, ante a una controversia o litigio adoptará un comportamiento «reactivo» al mismo. Se trata de aquellos supuestos en que la empresa actúa una vez han tenido lugar la controversia o

---

[57] La definición de *log* puede hallarse en el Oxford Dictionary como el registro oficial de eventos durante un periodo de tiempo en particular. Para los profesionales en seguridad informática un log es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (*who, what, when, where y why, W5*) un evento ocurre para un dispositivo en particular o aplicación. Si un *log* tiene la capacidad de registrar los eventos W5 entonces el propósito de un *log* es proveer a los profesionales de seguridad informática la habilidad de monitorear las actividades de la aplicación o dispositivo. Revisando las salidas de los archivos de *logs,* se puede obtener una buena oportunidad para determinar los eventos W5, y tomar la acción necesaria para corregir el problema o iniciar una investigación en caso de un incidente de seguridad.

Un *log* es un registro de actividad de un sistema, que generalmente se guarda en un fichero de texto, al que se le van añadiendo líneas a medida que se realizan acciones sobre el sistema. Se utiliza en muchos casos distintos, para guardar información sobre la actividad de sistemas variados. Tal vez su uso más inmediato en las actividades realizadas por desarrolladores del web sería el *log* de accesos al servidor web, que analizado da información del tráfico de un sitio. Cualquier servidor web dispone de un *log* con los accesos, pero además, suelen disponer de otros *log,* por ejemplo, de errores. Los sistemas operativos también suelen trabajar con *logs*, por ejemplo para guardar incidencias, accesos de usuarios etc. A través de los *log* se puede encontrar información para detectar posibles problemas en caso de que no funcione algún sistema como debiera o se haya producido una incidencia de seguridad. Información obtenida de la página web WIKILEARNING, puede consultarse en la siguiente dirección electrónica goo.gl/99cqw, página visitada el 19.07.12.

[58] Herramientas como «*text mining*» o «*IBM content analytic*» se utilizan en grandes empresas para poder prevenir el fraude y la corrupción. Estos software les ayudan a acceder, agregar, analizar y explorar visualmente grandes volúmenes de contenido no estructurado para desbloquear nueva información empresarial.

litigio y no con anterioridad al mismo. En este caso se procederá a identificar, preservar, recolectar, procesar, revisar, analizar y preparar para llevar ante un tribunal, realizando una investigación informático-forense posterior a la controversia. Ello supone un evidente incremento del coste para la empresa debido a la necesidad de llevar a cabo dicha investigación y una mayor dificultad en probar el hecho electrónico debido a los rasgos característicos del mismo.

Lo anterior no obsta a que cada empresa deba efectuar un análisis estratégico previo atendiendo a sus propias necesidades, y no acudir sin ningún planteamiento previo a un planteamiento defensivo o reactivo. Como señala MARTÍN LLORENTE la seguridad no es un problema tecnológico sino estratégico, «*es un error pensar en seguridad desde una perspectiva tecnológica. La instalación de tecnologías de seguridad debe ser un modo de implantar unas políticas de seguridad definidas en el modelo de seguridad guiado por los procesos de la organización*». Es decir, primero análisis de riesgos y definición de planes estratégicos y después aplicación tecnológica basada en la primera. La planificación de un modelo de seguridad es una herramienta que permite tomar decisiones, «*lo importante es poder contar con una herramienta de toma de decisiones que nos abstraiga tanto de la evolución tecnológica como de la creciente variedad de tipos de ataques*»[59].

* * *

[59] Véase la ponencia de MARTÍN LLORENTE, Ignacio (catedrático de la Facultad de Informática en la Universidad Complutense de Madrid), titulada *Modelo orientado a procesos para la toma de decisiones sobre seguridad en tecnologías de la información dentro de una organización*, Ponencia III, XX Seminario Duque de Ahumada. Puede consultarse en la página web con la siguiente dirección electrónica portal.uned.es.

CAPÍTULO II.- INVESTIGACIÓN Y PERICIA INFORMÁTICA.

2.1 Introducción

Uno de los aspectos de mayor interés en materia de prueba electrónica es el de la investigación del hecho electrónico. Es decir, el de la averiguación de aquellos hechos del mundo electrónico-digital que posteriormente van a ser objeto de prueba en el proceso. En este punto cabe destacar la necesidad de distinguir entre investigación y prueba del hecho. «Investigar» en palabras de MUÑOZ SABATE, es como abrir una puerta para descubrir lo que hay dentro[60]; mientras que «Probar», desde mi punto de vista, consiste en acreditar la existencia del hecho partiendo de que ese hecho existe. La investigación equivale a la búsqueda de conocimientos acerca de cómo ocurrió un determinado hecho, mientras que la prueba equivale al desarrollo de los medios pertinentes para trasladar su evidencia al proceso. Tratándose de hecho electrónico la prueba sobre el mismo versará sobre su naturaleza, componentes y efectos.

La investigación y la prueba no son dos operativas aisladas sino que guardan una completa sinergia. Así, por ejemplo, cuando en un proceso se solicita como prueba un informe a la Agencia Tributaria acerca de los ingresos o estado de fortuna del alimentista para fijar así la pensión que le corresponde pagar al alimentario, en este caso, la investigación ofrece un resultado fáctico que en muchos casos no precisará de mayor análisis técnico, de modo que el hecho, por sí, tal y como resulta de la investigación podrá ser propuesto como prueba y, en su caso, fundar la sentencia[61]. En otros casos, probablemente más numerosos, los hechos hallados en la actividad de investigación deban pasar por otra actividad antes de poder incorporarse como prueba al proceso. Nos referimos al análisis pericial de los hechos, mediante el cual se dictaminará sobre distintos aspectos del hecho partiendo de la necesidad de aplicar criterios científicos y técnicos que son los que justifican la necesidad de la pericia. Efectivamente no cabe practicar pericia sobre hechos «notorios» o «naturales» para cuya explicación y entendimiento no sean necesarios aquélla clase de conocimientos.

---

[60] Véase MUÑOZ SABATÉ, Lluís. *Introducción a la probática*. Serie Manuales y Monografías. núm. 1, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch. pág. 23; y del mismo autor, *Curso sobre Probática Judicial*, ed. La ley, Madrid, 2009, pág. 23.

[61] Véase MUÑOZ SABATÉ, Lluís. *Introducción a la probática*. Serie Manuales y Monografías. núm. 1, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, págs. 24-25; y MUÑOZ SABATE, LLuís. *Fundamentos de prueba judicial civil. LEC 14/2000*. Ed. Bosch, 2001. págs. 41- 45.

En el ámbito de la informática forense pueden darse distintas situaciones. En algunos casos, la investigación de los hechos permite obtener resultados «utilizables» directamente sin mayor actividad pericial y procesal. Así sucede en el caso de que el actor afirme haber recibido un e-mail de tal persona en una determinada fecha, y dispone de un papel impreso del mismo, entendemos que el perito podrá investigar en un supuesto de borrado para constatar y verificar tal hecho afirmado utilizando si es necesario herramientas como ENCASE para poder acceder y reconstruir los datos. En este caso, la búsqueda ciega que el perito lleva a cabo no supone la lectura de toda la información para detectar lo relevante para una de las partes sino la utilización de palabras clave que permiten rescatar lo que interesa, si es que no ha sido borrado en la reinstalación. El borrado usual (pues existen otros de bajo nivel que sí eliminan la información) no hace desaparecer los datos, sino que elimina las entradas de los mismos y hace imposible acceder a ellos al romperse el código de entrada al sistema binario, los datos permanecen, pero confundidos e indistinguibles en una enorme cantidad de ceros y unos, de modo que el programa empleado pretende detectar los patrones binarios de ciertas palabras, y una vez detectados, reinterpretar por encima y por debajo hasta reconstruir un texto[62]. En este caso el perito constata y verifica la existencia de un hecho, «fundiéndose» así investigación y pericia que se ofrecen como un resultado único.

En otros casos, la investigación será simplemente la base de una actividad pericial compleja y necesaria. Este es el caso, de informes más complejos como, por ejemplo, aquellos cuyo objeto va desde la reconstrucción o recuperación de un borrado con una mayor dificultad técnica hasta informes cuya finalidad es el hallazgo de hechos, como cuando se encarga una investigación a raíz de unos indicios o sospecha inicial para buscar información (contratos, correos electrónicos, facturación etc.) que permitan con posterioridad fundamentar una demanda. La investigación tiene que ver con la búsqueda y/o determinación del hecho, la pericia con su análisis.

La cuestión que se plantea es si corresponde al perito «investigar» o esa función debe quedar relegada a informes técnicos de expertos posteriormente objeto de dictamen pericial. Desde mi punto de vista deberá estarse al caso concreto, pero nada impide que el perito efectúe una valoración técnica tras efectuar él mismo una previa investigación y determinación del hecho. Lo determinante es que los hechos hallados accedan al proceso como prueba a través del dictamen pericial, cumpliendo con los requisitos de este tipo de prueba. Es decir, lo relevante desde un punto de vista procesal es cómo la parte decide que los

[62] Sentencia Audiencia Provincial de Barcelona, sec. 15ª, A 2-2-2006, nº 46/2006, rec. 711/2005. Pte.: González Navarro, Blas Alberto. Fdo. Jco. 4º.

hechos hallados accedan al proceso, o lo que es lo mismo el medio de prueba a través del cual los introduce.

El empresario que acude a un gabinete técnico de investigación digital alegando que uno de sus empleados está realizando actos de competencia desleal y encarga una investigación en términos generales a dicho gabinete está partiendo de una premisa: la sospecha de actos de competencia desleal. En este caso, el gabinete técnico o experto efectúa una investigación en el sistema informático. Los expertos deben tener conocimientos de investigación forense lo que incluye no sólo conocimientos técnicos sino también jurídicos para no vulnerar derechos constitucionales en su actuación y que los resultados obtenidos y convertidos luego en prueba no puedan ser calificados de ilícitos. En la práctica forense frecuentemente el informe emitido por el experto informático-forense se viene presentando como prueba pericial y quienes lo han emitido declaran como peritos. Lo fundamental es que se ha producido una investigación previa de los hechos, y que cuando éstos han sido identificados se trasladan al proceso junto a una valoración o análisis técnico, siendo presentados como prueba a través del dictamen pericial. El mismo experto actúa en las dos fases: investiga la existencia de hechos que de encontrarlos constituirán hechos fácticos objeto de afirmación en demanda y una vez encontrados constata y verifica los mismos aplicando sus conocimientos técnicos en un dictamen pericial en el que constará también el procedimiento efectuado para tal indagación, dicho dictamen se aportará al proceso como prueba de hechos afirmados por la actora en la demanda.

En aquellos supuestos en que existe investigación pero no análisis técnico de los hechos por parte de profesionales legalmente habilitados –detectives-, dicha investigación accederá al proceso por vía del artículo 265.1.5º como informes de testigos, declarando los investigadores como testigos o, de tener conocimientos técnicos, testigos-peritos[63], se trata en realidad de testificales documentadas[64]. No vemos objeción alguna a que la investigación efectuada por un detective experto en informática-forense pueda acceder al proceso como prueba pericial si se cumplen todos los requisitos requeridos al efecto. En este supuesto carece de relevancia que se trate de un detective legalmente

[63] A favor de la consideración de los detectives privados como testigos-peritos DÍAZ FUENTES, A.- *La prueba en la Ley de Enjuiciamiento Civil,* Ed. Bosch, pág.331; en contra de tal consideración ABEL LLUCH, X. *Derecho Probatorio,* Ed. Bosch, 2012, pág, 679.

[64] En el sector de la investigación privada los profesionales de la investigación habilitados –es decir, los detectives- sostienen que están padeciendo intrusismo profesional por parte de profesionales procedentes de la ingeniería con conocimientos informático-forenses, sosteniendo que sólo ellos pueden llevar a cabo investigación.

habilitado ya que en el proceso actúa y ha sido propuesto como perito por la parte y desempeña la función de perito no la de detective[65].

Por otro lado, la investigación topa con otros problemas en el ámbito civil como el hecho de no disponer de cauces procesales adecuados para que una parte de modo legítimo pueda obtener información que pueda fundar una demanda cuando dicha información se halla en poder de tercero. La investigación del hecho electrónico requiere obtención de información. No existe dificultad en el acceso a dicha información cuando ésta se halla en poder de la parte consultante. Se trataría de aquella información que quien consulta tiene en cualquiera de sus ordenadores u otros dispositivos, o de información pública obtenida a través de Web, siempre que no se requieran claves de ingreso para acceder a la misma. Sin embargo, cuando dicha información se halla en poder de tercero, o para acceder a la misma se requieren claves de acceso privadas será necesaria autorización judicial. En cualquiera de ambos casos se trata de mera «investigación» para el hallazgo de hechos que con posterioridad fundamentaran la demanda, sin perjuicio que dichos informes concretados en los hechos objeto de demanda sean asimismo objeto de dictamen pericial.

La cuestión a resolver en lo referente a la investigación informático-forense es determinar cuáles son los medios que nos brinda la LEC para poder efectuar una investigación dentro del proceso civil. La investigación se ubica de forma natural en la fase de instrucción en el proceso penal que, precisamente, tiene por finalidad esclarecer los hechos que posteriormente serán objeto de prueba. En el proceso civil la investigación de los hechos suele ser, por lo general, una actividad de parte ajena, en gran medida, a la actividad procesal. Efectivamente, en el ámbito civil lo usual será que las partes investiguen los hechos que puedan fundamentar pretensiones procesales por su propia cuenta y, sin colaboración alguna de la parte que en su día pueda ser demandada o del Tribunal. Esto plantea el problema de los límites de la investigación que queda limitada únicamente a aquellos hechos a los que tiene acceso el interesado. De ahí que el Tribunal Supremo haya sido flexible en la concreción de los hechos en la demanda en algunos supuestos como requisito para su posterior prueba procesal[66]. Sin embargo, resulta claro que, en muchas ocasiones, sería de gran

[65] SEGOVIA ARROYA opina que quien esté habilitado por el Ministerio del Interior como detective privado podrá actuar en el marco de un proceso judicial como perito sólo si reúne las condiciones que la LEC establece para esta figura y ha sido designado en tal concepto por el Juez o Tribunal, pudiendo emitir entonces el correspondiente dictamen pericial. Véase SEGOVIA ARROYA, J.A, *¿Es el informe profesional del detective privado equivalente a un dictamen pericial*?, Derecho.com, 15 de febrero de 2003, http://goo.gl/iSHW0q, página visualizada en fecha 6 de octubre de 2013.

[66] Dicha postura flexible por parte del tribunal ante la imposibilidad de la parte de concretar determinados hechos en la demanda para ser objeto de prueba se plasma en la Sentencia del

utilidad poder acceder a sistemas, archivos y/o edificios propiedad de terceros con la finalidad de poder determinar los hechos que pudieran fundar una demanda. A ese fin sirven las diligencias de comprobación de hechos previstas en la Ley de Patentes (artículo 129 a 132), naturalmente limitadas al ámbito específico de la Ley. También, con ámbito general, las diligencias preliminares reguladas en los arts. 256 a 263 LEC. No obstante, la regulación de las diligencias preliminares no permite solicitar y obtener, por ejemplo, investigación informática o técnica sobre hechos a los que no tiene acceso un particular. Es por ello que urge una reforma de la regulación vigente de las diligencias preliminares que en un nuevo apartado permita introducir supuestos de investigación en informática forense, adaptando la regulación de la LEC a las nuevas necesidades procesales dada la evolución de las NTIC. De ese modo la norma procesal general, no las leyes especiales, proporcionaría una vía de «investigación», dando solución de ese modo al problema sobre la admisión de «investigación» en el proceso civil. Véase sobre esta cuestión el § 3.2.2.

El acceso a la información no sólo implica dificultades desde un punto de vista procesal, es decir refiriéndonos a los cauces que brinda la ley para poder obtenerla, sino que también plantea problemas desde un punto de vista técnico-forense en cuanto a la posibilidad de limitar la información a que accedemos y por lo tanto no vulnerar derechos constitucionales como el derecho a la intimidad o a la protección de datos. Es decir, aun cuando existen herramientas de investigación que utilizan los expertos informático-forenses como ENCASE, que limitan por concepto las búsquedas que se efectúan por el experto, éste sigue accediendo a mucha información que no es relevante para el proceso, pero que puede tener un enorme valor fuera del mismo. Me refiero a información confidencial o privilegiada, principalmente en el ámbito corporativo. Información que a menudo se comparte con el cliente. De este modo puede darse el caso en que se utilicen solicitudes de autorización judicial de acceso a cierta información a efectos de fundamentar una posterior demanda cuando en realidad la pretensión de la parte es obtener información sensible o privilegiada, sin ninguna intención de interponer demanda posterior. La solución a ello pasa por el deber de confidencialidad del experto y sanciones o multas coercitivas tanto al experto como al cliente, que impliquen el desistimiento de tales actitudes, ya que si se imponen multas de bajo importe o sanciones leves, el beneficio obtenido a cambio sigue siendo mayor.

Tribunal Supremo de 8 de febrero de 1975: "*la doctrina legal viene afirmando que resulta lógica y frecuente que el arrendador no tenga medio normal de conocer con precisión y detalle las obras que en el interior del local arrendado se hayan verificado en la clandestinidad y no se le puede exigir que al formular la demanda las concrete.* MUÑOZ SABATE, LLuís. *Fundamentos de prueba judicial civil. LEC 1/2000*. Ed. Bosch, 2001, págs. 41- 45.

2.2 La informática forense

La Informática forense fue definida por McKemmish en 1999 como la identificación, conservación, análisis y presentación de pruebas electrónicas o digitales[67]. Tradicionalmente se clasifica atendiendo a su ámbito de actuación en computación forense, forensia en redes, y forensia digital. La «computación forense» (*computer forensics*) se entiende como aquella disciplina de las ciencias forenses que considerando las tareas propias asociadas con la evidencia procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; o como disciplina científica y especializada que entendiendo los elementos propios de las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos.

La «forensia en redes» (*network forensics*) actúa en un escenario más complejo, pues, es necesario comprender la manera en que los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento en particular. Se trata de un profesional que entendiendo las operaciones que las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer rastros, movimientos y acciones que un intruso ha desarrollado para concluir una acción. A diferencia de la definición de computación forense este contexto exige capacidad de correlación de eventos muchas veces disyuntos y aleatorios, que en equipos particulares es poco frecuente. Se trata de capturar, almacenar y analizar eventos de una red para descubrir el origen de un ataque o un posible incidente.

Y finalmente por «forensia digital» (*digital forensics*) se entiende aquella forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (¿Quién?, ¿Cómo?, ¿Dónde?, ¿Cuándo?, y ¿Por qué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las

[67] La definición de McKemmish sobre informática forense se cita por BECKETT, Jason, en Thesis, *Forensic Computing: A Deterministic Model for Validation and Verification through an Ontological Examination of Forensic Functions and Processes*. Adelaide South Australia, January 2010. School of Computer and Information Science. Division of Information Technology, Engineering, and the Environment, University of South Australia, pág. 19.

organizaciones en el contexto de la administración de la seguridad informática[68].

La Ciencia informático-forense desde un punto de vista técnico-científico comprende cualquier principio o técnica que pueda ser aplicada para individualizar, identificar, recuperar, reconstruir o analizar un hecho electrónico. Se trata de una actividad científica de indudable importancia en el proceso, pero que, sin embargo, no es suficientemente conocida y apreciada en el sistema de impartición de justicia. El principal problema que encuentra dicha disciplina y que afecta, como consecuencia, a la valoración que puedan efectuar los tribunales de la prueba pericial informático-forense, probablemente consista en la falta uniformidad y consenso de la comunidad científica tanto sobre el proceso como sobre la validación no solo de los resultados obtenidos sino también de las herramientas y las técnicas utilizadas para obtener la evidencia electrónica[69]. Efectivamente, puede constatarse en la actualidad la existencia de una gran diversidad de herramientas en uso por parte de los expertos en informática forense[70]. Por otro lado, la falta de homogeneización de protocolos de investigación y análisis del hecho electrónico suponen que no siempre la prueba cumpla con plena garantía tanto en su obtención como en su custodia,

---

[68] Las anteriores definiciones se han obtenido del artículo publicado por ZUCCARDI, Giovanni y GUTIÉRREZ, Juan David. *Informática Forense,* Artículo publicado en ECURED. Noviembre de 2006. Puede consultarse dicho artículo en la dirección electrónica http://goo.gl/j1XZu.

[69] Este concepto de calidad y revisión ha sido muy bien desarrollado por países como Estados Unidos (DAUBERT V. MERRELL, DOW PHARMACEUTICALS, 509 U.S. 579 (1993) y FRYE V. UNITED STATES, 293 F.1013 (D.C.Cir. 1923). La prueba de Frye introdujo la prueba de aceptabilidad en el sistema jurídico, es decir, si la metodología en cuestión es generalmente aceptada por la comunidad científica pertinente entonces también sería aceptada por la ley como prueba. Interesante también en CANADÁ RV. JOHNSTON en el que el Juez en un caso de ADN expuso los criterios que determinarían si la evidencia científica es útil para el juez: tasa de potencial error; respeto a las normas; cuidado con las técnicas científicas utilizadas y si son susceptibles de abuso; existencia de relaciones de analogía con otras técnicas científicas que habitualmente se admitieran como prueba; presencia de características a prueba de fallos; cualificación de los expertos; existencia de literatura especializada; novedad de la técnica y aplicación en el ámbito científico; si la técnica ha sido aceptada por expertos en la materia (prueba de Frye); naturaleza y alcance de la interferencia deducida; claridad de la explicación técnica; la medida en que los datos básicos pueden ser verificados por el tribunal y el jurado.

[70] Los investigadores forenses utilizan una variedad de herramientas: EnCase (http://www.guidancesoftware.com); AccessData FTK (http://www.accessdata.com);ProDiscover (http://www.techpathways.com); SleuthKit y autopsia (http://www.sleuthkit.org); SMART (http://www.asrdata.com/index.html); ilook (aplicación de la ley sólo) http://www.ilook-forensics.org); BlackBag (para Apple Mac); (http://www.blackbagtech.com/products.html); Paraben (también para PDAs) (http://www.paraben-forensics.com); Tucofs - herramientas web listado de muchos (http://www.tucofs.com/tucofs.htm); Las herramientas de código abierto (http://www.opensourceforensics.org)

de su autenticidad, su no alteración y su preservación. Dicha prueba para que pueda tener valor en el proceso deberá tener acceso a los tribunales sin que sea modificada y siendo correctamente preservada, todo ello, mediante una correcta cadena de custodia. Herramientas, método, cadena de custodia y legalidad son pilares básicos que fundamentaran el valor de la prueba informática-forense en juicio.

La prueba informático forense tendrá, por lo tanto, mayor o menor fundamento y valor procesal atendiendo a:

a.- Las Herramientas empleadas. Entendidas como aquellos programas informático forenses que ayudan al experto en su labor de captura de la evidencia digital. Herramientas que además deben ser empleadas por personas con formación informático-forense y conocimientos suficientes para análisis de este tipo, ya que las herramientas no pueden sustituir los conocimientos de un experto informático-forense.

En este sentido algunos autores como DARAHUGE Y ARELLANO critican el uso indiscriminado por parte de expertos de herramientas o productos de análisis informático forense llave en mano (las conocidas utilidades computacionales «enlatadas»), adaptadas a los mecanismos, métodos y normativa procesal de la Common Law, es decir, a su sistema legal y sin ninguna relación con el análisis pericial criminalístico. Sostienen que por muy prácticos que resulten los enlatados para la labor pericial, se muestran inútiles para suplir la falta de formación profesional legal y criminalística, por parte del profesional que los utiliza. Según dichos autores el empleo de estos productos con fines periciales no solo contribuye a estimular el desinterés por la capacitación permanente de quienes lo emplean, que lo hacen a modo de herramienta práctica, sin conocimientos respecto de su operación y estructura operativa. En efecto al ser vendidos como enlatados, sus componentes, algoritmos, estructuras de datos, metodología, sistemas de búsqueda, en definitiva su concepto de trabajo, se muestran al usuario como una «caja negra» cuya eficiencia, eficacia y efectividad se basa en la confianza que él mismo deposita en la idoneidad profesional de la empresa que lo vende al mercado y en sus desarrolladores. Es imposible corroborar el método utilizado para recolectar la información que luego brinda al usuario, porque forma parte del «secreto comercial», preservado por la empresa y que por supuesto no se ofrece al adquirente. En términos informáticos, no es posible disponer del código fuente de los programas que integran el paquete de Informática forense que se utiliza. En síntesis, o bien no es posible realizar el análisis crítico de los algoritmos que justifican los resultados obtenidos a partir de la aplicación del «enlatado» utilizado, que solo están disponibles para ciertas instituciones policiales o judiciales propias del país de origen. En ambos casos, resulta en el impedimento práctico de ejercer

supervisión y auditoría metodológica y de resultados de la prueba presentada como «confiable» a quién está obligado a tomar una decisión judicial (sentencia). Si no es posible conocer los algoritmos de búsqueda a partir de los cuales se obtienen los datos ofrecidos, la única manera de confiar en su certeza y pertinencia reside en adoptar una actitud de credulidad respecto de ésta (efectuar un auténtico acto de fe, indemostrable ante la ignorancia del código fuente que sustenta la aplicación)[71].

El reconocimiento nacional e internacional a nivel científico y técnico de determinadas herramientas utilizadas en la investigación del hecho electrónico será importante a efectos de valoración en el proceso de la prueba electrónica obtenida. En este sentido existen iniciativas a nivel internacional como la llevada a cabo por el Instituto Nacional de los Estándares y la Tecnología (*National Institute of Standards and Technology*), también conocido como NIST, que fue fundado en 1901 como una agencia federal que forma parte del Departamento de Comercio de los Estados Unidos. Su misión es elaborar y promover patrones de la medición, los estándares y la tecnología con el fin de crear productividad, facilitar el comercio y mejorar la calidad de vida. Este instituto lleva a cabo un proyecto para el testeo de herramientas de análisis forense de ordenadores (*computer forensic tool testing, CFTT*). Su principal objetivo es la certificación de herramientas de hardware y software con el fin de asegurar que su uso ofrece resultados fiables[72].

En España existen iniciativas como el «proyecto Konfía» de la Asociación Profesional de Peritos Informáticos (ASPEI) publicado en su página Web, cuyo objetivo es la recopilación de herramientas informáticas existentes útiles para el peritaje informático, comprobando su funcionamiento, utilidad y reproducibilidad. Dichas herramientas son gratuitas, de código abierto y están libremente disponibles en Internet. ASPEI asegura que ha personalizado mínimamente una conocida compilación de programas informáticos relacionados con la informática forense (DEFT, www.deftlinux.net), ha comprobado su contenido, y ha realizado un depósito notarial de los mismos junto con el resultado de su huella digital, o hash criptográfico. Según la ASPEI a partir de ahora, es posible iniciar cadenas de custodia o análisis de evidencias

[71] DARAHUGE, M.E Y ARELLANO GONZALEZ, L.E. *Manual de Informática Forense (Prueba Indiciaria Informático Forense)*. Ed. Errepar, 2012, págs. 5-6.

[72] Para más información, véase la página web http://www.nist.gov/. Puede consultarse también sobre este tema: RIFÀ POUS, HELENA, SERRA RUIZ, JORDI Y RIVAS LÓPEZ, JOSÉ LUIS, *Análisis Forense de Sistemas Informáticos,* Rifà Pous, Helena, y Serra Ruiz, Jordi coordinadores, septiembre de 2009, ed. UOC, pág. 35, disponible en la página web webs.uvigo.es.

digitales utilizando herramientas abiertas, comprobadas y de cuya integridad existe fe pública[73].

La distribución DEFT está disponible, en realidad, desde hace años (versión 3, la actual es la 7.2). Los responsables de la distribución colaboran habitualmente con fuerzas y cuerpos de seguridad en Italia y resto de Europa y organizan congresos al efecto. DEFT es una de las distribuciones más utilizadas, por lo que el número de profesionales con interés en su evaluación es notable. Por otro lado, los creadores de DEFT garantizan la integridad de la distribución con la publicación de los correspondientes «hashes» (ver http://na.mirror.garr.it/mirrors/deft/md5.txt). Los expertos informático-forenses utilizan esta distribución con asiduidad, siendo un valor el poder anexar la distribución (el DVD concreto) utilizada a los informes que lo requieren, así como la referencia a la página de descarga y los «hashes» de comprobación de integridad. Hay otras distribuciones que serían también adecuadas, pero hoy por hoy es la que según los expertos se mantiene más actualizada e incorpora un conjunto de herramientas más equilibrado. No obstante, esta distribución solo se cita a modo de ejemplo, ya que no cubre todos los posibles escenarios. Normalmente los peritos llevan habitualmente una decena de medios de arranque con distribuciones que incluyen herramientas especializadas.

b.- El Método técnico empleado: entendido como el conjunto de operaciones técnicas informáticas empleadas por el experto informático-forense desde el mismo momento de la identificación del hecho electrónico hasta la finalización de todo el proceso.

c.- La Cadena de Custodia. La cadena de custodia es un sistema cuyo objetivo es garantizar la integridad, conservación e inalterabilidad de los hechos electrónicos. Ello incluye su obtención, custodia, transporte y presentación en los tribunales hasta su disposición final por orden judicial.

El modo como la cadena de custodia se relaciona con la investigación y la prueba determina las características de la misma: 1.- Sirve como garantía de la autenticidad e indemnidad de la prueba; 2.- Constituye una garantía de que la evidencias que se analizan y cuyos resultados se contienen en el dictamen pericial son las mismas que se recogieron durante la investigación, de modo que no existan dudas sobre el objeto de la prueba pericial, a este respecto resulta evidente la relación entre la cadena de custodia y la prueba pericial, por cuanto la validez de los resultados de la pericia dependen de la garantía sobre

[73] Véase, el Portal de Peritos Judiciales y Tasadores en la dirección electrónica http://goo.gl/OtZNT. Página consultada en fecha 25.2.2013.

la procedencia y contenido de lo que es objeto de análisis[74]; 3.- La cadena de custodia se refiere y está asociada a la prueba como actividad y también como resultado, efectivamente, la cadena de custodia determina la validez de la prueba e, indirectamente, de su resultado por cuanto la infracción de sus normas puede determinar que se «aparte» o «expulse» del procedimiento la evidencia y/o el resultado que se contuviere en el informe pericial, no puede haber un juicio justo sin una actividad probatoria válida; y 4.- La cadena de custodia puede acreditarse documentalmente o mediante testimonio, efectivamente, nada impide que la cadena de custodia se acredite mediante el testimonio de las personas que recogieron, custodiaron y/o conservaron las evidencias[75].

Tal y como indica el Tribunal Supremo el problema que plantea la cadena de custodia, «*…es garantizar que desde que se recogen los vestigios relacionados con el delito hasta que llegan a concretarse como pruebas en el momento del juicio, aquello sobre lo que recaerá la inmediación, publicidad y contradicción de las partes y el juicio del tribunal es lo mismo; es decir, es necesario tener la seguridad de que lo que se traslada, analiza o, en este caso, se visiona, es lo mismo en todo momento, desde que se interviene hasta el momento final que se estudia y analiza*» (SSTS 6/2010, de 27 de enero, 776/2011 de 20 de julio y de 14-10-2011).

Las normas básicas existentes para una correcta cadena de custodia son aplicables a todas las disciplinas incluida la informático-forense[76]. Sin embargo, en informática forense existen actuaciones o metodologías específicas a dicho ámbito que es necesario conocer y aplicar para que la prueba informática no sea impugnada, como por ejemplo el empleo de «hash» para asegurar la integridad de un archivo copiado. En informática forense una correcta cadena de custodia supone: 1. La autenticidad de los hechos objeto de prueba que deben acceder al proceso sin confusión, adulteración ni sustracción; 2. La correcta identificación de toda persona interviniente; 3. La correcta

[74] «Apuntar a la simple posibilidad de manipulación para entender que la cadena de custodia se ha roto no parece aceptable, ya que debe exigirse la prueba de su manipulación efectiva» (STS 629/2011 de 23 de junio; 776/2001, de 20 de julio).

[75] Véase RICHARD GONZÁLEZ, M., *La cadena de custodia en el proceso penal español*, Diario La Ley 8236/2013, Año XXXIV, Número 8187, Viernes, 8 de noviembre de 2013, págs. 3-4, disponible en www.diariolaley.es.

[76] RICHARD GONZÁLEZ alude a la necesidad de una regulación legal sobre recogida, custodia y análisis de evidencias en su artículo *La cadena de custodia en el proceso penal español*, Diario La Ley 8236/2013, Año XXXIV, Número 8187, Viernes, 8 de noviembre de 2013, págs. 4-7, disponible en www.diariolaley.es.

identificación de todos los equipos locales o remotos involucrados, sean de almacenamiento, procesamiento o comunicaciones; 4. Descripción y modelos de las estructuras de distribución de la información a la que se ha accedido; 5. Y la constancia escrita de una descripción detallada de las anteriores, así como de las técnicas y procedimientos utilizados, y de las modificaciones que sufrió o de las que fue objeto.

d.- Y finalmente Legalidad y legitimidad. La prueba informático-forense deberá ser capturada y tratada conforme a la normativa vigente y desde luego siempre deberá ser obtenida preservando las garantías constitucionales: la vulneración de derechos fundamentales en su obtención supondrá la ilicitud de la prueba obtenida y su nulo valor probatorio.

Las pruebas informático forenses tienen por finalidad acreditar hechos en el proceso, siendo actualmente cuestionada su fiabilidad, por lo cual es necesario desarrollar una metodología para describir de manera adecuada, validar y documentar la evidencia, y posibilitar un método adecuado de reproducción o exposición en el juicio oral. Pero para todo ello es necesario el consenso de la comunidad científica. De existir procedimientos reconocidos como adecuados por la comunidad científica y seguidos por los expertos se evitará causar alteración de las pruebas electrónicas, vulnerando su función de asegurar la obtención de informaciones claves que aportan valor probatorio al proceso. Ello no supone generar una doctrina y una metodología particularizada y personalizada, para cada tipo de soporte de información, ya que ello no resulta posible dados los avances imparables técnicos y científicos –así lo sostienen los distintos tribunales de EEUU-. No es, por lo tanto, posible ni necesario crear un procedimiento para cada nueva tecnología que aparece en el mercado. Por ello, debe existir cohesión en los principios básicos de captura, certificación, traslado, verificación y supervisión, agregando únicamente aquellos elementos propios de la nueva tecnología analizada que deban ajustarse para asegurar la preservación y confiabilidad del hecho informático recopilado[77] .

La Recomendación nº R (95)13, del Comité de Ministros de los Estados Miembros sobre los problemas de derecho procesal penal relacionados con las tecnologías de la información, de 11 de septiembre de 1995 (543ª sesión de Diputados de los Ministros), ya establecía que deben desarrollarse métodos especiales en los procedimientos y técnicas para el manejo de pruebas electrónicas que garanticen y reflejen la integridad y autenticidad de la evidencia. La Exposición de Motivos de la recomendación explica las dificultades de admisibilidad en los Tribunales de las pruebas electrónicas señalando que

[77] En este sentido se pronuncian DARAHUGE, M.E Y ARELLANO GONZÁLEZ, L.E. en *el Manual de Informática Forense (Prueba Indiciaria Informático Forense)*, ed. Errepar, 2012, XX11.

seguirán existiendo sino se regulan los diferentes procedimientos para la autenticación de pruebas electrónicas como el establecimiento de una cadena completa de custodia (párrafo 161), e incidiendo en la necesidad de desarrollo de un enfoque armonizado en la materia a nivel internacional ya que los delitos a menudo cruzan las fronteras (párrafo 164).

Por otro lado, la Convención sobre Delito Cibernético del Consejo de Europa, de 23 de noviembre de 2001 (Budapest), que entró en vigor el 1 de julio de 2004, además de establecer una armonización de las definiciones de delitos cibernéticos, determina procedimientos para la captación de la evidencia y garantías a nivel de distintas jurisdicciones internacionales[78]. Es el primer instrumento jurídico internacional de la información de derecho y procedimiento penal vinculante con respecto a las consecuencias de la actual tecnología. Aunque el ámbito de actuación del Consejo de Europa sea limitado al ámbito europeo, la Convención establece un marco global de aplicación de la ley en el ciberespacio, los Estados no miembros del Consejo de Europa, como Canadá, Japón y los EE.UU. han contribuido a la preparación de la Convención y suscrito y apoyado el acuerdo. El Convenio tiene como objetivo la armonización de las definiciones de los diversos delitos informáticos, lo que permite la aceleración de cooperación mutua. La Convención también se extiende hacia cuestiones relacionadas con las pruebas.

Existen también algunas iniciativas en distintos países, principalmente en el ámbito penal, que han dado a luz manuales y guías para una buena praxis. En la mayor parte de ellas colaboran fuerzas de la ley, investigadores y expertos, y en la actualidad algunos de dichos procedimientos han sido reconocidos públicamente como «fiables» a la hora de recopilar y preservar la información digital. Entre dichos grupos, guías y normas con valor de recomendación podemos destacar los siguientes: La Guía de buenas prácticas para evidencia basada en computadoras (*Good Practice Guide for Comnputer-Based Electronic Evidence*) del Reino Unido[79], la Sección de Delitos Informáticos y Propiedad

[78] También denominado «Convención sobre delitos informáticos», «Convención sobre ciberdelincuencia» o «Convenio sobre cibercriminalidad»-

[79] *La «Good Practice Guide for Comnputer-Based Electronic Evidence»* elaborada por la Association of Chief Police Officers (ACPO), es una Guía creada por la Policía del Reino Unido, cuyo principal objetivo es el análisis forense de disco, PDA´s y teléfonos móviles. La ACPO, Association of Chief Police Officers (Asociación de Jefes de Policía), del Reino Unido mediante su departamento de crimen por computador, publicó la "Guía de Buenas Practicas para Evidencia basada en Computadores" (Good Practice Guide For Computer Based Evidence) [GoPra99]. La policía creó este documento con el fin de ser usado por sus miembros como una guía de buenas prácticas para ocuparse de computadores y de otros dispositivos electrónicos que puedan ser evidencia. Su estructura es: a) Los principios de la evidencia basada en computadores. b) Oficiales atendiendo a la escena. c) Oficiales investigadores. d) Personal para

Intelectual (CCIPS)[80], la Sala de lo Penal, del Departamento de Justicia de E.E.U.U, o el SWGDE[81], el RFC3227[82], la IOCE Guidelines for de best practices in de forensic examination of digital technology[83], el «Codes of Practises for Digital Forensics» (CP4DF)[84], el proyecto «Cyber Tools On-Line Search for

---

la recuperación de evidencia basada en computadores. e) Testigos de consulta externos. f) Anexos (legislación relevante, glosario y formatos).

Por otro lado, la guía «*Forensic Examination of Digital Evidence. A guide for law Enforcement*», es una guía orientativa en la obtención y presentación de evidencias digitales. Ha sido elaborada por U.S. Department of Hustice Programs. National Institute of Justice.

[80] *La Sección de Delitos Informáticos y Propiedad Intelectual (CCIPS),* Sala de lo Penal, del Departamento de Justicia de E.E.U.U. ofrece un manual, documentos, publicaciones y enlaces de interés, con referencias al Tratado sobre Cibercrimen de Europa.

[81] El SWGDE, es un Grupo de trabajo científico americano sobre evidencias digitales, constituido en 1998 y formado por Directores del Laboratorio Federal contra la Delincuencia.

[82] El RFC3227 es un breve documento escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros en network Working Group, establece una «Guideline for Evidence Collection and Archiving». Señala las mejores prácticas para determinar la volatilidad de los datos, decidir que recolectar, desarrollar la captación y determinar cómo almacenar y documentar los datos, así como explica conceptos relacionados a la parte legal. Se estructura del siguiente modo: 1. Principios durante la captación de la evidencia: orden de volatilidad de los datos, cosas que deben evitarse, consideraciones de privacidad y legales; 2. Proceso de captación: transparencia y pasos de la captación; 3. Proceso de archivo; cadena de custodia, donde y como archivar.

[83] La IOCE «Guidelines for de best practices in de forensic examination of digital technology» o «Guía para las mejores prácticas en el examen forense de la tecnología digital», señala una serie de estándares, principios de calidad y aproximaciones para la detección, prevención, recuperación, examen y uso de la evidencia digital para fines forenses. Trata los sistemas, procedimientos, personal, equipo y requerimientos de comodidad que se necesitan para todo el proceso forense de evidencia digital, desde examinar la escena del crimen hasta la presentación en la corte. Se estructura en: a) Garantía de calidad (enunciados generales de roles, requisitos y pruebas de aptitud personal, documentación, herramientas, validación de las mismas y espacio de trabajo); b) Determinación de los requisitos de examen del caso; c) Principios generales que se aplican a la recuperación de la evidencia digital (recomendaciones generales, documentación y responsabilidad); d) Prácticas aplicables al examen de la evidencia de digital; e) Localización y recuperación de la evidencia de digital en la escena: precauciones, búsqueda en la escena, recolección de la evidencia y empaquetado, etiquetando y documentación; f) Priorización de la evidencia; g) Examinar la evidencia: protocolos de análisis y expedientes de caso; h) Evaluación e interpretación de la evidencia; i) Presentación de resultados (informe escrito); j) Revisión del archivo del caso: Revisión técnica y revisión administrativa; k) Presentación oral de la evidencia; l) Procedimientos de seguridad y quejas.

[84] *El «Codes of Practises for Digital Forensics» (CP4DF)* es una Iniciativa española para el desarrollo de una metodología de procedimientos para análisis forense. Se trata de un proyecto abierto a cualquiera en Sourceforge. El 14 de noviembre se hizo pública la tercera revisión V1.3 durante el primer «*Flash mob sobre digital forensic"s»* en Barcelona. Trata las cuatro fases del análisis forense: aseguramiento de la escena; identificación de las evidencias digitales; preservación de las evidencias digitales y presentación y reportes.

Evidence» o «Instrumentos de investigación de pruebas electrónicas» (Proyecto CTOSE)[85], la Guía «Electronic Crime Scene Investigation, A Guide for First Responders» (Investigación de la escena del crimen electrónico)[86], la guía

---

[85] El proyecto «Cyber Tools On-Line Search for Evidence» o «Instrumentos de investigación de pruebas electrónicas» (Proyecto CTOSE), es un proyecto de investigación mantenido por la Comisión Europea que concluyó el 30 de septiembre 2003, combinando la experiencia del especialista francés de telecomunicaciones, Alcatel, la sociedad de seguridad británica QinetiQ y tres institutos de investigación, el CRID de la Universidad de Namur (Bélgica), la universidad de St. Andrews (Reino Unido) y el Fraunhofer Institut (IAO) de la Universidad de Stuttgart (Alemania), así como del Instituto para la Protección de la Seguridad del Ciudadano de la UE. Su objetivo es recopilar el conocimiento disponible de diferentes fuentes expertas en todos aquellos procesos relacionados en la recuperación de evidencias digitales y crear una metodología para definir como debe llevarse a cabo dicha recuperación cuando sea necesaria como resultado de cualquier tipo de conflicto en el que se vean envueltas transacciones electrónicas u otro tipo de delitos relacionados con las nuevas tecnologías. Lo cual incluye cómo las empresas deben manejar los incidentes que se produzcan y la información asociada a éstos.

El Centro Común de Investigación de la Comisión Europea ha creado un sistema para tratar las informaciones electrónicas que garantiza los derechos de los usuarios del ciberespacio y les protege contra el fraude cuando compran en Internet. El proyecto CTOSE permitirá identificar, garantizar, integrar y presentar pruebas electrónicas sobre «ciberdelitos». Su objetivo consiste en establecer con precisión lo que pasa durante los delitos informáticos, o incluso durante una simple operación en la web. Gracias a este nuevo desarrollo, los investigadores podrán utilizar «instrumentos de identificación criminal informática» para recoger pruebas que puedan ser producidas a lo largo de procedimientos judiciales en toda Europa. Para ello, los investigadores europeos han desarrollado, en cooperación con especialistas europeos de seguridad e informática, nuevos procedimientos normalizados. Ello permitirá garantizar que todas las pruebas electrónicas sean recogidas y preservadas legal y correctamente, y que constituyan pruebas «sanas e indiscutibles» de delito o fraude para la dirección de una empresa, un tribunal laboral o una jurisdicción civil o penal. Así, desde los administradores del sistema, el personal responsable de la seguridad de los sistemas de información y los investigadores encargados de incidentes informáticos hasta autoridades de policía y representantes de la ley, seguirán procedimientos coherentes y normalizados en las investigaciones sobre incidentes informáticos con la ayuda de «instrumentos de identificación criminal». Esta noticia ha sido tomada de http://goo.gl/wkNsj.

Véase también FERNANDEZ BLEDA, Daniel, *Informática Forense*. *Teoría y Práctica*. Sevilla, Hackmeeting, 2004 y ZUCCARDI, G. Y GUTIÉRREZ, J.D., *Informática forense*. Puede consultarse este último en la dirección goo.gl/bfxUG.

[86] La «*Electronic Crime Scene Investigation: A Guide for First Responders*» (Investigación de la escena del crimen electrónico) Guía DoJ 1) del Departamento de Justicia de EEUU, trata sobre la identificación y recolección de la evidencia. Esta guía se enfoca más que todo en identificación y captación de evidencia. Su estructura es: a) Dispositivos electrónicos (tipos de dispositivos que se pueden encontrar y cuál puede ser la posible evidencia). b) Herramientas para investigar y equipo. c) Asegurar y evaluar la escena. d) Documentar la escena. e) Captación de evidencia. f) Empaque, transporte y almacenamiento de la evidencia. g) Examen forense y clasificación de delitos. h) Anexos (glosario, listas de recursos legales, listas de recursos técnicos y listas de recursos de entrenamiento)

«Forensic Examination of digital evidence»[87], la Guía de Hong Kong sobre computación forense[88], la Guía australiana «Para El Manejo De Evidencia En IT»[89]. Y la norma ISO/IEC 27037:2012 «Information technology -Security techniques- Guidelines for identification, collection, adquisition and preservation of digital evidence» que viene a renovar a las ya antiguas directrices RFC 3227, estando las recomendaciones de la ISO 27037 más dirigidas a dispositivos actuales. Es una norma orientada al procedimiento de la actuación pericial en el escenario de la recogida, identificación y transporte y preservación. Dicha norma goza de reconocimiento mundial.

En el ámbito corporativo existen normas destinadas a las empresas como la ISO 17799 o la ISO 15489. La primera de carácter internacional tiene por objeto la seguridad de gestión de la información. Hace hincapié en los controles internos, la necesidad de respuesta a incidentes formales, así como en procedimientos y herramientas[90]. Con posterioridad la ISO/IEC 27001, sobre sistema de gestión

---

[87] La guía «F*orensic Examination of digital evidence, A guide for law enforcement» (FoEx04*), es una guía pensada para ser usada en el momento de examinar la evidencia digital. Se estructura del siguiente modo: a) Desarrollo de políticas y procedimientos con el fin de dar un buen trato a la evidencia. b) Determinación del curso de la evidencia a partir del alcance del caso. c) Adquisición de la evidencia. d) Examen de la evidencia. e) Documentación y reportes. f) Anexos (casos de estudio, glosario, formatos, listas de recursos técnicos y listas de recursos de entrenamiento).

[88] La Guía Hong Kong Computación Forense - Parte 2, Mejores Prácticas El ISFS, Information Security and Forensic Society (Sociedad de Seguridad Informática y Forense), creada en Hong Kong, publicó «*Computación Forense - Parte 2: Mejores Practicas*» (Computer Forensics – Part 2: Best Practices) [CoFor04]. Esta guía cubre los procedimientos y otros requerimientos necesarios involucrados en el proceso forense de evidencia digital, desde el examen de la escena del crimen hasta la presentación de los reportes en la corte. Se estructura del siguiente modo: a) Introducción a la computación forense. b) Calidad en la computación forense. c) Evidencia digital. d) Captación de Evidencia. e) Consideraciones legales (orientado a la legislación de Hong Kong). f) Anexos.

[89] La Guía Para El Manejo De Evidencia En IT (Guía Australia) Standards Australia (Estándares de Australia) publicó la «*Guía Para El Manejo De Evidencia En IT*» (HB171:2003 Handbook Guidelines for the management of IT evidence) [HBIT03]. Esta guía no está disponible para su libre distribución, por eso para su investigación se consultaron los artículos *«Buenas Prácticas En La Administración De La Evidencia Digital»* [BueAdm06] y «New Guidelines to Combat ECrime» [NeGu03]. Es una guía creada con el fin de asistir a las organizaciones para combatir el crimen electrónico. Establece puntos de referencia para la preservación y recolección de la evidencia digital. Detalla el ciclo de administración de evidencia de la siguiente forma: a) Diseño de la evidencia. b) Producción de la evidencia. c) Recolección de la evidencia. d) Análisis de la evidencia. e) Reporte y presentación. f) Determinación de la relevancia de la evidencia.

[90] En cuanto a los procedimientos para la seguridad de la gestión de la información la norma ISO 17799 señala que deben incluir: el análisis e identificación de la causa del incidente; planificación y solución; recolección de pistas de auditoría y evidencias similares; comunicación con los afectados o implicados con los hechos; informes de acción por parte de quien tenga la

de seguridad de la información, es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements). Fue aprobada y publicada como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission. Dicha norma específica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como «Ciclo de Deming»: PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI). Existe una nueva versión del año 2013.

La ISO 15489 es también una norma internacional, cuyo objetivo es regular la gestión de documentos creados o recibidos por una organización pública o privada en el curso de sus actividades con fines internos o externos, con independencia de su formato o soporte y de las tecnologías utilizadas. Entre muchas otras ventajas a nivel organizativo empresarial destaca, en lo que a nuestro trabajo respecta, la preservación del valor probatorio de los documentos ante posibles litigios[91].

Existen también iniciativas destinadas a establecer directrices en la presentación de la información ante los Tribunales como las desarrolladas por el Comité técnico de normalización AEN/CTN 197, informes periciales, perteneciente a la Asociación Española de Normalización y Certificación (AENOR). Su objeto es la normalización de criterios generales para la elaboración de informes de actuaciones periciales en todas las áreas existentes incluidas las TIC, que den respuesta a las necesidades de Justicia y a los profesionales que elaboran los informes periciales. En sus reuniones viene discutiéndose si deben incorporarse directrices exclusivamente respecto a la forma de presentación de los dictámenes periciales sobre TIC o también debe incluir directrices sobre la

competencia. La organización que sufre un incidente debe proceder a analizar los problemas internos, el uso como medio de prueba y la negociación para la compensación respecto a los proveedores en cuanto al software.

[91] El objetivo de la ISO 15489 es que dichas organizaciones puedan disponer de los documentos adecuados en cada momento para que puedan llevar a cabo su actividad y negocios, cumplan con el marco legal y reglamentario, y puedan rendir cuenta de su actividad cuando así se requiera. Por eso el sistema de gestión de documentos tiene que garantizar la autenticidad, fiabilidad, integridad, y disponibilidad de los documentos, identificándolos en el contexto de las actividades de la organización.

metodología empleada por los peritos para la emisión de los mismos[92]. Ha sido elaborada por dicho Comité la norma española UNE 197001; 2011 «Criterios generales para la elaboración de informes y dictámenes periciales»[93]. A nivel europeo el Centro Europeo de Normalización CEN 405 «European standard on Expertise Services». Ninguna de ellas es de obligado cumplimiento. Y a nivel internacional destaca la «American Society for Testing and Materials» (ASTM9).

En la actualidad existen dos proyectos en España por parte de AENOR el PNE 71505 y El PNE 71506. El primero de ellos trata el sistema de gestión de evidencias electrónicas y engloba la generación, gestión, seguridad, conservación y/o almacenamiento de la evidencia electrónica antes de la adquisición. El PNE 71505 Tecnologías de La Información (TI), Sistema de Gestión de Evidencias Electrónicas (SGEE), se halla dividido en tres partes: La primera se refiere al vocabulario y la determinación de principios generales; la segunda parte trata las buenas prácticas en la gestión de evidencias electrónicas; y la tercera parte alude a los formatos y mecanismos técnicos.

Por otro lado, el proyecto PNE 71506 sobre tecnología de la información y metodología para el análisis forense de las evidencias electrónicas tiene por objeto la metodología para el análisis forense de las evidencias electrónicas. Es decir, expone los métodos a emplear para preservar, adquirir, documentar, analizar y presentar las evidencias electrónicas. Es una norma dirigida especialmente a los equipos de respuesta a incidentes y seguridad, así como a cualquier profesional competente en este ámbito.

2.3 Investigación informático-forense: Fases

La investigación informático-forense tendrá por objeto el análisis de distintos hechos que tienen por base hechos electrónicos. Una conducta humana como el envío o recepción de un correo electrónico puede suponer una serie de hechos de naturaleza electrónica que pueden ser objeto de análisis por los expertos informático-forenses en una investigación de tal naturaleza. Dichos expertos concluirán verificando ese primer hecho a través del análisis de los demás. Es decir, a través del análisis efectuado por los expertos en informática forense de los metadatos, logs, copias de seguridad etc. podrá constatarse la

[92] La Secretaría Técnica de dicho Comité la desempeña el Colegio de Ingenieros Técnicos Industriales de Barcelona en nombre y representación del Consejo de Colegios Oficiales de peritos e Ingenieros Industriales. AENOR obtuvo la correspondiente autorización de Industria para asumir funciones de normalización en el ámbito de los informes de actuaciones periciales.

[93] Puede consultarse dicha norma en la página web www.enginyersbcn.cat.

actividad humana de remisión o envío de un correo electrónico, su fecha, autor y contenido. El análisis efectuado por los expertos en informática forense obrante en un informe, de cumplir con todos los requisitos legales, podrá constituir prueba en el proceso judicial. La acreditación a través del informe técnico del envío de uno o varios correos electrónicos podrá acreditar una actividad humana con consecuencias jurídicas. Para que dicha prueba informático-forense tenga credibilidad en el proceso requerirá, como anteriormente hemos señalado, de herramientas adecuadas, método técnico, cadena de custodia, legalidad y legitimidad.

Podemos estructurar la investigación informático-forense en tres fases sucesivas[94]:

1ª) Análisis preliminar, para la identificación de la prueba informática que se desea obtener, siendo aconsejable la implicación del experto desde el primer momento en la selección de la información a identificar;

2ª) Adquisición de los datos informáticos, a cuyo efecto es fundamental la identificación de las fuentes, la conservación de las copias y la constatación de las técnicas empleadas para garantizar la integridad de la información, siendo recomendable que la prueba sea obtenida a presencia de testigos o/e incluso de fedatarios públicos –notario o secretario judicial-, y, en su caso, se deposite en soporte adecuado en una notaría o bajo custodia del secretario judicial, mediante un acta de manifestaciones del experto en la que se detalle el proceso de obtención de la información[95]; y

---

[94] La distinción entre dichas fases se efectúan por muchos autores entre ellos PASAMAR, A., *Empresa y prueba informática*, en el libro del mismo título "Empresa y prueba informática", Abel Lluch, X. (dir.), Colección de Formación Continua de la Facultad de Derecho ESADE-URL, J.M. Bosch editor, Barcelona, 2006, págs.31-38.

[95] Sobre la intervención de fedatario público en la incautación y volcado de la información véase la jurisprudencia del Tribunal Europeo de Derechos Humanos, en concreto la SSTEDH de 7 de junio de 2007 (asunto Smirnov v. Rusia, núm. 71362/01); en similares términos la STEDH de 27 de septiembre de 2005 (asunto PETRI SALLINEN Y OTROS VS FINLANDIA, núm. 50882/99), y como más reciente la STEDH de 22 de mayo de 2008 (caso ILILLA STEFANOV V. BULGARIA, asunto núm. 65755/01).

En aras a garantizar la eficacia probatoria de las evidencias electrónicas obtenidas es fundamental la intervención de un fedatario público desde el primer momento de la intervención del informático forense en el dispositivo electrónico. Así se deduce del Auto de la Audiencia Provincial de Vizcaya, de 31 de marzo de 2008, en relación a un supuesto de investigación de un presunto delito contra la propiedad intelectual cometido por ex directivos y ex empleados de la misma, por presunta apropiación de determinadas aplicaciones informáticas de elaboración interna de la empresa, así como de determinadas plataformas y programas informáticos sobre los que la empresa denunciante poseía licencia para su exclusiva distribución

3ª) Análisis forense de la información digital, a cuyo efecto es conveniente que el experto, amén de la elevada cualificación técnica, atesore un mínimo conocimiento de la normativa legal. Dentro de dicha fase se incluyen: clasificación; identificación, individualización y asociación para una posterior fase que sería la presentación ante el juez de los hechos[96].

2.3.1 Análisis preliminar

La primera fase de una investigación para la constatación de hechos es el «análisis preliminar». Dicha fase consiste en la obtención por parte del experto informático-forense de toda la información necesaria sobre los hechos para poder llevar a cabo una labor de planificación de su intervención con la finalidad de obtención de la prueba electrónica. Esa fase puede desarrollarse con carácter previo al proceso judicial o bien dentro del ámbito del mismo.

En el supuesto que se actúe con carácter previo al proceso, la persona física o jurídica, normalmente una empresa, acudirá al experto informático-forense tras sospechar de la existencia de un presunto hecho ilícito que puede comprobar

---

en España. En dicho Auto se dictamina, a pesar de que la denuncia aparece acompañada de dictamen pericial, que «*respecto de la prueba pericial practicada para acreditar el volcado de archivos desde los ordenadores portátiles de los querellados a dispositivos USB, si bien es cierto que el informe encargado por la querellante deduce que ha existido, no lo es menos que los discos duros de aquellos ordenadores sufrieron diversas manipulaciones por parte de la empresa querellante hasta el momento en que fueron depositados ante un fedatario público para ser entregados al perito (...), sin que haya constancia de que se haya mantenido la cadena de custodia de los mismos (...), de modo que la capacidad de aquel informe para acreditar hechos adversos a los querellados debe ser relativizada, como hace la resolución recurrida", confirmándose el archivo provisional decretado por el Juzgado de Instrucción). Fuera de estos casos, otra posibilidad a la que siempre podrá acudir el Juzgado tras recibir la denuncia será la acordar una nueva pericial de contraste, esta vez sí revestida de las garantías propias de la actividad jurisdiccional, encomendando su práctica al Cuerpo técnico policial oportuno, si bien esta práctica, pese a otorgar mayores garantías al proceso, encontrará normalmente la resistencia por parte del órgano policial comisionado al efecto, que ya de por sí suele contar con efectivos personales y materiales manifiestamente insuficientes para acometer las investigaciones policiales acordadas de oficio, repercutiendo negativamente en la dilación contraanálisis pericial, el cual, lógicamente, salvo supuestos excepcionales, quedará postergado a la previa confección de pericias derivadas de la propia actuación policial»*. Auto de la Audiencia Provincial de Vizcaya, Sección 2.ª, de 31 de marzo de 2008, Pte. Da Silva Ochoa

[96] Véase BECKETT, Jason. Thesis, *Forensic Computing: A Deterministic Model for Validation and Verification through an Ontological Examination of Forensic Functions and Processes*. Adelaide South Australia, January 2010. School of Computer and Information Science. Division of Information Technology, Engineering, and the Environment. University of South Australia, pág. 112.

en sus propias instalaciones (competencia desleal, vulneración de los derechos de propiedad intelectual o industrial, vulneración de los derechos de consumidores o usuarios…). El experto recabará toda la información necesaria por parte de dicha persona a los efectos de poder diseñar la estrategia de actuación para la obtención de dicha prueba electrónica. En esta fase se recaba información, se determinan los hechos, y se planifica la intervención, detallando, por ejemplo, las posibles fuentes de las que deriven esos hechos. Cuando más compleja organizativamente sea una empresa y mejor dotada de protocolos y dispositivos de alerta más fácil resultará el trabajo del experto informático-forense. Ello siempre y cuando el aviso sea inmediato, ya que en algunos supuestos la empresa se excede haciendo copias o clonaciones de datos o archivos, perjudicando una futura investigación y análisis profesional. También, pueden darse actuaciones de la empresa que afecten a los hechos o derechos de algunas personas y que posteriormente permitan la impugnación de la prueba por la adversa.

Por otro lado, puede que el análisis de un dispositivo electrónico deba efectuarse en el ámbito del proceso, ya sea mediante medidas de aseguramiento previo al mismo solicitadas por una parte (clonado de un sistema informático de otra empresa) ya sea con posterioridad a la interposición de la demanda en el propio proceso (clonación o análisis de la clonación efectuada por la contraparte) el juez realizará un control «ex ante», debiendo determinar el modo de intervención y los extremos exactos sobre los que debe versar la diligencia. Es entonces cuando el juez que acuerde la práctica de dichas diligencias deberá tener suficiente apoyo técnico para poder precisar si la intervención solicitada es excesiva, o que medidas deben tenerse en cuenta a efectos de preservar los derechos constitucionales de los terceros afectados en el momento de practicarse la intervención. Es decir, en estos casos el juez acordará, con fundamento en un dictamen pericial, en qué dispositivos electrónicos y con qué procedimientos y límites deberá efectuarse la intervención y con qué fines, así como determinar los extremos sobre los que debe versar la misma. En estos casos el control judicial actúa con carácter previo a la intervención a diferencia de los supuestos en que se actúa fuera del proceso y el control judicial actúa con posterioridad a la actividad efectuada.

La investigación forense requiere celeridad en aras a preservar los hechos, lo cual es igualmente predicable en el supuesto del hecho electrónico. Una intervención rápida del experto informático-forense en el supuesto de un incidente informático asegurará en mayor medida la preservación del hecho electrónico y su inalterabilidad. El experto en informática forense procederá a identificar el tipo de prueba que se desea obtener, así como la fuente o fuentes de información en las que se puede encontrar dicha prueba, se establecerá una estrategia de obtención de las fuentes y una actuación acorde con el respeto a

los derechos fundamentales recogidos en la Constitución, y se asegurará una correcta cadena de custodia que garantice la valoración de la prueba electrónica en juicio.

Una intervención tardía del experto puede suponer la pérdida de información. Un ejemplo de ello sería el supuesto en que se recibe un correo electrónico anónimo y se pretende identificar al autor. El sujeto suele imprimir en papel el correo electrónico y hasta que interviene un experto en informática-forense pueden haber transcurrido días, semanas e incluso meses. Ante esta situación, señalan los técnicos, que bien poco puede hacerse, ya que la información que éste necesita para realizar un análisis adecuado son las cabeceras del correo electrónico, que se encuentran en el ordenador que recibió el correo y que no quedan impresas en el papel. Es muy habitual que el correo original haya sido borrado con el transcurso de los días y que sólo se haya conservado la copia en papel. El desconocimiento técnico ha dado lugar a este error, cuando el hecho de haber consultado a un experto en pruebas electrónicas en los primeros instantes hubiese evitado el problema de pérdida de la prueba[97]. La intervención inmediata del experto en informática-forense hubiera supuesto el análisis del correo electrónico, consistente en una serie de datos en un archivo informático, que no sólo contienen el texto del mensaje, sino un «encabezado de Internet», que contiene mucha información relevante, incluyendo el recorrido que ha hecho por Internet desde el emisor hasta el receptor (hora y fecha de envío, dirección electrónica de envío y de destino, asunto del mensaje, protocolo informático etc.), datos que verifican la autenticidad del correo. A su vez, además de los logs (registros) que archivan los correos electrónicos analizaría otras fuentes como las copias de seguridad para asegurar que no han sido objeto de manipulación, ya que la copia puede quedar archivada en los servidores por los que pasa, además del ordenador del emisor y receptor final. Y de tener un buen sistema implantado el formato de archivo incluiría en la copia los documentos adjuntos.

No obstante lo anterior, a nuestro modo de ver podemos calificar de errónea la tendencia habitual de muchos autores a calificar el hecho electrónico como volátil. Precisamente el hecho electrónico al contrario de lo que suele predicarse se caracteriza por una mayor persistencia o perdurabilidad frente a otros hechos. Es por ello que debemos matizar entre la persistencia del «hecho electrónico» y la volatilidad de la «expresión del hecho electrónico». Un registro electrónico es mucho más persistente que incluso una huella en un papel, por lo tanto el hecho electrónico se caracteriza por su persistencia y no por su volatilidad. Distinta del «hecho electrónico» en sí lo es «la expresión de ese

[97] Este ejemplo lo cita PASAMAR, A., en *Empresa y prueba informática*, en el libro del mismo título "Empresa y Prueba informática", Ob. Cit. pág. 32.

hecho electrónico» como, por ejemplo, una muestra de datos en pantalla o un bit producido en un determinado momento, esa expresión del mismo sí se caracteriza por su volatilidad.

La investigación informática tendrá por objeto de análisis distintos hechos que tienen base en hechos electrónicos. Es decir, se inicia la investigación porque, por ejemplo, pretendemos probar un daño producido por una actividad de competencia desleal y para ello utilizaremos como prueba la remisión de un correo electrónico. Para poder acreditar la remisión o envío de dicho correo electrónico –actividad humana- es necesario el análisis del hecho electrónico y para ello requeriremos de un experto en informática-forense, que emita posteriormente el correspondiente informe. Normalmente el hecho electrónico consistirá en una comunicación o transferencia de datos a través de internet, o bien un documento creado por el propio sistema informático. En el primero de los casos, una comunicación o transferencia de datos a través de una red, puede efectuarse a través de una Intranet (red privada o restringida), una Extranet (que permite el acceso a ciertos usuarios externos debidamente autorizados) o Internet. En estos casos los documentos electrónicos se archivan para ulterior recuperación. El ejemplo más habitual es el correo electrónico[98]. En el segundo supuesto se trataría de un documento creado por el propio sistema informático y que también se almacena para su posterior utilización (una contabilidad, base de datos, informe etc.).

Uno de los puntos de actuación que debe definir el experto en informática forense es su estrategia de actuación y dentro del ámbito de la misma la determinación de las fuentes de donde obtendrá la información. El estudio puede realizarse sobre cualquier dispositivo o medio que incorpore información digital por ejemplo: páginas Web, foros de Internet, redes sociales (como facebook, tuenti, etc.), correo electrónico, ordenadores personales y portátiles, teléfonos móviles, agendas electrónicas (PDA's) y smartphones[99], memorias

[98] En los supuestos en que una persona niega ser el autor y que el e-mail nunca partió de su computadora, existen aplicaciones de rastreo como las llamadas «*Sniffers*» cuya misión es la de, a partir del mensaje final y trabajando con el «*IP Address*» devolverse por cada nodo, servidor o proveedor de servicio por el que pasó tal información hasta llegar a la computadora del emisor real, trazando así la ruta real que siguió el documento que nos interesa. VAZQUEZ PERROTA, Manuel Ramón. *La prueba digital en los Tribunales de Justicia. Búsqueda, Obtención, Preservación, Presentación y Evaluación*, 2005, citado por RAMOS ROMEU, F. y CAÑABATE PÉREZ, J., en *Los datos digitales en el proceso civil: prevención, producción y autenticación*, Revista Jurídica de Catalunya, núm.1-2011, pág. 71.

[99] El teléfono inteligente («*smartphone*» en inglés) es un término comercial para denominar a un teléfono móvil que ofrece más funciones que un teléfono celular común. Casi todos los teléfonos inteligentes son móviles que soportan completamente un cliente de correo electrónico con la funcionalidad completa de un organizador personal. Una característica importante de casi todos los teléfonos inteligentes es que permiten la instalación de programas

flash, Ipod, PSP, cámaras digitales, memorias USB, discos duros externos, CDs, DVDs etc., y en múltiples puntos de los sistemas de gestión corporativo tanto informáticos (servidores de empresa, proxies, routers, sistemas de almacenamiento corporativos, sistemas de software comerciales o desarrollados propios, firewalls …) como no informáticos (copiadoras, faxes …) entre otros. Los datos pueden obtenerse de diversas fuentes. Podemos citar entre las mismas: Software de aplicación, software para evitar el fraude, ERP software para registrar la actividad de los empleados, archivos de sistema y de gestión; Monitoring Software tales como IDS (Intrusion Detection Software), Sniffers, registro de teclado (keylogger), y controlador de contenido; logs genéricos, logs de acceso, logs de impresión, tráfico de web, tráfico de red interna, tráfico de internet, transacciones con bases de datos, transacciones comerciales; otras fuentes como CCTV, registro de acceso de puertas, logs de los teléfonos, datos de la PABX, grabaciones de redes telefónicas, call centre logs, mensajes grabados; back-ups y archivos, laptops y desktops.

En el ámbito informático los técnicos distinguen dos tipos de pruebas atendiendo a los datos con los que tratan, distinguiendo entre «pruebas de background» y «pruebas de foreground». Cuando empleamos la expresión pruebas de background nos referimos a aquellos datos almacenados por el uso cotidiano de la empresa o negocio; cuando hablamos de pruebas foreground hacemos referencia a los datos almacenados para luchar contra el fraude o crimen.

La planificación de la intervención por parte del experto informático-forense incluye la determinación del lugar en que debe efectuar la captura, preservación y análisis, «in situ» o en el laboratorio, y por ejemplo si debe actuar en «frío» o

---

para incrementar el procesamiento de datos y la conectividad. Estas aplicaciones pueden ser desarrolladas por el fabricante del dispositivo, por el operador o por un tercero. El término «Inteligente» hace referencia a cualquier interfaz, como un teclado QWERTY en miniatura, una pantalla táctil (lo más habitual, denominándose en este caso «teléfono móvil táctil»), o simplemente el sistema operativo móvil que posee, diferenciando su uso mediante una exclusiva disposición de los menúes, teclas, atajos, etc. El completo soporte al correo electrónico parece ser una característica indispensable encontrada en todos los modelos existentes y anunciados en 2007, 2008, 2009 y 2010. Casi todos los teléfonos inteligentes también permiten al usuario instalar programas adicionales, normalmente inclusive desde terceros, pero algunos vendedores gustan de tildar a sus teléfonos como inteligentes aun cuando no tienen esa característica. Algunos ejemplos de teléfonos denominados inteligentes son: Serie MOTO Q de Motorola, Nokia series E y series N, Black Berry, iPhone, Nexus One, Samsung Wave y Sony Xperia. Entre otras características comunes está la función multitarea, el acceso a Internet via WiFi, a los programas de agenda, a una cámara digital integrada, administración de contactos, acelerómetros y algunos programas de navegación así como ocasionalmente la habilidad de leer documentos de negocios en variedad de formatos como PDF y Microsoft Office. Puede consultarse más información en la página web de Wikipedia.

«caliente» según la jerga técnica de los expertos. Es decir, si la fase de captura de la información debe efectuarse con el equipo apagado o encendido.

Precintar o llevarse los ordenadores o dispositivos electrónicos de cualquier clase no siempre es la opción más adecuada. En muchos casos, resulta inútil, por cuanto cada vez en mayor medida los proveedores de servicios están en otro país, por lo que resulta conveniente garantizar que la información pueda obtenerse «in situ». De este modo, además, se evita también el coste económico que supone para una empresa la interrupción de su actividad. Por otro lado, un documento informático (por ej. archivo de texto contenido en un ordenador), a diferencia de un documento escrito que puede ser examinado de manera autónoma, debe analizarse, si es posible, en el contexto del ordenador, pues si lo separamos del sistema operativo o resto de archivos puede perderse información clave[100]. Ello contrasta con el análisis forense tradicional que se efectúa en un entorno controlado de laboratorio.

2.3.2 Adquisición de datos

La intervención de expertos en informática-forense en una primera fase es crucial en aras a conseguir prueba electrónica que sea lícita, contrastable, reproducible y, a ser posible, auditable. A ese fin la fase de adquisición de datos la podemos dividir principalmente en los siguientes pasos: identificación de las fuentes, captura, preservación y custodia. Dicha fase de adquisición deberá efectuarse sin dañar ni alterar el original. El hecho electrónico debe ser preservado hasta el punto que un tercero pueda repetir el mismo proceso y llegar al mismo resultado que el presentado ante un tribunal.

Una adecuada recopilación de pruebas con el registro y documentación de cada uno de los pasos efectuados podrá determinar quién, cómo y porqué, sin que quede desacreditada la prueba en juicio de la evidencia digital, como cuando se alega por una parte que los hechos pudieran estar causados por un «caballo de Troya» con absolución de la parte imputada o demandada.

En aquellos supuestos en que la adquisición de datos se efectúa de modo extraprocesal las personas que intervengan en la adquisición deben estar debidamente autorizadas por la empresa u organización que se trate, ya sean

[100] Véase PASAMAR, A., *Empresa y prueba informática*, en el libro del mismo título "Empresa y Prueba informática", Abel Lluch, X. (dir), Colección de formación Continua de la Facultad de Derecho ESADE-URL, J.M. Bosch editor, Barcelona, 2006, pág. 24.

técnicos internos o en plantilla de la empresa o bien técnicos externos contratados por la misma.

2.3.2.1 Identificación de las fuentes

Una vez determinados los hechos sobre los que quiere obtenerse la prueba informática se procederá a la identificación de las fuentes. Por ejemplo, en el supuesto de un correo electrónico lo sería el propio correo, el archivo contenedor (normalmente el propio PC) y finalmente los *logs* o registros de los servidores, el disco duro del ordenador etc.

En esta primera fase, debe documentarse el lugar o los objetos sobre los que tiene lugar la investigación realizando los actos adecuados a ese fin. Entre los citados actos, pueden tomarse fotografías del lugar y/o de los componentes objeto de análisis, incluidos los cables y los puertos, reseña de los números de identificación de las partes o piezas, del lugar donde se hallen, etc. Todo ello con la finalidad de ofrecer la información veraz sobre el estado del sistema y, en su caso, para poder reconstruirlo con posterioridad. Así mismo, deberán adoptarse ciertas precauciones como que las impresoras terminen de imprimir y comprobar que el ordenador está apagado. Se procederá de modo distinto si se trata de un ordenador apagado o encendido adoptando las precauciones necesarias para que no exista pérdida de datos. De tratarse, por ejemplo, de un ordenador portátil es necesario extraer la batería con mucha precaución porque de estar funcionamiento podría ocasionar la pérdida de datos importantes. Es importante también que se desconecten la alimentación y dispositivos de *sockets* en el propio ordenador, con el fin de evitar un eventual acceso remoto al ordenador objeto de análisis, aún en reposo, al efecto de destruir o modificar datos o ficheros. Se dejará constancia y se documentará como se han obtenido las contraseñas (usuario, material cercano como documentos etc.). También, se identificarán los dispositivos y se determinará cuales servirán para la recuperación de datos de: la unidad principal; del monitor, teclado y ratón; cables; unidades de alimentación; modem (pueden contener números de teléfono); unidades y dispositivos externos; tarjetas de red inalámbricas; routers; lápices de memoria, tarjetas de memoria, Firewire conectado etc. Se tomarán los manuales de hardware y software; cualquier cosa que pueda contener una contraseña, claves de cifrado; claves de seguridad etc.

La información buscada puede hallarse no solo en computadoras sino en otros dispositivos electrónicos como las PDAs. Estos dispositivos contienen un microprocesador pequeño con un teclado en miniatura y una pantalla de visualización junto con la memoria en la que se almacena toda la información.

La memoria se mantiene activa por las baterías y si esto no funciona toda la información contenida en el organizador se puede perder. Sin embargo, los datos pueden ser recuperados de la memoria flash.

El proyecto de Norma 71506 sobre metodología para el análisis forense de las evidencias electrónicas, que establece la metodología para la preservación, adquisición, documentación, análisis y presentación de evidencias electrónicas, trata en su capítulo séptimo «la adquisición de evidencias electrónicas» detallando las precauciones a adoptar si el lugar del incidente está delimitado físicamente. Establece también una serie de recomendaciones en supuestos de adquisición de datos distinguiendo entre: los «sistemas apagados» dentro de los cuales destina un subapartado a dispositivos móviles; y los «sistemas encendidos» dentro de cuyo apartado incluye un subapartado referido a los dispositivos móviles y otro referido a los entornos virtualizados. En este último supuesto un equipo físico o varios están recreados de forma simulada dentro de una máquina física utilizando recursos disponibles. En un equipo están en funcionamiento a la vez todos ellos como si se tratara de varios equipos físicos individuales.

2.3.2.2 Captura de la información y copia

Tradicionalmente, se ha sostenido en informática forense la necesidad de efectuar copias de toda la información obrante en un dispositivo independientemente de la investigación que venga efectuándose. Sin embargo, ello en la actualidad cada vez es más difícil, en primer lugar, por la diversidad y aumento de tamaño de los dispositivos de almacenamiento, y en segundo lugar, por las normas protectoras del derecho a la intimidad y las órdenes judiciales que deben ser restrictivas. Una investigación que solo requiere un archivo único o la impresión de un correo electrónico no requiere de la conservación o copia de todo un servidor. El experto informático puede también encontrase en supuestos en que no puede efectuar una copia forense, ya porque no puede apagarse el ordenador o porque no puede acceder a él, en estos casos deberá actuar «en caliente» según terminología de los técnicos.

Por otro lado, se presentan otros problemas en cuanto a la conservación de la información ya que no toda es estática –como la que se halla en un disco duro- sino que la información también puede ser dinámica. La información es dinámica cuando los datos se hallan en movimiento, como en el tráfico de la red, o la memoria de un ordenador en constante estado de cambio. La conservación de la información en estos últimos supuestos no podrá cumplir con el principio de reproducción, por cuanto según el tiempo de captura dichos

datos habrán variado. A diferencia de los primeros que serán los mismos en dos tiempos diferentes.

En este sentido, cabe distinguir respecto a la información objeto de la investigación pericial, según el «estado» y/o el «dispositivo» en el que se halle. Así, podemos hablar de:

- Información almacenada o depositada en dispositivos electrónicos. En este caso, la información se halla en estado estático y es susceptible de ser recogida para su análisis sin mayores dificultades que las que tengan relación con el acceso al dispositivo y/o a los datos. El acceso a la información puede ser directo o remoto.

- Información dinámica. Se trata, en este caso, de información en procesamiento (*in working process*) que debe ser capturada mediante el uso de instrumentos y dispositivos electrónicos adecuados. Esta interceptación puede ocasionar la afectación del derecho fundamental a las comunicaciones. Aunque no siempre. En este sentido, podemos distinguir entre la captura de datos de, por ejemplo, las comunicaciones entre las computadoras de una empresa y la de los programas de correo electrónico de los empleados. En el primer caso, no se producirá mayor afectación de derecho fundamental alguno. Sin embargo, en el segundo caso, probablemente se produzca una intromisión ilícita en el derecho a la actividad y las comunicaciones de los afectados por la intervención.

El análisis y/o captura de la información dinámica o en procesamiento plantea, además, otros problemas referentes a la eficacia que pueda tener la investigación pericial. Desde este punto de vista, me refiero a los supuestos en los que se están produciendo infracciones o violaciones de derechos que son, precisamente, el objeto y la finalidad de la pericia. En este caso, más allá de la legitimidad del análisis y pericia, se plantea el problema del acceso a la información dinámica con la reserva y sigilo necesarios a fin de evitar la detección de la actividad investigadora por los intervinientes en el proceso electrónico objeto de investigación. En ese caso, se puede producir la pérdida de los hechos estudiados ante la cesación de la actividad o, incluso, la destrucción de las evidencias ante el conocimiento por parte de los infractores de la existencia de la investigación[101].

[101] A esta cuestiones se refieren DARAHUGE y ARELLANO que consideran que la información puede estar en uno de los siguientes estados: « *1- Almacenada: Se encuentra en un reservorio a la espera de ser accedida (almacenamiento primario, secundario o terciario), es un estado estático y conforma la mayoría de recolecciones posibles; sin embargo difiere de la mayoría de los indicios recolectados en que puede ser accedida por medios locales y/o remotos.; II - En desplazamiento: Es decir, viajando en un elemento físico determinado (cable, microonda, láser etc.) es susceptible de captura mediante intercepción de dicho elemento y está condicionada por las mismas cuestiones*

El modo en que pueden efectuarse las copias puede ser distinto, así la copia de información estática o datos estáticos puede efectuarse de dos formas: copia de archivo o copia del flujo de bits. Una «copia de archivo» también puede dar problemas en algunos sistemas de formateo y almacén de archivos ya que, aunque no necesariamente, puede que existan metadatos asociados al archivo. Un ejemplo es el sistema de archivos NTFS con la existencia de flujos de datos alternativos (ADS) donde es posible almacenar información extra como configuración, información dinámica etc. Cuando un archivo se copia utilizando el mismo sistema operativo es decir, de una carpeta a otra los datos ADS se conservan. Sin embargo, si el mismo archivo se copia en un dispositivo USB formateado con el sistema de archivos FAT los datos se perderían. Por otro lado, la «copia de flujo de bits» puede llevarse a cabo de forma prima bit a bit replicándose en un solo archivo o varios archivos segmentados; o en un archivo estructurado (EnCase), bite a bite de una manera estructurada, y en la mayoría de los casos con una función de protección, tales como segmentos de hashes MD5, metadatos del proceso de investigación, notas de los analistas.

La verificación de la copia forma parte del proceso forense. Tradicionalmente se utiliza una verificación matemática de la copia utilizando CRC, MD5 o SHA (*Secure Hash Algorithm*), técnicas de hashing. Un bit no es parecido sino idéntico a otro bit. La copia bit a bit sin incidencias hace que una archivo digital sea idéntico al original. Ello facilita que si se conserva el original en el Juzgado el perito pueda trabajar sobre una copia certificada sin riesgo a destrucción del primero a diferencia de un documento original escrito. Es fundamental documentar las diligencias, y actuar siempre de modo que se respete el derecho a la defensa y el sometimiento a contradicción.

---

legales que la escucha telefónica o la violación de la correspondencia; III -En procesamiento: Es el caso más complicado y constituye la primera decisión a tomar por el investigador. Ante un equipo en funcionamiento, donde la información está siendo procesada, es decir modificada, actualizada y nuevamente resguardada, debe decidir si apaga o no el equipo. Esta decisión es crítica y puede implicar la pérdida de información. Si decide mantener el equipo encendido, corre el riesgo de haber sido detectado durante su aproximación al equipo y que en realidad la actividad del mismo esté consistiendo en borrar de manera segura (técnicas específicas de eliminación de la información que hacen irrecuperable a los métodos informático-forenses, es decir, borra sin dejar trazas), con lo que cuanto más tiempo permanezca el equipo funcionando mayor será el daño producido. Si por el contrario decide apagar el equipo, es posible que éste tenga un mecanismo de seguridad ante estos eventos que dispare las mismas acciones de borrado sobre los equipos remotos, eliminando enlaces y reservorios dentro de la misma red o en redes externas (es muy común que con fines delictivos o no la información sea almacenada en un reservorio remoto, lo que aumenta su seguridad y confiabilidad, ya que está exenta de los riesgos edilicios, físicos y lógicos, del local donde se utiliza)». Véase DARAHUGE, M.E Y ARELLANO GONZALEZ, L.E., *Manual de Informática Forense* (*Prueba Indiciaria Informático Forense)*, Ed. Errepar, 2012, pág 64.

Según al tipo de replicación que se lleve a cabo hablaremos de[102]:

a) Copia: reproducción exacta de la información contenida en un elemento físico original, independiente del dispositivo de almacenamiento electrónico. Mantiene el contenido, pero los atributos pueden cambiar durante la reproducción
b) Duplicado: reproducción exacta digital de todos los datos contenidos en un dispositivo de almacenamiento digital. Mantiene el contenido y los atributos (por ejemplo, una copia de flujo bits, copia bit a bit y volcado sector)
c) Imagen: representación digital precisa de todos los datos contenidos en un dispositivo de almacenamiento digital. Mantiene los contenidos y atributos pero puede incluir los metadatos, como los CCR, el valor hash y la información de auditoría.

El proceso de «copia» se relaciona con el proceso de replicación lógica, es decir, un contenedor de datos (el objeto), como un archivo, se replica sobre la base de las dimensiones de los metadatos asociados con el dispositivo físico que se copió, pero no incluye los metadatos (atributos), sino forman parte del objeto que está siendo copiado. Por ejemplo, la copia de un archivo o un simple correo electrónico, incluirá el archivo o el contenido del correo electrónico, pero no necesariamente mantendrá la fecha de creación de los archivos o los datos de transporte de un correo electrónico. A diferencia del anterior el proceso de «duplicación» replica los datos físicos e incluye los atributos o metadatos, normalmente no integra ningún tipo de validación, o la información de autenticación como parte de la copia. Y finalmente la copia de la «imagen» duplica íntegramente la información y/o metadatos incluidos. Un ejemplo sería el archivo EnCase[103].

---

[102] Véase BECKETT, Jason. Thesis, F*orensic Computing: A Deterministic Model for Validation and Verification through an Ontological Examination of Forensic Functions and Processes*. Adelaide South Australia, January 2010. School of Computer and Information Science. Division of Information Technology, Engineering, and the Environment. University of South Australia, págs. 30-32.

[103] Actualmente se ha diseñado un procedimiento llamado de búsquedas ciegas que garantiza la no vulneración de los derechos fundamentales del secreto de comunicaciones y el derecho a la intimidad, mediante herramientas como ENCASE u otras similares que permiten la extracción de la información relevante para la empresa mediante la utilización de palabras clave cuya búsqueda se efectuará en los ficheros existentes, los borrados y el resto de disco, sin que se acceda a la lectura de toda la información obrante en el dispositivo electrónico (Autos 46/2006 y 27/2007 de la AP Barcelona-Juzgado de lo Mercantil 2 , STSJ del País Vasco, Sala de lo Social de 11 de octubre de 2005, y STSJC de Madrid, Sala de lo Social de 27 de diciembre de 2005).

Para el aseguramiento el informático forense se valdrá de unas particulares funciones matemáticas conocidas como las funciones de «Hash». Estas se aplican sobre la información que se adquiere –que se copia- y la identifican de forma única. De manera que si vuelven a aplicarse sobre la misma información original, o sobre cualquiera de sus copias, siempre devolverán el mismo identificador. De no ser así, querrá decir que la información ha sido alterada, bien sea de forma deliberada o accidental.

Una buena garantía de protección es hacer constar en acta notarial los datos identificativos de personas, fuentes de información y especialmente de los hashes. El valor probatorio aumentará considerablemente si la adquisición se ha efectuado ante acta, si los testigos se quedaron copia de los hashes, e incluso si se adjuntan fotografías o vídeo, y el proceso quedó registrado y plasmado en un documento público.

Técnicamente el experto efectúa una imagen o copia espejo, es decir, bit a bit. Una copia a nivel lógico desde el primer al último bit de información contenida en el disco, para lo cual deberá conocer técnicas distintas según el caso. No se trata de una copia de ficheros sino de una copia a más bajo nivel que se limita a transcribir la unidad de información más elemental (los bits: ceros y unos) desde el dispositivo original a otro de destino. El dispositivo copiado suele ser un disco duro pero puede tratarse también de una agenda electrónica, una memoria USB, una memoria RAM, un CD, un DVD, un teléfono móvil etc. Una vez efectuada la copia, debe calcularse el hash aplicando la función sobre la información a evaluar, se trata de su huella criptográfica. El resultado, según la función de hash que se utilice (comúnmente SHA-1 en la actualidad) es una cadena alfanumérica de longitud fija (160 bits, 40 caracteres en el caso SHA-1). Esta cadena es independiente del tamaño de la información sobre la que se ha calculado. Solo con variar un bit de la información original el hash resultante es completamente distinto al anterior. Las funciones del hash son un algoritmo matemático que además de las características mencionadas, verifican también que para un hash determinado es imposible reconstruir el mensaje o información original y tampoco es posible modificar la información original para conseguir un hash a voluntad. Actualmente se utiliza el Hash MD5 efectuándose la copia a través de un aparato «logic cube», reconocido a nivel pericial por su fiabilidad.

Como hemos señalado en ocasiones el proceso de adquisición de datos no contempla la copia completa de un dispositivo, sino que puede limitarse a determinados registros aislados, e-mails etc. En estos casos también debe garantizarse la mayor transparencia posible en la obtención de evidencias. El experto debe valorar según su criterio la procedencia o no del cálculo del hash, aunque, en general, deberá realizarse el proceso de cálculo de los hashes sobre

todas las fuentes de información que se adquieran siempre que sea técnicamente posible.

En el supuesto que la investigación y posterior informe versen sobre una página web, es aconsejable guardar el contenido en un disco duro de ordenador de modo que pueda acreditarse la fecha de entrada en el archivo informático y que se ha bajado de modo íntegro. Toda la actividad que se realiza navegando por Internet queda también registrada en el equipo del usuario. Los navegadores de cara a aumentar la velocidad guardan en un área del disco todas las imágenes de las páginas visitadas de forma que, al volver a dicha página el navegador recupera las imágenes del disco en vez de descargarlas de nuevo. Muchos navegadores permiten borrar esta información al salir del programa pero, la información sigue ahí y se puede recuperar. Lo mismo ocurre con el historial, que no es más que una lista de direcciones URL de las páginas visitadas, lo cual permite al usuario acceder de forma más rápida a una página que visitó previamente. Ejemplos de herramientas para ello lo son: Chat Sniper, IECacheView, MozillaCacheView, OperaCacheView, ChromeCacheView, VideoCacheView, MyLastSearch, SkypeLogView, LiveContactsView o FlashCookiView[104].

2.3.2.3 Preservación

La preservación de las pruebas electrónicas tiene como objetivo que éstas se conserven con la mayor calidad posible y estén disponibles manteniéndose la integridad de los datos. Ello garantiza la posibilidad de acceso, en cualquier momento, a los datos digitales. La preservación debe serlo a largo plazo, debe garantizar el acceso a los datos o información digital a lo largo del tiempo no solo con carácter inmediato, a pesar de su dificultad ya que las infraestructuras y elementos tecnológicos cambian rápidamente. El acceso a la prueba electrónica debe garantizarse mediante una correcta preservación de la misma en tres fases: durante el proceso de investigación digital; durante la tramitación del proceso judicial y finalmente una vez concluido éste en fase de archivo.

En general existen varias técnicas de preservación de la información digital[105]. La técnica de preservación más simple es la «preservación de los sistemas

[104] Véase MARTÍNEZ DE CARVAJAL HEDRICH, Ernesto. *Informática Forense, 44 casos reales*, ed. Ernesto Martínez de Carvajal Hedrich, Julio 2012, pág. 181.

[105] La información sobre las distintas técnicas de preservación de la información digital que se exponen a continuación se ha obtenido del artículo de ALEJANDRO BIA, A., titulado *La preservación digital ¿un problema tecnológico u organizativo?,* en la obra "El documento

originales». Consiste en mantener el equipo donde se contiene la información digital en funcionamiento. Sin embargo, esta técnica no parece demasiado razonable puesto que con el tiempo será más difícil encontrar repuestos y las prestaciones del equipo se volverán obsoletas.

Otra técnica, aunque también poco factible, sería la «emulación», que permite que el software original sea usado sin necesidad de que el sistema original que lo ejecutaba siga existiendo. La emulación obliga a preservar el emulador –aplicación de software-, el sistema operativo, la aplicación y los datos. La pérdida de uno de estos componentes hace imposible acceder a la información y el emulador, como aplicación de software, debe también ser preservado ya sea mediante emulación o actualización periódica, por lo que sería un nunca acabar.

Finalmente, existen otras técnicas como «la migración» y «el replicado y rejuvenecimiento». En cuanto a la migración consiste en convertir la información a nuevos formatos. Sabemos que los formatos de ordenador cambian continuamente y que algunos formatos y programas de hace unos años son difíciles de leer y ejecutar en la actualidad. Sin embargo, dicha técnica tiene la desventaja de ser pesada y de que los datos originales son modificados en dicho proceso, con el peligro de que se produzcan efectos acumulativos no deseados tras múltiples migraciones.

En cuanto al «replicado y rejuvenecimiento» es una técnica básica de procesamiento de datos. Los datos importantes de los que existe sólo una copia en un ordenador son altamente vulnerables, por ello los centros de procesamiento de datos hacen rutinariamente copias de seguridad y las almacenan en lugares seguros. Debido a que todos los tipos de almacenamiento en los que se graba información digital son efímeros debe planearse el rejuvenecimiento periódico de dicha información, debiendo transferirse los datos almacenados en el repositorio de preservación a nuevos soportes de almacenamiento.

Por otro lado, los soportes digitales son perecederos. Cualquier medio físico que elijamos para conservar información electrónica se degradará por envejecimiento durante el paso del tiempo, o también por circunstancias ambientales como temperatura, polvo, ondas magnéticas etc., con la consiguiente pérdida de información. La información digital también puede quedar dañada, entre otras causas, por un software defectuoso o incompatible, por un virus, por mala fe o negligencia o por una catástrofe. Es por ello que las

---

electrónico: aspectos jurídicos, tecnológicos y archivísticos", Universitat Jaume I, Castello de la Plana, 2008, págs. 433 a 434.

copias de preservación se suelen guardar en una caja de seguridad a prueba de fuego colocada en una habitación con las adecuadas condiciones ambientales para maximizar la vida útil de los soportes informáticos. De haber segundas copias se suelen guardar en otro sitio para maximizar la seguridad. Para detectar fallos, se realizan verificaciones periódicas de la integridad de los datos[106].

El proceso de investigación digital garantizará mejores resultados si con carácter preventivo las organizaciones, ya sea dentro o fuera del entorno empresarial, disponen de protocolos detallados que aseguren la integridad de los hechos electrónicos objeto de estudio forense, de tal forma que se evite la manipulación de los mismos por los efectos de la modificación intencionada o «tampering», descargas electrostáticas, campos magnéticos o conexión accidental a redes inalámbricas. Por su parte, los técnicos encargados de una primera respuesta sobre los hechos electrónicos objeto de estudio, deben poner especial cuidado en almacenar éstos en soportes adecuados para garantizar su integridad. De igual modo, deben manipularlos con indumentaria adecuada, especialmente adaptada para evitar descargas electrostáticas y no portar equipos que puedan crear señales de radiofrecuencia y alterar el espectro radioeléctrico de la escena de interés, lo cual lleva en ocasiones a la necesidad de utilizar soporte estancos o aislados que eviten las interferencias externas que puedan modificar los datos originales. Asimismo, es recomendable precintar y sellar en soportes adecuados todas las evidencias encontradas con atención especial a los dispositivos que requieren estar alimentados por una fuente de energía externa. Y es importante también almacenarlas en lugares seguros dedicados a tal fin, si los medios lo permiten, y en su defecto en una caja fuerte en el mismo entorno de trabajo[107].

Las baterías de los dispositivos electrónicos deben ser revisadas a intervalos regulares para preservar las pruebas hasta que se haya efectuado el análisis forense completo y el máximo de tiempo por si la parte contraria quisiera reproducir las operaciones forenses. Sin embargo, no es posible determinar la esperanza de vida de cualquier batería. Un equipo informático debe almacenarse en condiciones normales de temperatura ambiente y libre de influencias magnéticas, tales como receptores de radio. Algunas computadoras son capaces de almacenar datos internos mediante el uso de baterías. El polvo,

[106] Véase BIA, Alejandro. *La preservación digital ¿un problema tecnológico u organizativo?,* en "El documento electrónico: aspectos jurídicos, tecnológicos y archivísticos", Universitat Jaume I, Castello de la Plana, 2008, pág. 436.

[107] Todas ellas son recomendaciones obrantes en el proyecto de la norma 71506, *Tecnología de las Información. Metodología para el análisis forense de las evidencias electrónicas.*

el agua, la arena, el aceite etc. son perjudiciales para la conservación de los equipos informáticos.

Las previsiones anteriores deben tenerse en cuenta también durante el proceso judicial hasta una vez concluido éste. Los hechos electrónicos requieren ser preservados para poder garantizar su reproducibilidad en juicio así como la reproductividad de los estudios efectuados sobre los mismos en supuestos de contrapericias.

Es recomendable la regulación del depósito de dispositivos electrónicos una vez acceden al proceso y una vez concluido éste, así como que la Administración facilite el lugar y medios idóneos para la conservación de los mismos con máximas garantías de conservación y preservación, de modo que pueda accederse a los mismos en cualquier momento con garantía suficiente. Una vez concluido el proceso es fundamental tener en cuenta la regulación sobre protección de datos de carácter personal a efectos de destrucción de la información confidencial[108].

[108] La Agencia Española de Protección de Datos declaró en abril de 2008 que la Guardia Civil había incurrido en infracción grave por el hecho de devolver a un condenado por un delito contra la salud pública, una vez cumplida condena, el material incautado consistente en ordenadores y cámara que contenían información confidencial. Al parecer la Guardia Civil hizo uso de dichos dispositivos, sin autorización judicial, mientras estuvieron en su poder y procedió a un simple formateado previa entrega al sujeto. Con posterioridad el sujeto recuperó los documentos confidenciales que contenían información de investigaciones de la Guardia Civil en relación a seguimientos de sospechosos y escuchas telefónicas y fotografías de investigados y sospechosos en la tarjeta de memoria de la cámara. La Guardia Civil no adoptó las medidas pertinentes para que la información recogida en los mismos fuera eliminada de los respectivos soportes informáticos, antes de su devolución al mismo, sino que se limitó a realizar un formateado lógico del contenido de los discos duros de aquellos ordenadores, que no borra físicamente la información de los mismos y que permite su recuperación y restauración mediante herramientas informáticas de recuperación de archivos sencillas. Según señala la resolución dictada por la AEPD « …*El formateado lógico del disco duro de un ordenador no borra físicamente la información del mismo, sino que realiza una reasignación de sus sectores, (o mas concretamente de una determinada partición del disco, si éste tuviera varias), del tal forma que, si bien se pierde la vieja asignación que permitía acceder a los archivos, estos no son eliminarlos del disco, siendo posible, por tanto, mediante la utilización de herramientas informáticas de recuperación de archivos sencillas, volver a acceder a los mismos y proceder a su restauración. Indicar también, que al eliminar un archivo mediante el sistema operativo, la operación de borrado no asegura la destrucción de información contenida en el archivo, siendo posible la recuperación de la misma con las citadas utilidades informáticas*». Se trataba de una información que no podía ser facilitada a terceros y por lo tanto existió vulneración del deber de secreto garantizado en el artículo 10 de la LOPD, al haber posibilitado que un tercero tuviese acceso a datos personales sin el consentimiento de los afectados y sin que existiera habilitación legal para ello. A tenor del art. 10 LOPD «*El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo*». Como consecuencia la AEPD impuso una sanción por la infracción tipificada como muy grave

2.3.3 Análisis forense: clasificación- identificación- individualización y asociación

El siguiente paso en el análisis forense consiste en la clasificación, identificación, individualización y asociación de los datos y evidencias obtenidas y preservadas conforme se expuso en el apartado anterior. De este modo, adquirida y asegurada la información, entramos en la tercera fase, denominada análisis forense, en busca de evidencias probatorias, rastros o evidencias digitales que conformen los indicios o pruebas que demuestren los hechos que se desean probar. En informática forense toda actividad deja un rastro. Es fundamental que el experto sea un técnico muy bien preparado, conozca aspectos muy variados de sistemas operativos, sistemas de ficheros y multitud de tecnologías, además del conocimiento de las normas y leyes que regulan la prueba, respetando siempre los derechos fundamentales de las personas involucradas en la investigación.

Por regla general, se procederá a supervisar la cadena de custodia preprocesal hasta la llegada a dicha fase de análisis forense, lugar de almacenamiento y estado actual, y se procederá al volcado de datos en el laboratorio, la extracción de los mismos, el filtrado, y finalmente se emitirá el informe con enumeración de todos los acontecimientos. Dicho informe deberá *contener* de forma expresa y detallada los extremos solicitados y sobre los que debe investigar el experto, cada uno de los extremos anteriormente citados, y no sólo deberá contener las conclusiones, sino que deberá contener también, de forma resumida, el procedimiento a través del cual partiendo de determinadas fuentes identificadas y de una concreta metodología se ha llegado a las mismas. Véase el § 8.2.1 sobre la forma que debe revestir un dictamen pericial.

El análisis puede consistir, según el PNE 71506 sobre Tecnología de la Información, metodología para el análisis forense de las evidencias electrónicas, en:

1. La recuperación de ficheros borrados: Este proceso consiste en la localización de las entradas de archivos o carpetas borradas en las estructuras de

---

en el artículo 44.4.g) de la citada Ley Orgánica. De dicha resolución se desprende la importancia de la destrucción de información confidencial que queda bajo la tutela de la ley de protección de datos. Véase sobre el tema la información obtenida en la página web en la dirección http://goo.gl/e0l83G. He solicitado datos de la resolución a la AEPD el 4.12.2013 sin respuesta alguna.

Véase sobre el tema de la destrucción de documentación que contiene información confidencial el artículo publicado por LOSADA, GEMA, MARCO, CRISTINA Y ROMERO, CARLOS, *Destrucción de documentación oficial*, Universidad Complutense de Madrid. Puede consultarse en la página web gpd.sip.ucm.es.

localización de ficheros (tablas tipo FS, MFT, etc.). Es decir, se efectúa una recuperación parcial o total de la información borrada existente en los distintos soportes de almacenamiento, unido a una recuperación de los datos ubicados en las áreas o espacio de disco sin asignar actualmente por el sistema y en el espacio del disco sin utilizar, así como la obtención de las carpetas y archivos «huérfanos» contenidos dentro de los distintos ficheros, de los que se ha perdido su vinculación. Este proceso también supone una búsqueda de sus cabeceras, de archivos completos o fragmentos de éstos existentes en los dispositivos de almacenamiento (8.1).

Cuando se elimina un fichero, en realidad lo único que hace el sistema operativo es eliminarlo del índice de archivos y asignar el espacio que ocupaba a la cadena de espacio disponible, es decir, la información sigue ahí, mientras no se sobrescriba con otro fichero el espacio que ocupaba de ahí la importancia de salvaguardar la prueba en el estado en que se encontró. Basta con poner en marcha el equipo para que se altere el contenido del disco, pudiéndose perder información vital para el caso. Las herramientas de recuperación simplemente rastrean la cadena de espacio libre en busca de ficheros que aún sigan ahí y los deja en su estado original. Para ello los expertos utilizan herramientas como podrían ser: DisskDigger, Recuva, Pandora Recovery o TestDisk. Si sólo se desea recuperar las imágenes se dispone de herramientas específicas como por ejemplo Adroit Photo Recovery y Adroit Photo Forensics[109].

2. El estudio de las particiones y sistemas de archivos: Este proceso consiste en el estudio de las diversas estructuras de contenedores de almacenamiento de los dispositivos (particiones, volúmenes fisios, sistemas RAID, etc.), en los que se pueden encontrar diferentes volúmenes lógicos que contienen los sistemas de archivos (8.2). A veces el problema es que se ha dañado la información correspondiente a la partición, lo que impide totalmente el acceso a los datos. Muchas de las herramientas comentadas permiten a los expertos recuperar una partición perdida así como los sectores de arranque[110].

3. Estudio del sistema operativo: Este proceso consiste en el estudio del sistema o sistemas operativos instalados en los volúmenes lógicos de los dispositivos de almacenamiento, la actividad de los usuarios existentes en el mismo y su política de seguridad (8.3)

[109] Véase MARTÍNEZ DE CARVAJAL HEDRICH, Ernesto. *Informática Forense, 44 casos reales,* ed. Ernesto Martínez de Carvajal Hedrich, Julio 2012, pág. 180.

[110] Véase MARTÍNEZ DE CARVAJAL HEDRICH, Ernesto. Informática Forense, 44 casos reales, ed. Ernesto Martínez de Carvajal Hedrich, Julio 2012, pág. 180.

4. Estudio de la seguridad implementada: Este proceso tiene por finalidad estudiar si las evidencias electrónicas remitidas para su estudio han sido comprometidas. Existen distintos grados de vulnerabilidad de las evidencias electrónicas objeto de análisis, bien por métodos de intrusión, modificación, eliminación y sustracción de la información almacenada en los soportes originales. Se identificará el software malicioso (virus, troyanos, etc.) que pudiera existir en las distintas particiones identificadas, evaluando el grado de intrusión en el sistema informático y qué archivos se han visto comprometidos, identificando de qué modo (8.4).

5. Análisis detallado de los datos obtenidos. Incluye el análisis detallado de las evidencias electrónicas, aprovechando todos los análisis previos ya especificados. Para ello se utiliza un software contrastado en el ámbito forense. Este análisis se debe ajustar estrictamente a las cuestiones planteadas por el organismo o entidad que solicita el estudio forense. Conlleva la realización al mismo tiempo de una clasificación de los datos, así como opcionalmente de un proceso previo de indexado de los mismos, el cual agilizará posteriormente distintas búsquedas de los indicios a encontrar en los soportes digitales, utilizando para ello distintas palabras clave o códigos alfanuméricos preparados al efecto (8.5).

El experto seleccionará aquellas herramientas que sean necesarias para obtener los datos solicitados expresamente por el abogado y que son o pueden ser relevantes para el proceso. Para ello, se acotará la información contenida en el dispositivo digital, y al hacerlo deberán, también, preservarse los derechos fundamentales del usuario del mismo. Cuando se accede, por ejemplo, a la cuenta de correo electrónico de una persona con el objeto de capturar algunos mensajes es inevitable ver los restantes, y de igual modo cuando se pretenden capturar todos los documentos relacionados con una transacción determinada etc. De ahí la importancia de distinguir entre aquellos supuestos en que se puede acceder libremente a la información y aquellos otros que requieren de autorización judicial previa. Entre los primeros, es decir, entre los supuestos en que el experto puede acceder libremente a la información, se hallarían aquellos en que la información pertenece a la esfera privada del solicitante y se halla contenida máquinas de su propiedad, así como también aquellos supuestos en que se trata de información pública de la web (páginas de discusión etc. que no requieran para su acceso claves de ingreso). Entre los supuestos en que se requerirá previa autorización judicial para no vulnerar los derechos constitucionales de terceros se hallan, por ejemplo, aquellos en que se pretende acceder a información privada contenida en máquinas propiedad de terceros o webs de acceso con claves privadas.

Las resoluciones judiciales que autoricen dichas intervenciones deberán ser claras y precisas en cuanto a los extremos y límites de intervención por parte de los expertos en informática forense, garantizando de este modo la licitud de la prueba electrónica en el proceso y la protección de los derechos regulados en nuestra Constitución. Por otro lado, es necesaria la regulación del deber de secreto por parte de dichos profesionales respecto a la información o datos observados y que no tienen relación alguna con el objeto de la medida judicial autorizada.

Existen actualmente una amplia gama de herramientas forenses como ENCASE, Forensic tool Kit (FTK), Pro Discover, Smart, Sleuth Kit[111], Nuix Desktop y Enterprise[112].

Sin ánimo de efectuar un análisis exhaustivo, dado que la actuación informático-forense será efectuará de modo y con técnicas diferentes en cada supuesto, podemos señalar que el experto forense informático podrá efectuar la búsqueda y filtrado de documentación principalmente a través de tres métodos: Revisión exhaustiva, búsqueda ciega por palabras clave y técnicas heurísticas[113]. En primer lugar la «revisión exhaustiva» es aquel método que implica la revisión de todos y cada uno de los activos de la información presentes en el dispositivo digital a ser analizado. En el caso más común de un ordenador, se realiza mediante la apertura indiscriminada de todos los documentos, correos electrónicos y otros activos de información almacenados en el mismo, procediendo posteriormente a su lectura pormenorizada para dirimir si es pertinente a la pericial o no. Si bien es un método exhaustivo, es una técnica desaconsejable por cuanto la investigación se dilata indefinidamente en el

[111] Las herramientas por excelencia para esta fase de análisis e investigación son el *EnCase* y el *Sleunth kit & Autopsy*. El *EnCase* es una aplicación propietaria para la realización de análisis forense mientras que *Sleunth kit & Autopsy* es un conjunto de herramientas de software libre creadas por Dan Farmer y Wietse Venema. Estas aplicaciones funcionan sobre Windows y GNU/Linux respectivamente, pero son capaces de analizar sistemas Unix, Linux, Mac OS X y Microsoft. RIFÀ POUS, HELENA, SERRA RUIZ, JORDI *Análisis Forense de Sistemas Informáticos,* Rivas López, José Luis(coordinadores), septiembre de 2009, ed. UOC, pág. 27. Puede consultarse en la página web webs.uvigo.es.

[112] Véase BECKETT, Jason. Thesis, *Forensic Computing: A Deterministic Model for Validation and Verification through an Ontological Examination of Forensic Functions and Processes*. Adelaide South Australia, January 2010, School of Computer and Information Science, Division of Information Technology, Engineering, and the Environment. University of South Australia, págs. 121 y ss.

[113] En cuanto a los tres métodos e búsqueda y filtrado de documentación y las mejoras técnicas que se han propuesto se sigue en el presente trabajo el hilo expositivo de MENÉNDEZ FRAGUA, Sergio., *Aplicación de técnicas heurísticas como salvaguarda de los derechos fundamentales en la búsqueda y filtrado de documentación en periciales informáticas,* Artículo *INCIDE,* 2011.

tiempo, facilita la comisión de errores humanos dado el volumen de información y existe una elevada probabilidad de vulneración de los derechos fundamentales dado que no acota la información (Sentencia de fecha 29 de abril de 2001 del Juzgado de lo Social, núm. 3 de Vigo).

Un segundo método es el llamado método de «búsqueda ciega por palabras clave». Una vez conocido el objeto de la investigación, se definen una serie de palabras clave o expresiones relevantes asociadas a la misma (nombres de empresa, apodos, números de teléfono etc.), de forma que cualquier documento portador de alguna de esas palabras es seleccionado por el perito para ser revisado. Este método implica mayor eficacia por cuanto se revisan menos documentos y por lo tanto supone una menor inversión de tiempo, a la vez que se vela por una mayor garantía de los derechos fundamentales. Sin embargo, si el contexto de la investigación no está muy claro, pueden utilizarse términos muy genéricos que supondrían la revisión de gran cantidad de documentos cayendo en la trampa de la revisión exhaustiva y perdiendo las ventajas de la búsqueda a ciegas. Si por el contrario se es muy restrictivo en cuanto al listado de palabras clave puede descuidarse información relevante. Por otro lado, este método no puede garantizar de forma absoluta la protección de los derechos fundamentales constitucionalmente protegidos por cuanto por el mero hecho de que un documento contenga una palabra o término determinado no significa que dicho documento no pueda contener contenido personal o íntimo. Además esta técnica sólo es válida para la búsqueda de términos textuales siendo inaplicable a documentación que no esté basada en texto (fotografías, audio, vídeo…). La jurisprudencia viene avalando dicha técnica (Sentencia del Juzgado de lo Mercantil número 2 de Barcelona de fecha 9 de mayo de 2008, y Sentencia de la Audiencia Provincial de Barcelona, Sección 15, de fecha 2 de febrero de 2006[114]).

Finalmente hallamos las «técnicas heurísticas»[115]. Esta técnica se utiliza como complemento a la metodología de búsqueda ciega por palabras clave, está

[114] La Sentencia Audiencia Provincial de Barcelona, sec. 15ª, de fecha 2 de febrero de 2006, nº 46/2006, rec. 711/2005. Pte: González Navarro, Blas Alberto, concluye afirmando que la localización informática de los mensajes que incorpora el informe pericial no es contrario a la intimidad de los demandados: la búsqueda ciega discriminó desde el principio todo lo que pudiera tener alguna relación con ese ámbito, y con lo obtenido no se afecta a su vida íntima, a esa esfera personal y reservada que preserva la dignidad y la libertad individual, sino a ciertos actos puntuales de relevancia estrictamente comercial o empresarial. No es, por tanto, que la indagación efectuada afectara al derecho fundamental a la intimidad personal pero que la misma resultara justificada por un fin legítimo, proporcional, idóneo y necesario, sino que dicha pericial se mantuvo al margen del ámbito constitucionalmente protegido.

[115] En el ámbito de la computación, frente a un problema concreto, se define como «heurística» al método o algoritmo que permite obtener soluciones suficientemente cercanas a la solución óptima, y que son razonablemente aceptables como solución al problema planteado. A pesar de

siendo utilizada en periciales informáticas que son admitidas en procedimientos judiciales. Persigue poder acceder a los documentos electrónicos con la seguridad de que no contienen información personal y, a su vez, reducir el número de documentos a examinar. Aunque no está tampoco exenta de errores permite una mejora razonable sobre las técnicas existentes. Este método consiste en que, una vez efectuada la búsqueda ciega anteriormente descrita, se realiza una segunda criba sobre los resultados obtenidos con el objetivo de detectar los documentos electrónicos que, además de información relevante para el caso, contienen información íntima o personal. Para esta detección de información personal se utilizan diversas variantes del análisis heurístico, que consiste en asignar, de manera ciega y automatizada, una puntuación a cada documento electrónico, basándose en ciertos criterios que pueden variar en cada caso, descartando aquéllos sospechosos de contener información personal en base a dicha puntuación. La implementación exacta de esta técnica puede variar dependiendo de criterios utilizados por cada perito para la puntuación. Este método está basado en las técnicas existentes para la detección de correo basura o spam. En estos casos, el principal problema a abordar es poder detectar cuándo palabras como «sexo» o «juego» se utilizan en un contexto adecuado, y cuándo forman parte de un correo basura. La solución pasa por realizar diversos procesos automáticos sobre cada correo recibido, de forma que cada proceso asigna una puntuación concreta a cada uno de los correos. Cuando la suma total de esta puntuación supera un cierto umbral, el correo se trata como spam y se descarta. Tratándose de un contexto corporativo pueden elaborarse tres listados de palabras: 1. Un listado de palabras corporativas, formado por palabras propias del sector profesional en que se enmarca la pericial (por ejemplo factura, proveedor etc.); 2. Un listado de palabras clave, palabras relacionadas con la investigación (nombres de empresas, direcciones de correo, páginas web etc.); y 3. Un listado de palabras personales (por ejemplo amor, niño, enfermedad etc.). La decisión de si un documento es del ámbito personal responde en base a la diferencia entre el número de apariciones de palabras corporativas y clave de la investigación y el número de palabras personales que contiene un documento. Si esta suma da como resultado un número mayor que cero se considera que ese documento es lo suficientemente no personal como para ser integrado en la revisión manual.

Se han propuesto mejoras a las técnicas anteriores como: la aplicación de la metodología en función del tipo de ubicación del documento que se está procesando, empleando criterios más estrictos, por ejemplo, en el correo electrónico, frente a otros más laxos en supuestos como en un documento de

---

que para dicha metodología la función no tiene porqué ser perfecta, sí es deseable que exista un buen indicador, y por lo tanto que esté definida con rigor y conociendo el contexto del problema.

oficina; por otro lado se emplea también la técnica del proceso de *cropping* o recorte de resultados obtenidos, consistente en eliminar las palabras o los párrafos de los documentos que contengan palabras que hayan sido identificadas como del ámbito privado. Sin embargo, esta técnica puede descontextualizar el documento haciendo llegar al experto a conclusiones erróneas o sesgadas y rompe los principios forenses de no manipulación, asertividad y objetividad. Por otra parte, se plantea el problema de la afectación de la indemnidad o integridad de los hechos y documentos objeto de análisis a efecto de su valoración en sede judicial[116].

La búsqueda, filtrado y obtención de información por parte del informático-forense plantea un grave problema como es el acceso de forma habitual por parte del perito a información y/o datos que exceden de los extremos objeto de informe y que, eventualmente, pueden suponer la afectación de derechos fundamentales, como el derecho a la intimidad. Así sucede, por ejemplo, en aquellos supuestos en que los expertos acceden a una copia espejo o a un conjunto o masa de datos, para elaborar el informe respectivo. La situación expuesta de afectación de derechos puede producirse de forma meramente casual. Efectivamente, a pesar de que la actividad de investigación se realice mediante métodos lícitos de búsqueda, el investigador puede obtener aún involuntariamente datos que supongan una intromisión en los derechos y libertades de los ciudadanos[117]. No cabe ninguna duda que en ese caso el investigador debe apartarse de la fuente de datos y rechazar aquellos que hubiere obtenido y que supongan infracción de derechos y libertades. Ello plantea el problema de los límites de la investigación forense, especialmente en el ámbito civil y mercantil, y la posibilidad no recogida en la Ley de solicitar al Juez civil autorización para poder acceder a datos o informaciones que puedan afectar al derecho a la intimidad o a las comunicaciones de los ciudadanos (Véase sobre esta cuestión el § 3.2).

Por otro lado, el experto puede encontrase con información protegida con una clave. En estos casos es importante también que esté bien determinada judicialmente su actuación, ya que de estar autorizado puede acceder a determinar cuál es la contraseña. Existen muchas herramientas capaces de recuperar contraseñas no cifradas, ya sean las que el usuario utilizaba para acceder a las páginas que visitaba o para acceder a programas específicos,

---

[116] Véase MENÉNDEZ FRAGUA, Sergio., *Aplicación de técnicas heurísticas como salvaguarda de los derechos fundamentales en la búsqueda y filtrado de documentación en periciales informáticas,* Artículo doctrinal I*NCIDE,* 2011, pág. 33.

[117] Así sucede, en realidad, en muchas ocasiones en los que los ciudadanos realizan búsquedas en Internet que pueden finalizar, involuntariamente, en páginas Web donde se aloja contenido ilícito, al que no se debe acceder en previsión de poder incurrir en alguna clase de ilícito.

incluido correo electrónico, hojas de cálculo etc. Ejemplos de este tipo de herramientas son BrowserPasswordDecryptor, MessenPass, Mail PassView, BulletsPassView, ShoWin, AsteriskKey, WirelessKeyDumpo, Nirsoft o SecurityXploded. Otras herramientas son capaces de ir más allá y recuperar contraseñas cifradas, como en el caso de Cain"Abel u otras que se basan en la «fuerza bruta»[118].

* * *

[118] Véase MARTÍNEZ DE CARVAJAL HEDRICH, Ernesto. *Informática Forense, 44 casos reales.* Julio 2012, pág. 181.

CAPÍTULO III.- DERECHOS CONSTITUCIONALES Y LÍMITES PARA LA OBTENCIÓN DE LA PRUEBA INFORMÁTICA

3.1 Derechos y garantías fundamentales relativos a la esfera individual del ciudadano

La validez de cualquier prueba está sometida a la condición de no afectar los derechos y libertades de los ciudadanos que se concretan, en esta materia, en el art. 18 de la Constitución cuando establece la garantía del: *« 1. (…) derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en el sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos»*. Nótese la previsión del constituyente que en una fecha ya tan lejana como 1978 previó la importancia que iba a adquirir la informática en la sociedad y la posibilidad de que estos medios técnicos afectasen los derechos civiles de los ciudadanos reconocidos en los párrafos 1º a 3º del artículo 18 CE. En su virtud no cabe ninguna intromisión en la esfera privada de los ciudadanos salvo en los supuestos especialmente previstos en la Constitución que son: la orden judicial, el consentimiento del titular[119] y el flagrante delito[120] (Véase sobre estos límites el § 3.1.2.2.). De los supuestos expresados el de mayor interés es el de la autorización judicial supuesto en el

[119] El Tribunal Constitucional se ha pronunciado reiteradamente respecto al consentimiento en estos supuestos indicando que «El consentimiento eficaz del sujeto particular permitirá la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno (SSTC 83/2002, de 22 de abril, FJ 5 y 196/2006, de 3 de julio, FJ 5), aunque este consentimiento puede ser revocado en cualquier momento (STC 159/2009, de 29 de junio, FJ 3). Ahora bien, se vulnerará el derecho a la intimidad personal cuando la penetración en el ámbito propio y reservado del sujeto «aun autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida» (SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 5; y 70/2009, de 23 de marzo, FJ 2).

[120] Los supuestos de consentimiento y flagrante delito son de interpretación rígida y vienen referidos a supuestos muy concretos y detallados por la Jurisprudencia. Así, el consentimiento debe ser libre, claro y expresado por el titular de la vivienda o domicilio en el que se pretende entrar. Por su parte, el concepto de flagrancia debe entenderse en su sentido más literal y etimológico como una situación evidente, estridente a ojos de cualquier persona. Único supuesto en el que puede ser lícita la entrada en domicilio. Así, lo entendió la STC 341/1993, de 18 de noviembre, que declaró la inconstitucionalidad del artículo 20 de la Ley de protección de la seguridad ciudadana que interpretaba, inconstitucionalmente, el concepto de flagrancia.

que el Juez pondera los derechos afectados y puede autorizar una intromisión lícita en la esfera privada de los ciudadanos. En consecuencia, y en sentido negativo, será ilícita y, por tanto, nula cualquier prueba obtenida violando los derechos fundamentales lo que sucederá en el caso de intromisiones en la esfera privada de los ciudadanos sin respeto a los límites constitucionales (Véase sobre ilicitud de la prueba el § 3.3).

También resulta de interés en esta materia la normativa europea, concretamente: el art. 8 del Convenio Europeo para la protección de los derechos humanos y de las libertades fundamentales que establece: «*1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás»*. También en esta materia debe destacarse la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

El avance de la tecnología actual y el desarrollo de los medios de comunicación ha obligado a extender la protección a la vida privada personal y familiar más allá de la inviolabilidad de domicilio y de la correspondencia, como ámbitos que deben quedar excluidos del conocimiento ajeno y de las intromisiones de terceros ajenos a las mismas salvo autorización del interesado. Así lo ha entendido y declarado el TC que se ha pronunciado señalando que: *«El avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida»…/…* «*Estos derechos han adquirido también una dimensión positiva en relación con el libre desarrollo de la personalidad, orientada a la plena efectividad de estos derechos fundamentales. En efecto, habida cuenta de que nuestro texto constitucional no consagra derechos meramente teóricos o ilusorios, sino reales y efectivos …, se hace imprescindible asegurar su protección no sólo frente a las injerencias ya mencionadas, sino también frente a los riesgos que puedan surgir en una sociedad tecnológicamente avanzada*». (STC 110/1984, de 26 de noviembre, FJ 3).

A esta nueva realidad ha sido sensible la jurisprudencia del Tribunal Europeo de Derechos Humanos, como se refleja en las Sentencias de 21 de febrero de 1990, caso POWELL Y RAYNER CONTRA REINO UNIDO; de 9 de diciembre de 1994, caso LÓPEZ OSTRA CONTRA REINO DE ESPAÑA, y de 19 de febrero de 1998, caso GUERRA Y OTROS CONTRA ITALIA» (STC 119/2001, de 24 de mayo, FJ 5). El Tribunal Europeo de Derechos Humanos en su interpretación extensiva del concepto «*vida privada*» del art. 8 del Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales considera en la Sentencia de 16 de febrero de 2000, dictada en el caso AMANN CONTRA SUIZA, que «*el término «vida privada» no se debe interpretar de forma restrictiva»*, de forma que éste *«engloba el derecho del individuo de crear y desarrollar relaciones con sus semejantes»*, sin que «*ninguna razón de principio permita excluir las actividades profesionales o comerciales*».

En este sentido garantista se ha pronunciado la Recomendación sobre privacidad de Internet 1999 que en su Preámbulo señala que: «*el desarrollo de las tecnologías y la generalización de la recogida y del tratamiento de datos personales en las «autopistas de la información» suponen riesgos para la intimidad de las personas naturales…», «…las comunicaciones con ayuda de las nuevas tecnologías de la información están también sujetas al respeto de los derechos humanos y de las libertades fundamentales, en concreto al respeto a la intimidad y del secreto de las comunicaciones, tal y como se garantizan en el artículo 8 de la Convención Europea de los Derechos Humanos*», «*…el uso de Internet supone una responsabilidad en cada acción e implica riesgos para la intimidad» (introducción), por cuanto cada visita a un sitio de Internet deja una serie de «rastros electrónicos*» que pueden utilizarse para establecer *«un perfil de su persona y sus intereses*» (apartado II, 2), subrayando también que «*…La dirección de correo electrónico constituye «un dato de carácter personal que otras personas pueden querer utilizar para diferentes fines…*» (apartado II, 6)[121].

Por su parte, la Resolución del Parlamento Europeo, de 17 de septiembre de 1996, sobre el respeto de los derechos humanos en la Unión Europea establece en su apartado 53 que: «*el respeto de la vida privada y familiar, de la reputación, del domicilio y de las comunicaciones privadas, tanto de las personas físicas como jurídicas, así como la protección de datos de carácter personal son derechos fundamentales básicos respecto de los cuales los Estados miembros deben ejercer una especial protección, habida cuenta de la incidencia negativa que sobre los mismos tienen las nuevas tecnologías y que sólo la armonización de las*

[121] La recomendación sobre privacidad en Internet (R (99) 5, de 23 de febrero de 1999 junto a la recomendación sobre datos personales utilizados en el sector policial (1987) ambas del Comité de Ministros desarrollan el Convenio núm. 108 del Consejo de Europa sobre protección de datos informatizados de carácter personal del año 1981 vinculante para España.

legislaciones nacionales en la materia, confiriendo una alta protección, es susceptible de responder a este desafío». La Resolución de igual órgano de 17 de diciembre de 1998 señala, en su apartado 23, que «*el derecho al respeto de la vida privada y familiar, del domicilio y de la correspondencia, así como a la protección de los datos de carácter personal, representan derechos fundamentales que los Estados tienen la obligación de proteger y que, por consiguiente, toda medida de vigilancia óptica, acústica o informática deberá adoptarse dentro de su más estricto respeto y acompañada en todos los casos de garantías judiciales*».

3.1.1 Derecho fundamental del secreto de comunicaciones

La Constitución Española contempla como derecho fundamental el derecho a las comunicaciones en su artículo 18.3 al establecer que «… *Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicia*l». El art. 18.3 de la C.E. no define el término «*comunicación»*, pero la doctrina mayoritariamente entiende incluidos en dicho concepto todos los medios modernos de comunicación que existen en la actualidad y los futuros dada la ágil evolución de las nuevas tecnologías. En cualquier caso, se considera unánimemente requisito indispensable para que haya «*comunicación*», en los términos del art. 18.3 C.E., que: a) exista una infraestructura o artificio comunicativo, que no tiene que ser sofisticado; b) una distancia real entre los comunicantes; y c) que la comunicación se realice por canal cerrado (puesto que si la transmisión de la información o mensaje no se hace por canal cerrado, en modo alguno hay que considerar que estemos ante la posibilidad de aplicar el derecho al secreto de las comunicaciones ya que no habrá expectativa de secreto).

3.1.1.1 Definición y contenido del ámbito constitucional de la Comunicación

La comunicación, cuya interceptación prohíbe la Constitución, es la realizada sin publicidad y, por tanto, no susceptible de ser conocida por terceros[122]. En este

[122] Véase respecto de la clase de comunicaciones que no se hallan dentro de la esfera de protección del art. 18.3 CE., RIVES SEVA, Antonio Pablo, *La intervención de las comunicaciones en la Jurisprudencia Penal*, ed., Aranzadi, Navarra, 2000, pág. 22 y doctrina citada por el mismo, según el cual las comunicaciones de ámbito público (televisión, radio u otros canales, cuyos destinatarios son un número indeterminado de personas), no se hallan amparadas por el art. 18.3 C.E. sino por el art. 20.1 C.E., precepto que reconoce y protege los derechos a expresar y difundir libremente los pensamientos, ideas y opiniones. El mismo criterio es sostenido por

ámbito debemos incluir los sistemas de comunicación vía Internet. Estos sistemas pueden funcionar mediante canales abiertos y cerrados. Los primeros son aquellos, como los chats, grupos de discusión e, incluso, la comunicación pública general como la que se produce mediante la radio y la televisión. En estos casos la comunicación fluye libremente sin ninguna limitación ni exclusión entre los interlocutores. Es por ello que, en estos casos, nada impide que uno de los interlocutores pueda retener (grabar) el contenido de una conversación, e incluso mostrarla a un tercero, ya que no existe entre las partes un deber de reserva de lo comunicado. Ahora bien, cuestión distinta es el supuesto de los canales cerrados de comunicación que presentan una expectativa de que se garantice su libertad de comunicación. Este es el supuesto de los correos electrónicos, mensajes de texto o, incluso, comunicaciones en Chats eligiendo la opción: «privado». Todos estos tipos de comunicaciones están protegidas por el art. 18.3 CE, en tanto que lo que, en definitiva, se pretende es no permitir el acceso a un tercero a una comunicación privada[123].

La protección constitucional viene referida a la comunicación y a su contenido que resultan secretas para cualquiera ajeno a la misma. En este sentido, el concepto de secreto es de contenido formal al estar vinculado directamente con la comunicación y no con su contenido. De modo, que lo que se protege no es la clase o contenido de lo comunicado, sino la comunicación en sí misma. Precisamente en este sentido se pronunció la importante S.T.C. 114/1984, de 29 de noviembre, ponente Sr. Díez-Picazo y Ponce de León, la cual en su F.J. 7º dispuso que el secreto «*se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado*»[124]. De todo ello se deduce que a criterio del T.C. no toda comunicación es necesariamente íntima pero sí secreta y que la protección constitucional se extiende al propio proceso de comunicación.

La comunicación implica además de la protección de la comunicación en sí misma y de su contenido algunos otros aspectos referentes a la misma. En este sentido «e*l Tribunal Constitucional ha reiterado (entre otras, SSTC 281/2006, de 9 de octubre, FJ 4; 230/2007, de 5 de noviembre, FJ 2; 142/2012, de 2 de julio, FJ 3,*

LÓPEZ-FRAGOSO ALVÁREZ, Tomás, *Las intervenciones telefónicas en el proceso penal*, ed. Colex, Madrid, 1991, págs. 21 y 22.

[123] Véase FERNÁNDEZ RODRÍGUEZ, José Julio, *Secreto e intervención de las comunicaciones en Internet*, ed. Thomson Civitas, Madrid, 2004, pág. 99-100; y RODRÍGUEZ RUIZ, Blanca: *El secreto de las comunicaciones: tecnología e intimidad*, ed. Mc Graw Hill, Madrid, 1998, pág. 67.

[124] En igual sentido, la S.T.C. 34/1996, 2a, de 11 de marzo, ponente Excmo. Sr. de Mendizábal Allende, en su F.J. 4º así como la S.T.C. 70/2002, de 3 de abril, 1a, ponente Excmo. Sr. Garrido Falla, F.J. 9º.

y 241/2012, de 17 de diciembre, FJ 4) que el derecho al secreto de las comunicaciones (art. 18.3 CE) consagra tanto la interdicción de la interceptación como el conocimiento antijurídico de las comunicaciones ajenas, por lo que dicho derecho puede resultar vulnerado no sólo por la interceptación en sentido estricto –aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o captación, de otra forma, del proceso de comunicación sino también por el conocimiento antijurídico de lo comunicado, como puede suceder, sin ánimo de exhaustividad, en los casos de apertura de la correspondencia ajena guardada por su destinatario o de un mensaje emitido por correo electrónico o a través de telefonía móvil. Igualmente se ha destacado que el derecho al secreto de las comunicaciones protege no sólo el contenido de la comunicación, sino también otros aspectos de la misma, como la identidad subjetiva de los interlocutores, por lo que queda afectado por este derecho tanto la entrega de los listados de llamadas telefónicas por las compañías telefónicas como el acceso al registro de llamadas entrantes y salientes grabadas en un teléfono móvil (por todas, SSTC 123/2002, FJ 6; 56/2003, FJ 3; 230/2007, FJ 2; 142/2012, FJ 3, y 241/2012, FJ 4; así como las Sentencias del Tribunal Europeo de Derechos Humanos de 2 de agosto de 1984, caso Malone c. Reino Unido, § 84, y, de 3 de abril de 2007, caso Copland c. Reino Unido, § 43») STC Sentencia 115/2013, de 9 de mayo de 2013, FJ. 3.

En cuanto a los demás aspectos constitucionalmente protegidos relativos a la comunicación también la STC 114/1984, de 29 de noviembre, siguiendo la S.T.E.D.H. de 02.08.1984 (caso MALONE CONTRA EL REINO UNIDO) dispuso que «*el concepto de secreto no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales*». En este sentido se ha pronunciado también la STC 123/2002, de 20 de mayo negando que pueda accederse sin autorización judicial a la relación de llamadas telefónicas del titular de un teléfono, con independencia de su contenido, por considerar que tales datos están comprendidos en el ámbito del secreto de comunicaciones del art. 18.3 CE. En su Sentencia de 02.08.1984 (caso Malone) el T.E.D.H. se refería a la técnica de «*comptage*» la cual consiste en la utilización de un artificio técnico que registra los números marcados en un determinado teléfono, la hora y la duración de cada llamada, aunque no el contenido de la comunicación misma. El Alto Tribunal consideró que el empleo de dicha técnica por parte de la policía de Londres constituía una infracción del art. 8 del C.E.D.H[125].

[125] Para un análisis más detallado del citado pronunciamiento del T.E.D.H. puede consultarse RIVES SEVA, Antonio Pablo, *La intervención de las comunicaciones en la jurisprudencia penal*, ed. Aranzadi, Navarra, 2000, págs. 250 a 254.

De igual modo la sentencia del TEDH de 30 de julio de 1998 (TEDH 1998, 31) en el caso VALENZUELA CONTRERAS, califica como injerencia de la autoridad pública en el ejercicio del derecho al respeto de la vida privada y de la correspondencia el registro mediante aparato contador de los números de teléfono marcados desde un determinado aparato, aun cuando este tipo de vigilancia no implique acceso al contenido de la conversación, señala que desde esta perspectiva es claro que inviolable no solo es el mensaje, sino todos aquellos datos relativos a la comunicación que permitan identificar a los interlocutores o corresponsales o constatar la existencia misma de la comunicación, su fecha, duración y todas las demás circunstancias concurrentes, útiles para ubicar en el espacio y en el tiempo el hecho concreto de la conexión. Lo que supone en definitiva que no cabe disociar sin merma relevante de garantía, realidades tan sustancialmente integradas como son el mensaje y el proceso de transmisión

Entre los pronunciamientos judiciales en orden al concepto de «secreto» consagrado en el art. 18.3 C.E., cabe citar S.T.S. de 25.09.2003, 2a, ponente Excmo. Sr. Martínez Ariete, el Auto del T.C. nº 30/1998, 2ª, sección 4ª, y la S.T.C. 56/2003, Sala 2ª, de 24 de marzo, ponente Excma. Sra. Pérez Vera, los cuales mantienen de igual modo a las resoluciones anteriores que el secreto de las comunicaciones no cubre sólo el contenido de la comunicación sino también «la identidad subjetiva de los interlocutores». Concretamente, en la S.T.S. 25.09.2003, el recurrente alegó la vulneración del derecho al secreto de las comunicaciones por los funcionarios del servicio de vigilancia aduanera puesto que en el momento de su detención se intervinieron tres teléfonos móviles, considerando que se había manipulado los mismos, teniendo acceso a los datos memorizados en éstos. Sin embargo, el T.S., haciendo alusión a la doctrina jurisprudencial sobre la legitimidad de la indagación en la memoria del aparato móvil de la telefonía (S.S.T.S. 316/2000, de 3 de marzo,1235/2000, de 27 de junio y 1.086/2003, de 25 de julio), concluyó que en el caso enjuiciado la policía había actuado de forma proporcional puesto que únicamente se limitó a la comprobación de unos números de teléfono, sin que dicha operación permita comprobar el destinatario de la llamada, ni el tiempo.

El derecho al secreto de comunicaciones ampara no sólo ésta propiamente dicha sino también sus anexos (por ej., el texto, imagen, sonido o filmación unido a un correo-e o mensaje SMS), y asimismo, a los datos de tráfico. Ya que desde la perspectiva de los derechos fundamentales lo inviolable no sólo es el mensaje, sino todos aquellos datos relativos a la comunicación que permitan identificar a sus interlocutores o corresponsales, o constatar la existencia misma de la comunicación, su fecha, duración y todas las demás circunstancias concurrentes, útiles para ubicar en el espacio y en el tiempo el hecho concreto de la conexión –datos del tráfico-, pues, no cabe disociar sin merma relevante de garantías realidades sustancialmente integradas como son el mensaje y su

proceso de transmisión (SSTC 114/1984, de 29 de noviembre, 70/2002, de 3 de abril, 123/2002 de 20 de mayo, y 281/2006, de 9 de octubre).

Este derecho consagrado en el art. 18.3 C.E. protege «*la comunicación*» mientras dure el proceso comunicativo, puesto que una vez finalizado éste, la protección constitucional de lo comunicado o de lo recibido es objeto de protección por el «derecho a la intimidad» del art. 18.1 C.E. Así, en el supuesto de apertura de un correo electrónico cerrado nos hallaríamos dentro del ámbito del derecho al secreto de comunicaciones. Sin embargo, nos hallaríamos dentro del ámbito del derecho a la intimidad cuando a lo que se tiene acceso es a un correo cuya apertura ya consta efectuada por el titular. En dicho caso la comunicación ya ha terminado y solo se trata de un documento contenido en el ordenador, que no deja de asemejarse a la carta que uno recibe, abre y guarda en un cajón. Esta conclusión puede ser aplicada a un documento electrónico guardado en un ordenador, un móvil, o en cualquier otro dispositivo electrónico interceptado por la policía.

No obstante, la distinción entre ambos derechos no siempre es fácil. Así, se pone de manifiesto en la jurisprudencia que ha conocido de diversos supuestos en los cuales se cuestiona cuál sea el derecho afectado. Este es el caso de la STC 70/2002, Sala 1ª, de fecha 3 de abril de 2002[126], en la que se distingue entre el derecho a la intimidad y el derecho al secreto de comunicaciones. En la sentencia se valora la posible vulneración al derecho al secreto de comunicaciones postales y el derecho a la intimidad en un supuesto de intervención a un detenido de una carta que fue desdoblada y leída sin previa autorización judicial. Se trataba de una comunicación privada, que se hallaba en el interior de una agenda, guardando su contenido de terceros. Según la sentencia este es un supuesto de derecho a la intimidad del art. 18.1 CE y no de secreto de las comunicaciones. A ese fin el Tribunal fundamenta su decisión en el hecho de la falta de constancia de un proceso de comunicación en proceso que, en cualquier caso, ya habría finalizado.

En el mismo sentido se ha pronunciado el Tribunal Supremo en sentencias de 7 de julio de 2011, 26 de abril de 2011, 1 de marzo de 2011 y 21 de diciembre de 2010. Esta última sentencia dispone: «*La doctrina de esta Sala de Casación, según las reiteradas sentencias que ha dictado sobre casos similares relativos al conocimiento por los agentes policiales de los listados telefónicos de las agendas de teléfonos móviles(SSTS 316/2000 de 3-3;1235/2002 de 27-6;1086/2003 de 25-7;1231/2003 de 25-9;449/2006 de 17-4; y1315/2009 de 18-12), afirma que la agenda de un teléfono móvil, entendiendo por agenda, en este caso, el archivo de dicho aparato en el que consta un listado de números identificados normalmente*

[126] STC 70/2002, Sala 1ª, de fecha 3 de abril de 2002, rec. 3787/2001, Ponente Garrido Falla, Fernando.

por un nombre, es equiparable a una agenda en soporte de papel o electrónica con el mismo contenido de direcciones y números de teléfono. Por ello su registro u observación no supone la inmisión o injerencia en el derecho al secreto de las comunicaciones sino en el derecho a la intimidad, con las importantes consecuencias que de ello se derivan. Pues así como la injerencia en el primero de tales derechos requeriría, sin duda ni excepción, la previa autorización judicial, por venir así expresamente dispuesto en el artículo 18.3 de nuestra Constitución, la diligencia que afecta a la intimidad del investigado se encuentra, en cambio, legalmente autorizada a las fuerzas del orden, siempre por supuesto que la misma resulte justificada con arreglo a los criterios de urgencia y necesidad y que se cumpla el requisito de proporcionalidad al ponderar los intereses en juego en el caso concreto».

De igual modo la STC 115/2013, de 9 de mayo de 2013 plantea el supuesto de unos agentes de policía que accedieron a la agenda de direcciones del teléfono móvil que encontraron encendido en el invernadero del que salieron huyendo varias personas tras ser sorprendidas por la irrupción policial, pudiendo comprobar los agentes que dicha agenda telefónica contenía un nombre registrado como «mamá», correspondiente a un número de teléfono fijo de Cádiz perteneciente a la madre del recurrente en amparo. Dispone el Tribunal Constitucional en el FJ 4 y 5 que en este supuesto «*…No estamos, por tanto, ante un supuesto de acceso policial a funciones de un teléfono móvil que pudiesen desvelar procesos comunicativos, lo que requeriría, para garantizar el derecho al secreto de las comunicaciones (art. 18.3 CE), el consentimiento del afectado o la autorización judicial, conforme a la doctrina constitucional antes citada. El acceso policial al teléfono móvil del recurrente se limitó exclusivamente a los datos recogidos en la agenda de contactos telefónicos del terminal –entendiendo por agenda el archivo del teléfono móvil en el que consta un listado de números identificados habitualmente mediante un nombre–, por lo que debe concluirse que dichos datos «no forman parte de una comunicación actual o consumada, ni proporcionan información sobre actos concretos de comunicación pretéritos o futuros*» (STC 142/2012, FJ 3), *de suerte que no cabe considerar que en el presente caso la actuación de los agentes de la Policía Nacional en el ejercicio de sus funciones de investigación supusiera una injerencia en el ámbito de protección del artículo 18.3 CE. …». «…En efecto, con el acceso a la agenda de contactos del teléfono móvil del recurrente los agentes de policía no obtuvieron dato alguno concerniente a un proceso de comunicación emitida o recibida mediante dicho aparato, sino únicamente a un listado de números de teléfono introducidos voluntariamente por el usuario del terminal, equiparable a los recogidos en una agenda de teléfonos en soporte de papel (STC 70/2002, FJ 9). Por tanto, «siendo lo determinante para la delimitación del contenido de los derechos fundamentales garantizados por los artículos 18.1 y 18.3 CE … no el tipo de soporte, físico o electrónico, en el que la agenda de contactos esté alojada», ni «el hecho … de que*

la agenda sea un aplicación de un terminal telefónico móvil, que es un instrumento de y para la comunicación, sino el carácter de la información a la que se accede» (STC 142/2012, FJ 3), debe descartarse que el derecho al secreto de las comunicaciones (art. 18.3 CE) se haya visto afectado en el presente caso por la actuación policial descrita».

Dicha sentencia concluye en su FJ 5 que «*…el derecho fundamental afectado por el acceso policial a una agenda de contactos de un teléfono móvil, en los términos ya expuestos, es el derecho a la intimidad personal (art. 18.1 CE) y no el derecho al secreto de las comunicaciones ex artículo 18.3 CE (STC 142/2012, FJ 4), por no haberse accedido por los agentes de la Policía Nacional intervinientes a datos de una eventual comunicación telefónica que pudiera haber mediado entre el recurrente y otras personas»* (FJ 5). «*Distinto sería el caso si…el acceso policial lo hubiera sido a cualquier otra función del teléfono móvil que pudiera desvelar procesos comunicativos, supuesto en el que tal acceso solo resultaría constitucionalmente legítimo si media consentimiento del propio titular del terminal o autorización judicial, dada la circunstancia indubitada de que un teléfono móvil es un instrumento cuyo fin esencial es la participación en un proceso comunicativo protegido por el derecho al secreto de las comunicaciones ex artículo 18.3 CE, como también advertimos en la citada STC 142/2012, FJ 3*».

En consecuencia, con base en lo expuesto, resulta clara la distinción entre el «*derecho al secreto de las comunicaciones*» y el «*derecho a la intimidad*» que determina que no puedan quedar amparados dentro del primero aquellos supuestos en los cuales no existe comunicación, sino a lo sumo hechos que están relacionados con el ámbito personal íntimo de los ciudadanos como son los listados de contactos, fotografías u otros documentos que se puedan hallar eventualmente en dispositivos aptos para la comunicación electrónica. No obstante, existe otra línea interpretativa que considera, por ejemplo, que los listados de llamadas contenidos en la memoria de un teléfono móvil quedan amparados por el derecho al secreto de las comunicaciones para cuyo acceso por la Policía se precisa autorización judicial. Así se razona en la STC 230/2007, con invocación de la STEDH de 2 de agosto de 1984 (caso MALONE) y de 3 de abril de 2007 (caso COPLAND) que dicho derecho garantiza a los comunicantes tanto la confidencialidad de la comunicación misma y el contenido de la comunicado como los datos externos de la conexión telefónica tales como momento, duración y destino, con independencia de que se venga en conocimiento de los mismos una vez el proceso comunicativo haya finalizado. Dicha doctrina fue recogida por STS de 22 de junio de 2009.

3.1.1.2 Protección de datos relativos a las comunicaciones electrónicas

El derecho al secreto de las comunicaciones electrónicas incluye también los datos relativos a las redes públicas de comunicaciones. Estos datos pueden incluir el nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono etc. Se trata de datos que identifican al usuario y por ello son objeto de protección por la ley 25/2007, de 18 de octubre, de conservación de datos (LCDCE).

La ley 25/2007 se aparta del clásico concepto de «datos del tráfico»[127] e incluye dentro de dicho concepto tanto los datos de tráfico que se estén generando, como los que se hallen almacenados como datos de carácter personal, y amplia el concepto de componentes esenciales del dato de tráfico (terminales conectados, identificación de usuario, datación de la comunicación etc.) a los datos de localización sobre personas físicas y jurídicas y datos relacionados necesarios para identificar al abonado o usuario registrado (art. 2 LCDCE). Todos estos datos forman parte de una única disciplina jurídica, no pudiendo hablar, como con anterioridad a la publicación de la Ley de regímenes jurídicos distintos. La diferenciación vendrá dada por el origen de la captación, pues habrá sometimiento a la LCDCE cuando la información se recabe de bases de datos «almacenadas» por los sujetos obligados a que se refiere su artículo 2 será de aplicación la LCDCE y , una aplicación exclusiva del artículo 579 Lecrim o la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, en relación con los supuestos posibles de obtención de información desarrolladas en el art. 33 de la Ley 32/2003, de 3 de noviembre, general de telecomunicaciones, cuando se trate de interceptación de contenidos de comunicaciones y de los datos de tráfico asociados a las mismas que tengan lugar como consecuencia de una resolución judicial habilitante[128].

La LCDCE cuida expresamente de excluir de la obligación de conservación los datos que revelen el contenido de una comunicación (art. 3.2) lo que hubiere requerido ley orgánica al afectar a un derecho fundamental como el secreto de

[127] El RLGT define en su artículo 64 a) el «dato de tráfico» como «cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones o a efectos de facturación». Haciendo referencia al dato de tráfico dinámico no estático y también al aspecto económico de facturación ajena a la investigación.

[128] Véase RODRÍGUEZ LAINZ, José Luis, *El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones*, Diario La Ley, Nº 6859, Sección Doctrina, 11 Ene. 2008, Año XXIX, Ref. D-10, Editorial LA LEY; Diario La Ley, Nº 6860, Sección Doctrina, 14 Ene. 2008, Año XXIX, Ref. D-10, Editorial LA LEY, La Ley 7062/2007, pág. 10.

comunicaciones. Por otro lado los datos de tráfico, integrados ahora en el concepto más amplio de datos relativos a las comunicaciones electrónicas, basculan entre el derecho al secreto de comunicaciones y el derecho a la protección de datos. Entiendo como RODRÍGUEZ LAINZ que el derecho al secreto de comunicaciones queda afectado cuando exista un acto de injerencia que incida directamente sobre el proceso mismo de la comunicación, bien afecte la injerencia tanto al contenido de las comunicaciones como a los datos asociados a las mismas, o se limite la inmisión exclusivamente a estos últimos elementos externos o adyacentes. Por otro lado, cuando dichos datos relativos a la comunicación sin dejar de serlo se desgajan de la misma pasan a ser datos de carácter personal, aún relativos a las comunicaciones[129].

Como señalan las STC 114/1984, de 29 de noviembre, 70/2002, de 4 de abril y 123/2002, de 20 de mayo: «… *la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos»*. Y si bien el Tribunal Constitucional ha creado cierta confusión en el Tribunal Supremo con Sentencias como la 230/2007, de 5 de noviembre, como se aprecia en sentencias como la STS 1683/2003, de 11 de diciembre que son incapaces de separar del régimen de la garantía del derecho al secreto de las comunicaciones los datos de tráfico de comunicaciones ya consumadas, sometiéndolos al régimen de aquéllas, finalmente el Tribunal Supremo acertará en la diferenciación a partir de las SSTS 459/1999, de 22 de marzo, 1086/2003, de 25 de julio y 1231/2003, de 25 de septiembre, que en tal contexto, y ante la imputación por parte del recurrente de transgresión del art. 18.3 de la Constitución, afirmará: *«No se trata de una intervención en el proceso de comunicación, ya entendido como transmisión de conversaciones, ni localización, al tiempo de su realización, de las llamadas efectuadas, de la identificación de usuarios, limitándose a la comprobación de unos números»*. La sentencia del STS 780/2007, de 3 de octubre, centra ya de una forma incontestable el conflicto en la línea de considerar a los datos de tráfico de conversaciones ya mantenidas en el ámbito de la protección de los datos de carácter personal.

Como precedente de la ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (LCDCE) la Ley 34/2002, de 11 de julio, de Servicios de la

[129] Véase RODRÍGUEZ LAINZ, José Luis, *El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones*, Diario La Ley Diario La Ley, Nº 6859, Sección Doctrina, 11 Ene. 2008, Año XXIX, Ref. D-10, Editorial LA LEY; Diario La Ley, Nº 6860, Sección Doctrina, 14 Ene. 2008, Año XXIX, Ref. D-10, Editorial LA LEY, La Ley 7062/2007, págs. 34-38.

Sociedad de la Información y de Comercio Electrónico, regulaba, bajo la rúbrica «*Deber de retención de datos de tráfico relativos a las comunicaciones electrónicas»* en los tres primeros apartados del artículo 12, la retención de los datos electrónicos por parte de las empresas operadoras de servicios de comunicaciones limitándola estrictamente a los supuestos de «infracción penal» y consiguiente «investigación criminal»[130]. A tenor de lo previsto en dicho artículo: *«1. Los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos deberán retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información por un período máximo de doce meses, en los términos establecidos en este artículo y en su normativa de desarrollo.//2. Los datos que, en cumplimiento de lo dispuesto en el apartado anterior, deberán conservar los operadores de redes y servicios de comunicaciones electrónicas y los proveedores de acceso a redes de telecomunicaciones serán únicamente los necesarios para facilitar la localización del equipo terminal empleado por el usuario para la transmisión de la información./Los prestadores de servicios de alojamiento de datos deberán retener sólo aquéllos imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio./En ningún caso, la obligación de retención de datos afectará al secreto de las comunicaciones./Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios a que se refiere este artículo no podrán utilizar los datos retenidos para fines distintos de los indicados en el apartado siguiente u otros que estén permitidos por la Ley, y deberán adoptar medidas de seguridad apropiadas para evitar su pérdida o alteración y el*

[130] La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, incorpora al ordenamiento jurídico español la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (directiva sobre el comercio electrónico). Asimismo, incorpora parcialmente la Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores, al regular, de conformidad con lo establecido en ella, una acción de cesación contra las conductas que contravengan esta Ley. El objeto perseguido por dicha Ley, según establece su artículo I, es la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios. Incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de los contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información. Todo ello sin perjuicio de los dispuesto en otras normas estatales o autonómicas ajenas al ámbito normativo coordinado, o que tengan por finalidad la protección a la salud y seguridad pública, incluida la salvaguarda de la defensa nacional, los intereses del consumidor, el régimen tributario aplicable a los servicios de la sociedad de la información, la protección de datos personales y la normativa reguladora de la competencia.

acceso no autorizado a los mismos.//3. Los datos se conservarán para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces o Tribunales o del Ministerio Fiscal que así los requieran. La comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales».

El precepto fue derogado por la Ley 25/2007, de 18 de octubre de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Según el propio Preámbulo I de dicha Ley 25/2007 «*la aplicación de las nuevas tecnologías desarrolladas en el marco de la sociedad de la información ha supuesto la superación de las formas tradicionales de comunicación, mediante una expansión de los contenidos transmitidos, que abarcan no sólo la voz, sino también datos en soportes y formatos diversos. A su vez, esta extraordinaria expansión en cantidad y calidad ha venido acompañada de un descenso en los costes, haciendo que este tipo de comunicaciones se encuentre al alcance de cualquier persona y en cualquier rincón del mundo. La naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines indeseados, cuando no delictivos»*. Precisamente en el marco de este último objetivo se encuadra la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, cuya transposición a nuestro ordenamiento jurídico es el objetivo principal de la Ley[131].

[131] La Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas en su considerando núm. 6 resalta que «*Internet está revolucionando las estructuras tradicionales del mercado al aportar una infraestructura común mundial para la prestación de una amplia gama de servicios de comunicaciones electrónicas. Los servicios de comunicaciones electrónicas disponibles al público a través de Internet introducen nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad*». Además, recuerda en su considerando núm. 24 que «*los equipos terminales de los usuarios de redes de comunicaciones electrónicas, así como toda información almacenada en dichos equipos, forman parte de la esfera privada de los usuarios que debe ser protegida de conformidad con el Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales», advirtiendo que «los denominados programas espías (Spyware), web bugs, identificadores ocultos y otros dispositivos similares pueden introducirse en el terminal del usuario sin su conocimiento para acceder a información, archivar información oculta o rastrear las actividades del usuario, lo que puede suponer una grave intromisión en la intimidad de dichos usuarios».*

La ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones establece la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos los «agentes facultados».

La LCDCE no define, sin embargo, qué debe entenderse por «*operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones*» remitiendo en su artículo 2 a *«… los términos establecidos en la Ley 32/2003, de 3 de noviembre, general de Telecomunicaciones.»*. La Ley 32/2003 establece los requisitos para poder acceder a un sistema libre de competencia en sus artículos 5 y 6, y de igual modo el artículo 4 RLGT, pero no aportan ninguna definición. Habrá que acudir a la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco) que define el *«servicio de comunicaciones electrónicas»* como «*el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos* —art. 2.c) ; se considera «red de comunicaciones electrónicas» «*los sistemas de transmisión y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes terrestres fijas (de conmutación de circuitos y de paquetes, incluido Internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada* —art. 2.a) —; y «red pública de comunicaciones electrónicas», «*una red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público»* —art. 2.d) —.El carácter de acceso público a las redes y servicios de comunicaciones electrónicas referido a ambos conceptos por el art. 2 de la LCDCE deja fuera de dicha regulación el deber de conservación a los explotadores de redes y prestadores de servicios de comunicaciones electrónicas en régimen de «*autoprestación»,* es decir, a las redes privadas; criterio de exclusión que es una consecuencia directa de la exceptuación del régimen general de la prestación de servicios de telecomunicaciones a aquéllos, como se colige del último inciso del art. 6.2 de la LGT). En lo que respecta al servicio de telefonía mediante tarjetas de prepago, la obligación de conservación y disponibilidad para su

cesión afecta a los operadores de servicios que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago[132].

Se entienden por «agentes facultados» los Cuerpos Policiales autorizados para ello en el marco de una investigación criminal por la comisión de un delito, el personal del Centro Nacional de Inteligencia para llevar a cabo una investigación de seguridad nacional amparada en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal y los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, de acuerdo a lo previsto en el artículo 587 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (art. 6.2 LCDCE) . Los destinatarios de la información, tratándose de Policía judicial, podrán ser la propia policía judicial en su labor de investigación previa a una causa judicial abierta en la que solicitan autorización judicial para acceder a la información, o la autoridad judicial que los comisiona.

La LCDCE facilita a los «agentes facultados» el acceso a los datos relativos a las comunicaciones que, relacionados con una investigación, se hayan podido efectuar por medio de la telefonía fija o móvil, así como por Internet. El establecimiento de esas obligaciones, justificado en aras de proteger la seguridad pública, se ha efectuado buscando el imprescindible equilibrio con el respeto de los derechos individuales que puedan verse afectados, como son los relativos a la privacidad y la intimidad de las comunicaciones. En este sentido, la Ley es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido emitiendo el Tribunal Constitucional, respeto que, especialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores del contenido de ésta (art. 1.3 LCDCE) ; y, en segundo lugar, que la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa (art. 6.1 LCDCE).

---

[132] Véase RODRÍGUEZ LAINZ, José Luis, *El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones*, Diario La Ley Diario La Ley, Nº 6859, Sección Doctrina, 11 Ene. 2008, Año XXIX, Ref. D-10, Editorial LA LEY; Diario La Ley, Nº 6860, Sección Doctrina, 14 Ene. 2008, Año XXIX, Ref. D-10, Editorial LA LEY, La Ley 7062/2007.

En relación con esta última precisión, cabe señalar que la Directiva traspuesta se refiere, expresamente, a que los datos conservados deberán estar disponibles a los fines de detección o investigación por «*delitos graves*», definidos éstos de acuerdo con la legislación interna de cada Estado miembro. Y así lo recoge el artículo 1 de dicha ley. Ello supone que no podrá averiguarse la identidad de una persona a partir de la dirección IP en delitos con una pena inferior a cinco años o faltas. No pudiendo en dichos supuestos acceder a dicha información ni siquiera con autorización judicial, ya que de concederse podría solicitarse la nulidad. La disposición adicional única relativa a la telefonía mediante tarjetas de prepago, en su apartado 4, permite la superación del límite de gravedad del delito, al hablar solamente de delito, aunque de igual modo rigen los principios de necesidad y proporcionalidad.

La posibilidad de obtención de los datos asociados a las comunicaciones queda siempre ceñida a procesos penales, siendo enormemente difícil por no decir prácticamente imposible que se obtengan en supuestos en que no exista delito. Es decir, difícilmente podrán personas interesadas acceder a dichos datos con el fin de interponer reclamaciones en vía civil. Un claro ejemplo de ello lo son los supuestos de reclamaciones en vía civil fundadas en los derechos de autor. Resulta en estos casos imposible reclamar a las compañías suministradoras de servicios electrónicos la identificación de los usuarios dada la prevalencia de la confidencialidad de las comunicaciones electrónicas frente a los derechos de autor[133].

En materia de los derechos de autor, es de especial relevancia la Sentencia dictada por el Tribunal de Justicia de las Comunidades Europeas, en fecha 29 de enero de 2008. Dicha sentencia se dicta a consecuencia de una decisión prejudicial planteada con arreglo al artículo 234 CE, por el Juzgado de lo Mercantil nº 5 de Madrid, mediante auto de 13 de junio de 2006, en el procedimiento entre Productores de Música de España (o PROMUSICAE) y Telefónica de España. Promusicae, asociación sin ánimo de lucro que agrupa a productores y editores de grabaciones musicales y audiovisuales, actuando por cuenta de los titulares de derechos de propiedad intelectual agrupados en ella, promovió diligencias preliminares ante el Juzgado de lo Mercantil nº 5 de Madrid contra Telefónica, reclamando a dicha compañía datos personales relativos al uso de Internet a través de conexiones suministradas por Telefónica, en cuanto compañía suministradora de servicios de acceso a Internet. En particular, Promusicae solicitaba que se ordenase a Telefónica revelar la identidad y la dirección de determinadas personas a las que ésta presta un

[133] Véase el artículo de LASARTE, Carlos, *Comunicaciones electrónicas peer-to-peer (P2P) versus Derechos de Autor*, publicado en La Ley. Puede consultarse en la dirección electrónica www.fundacionblu.org.

servicio de acceso a Internet y de las que se conoce su dirección «IP» y la fecha y hora de conexión. Según Promusicae, estas personas utilizan el programa de intercambio de archivos denominado «KaZaA», (conocido como «*peer to peer*» o «P2P»), y permiten el acceso, en una carpeta compartida de su ordenador personal, a fonogramas cuyos derechos patrimoniales de explotación corresponden a los asociados de Promusicae, cometiendo así actos de competencia desleal y vulneradores de los derechos de propiedad intelectual ajenos. Por consiguiente, solicitaba que se le facilitase la información referida para poder ejercitar contra los interesados las correspondientes acciones civiles.

Frente a dicha pretensión, Telefónica formuló oposición contra el auto judicial afirmando que, conforme a la LSSI, la comunicación de los datos solicitados sólo estaba autorizada en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y de la defensa nacional y no en el marco de un procedimiento civil o como medida preparatoria de un procedimiento civil. Por su parte, Promusicae alegó que el artículo 12 de la LSSI debía interpretarse conforme a diversas disposiciones de las Directivas 2000/31, 2001/29 y 2004/48, y a los artículos 17, apartado 2, y 47 de la Carta, textos que no permiten a los Estados miembros restringir únicamente a los fines a los que se refiere el tenor de esta Ley el deber de comunicar los datos de que se trata.

Ante dicho litigio, el Juzgado de lo Mercantil nº 5 de Madrid decidió suspender el procedimiento y plantear al Tribunal de Justicia la siguiente cuestión prejudicial: «*El Derecho comunitario y, concretamente, los artículos 15, apartado 2, y 18 de la Directiva 2000/31, el artículo 8, apartados 1 y 2, de la Directiva 2001/29, el artículo 8 de la Directiva 2004/48, y los artículos 17, apartado 2, y 47 de la Carta, ¿permiten a los Estados miembros restringir al marco de una investigación criminal o para la salvaguardia de la seguridad pública y de la defensa nacional, con exclusión, por tanto, de los procesos civiles, el deber de retención y puesta a disposición de datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, que recae sobre los operadores de redes y servicios de comunicaciones electrónicas, proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamientos de datos?*».

La sentencia acaba emitiendo, en relación con el sentido normativo de las Directivas aplicables al caso, el siguiente fallo: que tales Directivas «*no obligan a los Estados miembros a imponer, en una situación como la del asunto principal, el deber de comunicar datos personales con objeto de garantizar la protección efectiva de los derechos de autor en el marco de un procedimiento civil. Sin embargo, el Derecho comunitario exige que dichos Estados miembros, a la hora de adaptar su ordenamiento jurídico interno a estas Directivas, procuren basarse en una interpretación de éstas que garantice un justo equilibrio entre los distintos*

derechos fundamentales protegidos por el ordenamiento jurídico comunitario. A continuación, en el momento de aplicar las medidas de adaptación del ordenamiento jurídico interno a dichas Directivas, corresponde a las autoridades y a los órganos jurisdiccionales de los Estados miembros no sólo interpretar su Derecho nacional de conformidad con estas mismas Directivas, sino también no basarse en una interpretación de éstas que entre en conflicto con dichos derechos fundamentales o con los demás principios generales del Derecho comunitario, como el principio de proporcionalidad».

De todo ello se desprende que las reclamaciones judiciales en vía civil son condenadas, irremisiblemente, al fracaso, de manera tal que cualesquiera infracciones y conductas contrarias a la propiedad intelectual que no merezcan la calificación de delito propiamente dicho quedarán absolutamente impunes ante la imposibilidad de prueba de las descargas masivas y de la identificación de que las personas que las realizan. No obstante, se percibe cierta flexibilización en el ámbito civil por parte del legislador español. Parece que el legislador español se ha apercibido de que la vulneración de la propiedad intelectual no siempre lo ha de ser por vía delictiva, y que, en cambio, los derechos de autor deben ser objeto de protección y defensa incluso frente a los ilícitos de naturaleza civil. Así parece desprenderse de la derogación por el número primero de la disposición derogatoria de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, del artículo 12 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, precepto de particular atención en el caso objeto de la cuestión prejudicial y consiguiente STJCE. A su vez, la subsiguiente Ley 56/2007, de 28 de diciembre, de medidas de impulso a la sociedad de la información, ha introducido un nuevo artículo 12 bis en la Ley 34/2002, cuyo apartado cuarto es del siguiente tenor: «4. *Los proveedores de servicios mencionados en el apartado 1 facilitarán información a sus clientes acerca de las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos, en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industria*l»[134].

En lo referente al plazo obligatorio de conservación de datos el artículo 5 de la LCDCE establece «doce meses» computados desde la fecha en que se haya producido la comunicación. Dicha norma añade sin embargo que «*…reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o a una categoría de*

[134] Véase sobre este tema el artículo de LASARTE, Carlos, Comunicaciones electrónicas peer-to-peer (P2P) versus Derechos de Autor, publicado en La Ley. Puede consultarse en la página *www.fundacionblu.org,* pág.20.

datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores»[135]. Dicho plazo será aplicable a los datos dinámicos de las comunicaciones -datos del tráfico-, pero no respecto a los elementos estáticos como los datos de identificación de abonados o usuarios autorizados, mientras la relación contractual siga vigente.

El legislador establece un plazo de ejecución de la medida de cesión de datos. Plazo que será fijado por la propia resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad de la operación. En el caso de no establecer la resolución plazo alguno, la cesión deberá efectuarse dentro de las setenta y dos horas contadas a partir de las 8:00 horas del día laborable siguiente a aquél en el que el sujeto obligado reciba la orden (art. 7.3 LCDCE).

3.1.2 Derecho fundamental a la intimidad

3.1.2.1 Naturaleza y contenido

La Constitución Española garantiza en su artículo 18 apartado I «*…el derecho al honor, a la intimidad personal y familiar y a la propia imagen*», como derivación de la dignidad de la persona reconocida en el art. 10.1 CE que implica «*la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura para mantener una calidad mínima de la vida humana*» (SSTC 207/1996, de 16 de diciembre, FJ 3; 186/2000, de 10 de julio, FJ 5; 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 4; y 159/2009, de 29 de junio, FJ 3; 209/1988, de 27 de octubre; 231/1988; 197/1991, de 17 de octubre; 99/1994, de 11 de abril; 143/1994, de 9 de mayo, FJ 6; 207/1996, de 16 de diciembre, FJ 3; 98/2000,de 10

[135] En la Unión Europea la Directiva 2006/24/CE establece que las empresas proveedoras de servicios sólo tienen obligación de conservar los datos de tráfico en un plazo común de entre seis meses y dos años, pudiendo ampliarse 90 días si se remite una orden de preservación vía Interpol, pero debe tratarse de delitos graves como terrorismo o crimen organizado. La obtención de dichos datos se complica todavía más cuando la cuenta de correo usada pertenece a una empresa cuya sede esté en EEUU (como Hotmail, Yahoo, Gmail) pues su legislación (Electronic Communications Privacy Act (ECPA) de 1986), exige que además de tener que pedirlos a través de Comisión Rogatoria, lo cual suele suponer demoras, las empresas proveedoras de servicios sólo tienen obligación de conservar los datos de tráfico entre veinte y sesenta días.

de abril, FJ 5; 156/2001, de 2 de julio, FJ 4, entre otras). De forma que «*lo que el art. 18.1 garantiza es un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuales sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio*» (SSTC 127/2003, de 30 de junio, FJ 7 y 89/2006, de 27 de marzo, FJ 5).

Del precepto constitucional citado se deduce que el derecho a la intimidad confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido (SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 5; y 70/2009, de 23 de marzo, FJ 2). «*El artículo 18.1 CE garantiza al individuo un ámbito reservado de su vida «vedando que terceros, sean particulares o poderes públicos, decidan cuales sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio» (SSTC 127/2003, de 30 de junio, FJ 7, y 89/2006, de 27 de marzo, FJ 5, entre otras). La protección de ese ámbito reservado confiere a la persona, así, el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido (SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 5; 70/2009, de 23 de marzo, FJ 2, y 241/2012, FJ 3, entre otras muchas)*» (STC Sentencia 115/2013, de 9 de mayo de 2013).

Ahora bien, el derecho a la intimidad *«no es absoluto»*, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquel haya de experimentar se revele como necesario para lograr un fin constitucionalmente legítimo, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho. En este sentido se ha pronunciado reiteradamente el Tribunal Constitucional (SSTC 57/1994, de 28 de febrero, FJ 6; 143/1994, de 9 de mayo, FJ 6; 98/2000, de 10 de abril, FJ 5, 186/2000, de 10 de julio, FJ 5;156/2001, de 2 de julio, FJ 4, 70/2009, de 23 de marzo, FJ 3, STC Sentencia 115/2013, de 9 de mayo de 2013, FJ 5). En este sentido, el derecho a la intimidad puede resultar afectado en determinados supuestos de afectación leve sin necesidad de una resolución judicial, siempre que exista una habilitación legal previa. Así sucede, en los supuestos previstos en la LO de seguridad ciudadana 1/1992 en cuyos arts. 19 y ss se prevé la inspección y registro de sospechosos por parte de la policía que, en cualquier caso, deberá respetar los principios de proporcionalidad y razonabilidad[136]. Téngase presente

[136] Al hilo de lo expuesto señala la STC 173/2011, de 7 de diciembre, FJ 2 «*…De manera significativa hemos resaltado en la STC 70/2002, de 3 de abril, que «la regla general es que el*

que las limitaciones de cualquier derecho fundamental, incluido en derecho a la intimidad deben venir expresamente autorizadas por la Ley. Sobre este requisito la STC 49/1999, de 5 de abril, FJ 4, indica que «*por mandato expreso de la*

ámbito de lo íntimo sigue preservado en el momento de la detención y que sólo pueden llevarse a cabo injerencias en el mismo mediante la preceptiva autorización judicial motivada conforme a criterios de proporcionalidad. De no existir ésta, los efectos intervenidos que puedan pertenecer al ámbito de lo íntimo han de ponerse a disposición judicial, para que sea el juez quien los examine. Esa regla general se excepciona en los supuestos en que existan razones de necesidad de intervención policial inmediata, para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias. En esos casos estará justificada la intervención policial sin autorización judicial, siempre que la misma se realice también desde el respeto al principio de proporcionalidad» [FJ 10 b) 3]. Bien entendido que «la valoración de la urgencia y necesidad de la intervención policial ha de realizarse ex ante y es susceptible de control judicial ex post, al igual que el respeto al principio de proporcionalidad. La constatación ex post de la falta del presupuesto habilitante o del respeto al principio de proporcionalidad implicaría la vulneración del derecho fundamental y tendría efectos procesales en cuanto a la ilicitud de la prueba en su caso obtenida, por haberlo sido con vulneración de derechos fundamentales» [FJ 10 b) 5]. En esta línea en la STC 206/2007, de 24 de septiembre, FJ 8, afirmábamos que «la regla general es que sólo mediante una resolución judicial motivada se pueden adoptar tales medidas y que, de adoptarse sin consentimiento del afectado y sin autorización judicial, han de acreditarse razones de urgencia y necesidad que hagan imprescindible la intervención inmediata y respetarse estrictamente los principios de proporcionalidad y razonabilidad». En esta Sentencia razonábamos que no había existido una autorización judicial previa para la injerencia acaecida en el derecho a la intimidad (en este caso un análisis de sangre interesado por la Guardia Civil), entendiéndose como relevante el hecho de que tampoco por los órganos judiciales se había efectuado posteriormente una «ponderación de los intereses en conflicto teniendo en cuenta el derecho fundamental en juego que les condujera a considerar justificada –a la vista de las circunstancias del caso- la actuación policial sin previa autorización judicial» (mismo fundamento jurídico)».

La STC Sentencia 115/2013, de 9 de mayo de 2013 dispone en su FJ 3º «*…este Tribunal ha señalado que si bien, de conformidad con el artículo 18.3 CE, la intervención de las comunicaciones (telefónicas, telegráficas, postales o de cualquier otro tipo) requiere siempre de autorización judicial (a menos que medie el consentimiento previo del afectado), el artículo 18.1 CE no prevé esa misma garantía respecto del derecho a la intimidad, de modo que se ha admitido la legitimidad constitucional de que en algunos casos y con la suficiente y precisa habilitación legal, la policía realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas sin previa autorización judicial (y sin consentimiento del afectado), siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad (por todas, SSTC 70/2002, de 3 de abril, FJ 10; 123/2002, de 20 de mayo, FJ 4; 56/2003, de 24 de marzo, FJ 2; 281/2006, de 9 de octubre, FJ 4, y 142/2012, de 2 de julio, FJ 2)*». Y reitera en si FJ 5 : «*…Asimismo hemos señalado, como antes se dijo, que a diferencia de lo que sucede en el caso del derecho garantizado por el artículo 18.3 CE, el artículo 18.1 CE no prevé la misma garantía de autorización judicial respecto de las intervenciones que afectan al derecho a la intimidad, de modo que excepcionalmente se ha admitido la legitimidad constitucional de que en algunos casos y con la suficiente y precisa habilitación legal, los agentes policiales pueda realizar en el ejercicio de sus funciones de investigación determinadas actuaciones que constituyan una injerencia leve en la intimidad de las personas sin previa autorización judicial (y sin consentimiento del afectado), siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad (por todas, SSTC 123/2002, FJ 4; 281/2006, FJ 4;173/2011, FJ 2, y 142/2012, FJ 2)…».*

Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas, ora incida directamente sobre su desarrollo (art. 81.1 CE), o limite o condicione su ejercicio (art. 53.1 CE), precisa una habilitación legal». Una reserva de ley que «*constituye, en definitiva el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas*» y que «*no es una mera forma, sino que implica exigencias respecto del contenido de la Ley que, naturalmente, son distintas según el ámbito material de que se trate», pero «que en todo caso el legislador ha de hacer el «máximo esfuerzo posible» para garantizar la seguridad jurídica o dicho de otro modo, «la expectativa razonablemente fundada del ciudadano en cuál ha de ser la actuación del poder en aplicación del Derecho» (STC 36/1991, FJ 5)»*. Y, profundizando en esa exigencia, en la STC 169/2001, de 16 de julio, FJ 6, se sostiene, con abundante cita de Sentencias del Tribunal Europeo de Derechos Humanos, en cuanto a las características exigidas por la seguridad jurídica respecto de la calidad de la ley habilitadora de las injerencias en un derecho reconocido en el Convenio, que «*la ley debe definir las modalidades y extensión del ejercicio del poder otorgado con la suficiente claridad para aportar al individuo una protección adecuada contra la arbitrariedad*»[137].

[137] El Tribunal Constitucional reitera en su Sentencia 173/2011, de 7 de diciembre, FJ 2, la necesidad de que el legislador habilite las potestades o instrumentos jurídicos que sean adecuados para que, dentro del respeto debido a los principios y valores constitucionales, las fuerzas y cuerpos de seguridad del Estado cumplan con esta función de averiguación del delito. «*Como reseñamos en la STC 70/2002, de 3 de abril, FJ 10, «por lo que respecta a la habilitación legal en virtud de la cual la policía judicial puede practicar la injerencia en el derecho a la intimidad del detenido, en el momento de la detención, las normas aplicables son, en primer lugar el art. 282 LECrim, que establece como obligaciones de la policía judicial la de ''averiguar los delitos públicos que se cometieron en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro poniéndolos a disposición de la Autoridad Judicial''. En la misma línea, el art. 11.1 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, establece como funciones de éstos, entre otras, f) ''prevenir la comisión de actos delictivos''; g) ''investigar los delitos para descubrir y detener a los presuntos culpables, asegurar los instrumentos, efectos y pruebas del delito, poniéndolos a disposición del Juez o Tribunal competente y elaborar los informes técnicos y periciales procedentes''. Por último, el art. 14 de la Ley Orgánica 1/1992, de 21 de febrero, sobre protección de la seguridad ciudadana, establece que las autoridades competentes podrán disponer las actuaciones policiales estrictamente necesarias para asegurar la consecución de las finalidades previstas en el art. 1 de esta Ley, finalidades entre las que se encuentra la prevención de la comisión de delitos». Según la citada Sentencia (mismo fundamento jurídico) existe, por tanto, «una habilitación legal específica que faculta a la policía para recoger los efectos, instrumentos y pruebas del delito y ponerlos a disposición judicial y para practicar las diligencias necesarias para la averiguación del delito y el descubrimiento del delincuente. Entre esas diligencias (que la Ley no enumera casuísticamente, pero que limita adjetivándolas y orientándolas a un fin) podrá encontrarse la de examinar o acceder al contenido de esos instrumentos o efectos, y en concreto, de documentos o papeles que se le ocupen al detenido, realizando un primer análisis de los mismos, siempre que –como exige el propio texto legal– ello sea necesario (estrictamente necesario, conforme al art. 14 de la Ley Orgánica 1/1992), estricta necesidad que habrá de*

3.1.2.2 La injerencia en el derecho a la intimidad. Especial mención al ámbito laboral.

Conforme a lo expuesto el derecho a la intimidad puede quedar limitado por una previsión legal, por la propia voluntad del individuo o por resolución judicial motivada que deberá observar los requisitos que ha establecido el Tribunal Constitucional (SSTC 207/1996, de 16 de diciembre, FJ 4; 25/2005, de 14 de febrero, FJ 6; y 233/2005, de 26 de septiembre, FJ 4).

Aquellos supuestos en que la inmisión en la esfera privada se lleva a término con consentimiento del interesado, dicho consentimiento deberá ser expreso. Véase en cuanto a la prestación de consentimiento expreso o tácito la STC 173/2011, de 7 de diciembre. Dicha sentencia, que recoge la doctrina constitucional anterior, analiza el supuesto de un sujeto que acudió a un establecimiento de informática le hizo entrega de su ordenador portátil con el encargo de cambiar la grabadora que no funcionaba. Al recibir el encargo el titular del establecimiento preguntó al recurrente si el ordenador tenía contraseña de acceso, respondiendo éste negativamente y sin manifestar limitación alguna en el uso del ordenador y acceso a los ficheros que almacenaba. Una vez efectuada la reparación y para comprobar el correcto funcionamiento de las piezas sustituidas el encargado escogió al azar diversos archivos para proceder a su grabación y posterior reproducción en el ordenador, lo que, al parecer, suele ser práctica habitual en estos casos, visualizando entonces las imágenes pornográficas de los menores que contenía. El testigo puso entonces tal circunstancia en conocimiento de la Policía Nacional que procedió a la intervención del portátil.

Dicha sentencia concluye en su FJ 6º que el encargado de la tienda no se extralimitó en su mandato estando amparado su proceder, que llevó al descubrimiento del material ilícito, por la propia autorización expresa del cliente, y en consecuencia su conducta no vulneró el derecho a la intimidad del sujeto (art. 18.3 CE) por haber sufrido una supuesta intromisión indebida en su esfera íntima. Sin embargo, dicha sentencia en su FJ 6ª entiende que la posterior actuación de la policía que encendió el ordenador entregado por el encargado de la tienda y accedió no sólo a la carpeta «mis documentos» sino también a la carpeta denominada «incoming» perteneciente al programa de intercambio de archivos eMule excede de la autorización que el titular de la

---

valorarse atendidas las circunstancias del caso y que ha de entenderse como la exigencia legal de una estricta observancia de los requisitos dimanantes del principio de proporcionalidad. Así interpretada la norma, puede afirmarse que la habilitación legal existente cumple en principio con las exigencias de certeza y seguridad jurídica dimanantes del principio de legalidad, sin perjuicio de una mayor concreción en eventuales reformas legislativas».

computadora prestó para el acceso a su ordenador al establecimiento de informática. «… *Tal como hemos afirmado anteriormente, el derecho a la intimidad personal se vulnera también cuando, aun autorizada su intromisión en un primer momento, se subvierten después los términos y el alcance para el que se otorgó. Como hemos visto, en el presente caso el alcance de la autorización dada se circunscribía a la manipulación por parte de dicho profesional del portátil para que procediera a la reparación del equipo informático, lo que no puede erigirse en legitimación para una intervención posterior realizada por personas distintas y motivada por otros fines. Lo contrario significaría asignar a un acto concreto de autorización una eficacia genérica erga omnes y temporalmente indeterminada, argumento que, sin duda, se revela contrario a los márgenes de disponibilidad de los derechos fundamentales, basados en la voluntad de su titular y cuyo alcance sólo a él corresponde delimitar. Esta conclusión aparece, además, avalada por la circunstancia de que los funcionarios policiales no se limitaron, una vez incautado el ordenador, a acceder, tal como había efectuado el denunciante, a la carpeta «mis documentos» del usuario, sino que ampliaron su análisis supervisando en particular la carpeta «eMule/Incoming», como hemos dicho.Conviene reseñar en este momento que fue el hallazgo de este último programa, que estaba configurado de forma que los archivos pedófilos depositados en el ordenador pudieran ser descargados por otras personas a través de Internet, lo que ha fundado la condena del recurrente por la modalidad específica de distribución de material pornográfico infantil del art. 189.1 b) del Código penal. En este sentido, tampoco el hecho de que el recurrente permitiera, a través del programa eMule este acceso de otros usuarios a sus archivos, puede erigirse en una suerte de autorización genérica frente a posteriores y distintas injerencias en el ámbito reservado de su intimidad, a pesar de que ha sido éste el argumento utilizado aquí tanto por la Audiencia Provincial de Sevilla como por la Sala Segunda del Tribunal Supremo. En efecto, además de que el acceso a los expresados archivos sólo es factible para los usuarios que tengan instalada su misma aplicación, es lo cierto que la policía tan solo tiene conocimiento de la utilización del referido programa cuando accede al ordenador, siendo así que, conforme hemos expuesto, las circunstancias que permiten afirmar la existencia del presupuesto habilitante para penetrar en la esfera de la intimidad del titular del derecho deben evaluarse y apreciarse ex ante, sin que dicho acceso pueda justificarse ex post a partir de hechos sólo descubiertos después y como consecuencia del mismo»*. Descartada la anterior autorización estima la actuación policial ajustada al principio de proporcionalidad. Concluyendo que «*…siendo la actuación policial constitucionalmente legítima, el sacrificio del derecho fundamental afectado estaba justificado por la presencia de otros intereses constitucionalmente relevantes, no pudiendo apreciarse vulneración alguna del derecho a la intimidad personal del recurrente…. »*.

Cualquier afectación del derecho a la intimidad que no haya consentido expresamente el individuo afectado y para la que exista una expresa habilitación

legal deberá ser autorizada expresamente por el Juez en auto motivado en el que se deberá contener una justificación objetiva y razonable de la injerencia en el derecho a la intimidad.

A este respecto resulta necesaria la observancia de los siguientes requisitos: — la existencia de un fin constitucionalmente legítimo; — que la medida limitativa del derecho esté prevista en la ley (principio de legalidad); — que como regla general se acuerde mediante una resolución judicial motivada (si bien, reconociendo que debido a la falta de reserva constitucional a favor del Juez, la Ley puede autorizar a la policía judicial para la práctica de inspecciones, reconocimientos e incluso de intervenciones corporales leves, siempre y cuando se respeten los principios de proporcionalidad y razonabilidad); — y, finalmente, la estricta observancia del principio de proporcionalidad, concretado en tres requisitos o condiciones: «idoneidad» de la medida -si tal medida es susceptible de conseguir el objetivo propuesto-, «necesidad» de la misma -en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia-, y «proporcionalidad» en sentido estricto es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (SSTC 207/1996, de 16 de diciembre, FJ 4, 70/2002, de 3 de abril, FJ 4, STC 89/2006, de 27 de marzo, FJ 3 y STC 173/2011, de 7 de diciembre, FJ 2).

En su virtud, resultará necesario obtener una autorización judicial al objeto de poder acceder a documentos, lugares u objetos que estén relacionados directamente con la intimidad de la persona. La petición al Juez puede efectuarse en el ámbito de cualquier clase de procedimiento judicial, aunque es cierto que existe poca o escasa tradición de esta clase de solicitudes en el ámbito del derecho civil. Igual sucede en el ámbito del proceso laboral, en el que sin embargo, se va abriendo la posibilidad de esta clase de actuaciones judiciales.

Precisamente, es en el ámbito laboral donde se suscita con mayor frecuencia e interés el problema de la obtención de pruebas electrónicas lícitas y admisibles en un proceso jurisdiccional, especialmente en el supuesto de uso por parte de los trabajadores de los instrumentos de titularidad de la empresa para fines particulares. A ese fin resulta necesario el uso de métodos periciales forenses no lesivos con los derechos fundamentales y una correcta cadena de custodia que garantice que la prueba no sea declarada nula en el proceso (arts. art. 18.3 CE, 11.1 LOPJ, 9.1 de las Ley de Procedimiento Laboral).

Respecto a si es procedente reconocer o no a los trabajadores el derecho de uso de las nuevas tecnologías de la empresa para fines personales, parte de la doctrina aboga por un uso «razonable» de las mismas para fines personales.

Jurisprudencialmente viene aplicándose la teoría gradualista del Tribunal Supremo, admitiendo un cierto uso razonable de las nuevas tecnologías en la empresa (STSJ Cantabria de 20 de febrero de 2004), y teniendo en cuenta determinadas circunstancias como: 1) los costes técnicos (introducción de programas en el sistema que pueden perjudicar el funcionamiento de la red o significar virus, etc.); 2) los costes en tiempo de trabajo, es decir, el impacto de dicho uso en la prestación de servicios, y 3) cuál es el marco de uso en la empresa, esto es, la existencia de acuerdos que articulan la utilización de las nuevas tecnologías en la empresa.

El principal objeto de debate jurídico, a efectos de licitud de la prueba electrónica, es el «*control de uso*» por parte del empresario frente a los derechos fundamentales del trabajador protegidos constitucionalmente. Y si dentro del poder de vigilancia del empresario previsto en el art. 20.3 del Estatuto de los Trabajadores se incluye la facultad de registro unida a la obligación de cumplir las previsiones del artículo 18 del mismo Cuerpo legal.

El artículo 18 de la CE en sus apartados 1 y 3 recoge los derechos fundamentales a la intimidad y al secreto de comunicaciones. El artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos establece que toda persona tiene derecho al respeto de la vida privada y familiar y prohíbe la injerencia que no esté prevista en la ley y que no se justifique por razones de seguridad, bienestar económico, defensa del orden, prevención de las infracciones penales, protección de la salud, de la moral o de los derechos y libertades de los demás. En este sentido, el derecho a la intimidad, según la doctrina del Tribunal Constitucional, supone «*la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana» y ese ámbito ha de respetarse también en el marco de las relaciones laborales, en las que «es factible en ocasiones acceder a informaciones atinentes a la vida íntima y familiar del trabajador que pueden ser lesivas para el derecho a la intimidad*» (SSTC 142/1993, 98/2000 y 186/2000).

La Sentencia del Tribunal Europeo de Derechos Humanos, de 3 de abril de 2007, caso *COPLAND CONTRA EL REINO UNIDO*, señala que están incluidos en la protección del Convenio Europeo de derechos humanos «*la información derivada del seguimiento del uso personal de Internet*», expresión de la máxima preservación de la intimidad. Dicha sentencia considera en su § 41 que tanto «*los correos electrónicos enviados desde el lugar del trabajo*» como «*la información derivada del seguimiento del uso personal de Internet*» están incluidos en el ámbito de protección del art. 8 del Convenio europeo, por cuanto pueden contener datos sensibles que afecten a la intimidad. En este caso, precisa el Tribunal, a la demandante no se le advirtió de que podría ser

objeto de un seguimiento, por lo que podía razonablemente esperar que se reconociera el carácter privado «en lo que respecta al correo electrónico y la navegación por Internet» (§ 42).

Las SSTC de 15 de noviembre de 2004 o 10 de abril de 2000 expresaban que «*estando en cuestión la posible vulneración del artículo 18.1 CE en el marco de una relación laboral, debe recordarse que la celebración de un contrato de trabajo no implica en modo alguno la privación para una de las partes, el trabajador, de los derechos que la Constitución le reconoce como ciudadano, entre ellos el derecho a su intimidad personal. Las organizaciones empresariales no forman mundos separados y estancos del resto de la sociedad ni la libertad de empresa que establece el artículo 38 del Texto constitucional legitima que quienes prestan servicios en aquéllas, por cuenta y bajo la dependencia de sus titulares, deban soportar despojos transitorios o limitaciones injustificadas de sus derechos fundamentales y libertades públicas*». Sin embargo, también es conocido que, para el mismo Tribunal, los hechos referidos a las relaciones sociales y profesionales en que el trabajador desempeña su actividad no se integran, en principio, en la esfera privada de la persona (SSTC 180/1987, de 12 de noviembre, 142/1993, de 22 de abril, 202/1999, de 8 de noviembre y ATC 30/1998, de 28 de enero), lo que no significa que en dichos ámbitos no puedan encontrarse facetas del individuo; y que es factible en ocasiones acceder a informaciones atinentes a la vida íntima, personal y familiar del trabajador (SSTC 142/1993, de 22 de abril, 202/1999, de 8 de noviembre, y 98/2000, de 10 de abril).

El artículo 20.3 del Estatuto de los Trabajadores permite al empresario, frente a los derechos del trabajador, adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales guardando la consideración debida a su dignidad humana, lo cual supone reconocer que el derecho a la libertad de empresa y a la dirección de la actividad laboral que tiene el empresario tiene que compatibilizarse con el respeto a los derechos fundamentales del trabajador. Concretando esta previsión, las SS TSJ Cataluña, Sala de lo Social, de 11 de marzo de 2004 y 14 de noviembre de 2000 , TSJ País Vasco, Sala de lo Social, de 27 de marzo de 2001 , o TSJ Andalucía, Sala de lo Social, de 9 de mayo o 13 de noviembre de 2003, entre otras, son unánimes al recordar que el sistema informático es un instrumento de trabajo que la empresa proporciona al trabajador para desarrollar sus cometidos laborales y que dicho artículo 20 ET legitima la vigilancia por parte del empresario. En relación con esta cuestión, el Tribunal Constitucional ha insistido en el ámbito laboral en la posibilidad de recortes que resulten proporcionados, idóneos y necesarios, lo que ha llevado a los TSJ, en una ponderación «ad casum», a considerar que estos controles sobre

los medios informáticos de la empresa no son ilícitos pues el empresario no es ajeno al ámbito en el que operan.

Es, pues, doctrina del Tribunal Constitucional que los medios empleados por el empresario deben ser razonables y proporcionados a las circunstancias (STC 98/00 y 186/00, entre otras) debiendo garantizarse el derecho a la dignidad e intimidad de las personas (art. 10 y 18 CE), lo que en el proceso laboral tiene características peculiares a la vista de los derechos garantizados a los trabajadores en los art. 4.2 e) y 20.3 del Estatuto de Trabajadores. Asimismo, es doctrina constitucional que para el control de la actividad del trabajador en su puesto de trabajo cabe por parte del empresario la adopción de medidas siempre que la medida sea: 1) Idónea para el fin perseguido; 2) sea necesaria al no existir otra vía de actuación menos fuerte; 3) sea equilibrada o proporcionada, al limitarse al lugar y tiempo imprescindibles para comprobar el comportamiento inadecuado (STC 186/00).

La medida adoptada por el empresario deberá ser lo menos intrusiva posible. Por ejemplo, no será lícito acceder a los archivos personales del trabajador para controlar el uso desviado del correo cuando para ello baste con una simple impresión de la relación de dichos correos (STSJ Andalucía, Sala de lo Social, Sec. 2ª, de 8 de julio de 2010); ni extraer rastros o huellas como los archivos temporales que incorporen información sobre aspectos de la vida privada (ideología, orientación sexual, aficiones etc.), como ocurre en con el simple dominio de las páginas Web que en la mayoría de los casos son reveladoras de su contenido.

En cuanto a si las facultades de vigilancia y control por parte del empresario (art. 20 ET) facultan al empresario para el registro de dispositivos electrónicos facilitados por aquel al trabajador, sin que sean de aplicación las previsiones del artículo 18 del Estatuto de los Trabajadores, la jurisprudencia ha sido vacilante, inclinándose finalmente por la no aplicación de dicho artículo. Así lo determina la Sentencia del Tribunal Supremo, Sala 4ª, de fecha 26 de septiembre de 2007, entendiendo que en estos supuestos el empresario no está efectuando una función de policía que se vincule a la protección del patrimonio del empresario y de los demás trabajadores sino a la protección de un medio de trabajo. El artículo 18 ET establece que «*sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo*», añadiendo que en la realización de estos registros «*se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de*

la empresa, siempre que ello fuera posible».

Según la citada STS de 2007 tanto la persona del trabajador, como sus efectos personales y la taquilla forman parte de la esfera privada de aquél y quedan fuera del ámbito de ejecución del contrato de trabajo al que se extienden los poderes del artículo 20 del Estatuto de los Trabajadores. Por el contrario, las medidas de control sobre los medios informáticos puestos a disposición de los trabajadores se encuentran, en principio, dentro del ámbito normal de esos poderes: el ordenador es un instrumento de producción del que es titular el empresario «como propietario o por otro título» y éste tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen. Por otra parte, con el ordenador se ejecuta la prestación de trabajo y, en consecuencia, el empresario puede verificar en él su correcto cumplimiento, lo que no sucede en los supuestos del artículo 18, pues incluso respecto a la taquilla, que es un bien mueble del empresario, hay una cesión de uso a favor del trabajador que delimita una utilización por éste que, aunque vinculada causalmente al contrato de trabajo, queda al margen de su ejecución y de los poderes empresariales del artículo 20 del Estatuto de los Trabajadores para entrar dentro de la esfera personal del trabajador. De ahí, que los elementos que definen las garantías y los límites del artículo 18 del Estatuto de los Trabajadores no sean aplicables al control de los medios informáticos. No cabe, aplicación directa del artículo 18 del Estatuto de los Trabajadores al control del uso del ordenador por los trabajadores, ni tampoco su aplicación analógica, porque no hay ni semejanza de los supuestos, ni identidad de razón en las regulaciones (artículo 4.1 del Código Civil).

Parte de la jurisprudencia había hecho extensiva la presunción *iuris et de iure* de ámbito reservado que la ley reconoce a la persona del trabajador, sus efectos personales y taquillas a la mesa y ordenador de trabajo. Por cuanto por un lado, tienen en común que son bienes del empresario destinados a la actividad productiva y, por otro, existe en tales ámbitos un posible espacio de intimidad del trabajador. Así, los tribunales admitían como lícito el registro de los servidores de las empresas con la finalidad de descubrir las conductas que representan un perjuicio sobre el sistema. En estos casos, los registros no se efectuaban de forma directa y física sobre el terminal del trabajador sino que el control se efectúa de modo indirecto a través del servidor. Tal sería el caso, por ejemplo, de la auditoría del servidor que permite revelar la introducción del programa incompatible con la configuración del sistema y que provoca anomalías en los ficheros del sistema (STSJ Madrid de 21 de noviembre de 2000; o de la exploración del servidor que permite advertir el acceso no autorizado a ciertos ficheros de la empresa (STSJ Madrid de 12 de junio de 2001); o, en fin, de los supuestos en los que se tiene conocimiento de la modificación de archivos del servidor de la empresa (STSJ Madrid de 28 de noviembre de 2000).

Sin embargo, la doctrina judicial difería en cuando lo que se trata es de registrar la memoria del terminal empleado por el trabajador (disco duro). Mientras que algunos pronunciamientos han sostenido la aplicación analógica del artículo 18 TRLET cuando se interviene la memoria del ordenador con el fin de revelar eventuales incumplimientos contractuales del trabajador (SSTSJ de Castilla-La Mancha de 16 de junio de 1999, de Andalucía/Málaga de 25 de febrero de 2000 y de Cantabria de 20 de febrero de 2004), en otros casos, por el contrario, se rechazaba la eventual aplicación del artículo 18 TRLET *«ya que el útil de trabajo no puede considerarse como un efecto personal*» (STSJ Madrid de 13 de noviembre de 2001, STSJ Murcia de 15 de junio de 1999 y STSJ Cantabria de 20 de febrero de 2004).

La STSJ Galicia, Sala de lo Social, de 4 de octubre de 2001, recoge el supuesto de la empresa que asigna al trabajador una dirección de correo electrónico personal y pleno acceso a Internet, pero enfatiza que lo hace para el desarrollo de su actividad dentro de la Empresa, no para su utilización en asuntos privados o particulares: «*el hecho de que sea una dirección "personal" no desquita que es un instrumento empresarial para que el trabajador desarrolle sus funciones dentro de la misma. En consecuencia, el empresario puede utilizar su derecho a vigilar y controlar los instrumentos de trabajo y de controlar cómo el trabajador da cumplimiento a sus obligaciones laborales (art. 5.a) ET), puesto que es deber del mismo realizar el trabajo convenido bajo la dirección del empresario (art. 20.1 ET), el cual puede «adoptar las medidas que estime oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales (art. 20.3 ET)*» Los ordenadores portátiles están pensados para su uso dentro y fuera de las instalaciones de la empresa. En igual sentido, la Sentencia Audiencia Provincial de Barcelona, sec. 15ª, nº 46/2006, de dos de febrero, rec. 711/2005. Pte: González Navarro, Blas Alberto.

Por su parte, la Sentencia del Juzgado de lo Mercantil número 1 de Bilbao, de fecha 30 de diciembre de 2005[138] si bien señala que no es reprochable que una empresa decida recuperar la información que contiene un ordenador de su propiedad, instalado en un centro productivo y destinado a facilitar la prestación laboral de sus empleados, desde el momento que ese ordenador está conectado a la red, es posible que un trabajador tenga acceso, desde el mismo, a su propio servidor, y que utilice su correo electrónico particular. Esa circunstancia impide, entonces, la obtención del contenido del rastro de información que pueda haber dejado en el ordenador de la empresa, puesto que aunque el terminal desde el que accede sea de su titularidad, el lugar en que entra es particular y en consecuencia, puesto que ofrece un sistema de

[138] Sentencia del Juzgado de lo Mercantil número 1 de Bilbao, de fecha 30 de diciembre de 2005, nº 517/2005, nº autos 75/2004. Pte.: Rodríguez Achutegui, Edmundo. F. J. Primero.

comunicación universal, queda amparado por el art. 18.3 CE y el art. 8 CEDH. Aunque el ordenador desde el que se accede a la Web sea particular, propiedad de la empresa, el contenido de aquella página es de acceso público, y los servidores a través de los que se produce la comunicación electrónica merecen el mismo amparo constitucional que las tradicionales comunicaciones «postales, telegráficas, telefónicas» a las que alude el art. 18.3 CE. Entiende amparados también por dicho derecho fundamental incluso a aquellos correos particulares privados dirigidos al correo laboral. Dicha sentencia entiende vulnerado el derecho fundamental al secreto de comunicaciones al haberse obtenido dichos archivos sin autorización judicial.

Existe una regla de buena fe reconocida jurisprudencialmente en el deber del empresario y correspondiente «*derecho del trabajador de información*» sobre las medidas de control que pueda ejecutar o ejecute la empresa sobre dichos instrumentos. Los técnicos aconsejan que las empresas pacten sus políticas de privacidad y fijen las reglas de uso de los medios informáticos, habiéndose adoptado iniciativas de este tipo en los Convenios Colectivos y cuyo contenido se encuentra cada vez con mayor habitualidad en los contratos de trabajo, estableciéndose condiciones de uso de dichos instrumentos y responsabilidades disciplinarias.

La jurisprudencia refiere el establecimiento previo por parte de las empresas de unas «*reglas de uso de dichos medios*», de informar al trabajador de que va a existir control, y de los medios que, en su caso van a utilizarse. En este sentido, se pronuncia la mencionada Sentencia del Tribunal Supremo, Sala 4ª, de fecha 26 de septiembre de 2007[139] señalando que «*de esta manera, si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado «una expectativa razonable de intimidad» en los términos que establecen las sentencias del Tribunal Europeo de Derechos Humanos de 25 de junio de 1997 (caso Halford) y 3 de abril de 2007 (caso Copland) para valorar la existencia de una lesión del artículo 8 del Convenio Europeo para la protección de los derechos humanos*». De igual modo la Sentencia del Tribunal Supremo, de 8 de marzo de 2011, estima improcedente la admisión de la prueba obtenida por la empresa a partir de una auditoria interna sin información previa al trabajador sobre la existencia de controles ni advertencia de reglas de uso de los ordenadores, en un supuesto en que el empleado había accedido a 5.566 visitas de contenido multimedia, piratería informática, anuncios y otros. Finalmente la Sentencia del Tribunal Supremo de 6 de octubre de 2011 unifica la doctrina en la materia, habilitando al empresario a controlar el correo electrónico y demás medios informáticos que aquel

[139] Sentencia del Tribunal Supremo, Sala 4ª, de fecha 26 de septiembre de 2007 rec. 966/2006. Pte. Desdentado Bonete, Aurelio, F. Jco. cuarto.

entrega a los trabajadores para el desarrollo de su actividad laboral, siempre que se haya informado acerca de las prohibiciones al trabajador y pueda demostrarse que efectivamente se ha realizado esa información. La prueba obtenida del control es lícita en cuanto no incumple derechos fundamentales.

La reciente Sentencia del Tribunal Constitucional de 7 de octubre de 2013, que resuelve el recurso de amparo número 2907/2011, declara procedente el despido disciplinario de un trabajador que traspasó información confidencial de la empresa en que trabajaba a otra entidad utilizando medios de comunicación corporativos, en concreto por correo electrónico y teléfono móvil de empresa. La empresa constató las sospechas tras efectuar un examen, por perito y en presencia notarial, del contenido de las comunicaciones que efectuó el trabajador a través del teléfono móvil de empresa facilitado para llevar acabo sus funciones y por correo electrónico. Destaca dicha sentencia por cuanto si bien en dicho supuesto la empresa no tenía política empresarial interna –protocolos- en cuanto al uso de dichos medios de comunicación, el Convenio Colectivo de aplicación sancionaba, de modo leve, «*el uso de medios informáticos propiedad de la empresa para fines distintos de los relacionados con el contenido de la prestación laboral*», y como falta muy grave «*la revelación a elementos extraños a la empresa de datos de reserva obligada*». El Tribunal Constitucional resuelve que no existe vulneración del derecho al secreto de comunicaciones por cuanto queda implícito dentro de la prohibición que consta en el Convenio colectivo, la posibilidad de que el empresario tuviera acceso a dichos medios para verificar que se le daba el uso adecuado y se cumplía con dicha prohibición. Tampoco se vulneró el derecho a la intimidad en cuanto el trabajador no podía tener una expectativa razonable de privacidad en cuanto existía un Convenio que establecía la prohibición de uso de medios informáticos propiedad de la empresa con fines no profesionales. Por lo tanto, en dicha sentencia no se exige política interna empresarial sobre dichos medios de comunicación corporativos para que la empresa pueda efectuar control y vigilancia del uso que hacen los trabajadores de dichos medios, sino que basta la existencia de un Convenio Corporativo de aplicación que así lo prevea.

La Sentencia del Tribunal Constitucional 241/2012, de 17 de diciembre deniega el amparo constitucional a una de las trabajadoras que instalaron el programa «Trillian» de mensajería instantánea en un ordenador de la empresa sin permiso de la misma –que lo había prohibido expresamente- y sin clave de acceso. Con dicho sistema de mensajería llevaron a cabo, entre ellas, diversas conversaciones en las que se vertían comentarios críticos, despectivos o insultantes en relación con compañeros de trabajo, superiores y clientes. Dichas conversaciones fueron descubiertas, por casualidad, por un empleado que intentó utilizar la unidad «C» de ese ordenador, dando cuenta de ello a la empresa. El Tribunal Constitucional entiende que no cabe apreciar afectación

del derecho a la intimidad regulado en el artículo 18 CE desde el momento en que fue la propia demandante y otra trabajadora quienes realizaron actos dispositivos que determinaron la eliminación de la privacidad de sus conversaciones, al incluirlas en el disco del ordenador en el cual podían ser leídas por cualquier otro usuario, pudiendo trascender su contenido a terceras personas, como aquí ocurrió al tener conocimiento la dirección de la empresa. Dicha Sentencia recuerda de nuevo las facultades de vigilancia y control del empresario en estrecha proporción a los derechos y dignidad del trabajador y desestima la vulneración del de secreto de las comunicaciones, pues éstas estaban abiertas y no rodeadas de las condiciones que pudieran preservarlas, al tratarse de un ordenador de libre acceso, sin clave de seguridad, y existiendo un protocolo de uso establecido por la propia empresa.

La Justicia, no obstante, ha avalado en alguna ocasión –jurisprudencia menor- que el empresario acceda al ordenador del trabajador sin su consentimiento y sin haber pactado antes la política de privacidad. Un auto de la Audiencia de Madrid, de 14 de mayo de 2010, avala el acceso al ordenador del trabajador, sin su consentimiento, pese a no haberle informado de los controles ni haber establecido las reglas de uso de los medios informáticos. En este auto, considera el juez que «*el ordenador es un instrumento del que es titular el empresario como propietario y que éste tiene facultades de control de su utilización que incluyen su examen*». El auto estima que los intereses de la compañía prevalecen.

En conclusión, en el ámbito laboral el empresario está facultado para efectuar controles de los instrumentos electrónicos facilitados a sus trabajadores, pudiendo efectuar registros informáticos y adoptar las medidas oportunas para vigilar el cumplimiento de las obligaciones laborales de sus empleados. Evidentemente, no de un modo arbitrario, sino respetando la dignidad del trabajador y los derechos fundamentales relacionados con la misma. Equilibrio que debe obedecer a los citados principios de idoneidad, necesidad y proporcionalidad, que, en su caso, serán valorados por los Tribunales. Y siempre, previa comunicación a los trabajadores de los sistemas de control y consecuencias disciplinarias en caso de mal uso de los mismos, en aras al principio de buena fe.

3.1.3 Derecho a la protección de datos

La implantación de las nuevas tecnologías en nuestra sociedad ha supuesto la posibilidad de acumular, tratar y ceder en forma masiva gran cantidad de datos personales con el correspondiente peligro que ello supone para el derecho a la privacidad de las personas. Es por ello que el Derecho a la protección de datos

se erige como derecho fundamental previsto en el artículo 18.4 de la Constitución Española. Dicho artículo establece que «l*a ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derecho*». Se trata de un derecho fundamental autónomo del resto de los previstos en el artículo 18 de la Constitución Española, tal y como ha sido declarado por la STC 292/2000, de 30 de noviembre.

Según el Tribunal Constitucional el objeto de protección de este derecho fundamental no se reduce sólo a los datos íntimos de la persona, sino de cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es la intimidad individual, ya protegida en el artículo 18.1 CE sino los datos de carácter personal. Se trata de un derecho fundamental que no se ciñe exclusivamente a los datos relativos a la vida privada de la persona sino que se hace extensivo a los datos públicos, que por el mero hecho de serlo no pueden escapar al poder de disposición y control del titular de los mismos. El derecho fundamental a la protección de datos amplia la garantía constitucional a «*aquellos de esos datos que sean relevantes o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado*». Y reconoce el derecho de la persona afectada al control sobre los datos relativos a su propia persona, derecho a controlar el uso efectuado de los mismos y a oponerse a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención. Control sobre sus propios datos personales, entre los que se encuentran no sólo los relativos a la vida privada o íntima de la persona, sino, como reconoce la sentencia del Tribunal Constitucional de 30 de noviembre de 2000, también todos aquellos que «*identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo*».

El derecho a la intimidad personal y familiar y el derecho a la protección de datos difieren, a pesar de tener como fundamento común la dignidad de la persona humana y los derechos inviolables que le son inherentes en los términos reconocidos en el art. 10.1 de la Constitución y en los Tratados Internacionales. Las diferencias son evidentes: mientras que la protección de la intimidad tiene un carácter «defensivo» excluyendo del conocimiento ajeno la «vida personal y familiar», vetando incluso las intromisiones de tercero contra la voluntad del titular. En el caso de la Protección de los Datos Personales, aun reconociendo la dinamicidad de su contenido objetivo derivado de los cambios tecnológicos, este derecho fundamental garantiza a la persona un poder de

control --de contenido positivo-- sobre la captura, uso, destino y posterior tráfico de los datos de carácter personal[140].

El derecho fundamental a la protección de datos es un derecho constitucional, lo cual no significa que en el supuesto de entrar en conflicto con otros derechos o intereses legítimos no pueda efectuarse una ponderación entre los mismos atendiendo al caso concreto. Dicha postura es la mantenida por el Tribunal de Justicia de la Unión Europea en la Sentencia dictada en fecha 24 de noviembre de 2011, que resuelve las cuestiones prejudiciales planteadas por el Tribunal Supremo, sobre la interpretación del artículo 7 letra f) de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

El artículo 7 letra f) de la Directiva 95/46/CE establece que «Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si…f) *es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva*», (en particular, los derechos a la intimidad y a la protección de datos personales, consagrados ahora en los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea).

El Tribunal entiende que el artículo 7 f) tiene efecto directo y al mismo tiempo, precisa el alcance normativo del precepto, señalando que no admite que las normativas nacionales, en ausencia del consentimiento del interesado, exijan para permitir el tratamiento de datos personales «necesario para la satisfacción de un interés legítimo», además del respeto de los derechos y libertades fundamentales del interesado, que los datos se encuentren siempre en fuentes accesibles al público, «excluyendo así de forma categórica y generalizada todo tipo de tratamiento de datos que no figuren en tales fuentes».

Ello no significa, sin embargo, que la mera invocación de un interés legítimo deba considerarse suficiente para legitimar el tratamiento de datos personales sin el consentimiento del afectado. En los fundamentos de la Sentencia, el propio Tribunal precisa la interpretación que debe darse a dicho artículo,

---

[140] Véase ALVAREZ-CIENFUEGOS SUAREZ, José María, *La libertad informática, un nuevo derecho fundamental en nuestra Constitución, Comentario a las sentencias del Tribunal Constitucional 290/2000 y 292/2000, de 30 de noviembre, sobre la Ley de Protección de Datos*, publicado en el diario "La Ley" de 22/01/01, sección doctrina.

subrayando la necesidad de realizar en cada caso concreto una ponderación entre el interés legítimo de quien va a tratar los datos y los derechos fundamentales de los ciudadanos afectados, con el fin de determinar cuál prevalece atendiendo a las circunstancias concurrentes.

En este sentido, recuerda que el artículo 7 f) de la Directiva «*establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado*». Acto seguido, el Tribunal advierte que «*el segundo de esos requisitos exige una ponderación de los derechos e intereses en conflicto que dependerá, en principio, de las circunstancias concretas del caso particular de que se trate*». Y deja claro que en este marco «*la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea confieren al interesado*», permitiendo que a la hora de adaptar su ordenamiento jurídico a la Directiva 95/46, *«los Estados miembros establezcan los principios que deben regir dicha ponderación»*.

Entre dichos criterios de ponderación, la Sentencia se refiere, en particular, al hecho de que los datos no se encuentren en fuentes accesibles al público, recordando que «*a diferencia de los tratamientos de datos que figuran en fuentes accesibles al público, los tratamientos de datos que figuran en fuentes no accesibles al público implican necesariamente que el responsable del tratamiento y, en su caso, el tercero o terceros a quienes se comuniquen los datos dispondrán en lo sucesivo de ciertas informaciones sobre la vida privada del interesado. Esta lesión, más grave, de los derechos del interesado consagrados en los artículos 7 y 8 de la Carta debe ser apreciada en su justo valor, contrapesándola con el interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos*».

A la vista de todo ello, cabe recordar que en la interpretación y la aplicación que hasta el momento se ha venido realizando en España, tanto por la AEPD como los órganos judiciales, ya se estaba llevando a cabo una ponderación en la línea de lo exigido por el artículo 7 f) de la Directiva, atendiendo a criterios diversos, tales como la finalidad del tratamiento de los datos, el marco legal aplicable, -p. ej. la existencia de una ley que ampare intereses legítimos- o circunstancias concurrentes en el caso como, entre otras, la existencia de una relación jurídica, o que los datos figuren o no en fuentes accesibles al público. En consecuencia, de la Sentencia del TJUE no parece derivarse una alteración sustancial del marco vigente de protección de los datos personales en España ni que el fallo

comporte una merma en el grado de protección de los derechos de los ciudadanos, si bien en el futuro será preciso acentuar la ponderación de las circunstancias que concurran en cada supuesto concreto para decidir sobre la legitimidad del tratamiento[141].

En lo referente a su regulación, en el ámbito comunitario cada Estado miembro de la Unión Europea trata de adaptar sus normas internas a las normas y directrices europeas sobre protección de datos. En este sentido el Convenio 108/1981, de 28 de enero del Consejo de Europa para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal, cuyo contenido se incorporó al derecho comunitario a la citada Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas con relación al tratamiento de datos personales y a la libre circulación de estos datos. Esta directiva fue transpuesta al ordenamiento jurídico español por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que se desarrolla en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD. Actualmente se halla en trámite la Propuesta de Reglamento Europeo que publicó en enero del 2012 el Parlamento Europeo junto con el Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos. Cuando dicho Reglamento entre en vigor (fecha límite para su aprobación mayo de 2014), será de aplicación directa y prevalente sobre nuestro actual sistema de protección de datos personales[142].

---

[141] El anterior comentario sobre la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, C-468/10, sigue el hilo expositivo de la Nota Informativa de la Agencia Española de Protección de Datos de igual fecha. Puede consultarse en la página web de la AEPD *www.agpd.es*. Página visitada en fecha 6/11/2013.

[142] El formato jurídico de Reglamento y no de Directiva permite homogeneizar la regulación de los estados Miembros. Se trata de un reglamento que amplía el ámbito de aplicación a todas las empresas que ofrezcan productos y servicios a residentes en Europa (sean o no europeas), y centraliza todos los procesos administrativos relacionados con la protección de datos mediante el mecanismos de la ventanilla única en el país del «establecimiento principal» de la empresa. El mecanismo de ventanilla única con una sola Autoridad de protección de Datos se complementa con un mecanismo de cooperación y coherencia entre las distintas Autoridades de Protección de Datos europeas. La Comisión Europea plantea la inclusión del derecho al olvido y a la portabilidad de los datos. Como señalaba el grupo de Expertos de Alto nivel de la Agenda Digital para España (18 de junio de 2012) «*… si bien la propuesta de la Comisión Europea permite solventar algunas de las barreras principales para una gestión eficiente de los datos de Europa – como es la actual dispersión normativa- su redacción actual mantiene disposiciones que limitan transferencias internacionales de datos personales, que pueden dificultar el desarrollo de servicios innovadores relacionados con la elaboración de perfiles o que mantiene una asignación de responsabilidades poco flexible que puede desincentivar el desarrollo de nuevos servicios de «cloud computing»…*» (§ IV.2 *Privacidad y protección de Datos*)

El objeto de la LOPD es garantizar y proteger, en lo concerniente al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar (art. 1 LOPD). Conforme al art. 3 LOPD son datos de carácter personal «*cualquier información concerniente a personas físicas identificadas o identificables*», precepto que se desarrolla por el RD 1720/07 al definir en el art. 5.1 letra o) a persona identificable como «*toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social»*.

La normativa sobre protección de datos se desarrolla sobre principios fundamentales que pueden concretarse con carácter general en los siguientes: «*el principio de consentimiento*», es decir, no pueden recogerse o tratarse datos personales sin que exista el consentimiento inequívoco del titular de dichos datos (con algunas excepciones como cuando una ley permita el tratamiento sin consentimiento, o en el marco de las competencias propias de las administraciones Públicas etc.) ; «*el principio de información»*, conforme al cual la persona a quien se soliciten los datos personales debe ser informada previamente de la existencia del fichero, de su finalidad y de quien es el responsable del mismo; «*el principio de calidad de datos*», conforme al cual los datos solo pueden ser recogidos y tratados para fines legítimos y específicos y, por lo tanto, no podrán ser utilizados para fines incompatibles con aquellos para los cuales fueron recogidos, además deben ser adecuados y no excesivos para la finalidad para la cual se recogieron; «*el principio de conservación*», en virtud del cual los datos personales, una vez tratados, deben ser cancelados cuando ya no sean necesarios para la finalidad para la que se recogieron, es decir, no pueden conservarse más del tiempo estrictamente necesario; y «*el principio de seguridad de los datos*», es decir, todo tratamiento de datos personales, automatizado o no, debe contar con las medidas de seguridad necesarias, tanto físicas como lógicas para impedir que puedan producirse accesos, alteraciones, cesiones o pérdidas de datos no autorizadas . El nuevo Proyecto de Reglamento añade algunos otros principios como «*el principio de rendición de cuentas*» (Accountability) estableciendo la responsabilidad de las Compañías en la implantación de mecanismos que garanticen el cumplimiento de los principios y obligaciones en materia de protección de datos así como a los métodos de validación que garanticen su fiabilidad.

También regula los llamados derechos ARCO del titular de los datos personales: «*derecho de acceso*», de «*rectificación»*, de «*cancelación»* y de «*oposición*». Y finalmente dicha normativa también prevé en cada Estado miembro una Autoridad de Control Independiente encargada de supervisar en cumplimiento de todo lo anterior, en España la Agencia Española de Protección de Datos o las diferentes Agencias autonómicas.

En lo referente a la obtención de prueba electrónica resulta fundamental atender a la regulación específica que sobre recogida y tratamiento de datos personales efectúa la normativa de protección de datos personales. Son importantes al efecto el principio del consentimiento por parte del titular de esos derechos, así como el principio de confidencialidad o secreto por parte del responsable del fichero o del encargado del tratamiento, y la información al titular de los datos personales de la finalidad de dicha recogida y tratamiento así como de su destino. Es por ello que uno de los aspectos más relevantes en este ámbito será «*la cesión o comunicación de datos de carácter personal a terceros*», entendiendo como tal y según viene definida en el artículo 3 i) de la LOPD «toda revelación de datos realizada a una persona diferente del interesado». Es «*interesado*» o «*afectado*», según define la propia LOPD, la persona física titular de los datos que sean objeto de tratamiento, es decir, de operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias (art. 3. e) y c)).

Como regla general los datos de carácter personal objeto de tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el «*previo consentimiento del interesado*» (art. 11.1 LOPD).

Sin embargo, la LOPD prevé en el art. 11.2 algunas excepciones en las que no se precisa el consentimiento del interesado para que sus datos sean comunicados a un tercero. Dicho artículo determina los siguientes supuestos: a) cuando la cesión está autorizada en una ley; b) cuando se trate de datos recogidos de fuentes accesibles al público[143]; c) cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique; d) cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación

[143] La LOPD define en su artículo 3 letra j) «las fuentes accesibles al público» como aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas; e) cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos; f) cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

También como excepción a la norma general que exige el consentimiento por parte del «interesado o afectado» para poder comunicar sus datos personales a terceros, la LOPD establece la posibilidad de que las Fuerzas y Cuerpos de Seguridad recaben y traten para fines policiales datos de carácter personal sin consentimiento de las personas afectadas limitados a los supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto (art. 22.2 LOPD). Conforme a la LOPD los cuerpos policiales podrán recoger datos personales que revelen la ideología, afiliación sindical, religión, creencias, origen racial, salud, y vida sexual (art. 7.2 y 7.3 LOPD) exclusivamente en los supuestos en que sea necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales (art. 22.3 LOPD).

La policía, por lo tanto, como norma general, puede acceder a cualquier dato de carácter personal por la vía del art. 22 LOPD de forma directa o por la vía indirecta del artículo 11.2d del mismo cuerpo legislativo, al entender que por tratarse de policía judicial actúa a prevención y por delegación de órganos judiciales o Ministerio Fiscal, habiendo tratado ya esta cuestión la Agencia Española de Protección de Datos en informe jurídico 133/2008. Existen, no obstante, limitaciones a dicha norma general, en concreto aquellos supuestos en los que existe una previsión legal que lo impide, previsión legal que debe ser considerada conforme al principio de especialidad. Tal es el caso de la previsión de los artículos 3 y 4 de la Ley 25/2007, de 18 de octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones que exige autorización judicial, y a la referente a Ley 41/2002, de 14 de noviembre reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica que exige que sea autoridad judicial. Otro supuesto, es el relativo al posible acceso por parte de la policía a los datos obrantes en los ficheros de la Tesorería de la Seguridad Social (art. 66 de la Ley General de la Seguridad Social, RDL 1/1994 de 20 de junio). Cuando se persiga como fin la investigación de delitos públicos, y

conforme la LGSS, será preceptiva habilitación fiscal o judicial para acceder a los ficheros de la Seguridad Social. Esta habilitación no será preceptiva cuando se persiga el fraude en la obtención o percepción de ayudas o subvenciones a cargo de fondos públicos, incluidos los de la Unión Europea, así como en la obtención o percepción de prestaciones incompatibles en los distintos regímenes del sistema de la Seguridad Social, al encontrarse la previsión en otro apartado del art. 66 LGSS[144].

El artículo 66 LGSS prevé también la cesión o comunicación por parte de la Tesorería de la Seguridad Social de los datos de que dispone cuando tenga por objeto la protección de derechos e intereses de los menores o incapacitados por los órganos jurisdiccionales o el Ministerio Público (letra f) y la colaboración con los jueces o tribunales en el curso del proceso y para la ejecución de resoluciones judiciales firmes. En este último supuesto se exige para la solicitud judicial de información resolución expresa, en la que, por haberse agotado los demás medios o fuentes de conocimiento sobre la existencia de bienes y derechos del deudor, se motive la necesidad de recabar datos de la Administración de la Seguridad Social (letra h).

3.1.4 Derecho a la inviolabilidad de domicilio

3.1.4.1 Contenido del derecho fundamental a la inviolabilidad domiciliaria

El artículo 18.2 de la Constitución Española garantiza la inviolabilidad del domicilio como uno de los derechos fundamentales de la persona. Dicho artículo dispone que «… 2. *El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito».*

El «derecho a la inviolabilidad del domicilio» se distingue del «derecho constitucional a la intimidad personal y familiar» regulado en el artículo 18.1 CE, en cuanto este último tiene por objeto la protección de un ámbito reservado de la vida de las personas excluido del conocimiento de terceros, sean éstos poderes públicos o particulares, mientras que el derecho a la inviolabilidad del domicilio protege un ámbito espacial determinado, el «domicilio», por ser aquél

[144] Véase sobre la posibilidad de acceso de los Cuerpos y Fuerzas de Seguridad del Estado a los datos de carácter personal: FRÍAS MARTÍNEZ, Emilio, *El acceso a los datos de carácter personal por la Policía. Referencia a los datos de la Seguridad Social*, en artículos doctrinales sobre Derecho Informático, publicado en julio de 2012 en Noticias Jurídicas. Puede consultarse en la siguiente dirección electrónica: http://goo.gl/B78QYd (página consultada el 5 de noviembre de 2013).

en el que los individuos, libres de toda sujeción a los usos y convenciones sociales, ejercen su libertad más íntima, siendo objeto de protección de este derecho tanto el espacio físico en sí mismo considerado, como lo que en él hay de emanación de la persona y de su esfera privada (SSTC 22/1984 , 94/1999, 144/1999 y 119/2001).

Ahora bien, la anterior construcción, estructurada más bien desde una perspectiva más próxima a la noción de individuo, no obsta, a que el propio Tribunal Constitucional, haya reconocido asimismo el derecho fundamental a la inviolabilidad del domicilio, a las personas jurídicas. Son titulares de este derecho no solo las personas físicas nacionales, extranjeras o apátridas sino también las personas jurídicas nacionales (SSTC 23/1989, de 2 de febrero, 137/1985 de 17 de octubre[145], 160/1991 de 18 de julio, 50/1995 de 23 de febrero, 64/1998 de 17 de marzo y 69/1999 de 26 de abril, y SSTS de 19 de diciembre de 1986 y 28 de octubre de 1997). *«… Si bien esta afirmación de principio se ha hecho no sin matizaciones relevantes, entre ellas la consideración de la "naturaleza y especialidad de fines" de dichas personas (STC 137/1985, fundamento jurídico 5º). Tal afirmación no implica, pues, que el mencionado*

[145] La STC 137/1985, de 17 de octubre, en su FJ.3º reconoce también el derecho a la inviolabilidad del domicilio de las personas jurídicas, dicha sentencia señala: «*3. Ausente de nuestro ordenamiento constitucional un precepto similar al que integra el art. 19.3 de la Ley Fundamental de Bonn, según el cual los derechos fundamentales rigen también para las personas jurídicas nacionales, en la medida en que, por su naturaleza, les resulten aplicables, lo que ha permitido que la jurisprudencia aplicativa de tal norma entienda que el derecho a la inviolabilidad del domicilio conviene también a las Entidades mercantiles, parece claro que nuestro Texto Constitucional, al establecer el derecho a la inviolabilidad del domicilio, no lo circunscribe a las personas físicas, siendo pues extensivo o predicable igualmente en cuanto a las personas jurídicas, del mismo modo que este Tribunal ha tenido ya ocasión de pronunciarse respecto de otros derechos fundamentales, como pueden ser los fijados en el art. 24 de la misma C.E., sobre prestación de tutela judicial efectiva, tanto a personas físicas como a jurídicas. Este es también el criterio aceptado por la doctrina generalizada en otros países, como pueden ser, dentro de Europa, en Alemania, Italia y Austria, donde se sigue un criterio que puede reputarse extensivo, llegado el momento de resolver esta misma cuestión, pudiendo entenderse que este derecho a la inviolabilidad del domicilio tiene también justificación en el supuesto de personas jurídicas, y posee una naturaleza que en modo alguno repugna la posibilidad de aplicación a estas últimas, las que -suele ponerse de relieve- también pueden ser titulares legítimos de viviendas, las que no pueden perder su carácter por el hecho de que el titular sea uno u otra, derecho fundamental que cumple su sentido y su fin también en el caso de que se incluyan en el círculo de los titulares de este derecho fundamental a personas jurídicas u otras colectividades. En suma, la libertad del domicilio se califica como reflejo directo de la protección acordada en el ordenamiento a la persona, pero no necesariamente a la persona física, desde el momento en que la persona jurídica venga a colocarse en el lugar del sujeto privado comprendido dentro del área de la tutela constitucional, y todas las hipótesis en que la instrumentación del derecho a la libertad no aparezcan o sean incompatibles con la naturaleza y la especialidad de fines del ente colectivo»*.

derecho fundamental tenga un contenido enteramente idéntico con el que se predica de las personas físicas. Basta reparar, en efecto, que, respecto a éstas, el domicilio constitucionalmente protegido, en cuanto morada o habitación de la persona, entraña una estrecha vinculación con su ámbito de intimidad, como hemos declarado desde la STC 22/1984, fundamento jurídico 5º (asimismo, SSTC 160/1991 y 50/1995, entre otras); pues lo que se protege no es sólo un espacio físico sino también lo que en el hay de emanación de una persona física y de su esfera privada (STC 22/1984 y ATC 171/1989), lo que indudablemente no concurre en el caso de las personas jurídicas. Aunque no es menos cierto, sin embargo, que éstas también son titulares de ciertos espacios que, por la actividad que en ellos se lleva a cabo, requieren una protección frente a la intromisión ajena. Por tanto, cabe entender que el núcleo esencial del domicilio constitucionalmente protegido es el domicilio en cuanto morada de las personas físicas y reducto último de su intimidad personal y familiar. Si bien existen otros ámbitos que gozan de una intensidad menor de protección, como ocurre en el caso de las personas jurídicas, precisamente por faltar esa estrecha vinculación con un ámbito de intimidad en su sentido originario; esto es, el referido a la vida personal y familiar, sólo predicable de las personas físicas. De suerte que, en atención a la naturaleza y la especificidad de los fines de los entes aquí considerados, ha de entenderse que en este ámbito la protección constitucional del domicilio de las personas jurídicas y, en lo que aquí importa, de las sociedades mercantiles, sólo se extiende a los espacios físicos que son indispensables para que puedan desarrollar su actividad sin intromisiones ajenas, por constituir el centro de dirección de la sociedad o de un establecimiento dependiente de la misma o servir a la custodia de los documentos u otros soportes de la vida diaria de la sociedad o de su establecimiento que quedan reservados al conocimiento de terceros» (STC 69/1999, de 26 de abril, FJ 2º).

El concepto de «domicilio» desde un punto de vista constitucional no coincide con el concepto emanado de una perspectiva jurídico-privada (SSTC 22/1984, fundamentos 2º y 5º, 160/1991, fundamento jurídico 8º, y 50/1995, fundamento jurídico 5º, 69/1999, de 26 de abril FJ 2º, entre otras), ni de «… *concepciones reduccionistas como las que lo equiparan al concepto jurídico-penal de morada habitual o habitación*» (STC 94/1999). Desde el ámbito jurado-privado o jurídico-administrativo el Código Civil y la Ley General Tributaria consideran como domicilio de las personas físicas su residencia habitual (art 40 Cc y art. 48.2 LGT). En cuanto a las personas jurídicas el Código Civil considera como tal el lugar en que se halle su representación legal o donde ejerzan sus funciones fundamentales respecto a las personas jurídicas (art 41 Cc) y la Ley de Sociedades de Capital lo define como el lugar en que se halle el centro de su efectiva administración y dirección, o en el que radique su principal establecimiento o explotación (art. 9 LSC). Por su parte, la Ley de Enjuiciamiento Civil refiere el que aparezca en el padrón municipal o el que conste oficialmente

a otros efectos, así como el que aparezca en Registro oficial o en publicaciones de Colegios profesionales, cuando se tratare, respectivamente, de empresas y otras entidades o de personas que ejerzan profesión para la que deban colegiarse obligatoriamente, el lugar en que se desarrolle actividad profesional o laboral no ocasional. Si la demanda se dirigiese a una persona jurídica, el domicilio de cualquiera que aparezca como administrador, gerente o apoderado de la empresa mercantil, o presidente, miembro o gestor de la Junta de cualquier asociación que apareciese en un Registro oficial (art. 155 LEC).

No obstante, la protección constitucional al derecho a la inviolabilidad del domicilio no se refiere a éste en su sentido conceptual jurídico-privado o jurídico-administrativo, en cuanto a lugar en que la persona ejerce sus derechos y obligaciones o a efectos de comunicaciones sino que viene referido a «*aquel lugar en que la persona desarrolla su privacidad*». Tal y como indicaba el Tribunal Constitucional en su Sentencia 22/1984, de 17 de febrero «*…la idea de domicilio que utiliza el art. 18 de la Constitución no coincide plenamente con la que se utiliza en materia de Derecho Privado y en especial en el art. 40 del Código Civil como punto de localización de la persona o lugar de ejercicio por ésta de sus derechos y obligaciones. Como se ha dicho acertadamente en los alegatos que en este proceso se han realizado, la protección constitucional del domicilio es una protección de carácter instrumental, que defiende los ámbitos en que se desarrolla la vida privada de la persona. Por ello, existe un nexo de unión indisoluble entre la norma que prohíbe la entrada y el registro en un domicilio (art. 18.2 de la Constitución) y la que impone la defensa y garantía del ámbito de privacidad (artículo 18.1 de la Constitución). Todo ello obliga a mantener, por lo menos prima facie un concepto constitucional de domicilio de mayor amplitud que el concepto jurídico privado o jurídico-administrativo*».

Es indiferente al concepto constitucional de domicilio el «título jurídico» que habilita el uso del espacio en cuestión, su carácter de bien mueble o inmueble, la intensidad o periodicidad con la que se desarrolle la vida privada en el mismo (STS 10/2002). Las estancias en el domicilio son irrelevantes a tal efecto de este modo el Tribunal Constitucional ha considerado domicilio a una vivienda aun cuando en el momento del registro no se hallaba habitada (STS 94/1999). Lo fundamental es la idea de «privacidad» por lo que no todo recinto cerrado se considerará domicilio a efectos constitucionales no siendo extensible, por ejemplo, a aquellos lugares cerrados que, por su afectación –almacenes, fábricas, oficinas, bares y locales comerciales- (ATC 171/1989) tienen un destino o sirven a cometidos incompatibles con la idea de privacidad (SSTC 228/1997 y 283/2000). El Tribunal Supremo considera que en el caso de las personas jurídicas tienen la consideración de domicilio a efectos de la protección constitucional otorgada por el artículo 18.2 de la Constitución «… *los espacios que requieren reserva y no intromisión de terceros en razón a la actividad que en*

los mismos se lleva a cabo; esto es, los lugares utilizados por representantes de la persona jurídica para desarrollar sus actividades internas, bien porque en ellos se ejerza la habitual dirección y administración de la sociedad, bien porque sirvan de custodia de documentos u otros soportes de la vida diaria de la sociedad o de su establecimiento, exigiéndose en estos casos la autorización judicial o el consentimiento del interesado», «*… todo ello con independencia de que sea el domicilio fiscal la sede principal o la sede secundaria, exigiéndose en estos casos la autorización judicial o el consentimiento del interesado. En cambio, no son objeto de protección los establecimientos abiertos al público o en que se lleve a cabo una actividad laboral o comercial por cuenta de la sociedad mercantil que no esté vinculada con la dirección de la sociedad ni sirva a la custodia de su documentación. Tampoco, las oficinas donde únicamente se exhiben productos comerciales o los almacenes, tiendas, depósitos o similares…».)-»* (STS , Sala 3º, de 24 de enero de 2012, FL 5º, que cita jurisprudencia anterior del Tribunal Supremo como las sentencias de 23 de abril de 2010 (Pleno) -R.C. números 5910/06 (F.D. 5.º; 6.º y 7.º); 704/04; 3791/06; 4572/04 y 4888/06, respectivamente - y la de 30 de septiembre de 2010 -R.C. n.º 364/2007 (F.D. 3.º)).

3.1.4.2 Intromisión lícita en el ámbito domiciliario y en la esfera privada no domiciliaria

Señalábamos anteriormente que los derechos fundamentales no son absolutos sino que pueden entrar en conflicto con otras libertades y ser sometidos a restricciones y limitaciones. En este sentido el derecho fundamental a la inviolabilidad del domicilio supone que ninguna entrada y registro podrá llevarse cabo sin el consentimiento del titular o resolución judicial salvo en los casos de flagrante delito[146]. Previsión taxativa según la doctrina constitucional, véase por ejemplo las SSTC 22/1984, 17 de febrero, FJ 3º, 160/1991, de 18 de julio, FJ 8º, 341/1993, de 18 de noviembre, FJ 8º y 136/2000, de 29 de mayo. No obstante, la propia Constitución establece otros límites a la inviolabilidad de domicilio como los estados de excepción y de sitio (art. 55.1) y las investigaciones relativas a la actuación de bandas o elementos terroristas (art. 55.2), a los que pueden añadirse estados de necesidad como causa de justificación.

Ahora bien, que el domicilio sea objeto de especial protección constitucional, no supone que otros recintos tales como oficinas, locales o industrias no se hallen también protegidos sin que sea lícita una entrada no autorizada ya sea

[146] Véase la doctrina del constitucional sobre «flagrante delito» en la STC 341/1993, de 18 de noviembre.

por el titular del lugar o por una resolución judicial. Lo que sucede es que los requisitos para esa entrada no tendrán la misma entidad y exigencia que en el supuesto de un domicilio. Es por lo tanto necesaria autorización judicial, si no media consentimiento del interesado, para acceder a un espacio no domiciliario pero que constituye propiedad privada.

El Tribunal Constitucional se ha pronunciado respecto al consentimiento indicando que «*…El consentimiento eficaz del sujeto particular permitirá la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno*…» (SSTC 83/2002, de 22 de abril, FJ 5 y 196/2006, de 3 de julio, FJ 5), aunque este consentimiento puede ser revocado en cualquier momento (STC 159/2009, de 29 de junio, FJ 3). Ahora bien, se vulnerará el derecho a la intimidad personal cuando la penetración en el ámbito propio y reservado del sujeto «*aún autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida*» (SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 5; y 70/2009, de 23 de marzo, FJ 2).

En lo relativo a la forma de prestación del consentimiento debe ser «expreso», es decir, se exige que el consentimiento sea plenamente consciente por parte del interesado. En este sentido la STC 209/2007, de 24 de septiembre dispone que: «*salvo casos excepcionales, la mera falta de oposición a la intromisión domiciliar no podrá entenderse como un consentimiento tácito» (*FJ 5). *«…La validez del consentimiento exige, de conformidad con la jurisprudencia de la Sala Segunda de este Tribunal* -sentencias, entre otras, de 1 de abril de 1996, 4 de marzo de 1999 y 18 de febrero de 2005-, *que esté absolutamente desprovisto de toda mácula que enturbie el exacto conocimiento de lo que se hace y la libérrima voluntad de hacerlo, debiendo estar también exento de todo elemento susceptible de provocar o constituir error, violencia, intimidación o engaño; por lo que el interesado debe ser enterado de que puede negarse a autorizar la entrada y registro que se le requiere*». Por otro lado, tratándose de personas jurídicas el consentimiento debe prestarse «*…por parte de quien ostenta la representación legal de la mercantil, o ejerce labores de dirección o administración de la misma, con efectiva intervención en las decisiones de la empresa…*» (STS, Sala 3º, de 24 de enero de 2012, FJ 5º).

No obstante, alguna sentencia del TC como, por ejemplo, la STC 22/1984, de 17 de febrero, entraña cierta confusión al señalar que el consentimiento en supuestos referentes al derecho a la inviolabilidad del domicilio del art. 18.2 CE, no necesita ser «expreso» (FJ 3). En cuanto al consentimiento prestado en forma tácita, véase la STC 196/2004, de 15 de noviembre, en que se analizaba si un

reconocimiento médico realizado a un trabajador había afectado a su intimidad personal, estableciéndose no sólo la eficacia del consentimiento prestado verbalmente, sino además la del derivado de la realización de actos concluyentes que expresen dicha voluntad (FJ 9). A igual conclusión llegan las SSTC 22/1984, de 17 de febrero, y 209/2007, de 24 de septiembre, en supuestos referentes al derecho a la inviolabilidad del domicilio del art. 18.2 CE, manifestando en la primera que este consentimiento no necesita ser «expreso» (FJ 3) y en la segunda que, «salvo casos excepcionales, la mera falta de oposición a la intromisión domiciliar no podrá entenderse como un consentimiento tácito (FJ 5)».

Otra cuestión que se ha planteado es la necesidad o no de consentimiento de todas las personas que viven en un mismo domicilio. A este respecto el Tribunal Constitucional ha señalado que «*la inviolabilidad domiciliaria, como derecho, corresponde individualmente a cada uno de los que moran en el domicilio*» (STC 22/2003, de 10 de febrero FJ 7), «*…sin que esta titularidad individual se pierda por el hecho de que un mismo domicilio sea compartido por varias personas. El ejercicio del derecho, de contenido «fundamentalmente negativo», consiste en el ejercicio de la facultad de exclusión que conforma su contenido, esto es, de la «facultad del titular de excluir a otros de ese ámbito espacial reservado, de impedir o prohibir la entrada o la permanencia en él de cualquier persona y, específicamente, de la autoridad pública para la práctica de un registro»* (STC 22/2003, FJ 3). No en vano la Constitución se refiere al derecho a la inviolabilidad del domicilio como preservación de un determinado espacio *(«*el domicilio es inviolable») y configura su garantía esencial a través de la interdicción de toda entrada en el mismo que no sea consentida por su titular o autorizada judicialmente, «salvo en caso de flagrante delito» (art. 18.2 CE).

Si la convivencia en un mismo domicilio no altera, en principio, ni la titularidad del derecho ni la posibilidad de su ejercicio, resulta que cada titular del mismo mantiene una facultad de exclusión de terceros del espacio domiciliario que se impone al ejercicio del libre desarrollo de la personalidad del comorador que desea la visita de un tercero que no mora en él. Ello no obsta para que la composición razonable de los intereses en juego de los compradores haga que usualmente pacten explícita o implícita mente la tolerancia de las entradas ajenas consentidas por otro comorador y que los terceros que ingresen en el domicilio puedan así confiar a priori en que la autorización de uno de los titulares del domicilio comporta la de los demás. En este sentido hemos dicho que «*cada uno de los cónyuges o miembros de una pareja de hecho está legitimado para prestar el consentimiento respecto de la entrada de un tercero en el domicilio, sin que sea necesario recabar el del otro, pues la convivencia implica la aceptación de entradas consentidas por otros convivientes*» (STC 22/2003, de 10 de febrero, FJ 7). Puede suceder, naturalmente, que excepcionalmente aquel

pacto no exista como tal, o que sea evidente que no concurra respecto a determinadas entradas domiciliares por el perjuicio que puedan comportar para alguno de los moradores. Así, para el caso de una cónyuge separada que autorizó el registro de la vivienda común en unas diligencias en las que se imputaba a su marido un delito contra ella, el Tribunal Constitucional afirmó en la STC 22/2003, FJ 8, que «*el consentimiento del titular del domicilio, al que la Constitución se refiere, no puede prestarse válidamente por quien se halla, respecto al titular de la inviolabilidad domiciliaria, en determinadas situaciones de contraposición de intereses que enerven la garantía que dicha inviolabilidad representa* » (STC 209/2007, de 24 de septiembre, FJ 3).

En el supuesto que no medie consentimiento la entrada debe fundamentarse en una resolución judicial deberá ser motivada y basarse en el principio de proporcionalidad. El juez efectuará una ponderación entre el derecho constitucional a la inviolabilidad de domicilio y lo demás derechos o intereses legítimos afectados en el supuesto en concreto de que se trate.

3.2 Los límites de la actividad de investigación informática

3.2.1 Investigación y derechos constitucionales

La actividad de investigación y pericia en materia de prueba electrónica puede colisionar o afectar los derechos fundamentales de los ciudadanos. Así resulta de una simple descripción de su objeto que vendrá referido al examen de dispositivos electrónicos en los que se pueden contener datos, informes y cualquier otro hecho relativo o perteneciente a la esfera privada de los ciudadanos.

No resulta fácil determinar a priori cuales sean los dispositivos y hechos relacionados con el ámbito de derechos fundamentales protegidos. En este sentido el considerando 24 de la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas establece que: *«Los equipos terminales de los usuarios de redes de comunicaciones electrónicas, así como toda información almacenada en dichos equipos, forman parte de la esfera privada de los usuarios que debe ser protegida de conformidad con el Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales»*. Por su parte, el Tribunal Constitucional sostiene que *«…Si no hay duda de que los datos personales relativos a la persona individualmente considerados…»*, tales como datos

médicos, datos relativos a su situación económica etc.[147] «*…están dentro del ámbito de la intimidad constitucionalmente protegido, menos duda aún puede haber de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) –por lo que sus funciones podrían equipararse a los de una agenda electrónica, no sólo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad*

[147] El Tribunal Constitucional ha considerado datos protegidos por el derecho constitucional a la intimidad: la información relativa a la salud física y psíquica de las personas (SSTC 70/2009, de 23 de marzo, FJ 2 y 159/2009, de 29 de junio, FJ 3), los datos relativos a la situación económica de una persona (STC 233/1999, de 16 de diciembre, FJ 7), datos del sujeto pasivo del IRPF (STC 47/2001, de 15 de febrero, FJ 8), y la información concerniente al gasto en que incurre un obligado tributario (STC 233/2005, de 26 de septiembre, FJ 4). También ha considerado que «*…la apertura de una agenda, su examen y la lectura de los papeles que se encontraban en su interior supone una intromisión en la esfera privada de la persona a la que tales efectos pertenecen, esto es, en el ámbito protegido por el derecho a la intimidad, tal como nuestra jurisprudencia lo define*» (FJ 10). Finalmente, en la Sentencia 14/2003, de 28 de enero, FJ 6, el Tribunal Constitucional afirmó que la reseña fotográfica de un detenido, obtenida durante su permanencia en dependencias policiales, «*ha de configurarse como un dato de carácter personal*», respecto del cual los miembros de las fuerzas y cuerpos de seguridad del Estado «*están obligados en principio al deber de secreto profesional*».

personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información» STC 173/2011, de 7 de diciembre, F.Jco. 3º.

La necesaria protección de datos y hechos pertenecientes a la «esfera privada» del individuo no se concreta exclusivamente en las computadoras sino también en cualquier otro dispositivo electrónico, como, por ejemplo, en el caso de los actuales teléfonos móviles. Tal y como señala el Tribunal Constitucional «*… la versatilidad tecnológica que han alcanzado los teléfonos móviles convierte a estos terminales en herramientas indispensables en la vida cotidiana con múltiples funciones, tanto de recopilación y almacenamiento de datos como de comunicación con terceros (llamadas de voz, grabación de voz, mensajes de texto, acceso a internet y comunicación con terceros a través de internet, archivos con fotos, videos, etc.), susceptibles, según los diferentes supuestos a considerar en cada caso, de afectar no sólo al derecho al secreto de las comunicaciones (art. 18.3 CE), sino también a los derechos al honor, a la intimidad personal y a la propia imagen (art. 18.1 CE), e incluso al derecho a la protección de datos personales (art. 18.4 CE), lo que implica que el parámetro de control a proyectar sobre la conducta de acceso a dicho instrumento deba ser especialmente riguroso, tanto desde la perspectiva de la existencia de norma legal habilitante, incluyendo la necesaria calidad de la ley, como desde la perspectiva de si la concreta actuación desarrollada al amparo de la ley se ha ejecutado respetando escrupulosamente el principio de proporcionalidad*» (STC Sentencia 115/2013, de 9 de mayo de 2013., FJ.4).

La anterior doctrina jurisprudencial no hace sino constatar la necesidad de proteger toda la información o hechos que se desprendan de un dispositivo electrónico, y que forman parte de la «esfera privada» del individuo protegida por la Constitución Española. Es por ello que cualquier inmisión en la «esfera privada» a través del acceso a dichos dispositivos electrónicos debe fundamentarse en la ley –norma legal habilitante- y desarrollarse para ser lícita después de una adecuada ponderación de los derechos o intereses en juego –principio de proporcionalidad-.

La investigación o pericia en el marco del hecho electrónico implica el acceso a datos u hechos a través de dichos dispositivos electrónicos. Esos datos o hechos serán objeto de análisis en los informes periciales que, en el proceso civil, corresponde aportar a las partes. Los informes correspondientes se realizarán por expertos informático-forenses que deberán ser especialmente cautelosos en sus intervenciones en dispositivos electrónicos para no vulnerar los derechos constitucionales de los sometidos a dicha actividad de investigación y pericia y garantizar la legalidad en la obtención de la prueba electrónica y su autenticidad.

En definitiva, la cuestión del respeto de los derechos fundamentales en la obtención de las pruebas examinadas en la pericia electrónica resulta de especial importancia por afectar a la futura eficacia de tales informes que no tendrán valor probatorio cuando los hechos que contienen se hubiesen obtenido con violación de los derechos y libertades fundamentales previstos en el art. 18 CE. A ese fin se dirige el artículo 11 de la Ley Orgánica del Poder Judicial, que recoge la doctrina sentada por el Tribunal Constitucional en su Sentencia 114/1984, de 29 de noviembre y dispone la falta de eficacia de pruebas obtenidas directa o indirectamente violentando los derechos o libertades fundamentales.

El respeto del ámbito de derechos de los ciudadanos por parte de la investigación informático-forense exige un conocimiento y una previa delimitación de cuáles son los datos y las comunicaciones a los que puede acceder el experto o perito y cuales otros están sometidos a la garantía constitucional. El acceso a la información cuando se halla en poder de la parte consultante no genera ninguna dificultad. Se trataría en este caso de aquella información que quien consulta tiene en cualquiera de sus ordenadores u otros dispositivos, o también de aquella información pública obtenida a través de Web, siempre que no se requieran claves de ingreso para acceder a la misma. No obstante, en aquellos supuestos en que se trate de información que se halla en poder de tercero o que requiere para acceder a la misma claves de acceso privadas será necesaria autorización judicial.

En este sentido, piénsese que en un ordenador sito en el puesto de trabajo puede contenerse el acceso al correo privado del trabajador junto con el acceso al correo o a los foros o la intranet de la empresa. Los datos residentes o a los que se puede acceder en el primer caso estarán protegidos por el art. 18 CE por pertenecer a su intimidad. Ahora bien, los contenidos en los instrumentos de comunicación de la empresa podrán ser captados, analizados y utilizados en los informes informáticos que procedan solicitados por el empleador, por no afectar a derechos fundamentales, sin perjuicio del cumplimiento de otras normas de carácter laboral.

Una vez el experto informático-forense accede a la totalidad de la información, la búsqueda, filtrado y obtención de la misma plantea un grave problema como es el acceso de forma habitual por parte del mismo a información y/o datos que exceden de los extremos objeto de informe y que, eventualmente, pueden suponer la afectación de derechos fundamentales, como el derecho a la intimidad. Así sucede, por ejemplo, en aquellos supuestos en que los expertos acceden a una copia espejo o a un conjunto o masa de datos, para elaborar el informe respectivo. La situación expuesta de afectación de derechos puede producirse de forma meramente casual. Cuando se accede, por ejemplo, a la

cuenta de correo electrónico de una persona con el objeto de capturar algunos mensajes es inevitable ver los restantes, y de igual modo cuando se pretenden capturar todos los documentos relacionados con una transacción determinada etc. Efectivamente, a pesar de que la actividad de investigación se realice mediante métodos lícitos de búsqueda, el investigador puede obtener aún involuntariamente datos que supongan una intromisión en los derechos y libertades de los ciudadanos. No cabe ninguna duda que en ese caso el investigador debe apartarse de la fuente de datos y rechazar aquellos que hubiere obtenido y que supongan infracción de derechos y libertades. Ello plantea el problema de los límites de la investigación forense, especialmente en el ámbito civil y mercantil, y la posibilidad no recogida en la Ley de solicitar al Juez civil autorización para poder acceder a datos o informaciones que puedan afectar al derecho a la intimidad o a las comunicaciones de los ciudadanos.

Las dificultades expuestas son especialmente patentes en el proceso civil en el que el perito no suele contar con la previa legitimación del auto judicial en el que se autoriza una determinada intervención. Así sucede en el proceso penal en el que las partes podrán solicitar, en su caso, la intervención de las comunicaciones o la entrada y registro en un domicilio o empresa. En este caso el auto judicial contendrá la debida autorización con base en la valoración de las circunstancias concurrentes. Esta posibilidad no se da en un proceso civil o laboral, por cuanto un juez difícilmente accederá a la apertura de un correo electrónico cerrado en un proceso amparado en el principio de proporcionalidad o accederá a ordenar una diligencia de entrada y registro en un domicilio para averiguar unos hechos fuera de aquellos casos en que existe previamente el incumplimiento de un requerimiento judicial previo.

El derecho a la prueba cede en el proceso civil ya sea por imperativo legal ya sea con fundamento en el principio de proporcionalidad casi automáticamente frente a los derechos a la intimidad, a la protección de datos o a la protección de las comunicaciones, cuando a mi modo de ver existen en muchos supuestos pretensiones civiles de gran importancia que implican derechos o intereses que debieran prevalecer frente aquellos. En definitiva se respeta el principio de proporcionalidad cuando el objetivo perseguido sólo puede ser alcanzado por el medio utilizado –idoneidad-y no a través de otro distinto y menos gravoso –necesidad-, y que las ventajas derivadas del mismo sean razonables para la generalidad y para el sujeto afectado. Superados los juicios de idoneidad y de necesidad, debe comprobarse el equilibrio entre las ventajas y los perjuicios que se generan por la limitación de un derecho para la protección de otro bien o derecho constitucionalmente protegido, para lo que es fundamental valorar los intereses contrapuestos y las circunstancias concurrentes del caso[148].

[148] Respecto al principio de proporcionalidad véanse SSTC 66/1995, 55/1996 y 207/1996.

Las limitaciones en el acceso a la información por imperativo legal en el ámbito civil son patentes, por ejemplo, en materia de protección de «datos asociados a las comunicaciones electrónicas» donde la averiguación de datos o acceso a la información sin consentimiento del titular se ciñe en exclusiva al proceso penal, sin que las partes tengan acceso a la misma en un proceso civil y por lo tanto se conceda al juez civil la posibilidad de efectuar una ponderación de derechos e intereses en el caso concreto. La posibilidad de obtención de los «datos asociados a las comunicaciones electrónicas», como son el nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono etc., se regula en la ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (LCDCE)[149] que la limita a procesos penales, siendo imposible que dichos datos se obtengan en supuestos en que no exista delito. Por otro lado, con arreglo a dicha Ley no pueden acceder a dichos datos las personas interesadas con el fin de interponer reclamaciones en vía civil sino sólo «agentes facultados», es decir, los Cuerpos Policiales autorizados para ello en el marco de una investigación criminal por la comisión de un delito, el personal del Centro Nacional de Inteligencia para llevar a cabo una investigación de seguridad nacional, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, y los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial[150]. En definitiva, dichas limitaciones suponen que no podrá averiguarse la identidad de una persona a partir de la dirección IP en delitos con una pena inferior a cinco años o faltas, no pudiendo en dichos supuestos acceder a dicha información ni siquiera con autorización judicial, ya que de concederse podría solicitarse la nulidad. Por lo tanto la posibilidad de obtención de los datos asociados a las comunicaciones queda siempre ceñida o limitada a procesos penales, siendo imposible que se obtengan en supuestos en que no exista

[149] La ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (LCDCE) se desarrolló en aplicación de la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio.

[150] Precisamente a raíz de la imposibilidad de acceder a dichos datos en un proceso civil, se planteó en materia de los derechos de autor, por el Juzgado de lo Mercantil nº 5 de Madrid decisión prejudicial con arreglo al artículo 234 CE, en el procedimiento entre Productores de Música de España (o Promusicae) y Telefónica de España, mediante auto de 13 de junio de 2006, que terminó con la Sentencia dictada por el Tribunal de Justicia de las Comunidades Europeas, en fecha 29 de enero de 2008.Véase § 3.1.1.2.

delito. Es decir, difícilmente podrán personas interesadas acceder a dichos datos con el fin de interponer reclamaciones en vía civil.

En el ámbito del proceso civil la Ley no solo no permite que sea un juez civil quien pondere los derechos o intereses legítimos concurrentes sino que tampoco ofrece otras fórmulas de acceso a la investigación en vía civil. Es decir, si lo que quiere evitar el legislador es dejar en manos de los jueces tal posibilidad debiera cuanto menos ofrecer otras vías como podrían ser supuestos concretos permitidos de acceso a la información en vía civil, cuantías mínimas etc. Por otro lado, la supremacía del proceso penal en este sentido sobre el proceso civil parece olvidar también que existen procedimientos civiles de carácter no dispositivo como familia, capacidad etc., u otros de carácter dispositivo pero de suficiente entidad que entiendo protegen derechos e intereses que no debieran ceder ante los derechos antes citados de modo generalizado y que analizando circunstancias concretas puedan requerir preferente protección frente aquellos.

Las limitaciones expuestas también son patentes cuando concurre el «derecho a la prueba» junto al «derecho constitucional a la inviolabilidad de domicilio». Pensemos en la necesidad de acceder a un domicilio para efectuar la investigación de datos o hechos a través de dispositivos electrónicos en él ubicados. Los Juzgados del orden jurisdiccional civil pueden acordar la entrada en un domicilio en cuanto así lo permite el artículo 18.2 de la CE (STC 22/1984 y 50/85[151]), por lo tanto no existe ningún obstáculo legal para ello, sin embargo, es necesario que la LEC establezca dicha medida y los presupuestos para su adopción.

En proceso civil pocos son los casos en que se regula expresamente la posibilidad de entrar en un domicilio. Por un lado, se regula la entrada y registro en el domicilio del deudor como efecto que produce la situación de concurso sobre el mismo, en el artículo 1.1.3ª de la Ley Orgánica 8/2003, de 9 de julio, para la reforma concursal. Por otro lado, la Ley de Enjuiciamiento Civil, dejando al margen la posibilidad de entrar en un domicilio como medida en la fase de ejecución del juicio de desahucio regula de forma muy restrictiva la entrada en los supuestos de ejecución de títulos que condenen a la entrega de cosa mueble cierta y determinada, estableciendo que el tribunal podrá ordenar la entrada en lugares cerrados y podrá auxiliarse de la fuerza pública si el ejecutado no lleva a cabo la actividad de entrega requerida en el plazo establecido (art. 701 LEC), en materia de reconocimiento judicial (art. 354.1 LEC), y en diligencias preliminares. En este último caso prevé la entrada en los

[151] Véanse SSTC 22/1984 EDJ 1984/22, 50/85 EDJ 1995/454 y 174/93 EDJ 1993/5035 y ATC 272/85.

supuestos en que previo requerimiento judicial la persona citada no atendiese al mismo ni formulara oposición, en los casos de exhibición de títulos o documentos (art. 261.2ª LEC), exhibición de una cosa (art. 261.3ª LEC) y en procesos para la defensa para los intereses colectivos de consumidores y usuarios al objeto de concretar el grupo de afectados (art. 261.5ª LEC). Es decir, se regula la entrada en lugar cerrado como una consecuencia ante la negativa de llevar a cabo determinadas diligencias preliminares. Como podemos apreciar todos los supuestos previstos en la LEC de entradas domiciliarias son «consecuencia» directa del incumplimiento de una resolución judicial previa. No obstante, la LEC no prevé la posibilidad de solicitar una entrada domiciliaria a los efectos de averiguación de hechos que puedan constituir prueba en el proceso. Las únicas disposiciones con base a las cuales vienen habilitándose diligencias de entrada con arreglo a la LEC son la relativas las medidas de aseguramiento (art. 297 LEC) y las medidas cautelares (art. 732.2 LEC), sin perjuicio de los supuestos regulados en leyes especiales, como las «diligencias de comprobación de hechos» que contempla la Ley 11/1986, de 20 de marzo de Patentes (art. 129 a 132) y la Ley 3/1991, de 10 de enero de 1991, de Competencia Desleal (art. 24)[152]. Nótese que la finalidad de las medidas de aseguramiento es preservar las fuentes de prueba y la de las medidas cautelares es garantizar que pueda ejecutarse una sentencia[153], por lo tanto ninguna de ellas hace referencia al supuesto de «investigación» que nos ocupa, a salvo los supuestos previstos en leyes especiales a los que posteriormente haremos referencia.

En lo referente al principio de proporcionalidad y por ende la ponderación de los intereses y derechos concurrentes en un supuesto específico por parte del juez, no debemos olvidar, aun cuando nos hallemos en la jurisdicción civil, que

[152] Véase entre otras el Auto de la AP de Valencia, secc. 6ª, de fecha 29 de junio de 2002, núm. 147/2002, rec. 65/2002, que confirma el auto del Juez de Primera Instancia (Juez civil) que acordó diligencias de investigación sobre los programas de ordenador del recurrente en autos de medidas cautelares; y Sentencia del Juzgado de lo Mercantil núm. 1 de Madrid, de fecha 18 de febrero de 2010, nº autos 36/2010, Pte.: Nieto Delgado, Carlos, EDJ 2010/310973, por la que se acuerdan diligencias de investigación en un supuesto de propiedad intelectual consistentes en el examen por una comisión judicial acompañada de un técnico informático del contenido de los discos duros del servidor, los distintos ordenadores y demás soportes informáticos en posesión de la compañía requerida, vía artículo 732.2 LEC.

[153] Nótese que en el supuesto del artículo 732.2 LEc en sede de medidas cautelares se autoriza al juez a ordenar las «investigaciones» que resulten necesarias y que el solicitante de las medidas no pueda aportar o llevar a cabo por sí mismo. A tenor de dicho artículo: «…*Cuando las medidas cautelares se soliciten en relación con procesos incoados por demandas en que se pretenda la prohibición o cesación de actividades ilícitas, también podrá proponerse al tribunal que, con carácter urgente y sin dar traslado del escrito de solicitud, requiera los informes u ordene las investigaciones que el solicitante no pueda aportar o llevar a cabo y que resulten necesarias para resolver sobre la solicitud*».

el derecho a la inviolabilidad del domicilio no es un derecho constitucional absoluto, al igual que tampoco los son los demás derechos constitucionales. Ello supone que puede ceder ante otros derechos o intereses legítimos concurrentes y la LEC debería ofrecer cauces para que el juez civil pueda ponderarlos así como determinar los requisitos que deben concurrir para acordar una diligencia de entrada. Dichos requisitos tampoco han sido claramente señalados por la jurisprudencia como sí lo han sido en vía penal en que claramente además de la adecuación, la necesidad y la proporcionalidad en sentido estricto se exige para acordarla que se trate de delitos graves.

En lo referente a la investigación informático forense las diligencias de entrada y registro van dirigidas a la obtención de hechos que constituyan pruebas. Por ello frente al «derecho a la inviolabilidad de domicilio» el juez deberá ponderar principalmente el «derecho a la prueba» que se erige también en derecho constitucionalmente protegido. El TC se ha pronunciado indicando que «*la garantía del art. 24.2, del derecho a defensa, consiste en que las pruebas pertinentes propuestas sean admitidas y practicadas por el Juez o Tribunal y al haber sido constitucionalizado impone una nueva perspectiva y una sensibilidad mayor en relación con las normas procesales atinentes a ella, de suerte que deban los Tribunales de justicia proveer a la satisfacción de tal derecho, sin desconocerlo ni obstaculizarlo»* (STC 30/1986). Los tribunales deben cuidar de que los medios de prueba que sean pertinentes y útiles, puedan realizarse efectivamente, pues lo contrario supone vulneración del derecho a la tutela judicial. Esto mismo ha recogido la STS (Sala 1ª) de 18 de julio de 1991, de forma que existe un mandato constitucional dirigido a los órganos jurisdiccionales, que con los controles de legalidad pertinentes (que la prueba no sea ilícita, que sea pertinente...), debe admitir aquellos medios de prueba conducentes para una determinada finalidad procesal, como la demostración de un hecho relevante para la pretensión[154]. El Tribunal Supremo en Sentencia de fecha 30 de enero de 2008 (EDJ 2008/31022) ha admitido que no se conculca el derecho a la inviolabilidad de domicilio cuando, en el marco de unas diligencias preliminares destinadas a iniciar un pleito en materia de competencia desleal se autoriza la entrada en el domicilio por entender que dicho derecho puede y debe ceder ante los intereses de la otra parte en el procedimiento, de relevancia constitucional y amparados por una resolución judicial que ordena la misma. Sin

[154] Dicha doctrina se recoge en la Sentencia del Juzgado de lo Mercantil, número 1, de Bilbao, de fecha 30 de mayo de 2005, en la que el juez autoriza la entrada en una empresa a los efectos de obtener un informe pericial previo al juicio, mediante la observación en los ordenadores de la entidad que en el futuro será demandada, al objeto de comprobar si los programas que ejecuta que sean propiedad de los demandantes, cuentan o no con licencia y por lo tanto si su utilización es o no ilícita, además de constatar el número de copias no autorizadas que puedan estarse empleando. Sentencia del Juzgado de lo Mercantil, número 1, de Bilbao, de fecha 30 de mayo de 2005, nº autos 277/2005. Pte. Rodríguez Achutegui, Edmundo.

embargo, difícilmente hallamos muestras de la aplicación de tal doctrina jurisprudencial fuera del ámbito mercantil, ciñéndose la aplicación de la misma a supuestos de propiedad intelectual o competencia desleal.

Por otro lado, es fundamental tener en cuenta que la prueba solo tendrá eficacia en el proceso si es lícita, es decir, se obtiene sin vulneración de los derechos fundamentales previstos en la Constitución española. A tal efecto los expertos informático-forenses que lleven a cabo la investigación informático-forense y las fuerzas y cuerpos de seguridad que les asistan deben ser especialmente cautelosos al llevar a cabo la práctica de la diligencia de entrada y registro acordada judicialmente, en cuanto cualquier actuación de los mismos que se extralimite de la estricta resolución judicial podrá suponer violación de otros derechos constitucionales (intimidad, comunicaciones etc.) que no fueron en el momento de acordarse la misma objeto de ponderación por el órgano judicial. La autorización de entrada y registro se acuerda previa ponderación por parte del juez entre los derechos fundamentales o intereses legítimos concurrentes. Es por ello que la diligencia de entrada y registro debe ceñirse a lo autorizado judicialmente. La práctica de diligencias de investigación sobre dispositivos electrónicos incautados en una diligencia de entrada y registro es posible en tanto no afecten a otros derechos fundamentales distintos de aquellos que fundamentaron la resolución judicial autorizando dicha diligencia. Tratándose de dispositivos electrónicos, la autorización de entrada y registro con constancia de autorización expresa para proceder a la incautación del material y sistemas informáticos que pudieran encontrarse, implica autorización para el volcado de datos informáticos. Sin embargo, la resolución por la que se autoriza la entrada y registro y se decreta el volcado de datos informáticos contenidos en los ordenadores incautados en el registro judicial y la consiguiente copia de los discos duros, no implica la posibilidad de acceder al contenido de los mensajes de correo electrónico. Ello por cuanto éstos se hallan protegidos por el derecho fundamental al secreto de comunicaciones, siendo en este caso precisa nueva resolución judicial que autorice la diligencia y nuevo mandamiento judicial.

En definitiva, la afectación de los derechos constitucionales como consecuencia de la investigación informático-forense y la posibilidad no recogida en la Ley de solicitar al Juez civil autorización para poder acceder a datos o informaciones que puedan afectar al derecho a la intimidad o a las comunicaciones de los ciudadanos determina un ámbito de actuación más difuso por parte del experto que, en todo momento, deberá ser consciente de los límites existentes en orden a la obtención y análisis de datos para la elaboración de su dictamen pericial. A tal efecto será fundamental que los expertos en informática forense que intervengan en las investigaciones tengan conocimientos legales. El proceso civil requiere, además, frente al proceso penal un mayor esfuerzo de las partes para

garantizar la veracidad e inalterabilidad de la prueba de los hechos obtenida. Ello por cuanto la prueba obtenida mediante diligencias judiciales en el orden penal, informado por el principio de oficialidad, supondrá de por sí mayores garantías que la obtenida en el proceso civil. Es por ello recomendable en el ámbito civil, por ejemplo, se adopten determinadas precauciones en el momento de obtención de las pruebas de los hechos o su depósito como, por ejemplo, que se requiera la intervención del fedatario público y algunas actuaciones se practiquen, además, en presencia de testigos.

3.2.2 Medios procesales de investigación y de acceso a las fuentes de prueba en poder de terceros

El concepto de «investigación» o «acceso a las fuentes de prueba en poder de terceros» casa mal, a primera vista, con nuestro ordenamiento jurídico, en cuanto el proceso civil viene informado por principios como el de rogación y el principio dispositivo y se trata de un proceso que busca la verdad «formal» basada en las alegaciones que efectúan las partes. Esa búsqueda de la verdad formal y la regla general de que es la parte quien debe fundamentar su posición sin pedir nada al juez hacen difícil que se permita una injerencia lícita en los derechos fundamentales reconocidos constitucionalmente (derecho a la intimidad, derecho al secreto de comunicaciones etc.). El único modo en que tales injerencias puedan considerarse lícitas es que estén reguladas por la ley y sean autorizadas por el Juez, en cuyo caso no existiría afectación de derechos fundamentales protegidos por la Constitución Española.

En el vigente ordenamiento jurídico la investigación se ubica de forma natural en la fase de instrucción en el proceso penal que, precisamente, tiene por finalidad esclarecer los hechos que posteriormente serán objeto de prueba. En el proceso civil la investigación de los hechos suele ser, por lo general, una actividad de parte ajena, en gran medida, a la actividad procesal. Efectivamente, en el ámbito civil lo usual será que las partes investiguen los hechos que puedan fundamentar pretensiones procesales por su propia cuenta y, sin colaboración alguna de la parte que en su día pueda ser demandada o del Tribunal. Esto plantea el problema de los límites de la investigación que queda limitada únicamente a aquellos hechos a los que tiene acceso el interesado. De ahí que el Tribunal Supremo haya sido flexible en la concreción de los hechos en la demanda en algunos supuestos como requisito para su posterior prueba procesal[155]. Sin embargo, resulta claro que, en muchas ocasiones, sería de gran

[155] Dicha postura flexible por parte del tribunal ante la imposibilidad de la parte de concretar determinados hechos en la demanda para ser objeto de prueba se recoge en la Sentencia del Tribunal Supremo de 8 de febrero de 1975: «*la doctrina legal viene afirmando que resulta lógica*

utilidad poder acceder a sistemas, archivos y/o edificios propiedad de terceros con la finalidad de poder determinar los hechos que pudieran fundar una demanda e incluso obtener en el mismo acto aquella información que será presentada como prueba en el proceso.

La investigación en general, y en concreto la investigación en el ámbito del hecho electrónico, queda excluida de nuestra Ley de Enjuiciamiento Civil, que no regula de forma expresa y determinada la posibilidad de solicitar al juez autorización que suponga injerencias constitucionales, ni sus requisitos, ni establece un procedimiento unitario de tutela anticipatoria al proceso que dote de legitimidad a las mismas. Ello supone una evidente limitación a la «investigación» o el acceso a hechos o datos que se hallen en poder de terceras personas y que formen parte de la «esfera privada» de las mismas protegida constitucionalmente.

No obstante, la LEC recoge algunos supuestos puntuales de tutela judicial anticipatoria al proceso. Se trata de supuestos de distinta naturaleza y finalidad, que regulan de modo confuso, disperso y asistemático. Efectivamente la ley regula la posibilidad de acceder a información o a hechos que se hallan en poder de la parte contraria o de terceros, con finalidades distintas como la asegurativa, la probatoria, o la preparatoria. Se trata de normas que regulan distintos supuestos de modo independiente sin relación alguna entre ellos. Nótese que en el artículo 250 LEC, en el ámbito del juicio verbal, el legislador mezcla supuestos incardinados dentro del proceso declarativo como, por ejemplo, una reclamación de cantidad por impago de rentas (art. 250.1) con otros supuestos que en realidad los son de tutela anticipatoria y no declarativa como, por ejemplo, los interdictos. De igual modo el legislador en el artículo 727 LEC, en sede de medidas cautelares, mezcla las medidas cautelares con supuestos de tutela anticipatoria al proceso como el caso regulado en el apartado 7º relativo al cese provisional de una actividad. En concreto, en cuanto a la investigación y el acceso a las fuentes de prueba que se hallan en poder de terceros dicha tutela anticipatoria se aprecia también en las medidas preliminares reguladas en los artículos 256 a 263 de la LEC, en la exhibición documental prevista en los artículos 328 a 334 de la LEC dentro del ámbito del proceso y en las medidas de aseguramiento reguladas en los artículos 297 y 298 LEC.

---

y frecuente que el arrendador no tenga medio normal de conocer con precisión y detalle las obras que en el interior del local arrendado se hayan verificado en la clandestinidad y no se le puede exigir que al formular la demanda las concrete». MUÑOZ SABATE, Lluís, *Fundamentos de prueba judicial civil. LEC 1/2000*. Ed. Bosch, 2001, págs. 41- 45.

Dicha regulación no reúne una fórmula capaz de comprender todos los supuestos ni establece un procedimiento común que aúne todos los mecanismos legales existentes. Piénsese, por ejemplo, en el ámbito de la investigación informático-forense, en el supuesto en que sea necesario acceder a un domicilio para acceder a dispositivos electrónicos que contengan datos o hechos relevantes para el proceso o para un futuro proceso, se aseguren las fuentes de prueba y se practique prueba pericial informática «in situ», todo ello *inaudita parte* por existir riesgo demostrable de destrucción de pruebas. Con la actual regulación, dejando fuera casos específicos contemplados en leyes especiales como la Ley de Patentes y de Competencia Desleal, ello es imposible[156]. La existencia de un procedimiento unitario y bien regulado que pudiera comprender un supuesto como el anterior y cuya resolución correspondiera al juez, tras la presentación por la parte de prueba indiciaria suficiente, lograría que el principio dispositivo y de rogación de parte, que rigen en nuestro ordenamiento civil, no fueran objeto de quiebra en cuanto la parte se hallaría plenamente legitimada para ello.

En el ámbito civil, por lo tanto, no se dispone de cauces procesales adecuados para que una parte de modo legítimo pueda obtener información que pueda fundar una demanda cuando dicha información se halla en poder de tercero o afecta a derechos fundamentales protegidos por la Constitución Española.

A ese fin sirven las diligencias de comprobación de hechos previstas en la Ley de Patentes (artículo 129 a 132), naturalmente limitadas al ámbito específico de la Ley. También, con ámbito general, las diligencias preliminares reguladas en los arts. 256 a 263 LEC. No obstante, la redacción de las diligencias preliminares adolece de un contenido adecuado que permita solicitar y obtener, por ejemplo, investigación informática o técnicas sobre hechos a los que no tiene acceso un particular. No se prevé por parte de la regulación de las diligencias preliminares la posibilidad de obtener autorización judicial para poder acceder a información que se halle en poder de terceros o para cuyo acceso se requiera una clave, es decir, no puede llevarse a cabo a través de las mismas investigación informático-forense de dispositivos electrónicos. Tampoco es finalidad de las diligencias preliminares tal y como se hallan reguladas la obtención de prueba, por lo que a la luz de su regulación no parece posible solicitar un dictamen pericial[157].

---

[156] Las «diligencias de comprobación» previstas como veremos en la Ley de Patentes y de Competencia Desleal no dejan de ser supuestos regulados en leyes especiales a las que se remite en sede de diligencias preliminares, aun cuando se trata de diligencias de distinta naturaleza y finalidad más próximas a una prueba anticipada que a una diligencia preliminar.

[157] En este sentido se pronuncia el Auto 15/2002 del Juzgado de Primera Instancia número 1 de Pamplona de 15 de enero de 2002 (JUR 2002/158775). No obstante, podemos hallar algunas resoluciones judiciales que admiten un dictamen pericial como complemento a una diligencia

Las diligencias preliminares se regulan en el Capítulo II del título I de la Ley de Enjuiciamiento Civil (artículos 256 a 263). Dichas diligencias tienen por objeto la preparación de un juicio (AAP Valencia de 30 de junio de 2008, de 26 de noviembre de 2007, de 20 de octubre de 2006). Están destinadas a servir a la preparación del proceso principal y se articulan con el claro objetivo de preparar la demanda o el futuro proceso, por medio de la obtención de informaciones relativas a la legitimación activa, al objeto del juicio o a la personalidad del demandado. En definitiva, estas diligencias tienden a favorecer el cumplimiento de los presupuestos procesales y la correcta instauración del proceso, a través de la obtención de ciertos datos necesarios que, sin el auxilio del órgano jurisdiccional, el futuro demandante no podría lograr. Por lo tanto, comportan una excepción a la regla general que dispone que en el orden jurisdiccional civil la actividad preparatoria del litigio corresponde a las partes. Adviértase que en caso contrario los ciudadanos se verían avocados, como sostiene BANALOCHE PALAO a «*renunciar a acudir a los tribunales por no acceder a los datos esenciales determinantes para conocer si se dan o no determinados presupuestos procesales o si existe o no el derecho que se pretende obtener de la jurisdicción*». Se configura, por consiguiente, un interés público que tutela a las partes en la adquisición de los elementos que consideren imprescindibles para preparar el proceso, sirviéndose a este efecto de la intervención de los tribunales[158]. Las diligencias preliminares consisten primordialmente en medidas de investigación de hechos cuyo conocimiento permite obtener datos y elementos fácticos para la preparación de un futuro juicio. La finalidad de esas diligencias estrictamente consideradas no es hoy día asegurar o anticipar una prueba, ni permitir una medida cautelar, ni cualquier otra prevención indiscriminada, sino únicamente la de buscar unos datos cuyo conocimiento permita alegar, o desistir de alegar, un hecho o unos hechos[159]. Se trata no sólo de evitar procesos inútiles sino del «*interés público en que las partes puedan preparar bien un proceso, sirviéndose de la potestad de los tribunales para obtener datos y fuentes de prueba imprescindibles para saber si pueden reclamar fundadamente ante los tribunales una determinada pretensión*»[160].

---

preliminar, en concreto respecto a la exhibición de cosa a la que se deba referir el juicio (art. 256.2 LEC), en este sentido se pronuncia el auto del Juzgado de Primera Instancia número 2 de Cerdanyola, de 28 de enero de 2006.

[158] Véase RIZO GÓMEZ, Belén. *La anticipación de la prueba en el proceso civil*. Ed. Tirant Lo Blanc, 2010. págs. 45-46.

[159] Véase MUÑOZ SABATE, Lluís., *Fundamentos de la prueba judicial civil LEC 1/2000*. Ed. Bosch, págs. 46 y 48.

[160] Véase BANALOCHE PALAO, J., *Las diligencias preliminares*, Thomson-Civitas, Madrid, 2003.

La Ley de Enjuiciamiento civil vigente no permite ningún otro cauce para la investigación previa a demanda en disposiciones comunes a los procesos declarativos. Solo en sede de medidas cautelares solicitadas en relación a procesos incoados por demandas en que se pretenda la prohibición o cesación de actividades ilícitas se admite la propuesta al tribunal que, con carácter urgente y sin dar traslado del escrito de solicitud, requiera los informes u ordene las investigaciones que el solicitante no pueda aportar o llevar a cabo y que resulten necesarias para resolver la solicitud (art. 732 LEC)[161]. Sin embargo, en este último caso, el de las medidas cautelares, nos hallamos en medidas de naturaleza diferente cuyo objeto es asegurar la ejecución de una futura y eventual sentencia de condena.

El acceso a las diligencias preliminares queda, además, sujeto a la interpretación sostenida por el juez competente respecto a su carácter de «*numerus clausus*» o

[161] Véase, por ejemplo, el Auto del Juzgado de lo Mercantil núm. 1 de Bilbao, núm. autos 277/2005, EDJ 2005/76470, que autoriza la entrada en una empresa –demandada- por parte de la comisión judicial y un perito para la comprobación de los programas de ordenador que se utilizan y si se tratan de reproducciones no autorizadas por los titulares demandantes. A tenor de dicha resolución «*…Al amparo del artículo 95 del TR de la Ley de Propiedad Intelectual (LPI) aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, tras renumeración dada por la Ley 5/1998, de 6 de marzo, que dispone para los programas de ordenador un régimen de protección semejante al resto de derechos regulados en la norma, se solicita no sólo la adopción de las medidas cautelares que plantean sino la realización previa de actos de investigación que permitan constatar la comisión del ilícito civil, evitando la desaparición de las copias no licenciadas que ha detectado pueden estarse utilizando por la sociedad que en el futuro pretende demandarse. A tal fin pretende aplicar el art. 732.2 LEC…*« «*…En este caso se pretende obtener un informe pericial previo al juicio, mediante la observación en los ordenadores de la entidad que en el futuro será demandada, al objeto de comprobar si los programas que ejecuta que sean propiedad de los demandantes, cuentan o no con licencia y por lo tanto si su utilización es o no lícita, además de constatar el número de copias no autorizadas que pueden estarse empleando. Nos encontramos, en consecuencia con un supuesto de anticipación de la prueba, previsto en la LEC en los arts. 293 y ss. El actor alega que las copias que emplea el demandado carecen de licencia, y que si se advierte antes de constatar su existencia, puede producirse su borrado, sin rastro alguno, evitando la eficacia de las medidas cautelares solicitadas, del informe pericial que pretende obtener de manera anticipada y del proceso mismo. Al respecto el artículo 293.1 autoriza a practicar prueba anticipada…»* (FJ 1º). El juez señala que «… la medida de aseguramiento de la prueba es razonable, pero limitándola a los programas que sean titularidad de los demandantes, el perito que se designe para tal finalidad se limitará a comprobar si se utilizan reproducciones no autorizadas de los programas de ordenador de los que son titulares los solicitantes, dejando constancia del nombre de los programas de ordenador hallados que sean titularidad de los demandantes, cantidad de reproducciones encontradas, versión, número de serie y, en su caso, entidad o persona a favor de la cual aparecen licenciados…» aprecia la causa prevista en el art. 293.1 LEC , y añade en su FJ 3º «*…La práctica de la prueba con carácter anticipado se hará, además, con la debida contradicción, como exige el art. 295 de la LEC. Pero para posibilitarla es preciso, previamente, obtener datos no manipulados, por lo que habrá que proceder de la manera que se ha expresado sin que la futura demandada conozca de la intención de la actora*».

«*numerus apertus*». Siendo el criterio jurisprudencial mayoritario favorable a una interpretación restrictiva de las mismas, lo que supone que sea en la actualidad realmente difícil acceder a la investigación en las nuevas tecnologías de la información por vía civil (ATS de fecha 11 de noviembre de 2002 y jurisprudencia menor)[162].

Las deficiencias de la propia norma han intentado solventarse por el propio legislador por vía del artículo 256.1.9 LEC, aunque de forma limitada, ya que dicho apartado solo abre el camino para la solicitud de diligencias y averiguaciones que para la protección de determinados derechos prevean las correspondientes leyes especiales. Sólo en leyes especiales como la Ley 11/1986, de 20 de marzo, de Patentes (LPa) en sus artículos 129 a 132 y en la Ley 3/1991, de 10 de enero de 1991, de Competencia Desleal, artículo 24, se regulan «diligencias de comprobación de hechos». En este segundo supuesto el artículo 24 de la LCD establece la aplicación de los artículos 129 a 132 LPa a los procesos relativos a competencia desleal. En estos casos las personas legitimadas para ejercitar los derechos derivados de la patente pueden solicitar al juez que con carácter urgente acuerde la práctica de «diligencias para la comprobación de hechos» que puedan constituir violación del derecho exclusivo otorgado por la patente (art. 129 LPa). La diligencia de inspección de las máquinas, dispositivos o instalaciones que practica el juez asistido de uno o

[162] La jurisprudencia ha seguido mayoritariamente el criterio del Tribunal Supremo en el Auto dictado en fecha 11 de noviembre de 2002 que establece el carácter de «numerus clausus» de las diligencias preliminares. Así entre muchos otros los Autos de la AP Cáceres, Sección 1ª, de fecha 16 de enero de 2007, rec. 10/2007 y Auto de 29 de junio de 2004, rec. 286/2004, AP Barcelona, Sección 13, Auto de fecha 22 de enero de 2009, rec. 741/2008 (cita el Auto del Tribunal Supremo en igual sentido), AP Madrid, Sección 10, de 28 de mayo de 2008, rec. 357/2008 y Sección 11º, de 30 de junio de 2011, rec. 112/2011, AP Tarragona, Sección 3, de fecha 1 de septiembre de 2006, rec. 381/2005, AP de Valencia, Sección. 7, de fecha 28 de diciembre de 2010, rec. 779/2010.

La propia LEc también opta por el carácter tasado de las mismas cuando en el apartado X de su Exposición de Motivos y en relación a las diligencias preliminares señala: «*…Sin embargo, la presente Ley se asienta sobre el convencimiento de que caben medidas eficaces para la preparación del proceso. Por un lado, se amplían las diligencias que caben solicitar, aunque sin llegar al extremo que sean indeterminadas (…)*».

Ello, no obstante, parte de la doctrina sostiene una interpretación amplia y flexible de cada una de las diligencias inventariadas pero sin romper el «numerus clausus», en este sentido se pronuncia MUÑOZ SABATÉ, Lluís, en *Fundamentos de prueba judicial civil. LEC 14/2000*. Ed. Bosch, 2001, pág. 53. A dicho criterio interpretativo alude también LORCA NAVARRETE, Antonio María, en "La regulación de las Diligencias preliminares en la nueva Ley de Enjuiciamiento Civil. Una regulación inconstitucional", La Ley 21122/2001, cuando indica en el punto 4 de dicho artículo doctrinal que «*solamente pueden solicitarse como diligencias preliminares las listadas en el artículo 256.1 de la LEC. Fuera de estos supuestos han de ser rechazadas «a limine» las diligencias que se postulan. El carácter listado de la diligencia preliminar no es óbice, sin embargo, a que se planteen problemas hermenéuticos relativos a la tipicidad de cada una de ellas y a cuál debe ser, por tanto, la extensión con la cual ha de interpretarse esa tipicidad*».

más peritos determinará si éstas están sirviendo para la violación de la patente. En dicha enumeración puede incardinarse cualquier dispositivo electrónico. En realidad las diligencias de comprobación de hechos lo que hacen es regular el acceso a las fuentes de prueba mediante el auxilio judicial, sin el cual ello no sería posible. Como señalan autores como DIEZ PICAZO las diligencias de comprobación de hechos «*exceden de la finalidad propia de las diligencia preliminares, consistente en la preparación del proceso mediante la obtención de ciertos datos, y se acercan más a la prueba anticipada*»[163].

La práctica de la diligencia de comprobación se efectúa por parte del Juez con la asistencia del perito o peritos por él designados y oídas las manifestaciones de la persona con quien se entienda la diligencia. El solicitante no participa de la misma, como se desprende del carácter secreto de la pieza separada que contiene las inspecciones, en el supuesto que el juez considere que no es presumible que los medios inspeccionados estén sirviendo para la violación de la patente. En cuyo caso el Secretario, por acuerdo del juez actuante, notificará al peticionario que no procede dar a conocer el resultado de las diligencias practicadas (130 LPa). En todo caso cuidará el Juez de que la diligencia de comprobación no sirva como medio para violar secretos industriales o para realizar actos que constituyan competencia desleal (130.4 LPa). De las diligencias de comprobación realizadas no podrán expedirse otras certificaciones ni copias que la destinada a la parte afectada y la precisa para que el solicitante de las mismas inicie la correspondiente acción judicial. El solicitante solo podrá utilizar esta documentación para plantear dicha acción, con prohibición de divulgarla o comunicarla a terceros (131.1 LPa). La solicitud de las diligencias de comprobación no excluye que la persona legitimada pueda solicitar otras diligencias al amparo del artículo 256.1 LEC (art. 129 LPa).

A salvo el supuesto anterior, las diligencias preliminares recogidas expresamente en la LEC engloban una serie de supuestos concretos destinados a obtener información que funde la demanda, información que será facilitada directamente por la parte requerida a través de declaración o exhibición documental (art. 256 LEC). Efectuada la correspondiente solicitud, y previa declaración de competencia (art. 257 LEC), el juez dictará un auto declarando, en su caso, que la diligencia es adecuada a la finalidad que el solicitante persigue y concurre en la solicitud justa causa e interés legítimo (art. 258.1 LEC). La práctica de dichas diligencias se realizará en sede de la Oficina Judicial o en el lugar o modo que se consideren oportunos, dentro de los diez días siguientes (art. 259.1 LEC). No obstante, la parte requerida, dentro de los cinco días siguientes a aquél en que haya recibido la citación, podrá oponerse a ella. En tal

[163] DÍEZ PICAZO GIMENEZ I., (con DE LA OLIVA SANTOS), *Derecho Procesal Civil. El proceso de declaración*. Ed. Universitaria Ramón Areces. Madrid, 2004. Pág. 260. Véase también GONZÁLEZ MONTES, Conceptos Básicos en Derecho Procesal Civil, Madrid, 2010, pág. 264.

caso se citará a las partes a una vista, que se celebrará en la forma establecida para los juicios verbales, y tras la cual el juez resolverá lo que estime mediante el correspondiente auto (art. 260 LEC). La ley regula de modo expreso en el artículo 261 LEC las consecuencias a la negativa a llevar a cabo el requerimiento por parte de las personas citadas y requeridas, en cuyos apartados 2º y 5º se realiza una especial mención a las diligencias de entrada y registro. Se trata de uno de los pocos casos en que dicha diligencia de entrada y registro se regula en la LEC y en este caso concreto nótese que es consecuencia del incumplimiento a un requerimiento previo. Es decir, la entrada y registro prevista en dichos apartados no es un medio de investigación sino una facultad jurisdiccional de hacer ejecutar lo juzgado (AAP Toledo, Sec. 1ª, de fecha 30 de marzo de 2005).

Si bien el documento objeto de exhibición previsto por las diligencias preliminares puede hallarse en formato electrónico[164] debemos tener en cuenta: en primer lugar, que la finalidad perseguida por las diligencias preliminares, como anteriormente hemos afirmado, persigue única y exclusivamente obtener información para fundamentar una demanda no obtener prueba; y en segundo lugar, aún cuando se entienda que ello no obsta para la obtención de prueba no se contempla en dicha institución el supuesto de averiguación de datos o hechos en el ámbito electrónico a través de la intervención de expertos en informática-forense, a salvo la remisión a leyes especiales. Nótese que el simple «pantallazo» o la impresión en papel no constituyen prueba del hecho electrónico en sentido estricto, se trataría simplemente de prueba documental.

La Ley de Enjuiciamiento Civil regula, también otro cauce de acceso a las fuentes de prueba que se hallan en poder de la adversa o de terceros. Lo hace en este caso en sede ya del proceso. Tal regulación se ubica en el Libro II relativo a los procesos declarativos, dentro del Capítulo VI que contempla los «medios de prueba» y en concreto en los artículos 328 a 334 bajo la rúbrica de «*Disposiciones comunes a las dos secciones anteriores*», es decir «*De los documentos públicos*» y «*De los documentos privados*». Se trata de una serie de normas que facilitan al litigante el acceso a documentos que se hallan en posesión de la parte contraria (art. 328 LEC) o de terceros, entendiendo por

[164] Nos llevan a pensar en el formato electrónico los apartados incorporados en el art. 256.1 LEC a raíz de la ley 19/2006, de 5 de junio, tales como la petición de la historia clínica de un centro sanitario o profesional que la custodie (apartado 5º bis) o de datos de los integrantes de un colectivo de consumidores y usuarios afectados con el fin de iniciar un proceso para la defensa de los intereses colectivos de los mismos (ap. 6º), o la solicitud de diligencias de obtención de datos sobre el origen y redes de distribución de las mercancías o servicios que infringen un derecho a la propiedad intelectual o industrial a través de exhibición documental (apartado 7º) o exhibición de documentos bancarios, financieros o aduaneros en supuestos de actos desarrollados a escala comercial (apartado. 8º).

«terceros» los no titulares de la relación jurídica controvertida o de las que sean causa de ella, aunque no figuren como partes en juicio (art. 330 LEC). Facilita, por lo tanto, a la parte, dentro ya del proceso, el acceso a medios de prueba que no se hallan en su poder con la finalidad de obtener la convicción del juez. Dicha regulación no hace sino aplicar la doctrina del Tribunal Constitucional con arreglo a la cual «*…cuando las fuentes de la prueba se encuentran en poder de una de las partes del litigio, la obligación constitucional de colaborar con los Tribunales en el curso del proceso (art. 118 CE) conlleva que dicha parte es quien debe aportar los datos requeridos, a fin de que el órgano judicial pueda descubrir la verdad, sin que los obstáculos y dificultades puestos por la parte que tiene en su mano acreditar los hechos determinantes del litigio, sin causa que lo justifique, pueda repercutir en perjuicio de la contraparte»* (STC 7/1994, de 17 de enero).

Constituyen el objeto de solicitud de exhibición entre las partes aquellos documentos que se refieran al objeto del proceso o a la eficacia de los medios de prueba (art. 328.1 LEC). La ley exige que junto a la solicitud se presente la copia simple del documento, aunque permite, si no existiere o no se dispusiere de la misma, la simple indicación en los términos más exactos posibles del contenido de aquél (art. 328.2 LEC). En concreto respecto a los procesos seguidos por infracción de un derecho de la propiedad industrial o de un derecho de propiedad intelectual, cometida a escala comercial la norma exige acompañar a la solicitud un «principio de prueba» como puede ser una muestra de los ejemplares, mercancías o productos en los que se hubiera materializado la infracción (art. 328.3 LEC). Se prevé también la posibilidad de que el tribunal atribuya carácter reservado a las actuaciones, para garantizar la protección de los datos e información que tuviera carácter confidencial (art. 328.3 LEC, último inciso).

La negativa injustificada a la exhibición producirá ciertos efectos, en concreto el tribunal podrá, tomando en consideración las restantes pruebas, atribuir valor probatorio a la copia simple presentada por el solicitante de la exhibición o a la versión que del contenido del documento hubiese dado (art. 329.1 LEC) o formular requerimiento, mediante providencia, para que los documentos cuya exhibición se solicitó sean aportados al proceso (art. 329.2 LEC). Nótese que existe una evidente dificultad en la calificación de la negativa como injustificada por cuanto la parte contraria siempre alegará causas o dará explicaciones para no aportar el documento, como no tener el documento en su poder.

La obligación de colaboración no se ciñe exclusivamente a las partes en el proceso sino que la ley la hace extensiva a terceras personas (art. 330 LEC) ajenas al proceso. Regula a tal efecto una comparecencia personal de los terceros, aun cuando, pese a la redacción del precepto en la práctica forense es usual proponer prueba y admitirla requiriendo directamente al tercero la

presentación del documento, y solo en el caso de incidencias en el requerimiento suele convocarse la comparecencia del tercero.

Mención especial efectúa la ley respecto a las entidades oficiales -dependencias del Estado, Comunidades Autónomas, Provincias, Entidades Locales y demás entidades de derecho público- (art. 332.1 LEC) así como de las entidades y empresas que realicen servicios públicos o estén encargadas de actividades del Estado, de las Comunidades Autónomas, de las Provincias, municipios y demás entidades locales (art. 332.2 LEC). Las anteriores personas o entidades tienen la obligación por ley de expedir certificaciones y testimonios y a exhibir los documentos que obren en sus dependencias y archivos, excepto cuando se trate de documentación legalmente declarada o clasificada como de carácter reservado o secreto, aunque es este caso deberá justificarse.

En definitiva el legislador regula a través de las «medidas preliminares» y de «los artículos 328 y ss.» la posibilidad de que en el proceso civil una persona pueda acceder a datos o hechos que se hallan en poder de la parte contraria o de terceros.

Con una finalidad distinta a las medidas anteriormente examinadas aunque con una relación implícita evidente -en cuanto aseguramos para acceder posteriormente a la información o a los hechos- la Ley de Enjuiciamiento Civil regula a través de las llamadas «medidas de aseguramiento» la posibilidad de garantizar la preservación de «objetos materiales» o «estados de cosas» que puedan con posteridad constituir prueba en el proceso (art. 297.1 LEC).

Las medidas de aseguramiento se regulan en sede de «*Disposiciones generales sobre la prueba*», Capítulo V del Libro II de la LEC, ubicándose en la Sección 4ª con la rúbrica «*De la anticipación y del aseguramiento de la prueba*». Los artículos 297 y 298 de la LEC pretenden dar cobertura legal a fin de evitar la pérdida de la prueba. Así pues, las medidas de aseguramiento de la prueba tienen por objeto evitar la pérdida o destrucción de aquello que constituirá prueba en el proceso, es decir, con dichas medidas se pretende la conservación y custodia de las pruebas. Dichas medidas permiten a cualquier persona que pretenda incoar un proceso o bien a quienes ya sean litigantes en el mismo pedir del tribunal su adopción *«para evitar que, por conductas humanas o acontecimientos naturales, que pueden destruir o alterar objetos materiales o estados de cosas, resulte imposible en su momento practicar una prueba relevante o incluso carezca de sentido proponerla*» (art. 297.1 LEC). Dichas medidas consistirán en las disposiciones, que a juicio del tribunal permitan conservar cosas o situaciones, o hacer constar fehacientemente su realidad y características, también podrán dirigirme mandatos de hacer o no hacer, bajo

apercibimiento de proceder, en el caso de infringirlos, por desobediencia a la autoridad (art. 297.2 LEC).

En cuanto al procedimiento para su solicitud, en el supuesto de medidas instadas y acordadas con carácter previo a demanda, el solicitante deberá interponer ésta en el plazo de veinte días siguientes a la fecha de la efectiva adopción de las medidas de aseguramiento acordadas. La solicitud deberá presentarse ante el juez competente, aplicándose en cuanto a jurisdicción y competencia lo dispuesto sobre prueba anticipada (art. 297.3 LEC). En el supuesto que el solicitante no presente la demanda en el plazo señalado las medidas de aseguramiento quedarán sin efecto y el tribunal, de oficio, acordará mediante auto que se alcen o revoquen los actos de cumplimiento que hubieran sido realizados, condenará al solicitante en las costas y declarará que es responsable de los daños y perjuicios que haya producido al sujeto respecto del cual se adoptaron las medidas (art. 297.4 LEC).

Deben concurrir los requisitos previstos por la LEC para que puedan acordarse por parte del juez las medidas de aseguramiento solicitadas, dichos requisitos son los siguientes: 1º) Que la prueba que se pretende asegurar sea posible, pertinente y útil al tiempo de proponer su aseguramiento; 2º) Que haya razones o motivos para temer que, de no adoptarse las medidas de aseguramiento, puede resultar imposible en el futuro la práctica de dicha prueba; 3º) y Que la medida de aseguramiento que se propone, u otra distinta que con la misma finalidad estime preferible el tribunal, pueda reputarse conducente y llevarse a cabo dentro de un tiempo breve y sin causar perjuicios graves y desproporcionados a las personas implicadas o a terceros (art. 298.1 LEC). La resolución judicial revestirá forma de providencia a tenor de lo dispuesto en el artículo 298.1 LEC. Para decidir sobre la adopción de las medidas de aseguramiento de una prueba, el tribunal deberá tomar en consideración y podrá aceptar el eventual ofrecimiento que el solicitante de la medida haga de prestar garantía de los daños y perjuicios que la medida pueda irrogar. También podrá el tribunal acordar, mediante providencia, en lugar de la medida de aseguramiento, la aceptación del ofrecimiento que haga la persona que habría de soportar la medida de prestar, en la forma prevista en el párrafo segundo del apartado 2 del artículo 64, caución bastante para responder de la práctica de la prueba cuyo aseguramiento se pretenda (art. 298.2 y 3 LEC).

La regla general es la audiencia previa de la persona que haya de soportar la medida de aseguramiento previa adopción o denegación, y de haberse iniciado el proceso del demandado (art. 298.4 LEC), no obstante, en el ámbito de prueba electrónica la mayor parte de los supuestos se incardinarán en el apartado 5 del artículo 298, es decir, la solicitud «inaudita parte» dado el riego concurrente de que se destruyan o alteren las pruebas. Tal y como señala dicho precepto «*No*

obstante lo dispuesto en el apartado anterior, cuando sea probable que el retraso derivado de la audiencia previa ocasione daños irreparables al derecho del solicitante de la medida o cuando exista un riesgo demostrable de que se destruyan pruebas o se imposibilite de otro modo su práctica si así se solicita, el tribunal podrá acordar la medida sin más trámites, mediante providencia…».

En cuanto a la forma de la resolución del juez en este caso adoptará también forma de providencia la cual «*…precisará, separadamente, los requisitos que la han exigido y las razones que han conducido a acordarla sin audiencia del demandado o de quien vaya a ser demandado».* Quizá hubiera sido más idónea la forma de un auto. «*..Esta providencia es irrecurrible y será notificada a las partes y a quien hubiera de soportarla sin dilación y, de no ser posible antes, inmediatamente después de la ejecución de las medidas.».* Si la medida de aseguramiento se hubiera adoptado sin audiencia previa, quien fuera a ser demandado o ya lo hubiera sido o quien hubiera de soportarla podrán formular oposición en el plazo de veinte días, desde la notificación de la providencia que la acordó de conformidad a lo previsto en los apartados 7 y 8 del artículo 298 LEC.

En el ámbito de la prueba sobre el hecho electrónico los riesgos existentes en cuanto a la eliminación, deterioro o manipulación de hechos electrónicos o incluso de los propios soportes o dispositivos electrónicos hace necesario en muchas ocasiones tener que acudir a las medidas de aseguramiento como vía necesaria para garantizar la prueba del hecho electrónico o las fuentes de donde deriva la misma. Pensemos por ejemplo: en un requerimiento para la conservación rápida de determinados datos digitales; un requerimiento para que se detenga o no se borre información relevante; la incautación del soporte, como el ordenador o disco duro, en que se encuentran los datos digitales; una orden de creación de copias de información (servidores dedicados, Hastings); un requerimiento al proveedor de servicios a los agentes de certificación para la conservación de los datos con la posibilidad de revelación sólo por orden del juez o la entrada en unas instalaciones para la obtención de una copia de los datos originales[165].

No obstante, si bien la regulación de las medidas de aseguramiento de modo independiente nos permiten, por ejemplo, cubrir algunos de los supuestos indicados como la incautación de un disco duro o una computadora, no existe en la regulación previsión legal alguna que permita o posibilite la «averiguación» de hechos electrónicos derivados del dispositivo electrónico

[165] Ejemplos citados por RAMOS ROMEU, F. y CAÑABATE PÉREZ, J. *Los datos digitales en el proceso civil: prevención, producción y autenticación,* Revista Jurídica de Catalunya. Núm.1-2011. Pág. 90.

asegurado, ya sea con carácter previo a la demanda o durante el proceso, ni la práctica simultánea de prueba pericial en caso de ser necesaria por motivos técnicos. Es decir, no existe normativa que nos permita obtener una autorización judicial para la práctica de diligencia de entrada, aseguramiento y/o práctica *in situ* de la prueba pericial. Se trataría en este supuesto de una actuación que engloba la ponderación judicial por afectación de derechos fundamentales, garantiza la preservación de la fuente de prueba y se practica prueba anticipada «inaudita parte»[166]. De nuevo se ponen de manifiesto las deficiencias de la actual regulación en el ámbito de la investigación y prueba del hecho electrónico.

Dicho vacío legal pudiera cubrirse a través de la reforma de la regulación vigente en la Ley de Enjuiciamiento Civil, mediante una regulación unitaria que aunara los mecanismos legales ya existentes, y fuera capaz de cubrir legalmente todos los supuestos planteables, estableciendo un procedimiento regulado y común, que permitiera incluso con anterioridad a la demanda asegurar la prueba electrónica, permitir el conocimiento de los hechos mediante una análisis informático-forense y/o practicar prueba pericial *in situ* de ser necesario. De ese modo la norma procesal proporcionaría una vía de «investigación» en el proceso civil que permitiría el acceso a hechos fundamento de posibles demandas. No circunscribiendo dicha posibilidad exclusivamente a supuestos de patentes o competencia desleal. Ello permitiría al juez ofrecer la tutela judicial efectiva de los derechos prevista en la Constitución Española. La previsión legal y la decisión judicial tras el procedimiento correspondiente garantizarían la no afectación de derechos procesales y derechos fundamentales.

Nuestra propuesta se concreta, pues, en la creación de un procedimiento que garantice los derechos procesales y los derechos constitucionales, asegurando una tutela judicial rápida y anticipada como la llamada «Justice of référes» o «procédure de référé» de Francia que legitime la investigación y permita en su

[166] En el ámbito mercantil, en supuestos de competencia desleal o vulneración del derecho de patentes y amparadas por las «diligencias de comprobación» resulta más habitual encontrar resoluciones judiciales que autorizan la entrada, registro y práctica de prueba pericial con carácter previo al juicio, así resulta de la Sentencia del Juzgado de lo Mercantil, número 1, de Bilbao, de fecha 30 de mayo de 2005, en la que el juez autoriza la entrada en una empresa a los efectos de obtener un informe pericial previo al juicio, mediante la observación en los ordenadores de la entidad que en el futuro será demandada, al objeto de comprobar si los programas que ejecuta que sean propiedad de los demandantes, cuentan o no con licencia y por lo tanto si su utilización es o no ilícita, además de constatar el número de copias no autorizadas que puedan estarse empleando. Sentencia del Juzgado de lo Mercantil, número 1, de Bilbao, de fecha 30 de mayo de 2005, nº autos 277/2005. Pte. Rodríguez Achutegui, Edmundo.

caso practicar prueba pericial simultánea. La regulación de un procedimiento de tales características permitiría, además, incluir todos aquellos supuestos que de forma desordenada se recogen en la Ley de Enjuiciamiento Civil y que en realidad están procurando al ciudadano una tutela anticipatoria, como algunos de los que se encuentran regulados en los artículos 250 y 727 de la LEC mezclándose con el proceso declarativo o las medidas cautelares.

La llamada «Justice of référes» o «procédure de référé» de Francia es un procedimiento sumario que permite obtener una solución, al menos temporalmente, y de forma más rápida sin valor de cosa juzgada. Se trata de la solicitud de medidas de carácter provisional a la autoridad judicial en supuestos determinados. Un procedimiento similar permitiría obtener una autorización sumaria en varios supuestos entre los que se hallaría la investigación. De ese modo se aseguraría la efectividad de la tutela judicial efectiva. Y por otro lado, se garantizaría la legitimidad de las injerencias en los derechos fundamentales protegidos constitucionalmente y los derechos procesales de las partes litigantes, que la investigación comporte. Este procedimiento facilitaría la posibilidad no recogida en la Ley de solicitar al Juez civil autorización para poder acceder a datos o informaciones que puedan afectar al derecho a la intimidad o a las comunicaciones de los ciudadanos. Dentro de la regulación de ese mismo procedimiento sumario de tutela anticipatoria podrían diferenciarse: por un lado, las «diligencias preliminares» como podría tratarse de la entrega o exhibición de un documento; y por otro lado, podrían regularse las «diligencias interdictales» entre las que se hallaría la averiguación. El juez en estos últimos supuestos entraría a valorar consecuencias, derechos fundamentales, valor etc. En las medidas interdictales la solicitud y resolución sería competencia de un juez especial.

3.3 Incidente por ilicitud

El problema en la investigación informático-forense surge en tanto que resulte necesario delimitar cuales son los datos y comunicaciones a los que puede acceder el experto o perito y cuales otros están sometidos a la garantía constitucional. En cualquier caso el experto informático-forense o perito nunca debe acceder a datos o hechos que forman parte de la «esfera privada» del individuo sin una autorización judicial y de hacerlo no intencionadamente debe apartarse inmediatamente de dichos contenidos que evidentemente no pueden entrar a formar parte de su informe o dictamen pericial.

Es de especial importancia que la obtención de las pruebas examinadas en la pericia electrónica se lleve a cabo respetando los derechos fundamentales, ya

que ello afectará a la futura eficacia de tales informes que no tendrán valor probatorio cuando los hechos que contienen se hubiesen obtenido con violación de los derechos y libertades fundamentales previstos en el art. 18 CE. A ese fin se dirige el artículo 11 de la Ley Orgánica del Poder Judicial, que recoge la doctrina sentada por el Tribunal Constitucional en su Sentencia 114/1984, de 29 de noviembre y dispone la falta de eficacia de pruebas obtenidas directa o indirectamente violentando los derechos o libertades fundamentales.

Veamos un ejemplo de ilicitud declarado judicialmente: «*no es reprochable que una empresa decida recuperar la información que contiene un ordenador de su propiedad, instalado en un centro productivo y destinado, precisamente, a facilitar la prestación laboral de sus empleados…» «…los correos electrónicos privados a los que se tenga acceso en la obtención de la prueba deben quedar fuera del dictamen pericial por estar protegidos por el derecho al secreto de las comunicaciones…*». Es decir, «*…desde el momento que ese ordenador está conectado a la red, es posible que un trabajador tenga acceso, desde el mismo, a su propio servidor, y que utilice su correo electrónico particular. Esa circunstancia impide entonces la obtención del contenido del rastro de información que pueda haber dejado en el ordenador de la demandante, puesto que aunque el terminal desde el que se accede sea de su titularidad, el lugar al que entra es particular, y en consecuencia, puesto que ofrece un sistema de comunicación universal, queda amparado por el art. 18.3 de la Constitución -EDL 1978/3879- y el art. 8 del CEDH -EDL 1979/3822-*» (Sentencia núm. 517/2005 de 30 diciembre, del Juzgado de lo Mercantil núm. 1 de Bilbao (Provincia de Vizcaya) -EDJ 2005/284080-). En este caso el acceso por parte del perito a los correos electrónicos privados y la constancia de los mismos en su dictamen pericial supondría la falta de eficacia de dicha prueba en juicio por vulnerar el derecho al secreto de comunicaciones.

De modo que es de especial importancia que la obtención de las pruebas examinadas en la pericia electrónica se lleve a cabo respetando los derechos fundamentales, ya que ello afectará a la futura eficacia de tales informes que no tendrán valor probatorio cuando los hechos que contienen se hubiesen obtenido con violación de los derechos y libertades fundamentales previstos en el art. 18 CE. A ese fin se dirige el artículo 11 de la Ley Orgánica del Poder Judicial, que recoge la doctrina sentada por el Tribunal Constitucional en su Sentencia 114/1984, de 29 de noviembre y dispone la falta de eficacia de pruebas obtenidas directa o indirectamente violentando los derechos o libertades fundamentales.

La ilicitud de la prueba se regula en la Ley de Enjuiciamiento Civil en los artículos 283 y 287 en los que se dispone, de conformidad con lo previsto en el

art. 11.1 LOPJ, la falta de validez y eficacia de la prueba obtenida violando derechos fundamentales. El precepto básico es el art. 283 LEC que dispone la ilicitud de cualquier prueba obtenida mediante la violación de la ley. La LEC literalmente establece que: «*.3. Nunca se admitirá como prueba cualquier actividad prohibida por la ley*». Este precepto se contiene en sede de disposiciones generales de prueba y se refiere a la inadmisibilidad de la prueba ilícita. Mediante la expresión «directa o indirectamente», recogida en el artículo 11.1 LOPJ al señalar que «*... no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales*», el legislador ha pretendido recoger la doctrina constitucional destacando la ineficacia procesal de todo elemento probatorio para cuya obtención se haya infringido directamente un derecho fundamental (por ejemplo, la inviolabilidad del domicilio, el derecho a la intimidad o el secreto a las comunicaciones), así como también la ineficacia del medio de prueba a través del cual se intenta dar entrada en el proceso a dicho elemento probatorio, ya que ello supone indirectamente conculcar otros derechos fundamentales (así, los referentes al proceso con todas las garantías y a la igualdad de las partes)[167].

[167] La redacción del artículo 283.3 de la LEC ha generado cierta confusión dada su redacción. No obstante, dicho artículo no supone la ampliación del concepto de prueba ilícita equiparándolo a la violación de cualquier ley, debiendo ceñirse la ilicitud de la prueba solo a aquella que ha sido obtenida violando los derechos y libertades constitucionales. En este sentido se pronuncia la citada STC 114/ 1989, de 24 de noviembre, (f.j. 4º), cuando afirma: "[...] *Estas últimas (las garantías -por el ordenamiento en su conjunto- de las situaciones jurídicas subjetivas de los ciudadanos) acaso puedan ceder ante la primera (la necesaria procuración de la verdad en el proceso) cuando su base sea estrictamente infraconstitucional, pero no cuando se trate de derechos fundamentales que traen su causa, directa e inmediata, de la norma primera del ordenamiento*". Es decir, a diferencia de la prueba obtenida con vulneración de los derechos constitucionales la prueba obtenida sin vulneración de los mismos podrá ser valorada por el juez en sentencia sin perjuicio de exigir la correspondiente responsabilidad civil, penal o disciplinaria en quien haya podido incurrir la persona que ha realizado tal irregularidad. El artículo 283.3 LEC solo recoge un criterio de admisión de pruebas. El juez sólo pueda admitir la prueba que sea pertinente y útil (art. 283.1. y 2 LEC) y además que no esté prohibida por la ley (art. 283.3 LEC), y la única prueba prohibida por la ley es la obtenida con vulneración de los derechos constitucionales. Autores como PICO i JUNOY, MARTIN OSTOS, ASENCIO MELLADO o FERNÁNDEZ URZINQUI sostienen que el artículo 283 LEC sólo recoge el principio de legalidad procesal en materia probatoria, esto es, la sumisión del juez al procedimiento probatorio legalmente previsto. En este sentido se pronuncian PICO i JUNOY, J., en *La prueba ilícita en el Proceso Civi Español*, artículo publicado en la revista electrónica "Temas Actuais de Processo Civil", V.I, N. 5, Noviembre de 2011; también MARTÍN OSTOS, J., *Comentario al art. 283*, en "Comentarios a la nueva Ley de Enjuiciamiento Civil", coord. A. Mª. Lorca Navarrete, vol. II, edit. Lex Nova, Valladolid, 2000, pág. 1764; ASENCIO MELLADO, J.M., *Comentario al art. 283,* en "Proceso Civil Práctico", T. IV, coord. V. Gimeno Sendra, edit. La Ley, Madrid, 2001, pág. 1-48; y FERNÁNDEZ URZAINQUI, F.J.: *Comentario al art. 283*, en "Comentarios a la nueva Ley de Enjuiciamiento Civil", vol. II, coord. M. A. Fernández-Ballesteros, J. Mª. Rifá Soler, y J. F. Valls Gombau, edit. Iurgium-Atelier, Barcelona, 2001, pág. 1312.

Por su parte, el art. 287 LEC dispone que: « *1. Cuando alguna de las partes entendiera que en la obtención u origen de alguna prueba admitida se han vulnerado derechos fundamentales habrá de alegarlo de inmediato, con traslado, en su caso, a las demás partes.*». Este precepto, muchas veces mal entendido, se ubica en sede de proposición y admisión de la prueba y está referido al supuesto en el que la prueba haya sido ya admitida. En ese caso, sin perjuicio de la primera decisión del Juez admitiendo la prueba, las partes o el Juez de oficio podrán impugnarla por su ilicitud. En cuanto a la resolución del incidente se producirá, conforme está previsto en el párrafo 2º del citado ar. 287 LEC al inicio del juicio o la vista. Ahora bien, esta norma no impide que las partes o el tribunal de oficio puedan, y todavía más, deban poner de manifiesto inmediatamente la ilicitud de cualquiera de las pruebas que se aportaran a un proceso, sin esperar, naturalmente, al momento de su admisión. De este modo corresponde a la parte, y al Juez de oficio, denunciar la ilicitud de la prueba obtenida violando derechos fundamentales tan pronto tuviera conocimiento de ello[168]. Ahora bien, si la impugnación no se hubiere producido e incluso se hubiere admitido la prueba aún podrá la parte, o el juez de oficio, solicitar la declaración de su ilicitud conforme está previsto en el artículo. 287 LEC.

[168] En cuanto a la necesidad de poner inmediatamente en conocimiento del juez la eventual ilicitud de una prueba y la inadmisión por extemporánea se pronuncia la sentencia núm. 143/2007, de 20 marzo, del Juzgado de lo Mercantil de Bilbao núm. 1 (Vizcaya) -EDJ 2007/151596-, con arreglo a la cual «*el art. 287.1 LEC -EDL 2000/77463- y el art. 11 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (LOPJ)- destierran que pueda tener eficacia probatoria la prueba obtenida ilícitamente. Pues bien, la parte demandada conoce desde el día seis de septiembre de dos mil seis esa grabación y no ha denunciado su ilicitud de manera expresa. No lo hizo al contestar la demanda, que sería la forma de cumplir el mandato de alegación inmediata que dispone el art. 287.1 LEC. Tampoco lo hizo en la audiencia previa, momento en que se procede a admitir las pruebas. Si la prueba era ilícita, debió recurrir su admisión, como autoriza el art. 285.2 LEC, para impedir que surtiera efecto procesal. Guardó silencio entonces, pues la queja sobre su contenido no se tradujo en una expresa reclamación de que se declarara ilícita, nada opuso al contestar la demanda y en el juicio es cuando afirma la ilicitud. No es posible que la prueba haya sido lícita durante todo el proceso y justo en el juicio, cuando la otra parte no puede realizar alegaciones ni proponer prueba para corroborarlas, transmute en ilícita»*. Por otro lado, la sentencia núm. 102/2010, de 26 febrero, de la AP de Alicante (Sección 9ª) -EDJ 2010/92546-, afirma que resulta extemporáneo alegar la ilicitud de una prueba documental cuando fue aportado por la parte demandada con su escrito de contestación, y que se tuvo por presentado dentro de plazo, dándose traslado a la parte actora, «*sin objeción alguna, y convocadas las partes a la celebración de la audiencia previa, y propuestas las pruebas, no se formuló alegación alguna de ilicitud de la prueba*" añadiendo que no es "*sólo en tramite de conclusiones, y practicadas que fueron las pruebas, cuando se denuncia la ilicitud de la prueba pericial de la parte demandada, con lo que resulta no sólo ser extemporánea esta impugnación, sino que aparece como un último recurso práctico al resultado probatorio, no pronunciándose lógicamente la Magistrada sobre tal extremo hasta la sentencia*». Véanse también sobre inadmisión por extemporánea la Sentencia núm. 260/2003, de 4 noviembre, de la AP Jaén (Sección 1) y la Sentencia núm. 102/2010, de 26 febrero, de la AP de Alicante (Sección 9ª).

La intervención en el incidente contradictorio por ilicitud de la prueba se ciñe a las partes litigantes en el proceso, habiendo declarado la jurisprudencia que no podrán intervenir en el incidente de ilicitud terceros ajenos al proceso que pudieran haber visto vulnerados sus derechos fundamentales (Sentencia núm. 229/2008, de 11 de marzo, de la Audiencia Provincial de Madrid (Sección 10ª)).

Conforme con lo expuesto, las partes pondrán en conocimiento del juez la ilicitud de la prueba obtenida violando los derechos constitucionales y efectuadas dichas alegaciones se dará traslado a las demás partes para ser oídas. Una vez ilustradas las demás partes, todas podrán proponer prueba sobre el concreto extremo de la referida licitud. El juez admitirá la prueba que considere pertinente y útil y una vez admitida se procederá a su práctica en el mismo acto. Praticada toda la prueba sobre la eventual ilicitud, el tribunal resuelve lo que estime adecuado, admitiendo o rechazando la eficacia de la prueba, siendo en ambos casos su decisión recurrible en reposición, que se interpondrá, sustanciará y resolverá oralmente en el mismo acto del juicio o vista, sin posibilidad de ulterior recurso, ya que el derecho de las partes a reproducir la impugnación de la prueba ilícita deberá formularse en la apelación contra la sentencia definitiva (art. 287.2 LEC). No obstante, también es posible la declaración de ilicitud en sentencia. Esta es una posibilidad que no debiera darse, ya que el Juez sea de oficio o bien a instancia de parte debe haber examinado la licitud de la prueba durante el transcurso del proceso. Ahora bien, si llegado al fin del proceso y debiendo valorar una prueba, el Juez entendiera que ésta es ilícita debería declararlo así y apartarla del proceso. La LEC no regula tal supuesto por lo que el Juez podría dictar sentencia sin tomar en consideración la prueba que considera ilícita, quedando a la parte que propuso la misma el derecho a recurrir la sentencia en apelación alegando tal extremo; o bien convocar a las partes litigantes a una audiencia contradictoria para que la parte que propuso la prueba pueda defender su eficacia[169].

A través del recurso ordinario de apelación se abre una segunda instancia procesal en la que el Tribunal *ad quem* puede revisar las decisiones del órgano *ad quo* sin más limites que la prohibición de la *reformatio in peius*. Será indispensable para interponer el recurso de apelación que la parte hubiere denunciado la ilicitud de la prueba en la instancia[170].

---

[169] A favor de convocar una audiencia contradictoria vía 227.2 LEC se pronuncia PICO i JUNOY, J. en *La prueba ilícita en el Proceso Civil Español*, artículo publicado en la revista electrónica "Temas Actuais de Processo Civil", V.I, N. 5, Noviembre de 2011.

[170] Véanse al respecto la Sentencia núm. 27/2009, de 29 enero, de AP Málaga (Sección 5ª) -EDL 2000/77463-. y la Sentencia núm. 744/2004, de 28 octubre, Audiencia Provincial de Barcelona (Sección 18ª) EDJ 2004/176548-. Según se manifiesta en la sentencia núm. 27/2009, de 29 enero, de AP Málaga «*…para que se pueda alegar en el recurso de apelación que la prueba es ilícita se exige que se haya hecho la denuncia en la instancia, requisito procesal que la parte apelante no*

* * *

cumple, desde el momento que en la Audiencia Previa se limitó a impugnar el informe, así como el emitido por la empresa de detectives privados, siendo finamente admitida la prueba por el Juzgador de Instancia, sin que conste denuncia ni resolución - ni siquiera oral- conforme establece el artículo 287 LEC»..

CAPÍTULO IV.- CONSIDERACIONES GENERALES SOBRE LA PRUEBA

4.1 Hechos y medios de prueba.

El ser humano vive una «realidad» constituida por un sinfín de hechos, como son las acciones, comportamientos, sensaciones, acontecimientos, fenómenos, sentimientos etc. No obstante, dicha «realidad» no debe confundirse con el «derecho» que no es más que un artificio creado por el propio ser humano para satisfacer sus intereses sociales. Es por ello, que no podemos confundir los «hechos» con los «medios de prueba», por cuanto los primeros pertenecen al mundo de lo real mientras que los segundos forman parte del mundo del derecho. Es decir, cuando hablamos de medios probatorios estamos incluyendo hechos que categorizamos porque nos interesa socialmente. Con arreglo a ello en primer lugar debemos, pues, distinguir entre hecho y medio de prueba[171].

Los hechos son anteriores, materiales e independientes del proceso (preexisten al mismo). Los hechos se introducen en el proceso a través del medio de prueba que será el que produzca un resultado probatorio. Así, son hechos, susceptibles en su caso de ser objeto de prueba, las palabras, los gritos, las heridas, en definitiva todas aquellas manifestaciones y acciones materiales que acaecen en nuestro universo sensible. Mientras que son medios de prueba la declaración de la parte o los testigos, los documentos o el examen técnico pericial de objetos, cosas o acciones. Los hechos son ilimitados en tanto que no puede existir un catálogo predefinido de acciones materiales. Sin embargo, los medios de prueba son limitados y tasados.

En el ámbito procesal la «prueba electrónica» es un concepto que utilizamos por un lado para reflejar una realidad plural (hechos de naturaleza electrónica) y por otro lado para referirnos a los medios de prueba previstos en la ley. Es decir, el conocimiento de los hechos de naturaleza electrónica en el proceso tendrá lugar a través de los medios de prueba. Y en un sentido estricto, como veremos más adelante, básicamente a través de un único medio de prueba: el dictamen pericial. Y ello por cuanto si bien el ser humano atiende a sus fines sociales con sus límites físicos, es decir, vemos, oímos etc., no dispone de un lenguaje que le

[171] El origen de la definición entre fuente y medio de prueba fue expuesta originariamente por CARNELUTTI, quien denomina fuente de prueba a «*los hechos que sirven para la deducción del hecho a probar y que están constituidos por la representación de éste*». CARNELUTTI, F., *La Prueba Civil*. Traducción por Niceto Alcalá Zamora y Castillo de la edición original italiana, "La prova civile", ed. Dell`Ateneo, 2º ed. De Palma, Buenos Aires, 1982, pág. 90; CARNELUTTI, F., *La Prueba Civil*, Buenos Aires, ed. Arayu, 1955, págs. 67 y ss.

permita leer hechos electrónicos, es por ello que para que en el mundo del derecho pueda alcanzar tal fin requerirá de la prueba pericial electrónica.

4.2 Derecho a la prueba y medios de prueba

El derecho a la prueba en el ámbito normativo europeo viene regulado en los artículos 6.3 b) y d) del Convenio Europeo de Derechos Humanos (CEDH) y en el artículo 14.3 b) y e) del Pacto Internacional de Derechos Civiles y Políticos (PIDCP). El artículo 6.3 CEDH reconoce los derechos de todo acusado a *«… b) a disponer del tiempo y de las facilidades necesarias para la preparación de su defensa; (y)…d) a interrogar o hacer interrogar a los testigos que declaren contra él y a obtener la citación y el interrogatorio de los testigos que declaren en su favor en las mismas condiciones que los testigos que lo hagan en su contra…»*. De igual modo reconoce el artículo 14.3 aparatados b) y e) del PIDCP que «*…3. Durante el proceso, toda persona acusada de un delito tendrá derecho, en plena igualdad, a las siguientes garantías mínimas: ….b) A disponer del tiempo y de los medios adecuados para la preparación de su defensa y a comunicarse con un defensor de su elección; ….e) A interrogar o hacer interrogar a los testigos de cargo y a obtener la comparecencia de los testigos de descargo y que éstos sean interrogados en las mismas condiciones que los testigos de cargo*».

En nuestro ordenamiento jurídico la Constitución Española reconoce las garantías procesales de rango constitucional, entre las que se incluye el «derecho a la prueba», en el art. 24 CE que establece que: «*1. Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión. 2. Asimismo, todos tienen derecho al Juez ordinario predeterminado por la Ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia…»*. Se trata de un precepto de importancia esencial en el ámbito de las garantías procesales, que probablemente debería haber sido regulado en distintos preceptos para dar debida y cumplida cuenta de las importantes garantías procesales que se contienen en el citado art. 24 CE.

Por otro lado, con fundamento en el propio artículo 24 CE el Tribunal Constitucional ha establecido en relación al derecho de prueba mandatos dirigidos al legislador, al juez y a las partes. Mandatos que pueden resumirse del siguiente modo: a) Como mandato dirigido al legislador, el derecho a la prueba reclama que se arbitren mecanismos y técnicas para asegurar su efectividad; b)

Como mandatos dirigidos al juez, el Tribunal Constitucional considera que el derecho a la prueba comporta, conforme a la Constitución, el pleno cumplimiento del art. 24.2 CE, con la finalidad de garantizar el contenido del derecho a la prueba y, en su virtud, la admisión de la prueba en tanto no resulte injustificada su práctica, garantizar la contradicción en las pruebas acordadas «ex officio iudicis» y evitar los formalismos enervantes; c) Y como mandatos y facultades otorgadas a las partes, el derecho a la prueba, comporta no solo la facultad de solicitar la admisión y la práctica de las pruebas pertinentes, sino también la de reclamar su efectividad, así como el deber de solicitar las pruebas en la forma y momento legalmente previsto y el deber de mantener una actitud de colaboración en la práctica de las pruebas[172].

El derecho a la prueba, desde una vertiente objetiva, se presenta como garantía esencial, como valor asumido en el sistema de una comunidad con fuerza vinculante en el ordenamiento jurídico, vinculando a todos los poderes públicos y a las partes (arts. 91.1 y 53.1 CE). Ello supone la necesidad de efectuar por parte del juez una lectura amplia y flexible de las normas probatorias, permitiendo la máxima actividad probatoria de las partes sin subordinar ese derecho fundamental a otro tipo de intereses como la economía procesal o la rapidez de los juicios (SSTC 10/2000, de 17 de enero, f.j.4º, 1/1992, de 13 de enero, f.j. 5º y 140/2000, de 29 de mayo, f.j 4º). Requiere, asimismo, la necesidad de realizar una interpretación restrictiva de los preceptos que limiten la eficacia del derecho a la prueba (STC 140/2000, de 29 de mayo, f.j. 4º), y en el supuesto que se limite deberá efectuarse mediante resolución judicial debidamente motivada en la que de forma expresa se admita o deniegue la prueba solicitada (STC 88/2004, de 10 de mayo, f.j. 4º). Asimismo, debe favorecerse la subsanación de los defectos susceptibles de reparación si ello no supone una ruptura de la regularidad del proceso y siempre que no suponga vulneración de los derechos de la contraparte (art. 11.3, 240,2, 242 y 243 LOPJ y 231 LEC), y finalmente debe reputarse nulo todo pacto que suponga una limitación al derecho de prueba (STS 19/1985, de 13 de febrero, f.j. 3º y STS de 5 de noviembre de 1982, f.j. 1º).

Por otro lado, el derecho a la prueba en su aspecto subjetivo, atribuye a una persona el poder ejercitar ese derecho en el proceso y, en su caso, solicitar su plena eficacia mediante los recursos previstos en la Ley, en el trámite de la admisión, práctica y valoración de la prueba. La Constitución Española garantiza el derecho a la prueba (art. 24.2 CE), por lo que cualquier parte en el proceso tiene derecho a la admisión y práctica de los medios de prueba previstos en la Ley. No obstante, como veremos, el derecho a la prueba queda modulado por

[172] Véase ABEL LLUCH, X., *Sobre la prueba y el derecho a la prueba en el proceso civil*, en "Objeto y carga de la prueba civil", Picó i Junoy, J. –Abel Lluch, X, J.M. Bosch Editor, 2007, págs. 35-40.

la pertinencia, la necesidad y los requisitos de admisión previstos por la ley (STC 30 de enero de 2003, entre otras).

En el mundo del derecho nos referimos a la prueba como aquella actividad desplegada generalmente por las partes, y excepcionalmente de oficio por el juez (art. 282 LEC), cuya finalidad es verificar las afirmaciones sobre los hechos aportados por las partes y determinar la certeza de los hechos controvertidos[173]. La prueba tendrá por objeto los hechos alegados por las partes y contenidos en sus respectivos escritos de demanda y contestación con la finalidad de servir para acreditar sus respectivas pretensiones. El objeto de la prueba es el hecho descrito e introducido por la parte en el proceso a través de la afirmación del hecho en la demanda[174]. Afirmación que en el ámbito del proceso se materializa en la demanda, en la que se deben incluir la relación de hechos en los que la parte demandante fundamenta su pretensión[175]. Ahora bien, no todos los hechos alegados por las partes serán objeto de prueba, sino sólo aquellos respecto de los que exista controversia. De este modo no serán objeto de prueba los hechos admitidos por todas las partes en el proceso. En este sentido señala el artículo 281.3 de la LEC) que «*…Están exentos de prueba los hechos sobre los que exista plena conformidad de las partes…*».

Los hechos introducidos por las partes en el proceso a través de la demanda o contestación no pueden calificarse, directamente, como prueba, ya que para ello deberán ser objeto de petición por la parte interesada y de admisión por el Juez

[173] Recogen la iniciativa probatoria de oficio los artículos 429.1, 435.2, 752.1, 759.1, 763.3, 770.4ª, 339.5, 306.1.II y 372.2 LEC. Tratamiento específico merecen el derecho extranjero y el derecho consuetudinario (art. 281.2 LEC) y la dispensa de prueba relativa a los hechos notorios (art. 281.4 LEC) y dispensa absoluta a los hechos respecto a los que exista conformidad (art.281.3 LEC).

[174] Según MUÑOZ SABATÉ el objeto de investigación es el hecho y el objeto de prueba, la afirmación. MUÑOZ SABATÉ señala como objeto de la prueba la afirmación de los hechos y no los hechos en sí mismos. Los hechos se investigan, a partir de una hipótesis o de una mera sospecha, pero una vez hallados no se exponen en el proceso como un capitel etrusco se exhibe en un museo, sino que procesalmente se transmudan en afirmaciones. Esas afirmaciones son necesarias porque sin ellas no habría fase de alegaciones, y por ende no habría proceso, y una vez formuladas exigen su debida verificación a través de la prueba. MUÑOZ SABATÉ, Ll., *Fundamentos de la Prueba judicial civil LEC 1/2000*, J.M. Bosch Editor, Barcelona 2001, pág. 102. En igual sentido MUÑOZ SABATÉ, Ll., *Introducción a la Probática*, Serie estudios prácticos sobre los medios de prueba, núm.4, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, Barcelona 2007, pág.11.

[175] Véase en ese sentido el art. 399 LEC que establece: «*… 1. El juicio principiará por demanda, en la que, consignados de conformidad con lo que se establece en el artículo 155 los datos y circunstancias de identificación del actor y del demandado y el domicilio o residencia en que pueden ser emplazados, se expondrán numerados y separados los hechos y los fundamentos de derecho y se fijará con claridad y precisión lo que se pida*».

conforme a las normas previstas a ese fin. La conversión de un hecho alegado en un hecho objeto de prueba se producirá por medio de la petición y admisión por parte del Juez. En este sentido ha de tenerse en cuenta que la parte en el proceso deberá proponer una prueba prevista en el ordenamiento jurídico. Es decir, los hechos objeto de prueba deberán acceder al proceso a través de los medios de prueba previstos en el art. 299 LEC.

Por otra parte, no pueden acceder al proceso y por lo tanto no pueden ser objeto de prueba aquellos hechos que se obtuvieron con violación de derechos fundamentales (art. 283, 287 de la LEC y 11 LOPJ). Como vimos en el § 3.3 para que una prueba pueda tener eficacia en el proceso debe ser obtenida con respecto a los derechos fundamentales.

Por otro lado, como hemos señalado con anterioridad, el derecho a la prueba queda modulado por la pertinencia, la necesidad y los requisitos de admisión previstos por la ley (STC 30 de enero de 2003, entre otras). La prueba debe ser pertinente, es decir, debe tener relación con el *thema decidendi; d*ebe proponerse en tiempo y forma (art. 284, 414.1, 429.1, 435.1, 444.4 y 460.2 LEC); y debe ser útil o necesaria, es decir, debe servir al fin de toda prueba lo que supone a esclarecer los hechos controvertidos. En consecuencia, deberá inadmitirse aquella prueba que según reglas y criterios razonables y seguros, en ningún caso pueda contribuir a esclarecer los hechos controvertidos (art. 283.2 LEC). Si la prueba se solicita en el momento procesal oportuno, y es pertinente, útil y lícita debe admitirse, debiendo el juez pronunciarse expresamente sobre su admisión o denegación, no siendo admisibles las admisiones condicionales de prueba, por ejemplo estableciéndose para mejor proveer en la anterior LEC (SSTS de 16 de enero de 2001, 18 de mayo de 1993), ni las denegaciones tardías de prueba aunque razonadas con fundamento en la certeza ya alcanzada (STC de 14 de enero de 2004).

Una vez propuesta el Juez dictará resolución admitiendo o inadmitiendo la misma. Téngase en cuenta que el derecho a la prueba es un soporte importante del derecho a la tutela judicial efectiva: de modo que la inadmisión de la prueba únicamente podrá producirse cuando a juicio del tribunal concurran motivos suficientes para entender que la prueba no debe ser admitida. Sobre ese particular, la jurisprudencia ha declarado que toda resolución de inadmisión debe ser motivada, sin que dicha resolución pueda incurrir en irrazonabilidad o arbitrariedad (STC de 14 de enero de 2004)[176].

[176] STC 14 enero 2004, fto. jco.2º, (EDJ 2004/389).

Una vez admitida la prueba debe ser practicada (STC de 14 de febrero de 2000 y STC de 12 de diciembre de 2005)[177]. La prueba debe practicarse en el juicio oral, conforme a las normas constitucionales y legales previstas en la Ley. Ello supone el pleno respeto de las normas procesales para la práctica de cada medio de prueba y además el cumplimiento del resto de la legalidad. De este modo, el interrogatorio del testigo, por ejemplo, deberá realizarse conforme con las normas previstas en la LEC (arts. 360 y ss LEC), pero, además deberán observarse y respetarse otros derechos que puedan resultar afectados en la práctica de la prueba. Así, el derecho a la intimidad del testigo, reconocido en el art. 18 CE, que no podrá resultar afectado con preguntas que se refieran a un ámbito personal de privacidad.

Por último, el resultado de la prueba se contendrá en la sentencia dictada por el Juez. Dicho resultado probatorio debe ser valorado por el órgano jurisdiccional que deberá motivar las sentencias como una exigencia constitucional a fin de dar cuenta del modo en el que ha formado su convicción (120.3 y 24.2 CE y 218.2 LEC). No existen reglas tasadas sobre el modo en el que el Tribunal debe motivar la sentencia, pero sí unas reglas orientativas que determinan que el Tribunal deba justificar suficientemente su decisión respecto a cada hecho y prueba practicada, evitando acudir a la criticable práctica forense de valoración conjunta de la prueba (STS de 12 de junio de 2000, f.j.2º). El Juez procederá a su valoración individualmente y en su conjunto tal y como expresamente refiere el art. 218 LEC en su apartado 2 al señalar que «*…la motivación deberá incidir en los distintos elementos fácticos y jurídicos del pleito, considerados individualmente y en su conjunto, ajustándose siempre a las reglas de la lógica y de la razón…*». El Juez como regla general valora libremente la prueba con arreglo a las reglas de la «sana crítica» (art. 316.2, 348, 376 y 382.3 LEC). Ello no obstante, la Ley también prevé supuestos que se denominan de «valoración tasada» (art. 326.1, 319 y 326 LEC o 1218 y 1225 Cc.)[178].

---

[177] STC de 12 de diciembre de 2005, fto. jco.4º (EDJ 2005/213561), la cual, a su vez, cita las SSTC de 17 de enero de 2005 (EDJ 2005/3244), de 26 de marzo de 2001 (EDJ 2001/2656), de 16 de octubre de 2000, (EDJ 2000/31691), y 24 de febrero de 2000 (EDJ 2000/1145).

[178] Véase, en este sentido, ABEL LLUCH, X., *Sobre la prueba y el derecho a la prueba en el proceso civil*, en "Objeto y carga de la prueba civil", Picó i Junoy, J. –Abel Lluch, X, J.M. Bosch Editor, 2007, págs. 19-46. La valoración por parte del juez del resultado de la prueba con arreglo a la sana crítica como norma general no es óbice para que también existan reglas tasadas de valoración de la prueba. Ahora bien se trata de una excepción, que en realidad lo que pretende es cierta normalidad probatoria, es decir, una serie de normas que dotan *a priori* de una determinada eficacia a la prueba pero que en realidad no dejarán de poder ser impugnadas, en su caso, y siempre valoradas finalmente por la sana crítica judicial. Un documento público en el que interviene un notario alcanza a lo que el notario ve, oye o percibe por los sentidos, la fecha etc. pero en realidad ello es cosa distinta de la veracidad intrínseca. En realidad no existen pruebas tasadas propiamente dichas sino que todas las pruebas se someterán a la sana crítica judicial.

Resulta difícil definir que sea la «sana crítica», más allá de entender que se trata de una suerte de criterio racional que en materia jurídica nos debe permitir obtener conocimiento sobre las materias sometidas a enjuiciamiento. Este criterio racional se fundamenta básicamente en la lógica y en las máximas de experiencia que deben ser aplicadas por el Tribunal en su valoración de los hechos y cuya ausencia se manifiesta claramente como arbitrariedad e irrazonabilidad[179]. En ese sentido se pronuncia RICHARD que señala que la: «… *Razón en nuestro oficio jurídico se llama sana crítica. Concepto difícilmente reducible a una definición, o mucho menos a fórmulas matemáticas, pero que sin embargo es fácilmente reconocible tanto su presencia como su ausencia…./…. la sana crítica no sabría definirla con exactitud pero reconozco perfectamente su presencia o su ausencia en una sentencia o resolución judicial*»[180].

Por su parte, TARUFFO señala que el Magistrado apreciará los medios de prueba conforme a principios o pautas seguros de enjuiciamiento de acciones, conductas y hechos de relevancia procesal depurándolos conforme a las máximas de la experiencia. De modo más pedagógico GUASP explicaba que las «reglas de la sana crítica» son los criterios normativos -reglas no jurídicas- que sirven al hombre normal, en una actitud prudente y objetiva -sana- para emitir juicios de valor -estimar, apreciar, «crítica» acerca de una realidad-[181]. COUTURE se refiere a las mismas como «*las reglas del correcto entendimiento humano*»[182]; SENTIS MELENDO como «*las reglas de prudente apreciación que permiten llegar a una convicción libre o persuasión racional*»[183;] FAIREN GUILLEN señala que

[179] La jurisprudencia enfatiza su vinculación a la lógica, la experiencia, racionalidad y razonabilidad. Véanse: SSTS de 13 de febrero de 1990 fto. jco.2º (RJ 1990\683); 18 de octubre 1994, fto. jco.3º (RJ 1994\7485); 8 de mayo de 1995 fto. jco.1º (RJ 1995\3938); STS 18 de julio de 2011, fto. jco.1º (RJ 2011\5221); 15 de diciembre de 2012, fto. jco.2º (RJ 2011\2012); 4 de junio de 2001 fto. jco.4º (RJ 2001\3879); 15 de octubre de 1991 fto. jco.2º (RJ 1991\7073); 24 de noviembre de 1995, fto. jco.2º (RJ 1995\8740); 17 de mayo de 2002, fto. jco.5º (RJ 2002\5342); de 5 de febrero de 2013, fto. jco.3º (RJ 2013\1999); y 20 de febrero de 2012, fto. jco.2º (RJ 2012\4044).

[180] Véase RICHARD GONZALEZ, M., *Reflexiones sobre la práctica y valor de la prueba científica en el proceso penal*, La Ley nº 7930, 2012, págs. 1 a 6.

[181] Véase TARUFFO, M., *La prueba de los hechos* (traducción Jordi Ferrer Beltrán), ed. Trotta, Madrid, 2002, pág. 202; y GUASP, J., *Comentarios a la Ley de Enjuiciamiento Civil*, T.II, Vol. 1º, 2ª parte, M. Aguilar, editor, Madrid, 1947, pág .647.

[182] COUTURE, E.J., *Fundamentos del Derecho Procesal Civil*, 4ª ed., ed. Bde. Montevideo-Buenos Aires, 2004, pág. 221; y *Estudios de Derecho Procesal Civil*, t.II, 3ª ed., ed. Depalma, Buenos Aires, 1989, pág.195.

[183] SENTIS MELENDO, S., *La prueba*, Los grandes temas del derecho probatorio, EJEA, Buenos Aires, 1979, pág. 272.

«*son máximas de la ciencia, de la técnica o de la experiencia*»[184]; BONORIO afirma que «*son las leyes de la lógica, de la experiencia y de la psicología común*»[185]; MANRESA Y NAVARRO las define como «*las reglas que nos conducen al descubrimiento de la verdad por los medios que aconseja la recta razón*»[186]; MONTON REDONDO indica que la «*sana crítica supone que el órgano jurisdiccional debe valorar las pruebas de acuerdo con las reglas de la lógica, de la psicología o de la experiencia que, según su criterio personal, sean aplicables a cada supuesto concreto*»[187], y finalmente ABEL LLUCH define las reglas de la sana crítica como «*las reglas derivadas de la lógica, la experiencia y la ciencia. Más ampliamente, que son las reglas no jurídicas derivadas de la lógica, la experiencia y la ciencia que sirven para fundar una valoración razonada de la prueba y permiten su control posterior por otro órgano superior*»[188].

4.3 Regulación legal de la prueba

El Borrador y el Anteproyecto de la LEC 2000, datado en 1998, recogieron como medios de prueba los tradicionales que habían sido regulados en la LEC de 1981. No obstante, dada la evolución de las tecnologías y medios de comunicación se introdujo una referencia en el artículo 354.2 del Borrador (351.2 del Anteproyecto) para admitir los: «*medios de reproducción de la palabra, el sonido y la imagen*». Añadiendo el artículo 354.3 que «*cuando por cualquier otro medio no expresamente previsto en el apartado anterior de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias*».

El debate, en aquel momento, se centró en la equiparación del documento clásico al documento electrónico. Por una parte, la normativa procesal se

---

[184] FAIRÉN GUILLÉN, V., *Casación, hechos, Derecho extranjero, reglas de la sana crítica en la Ley 10/992, de 30 de abril, de Medidas Urgentes de Reforma Procesal*, en Revista de Derecho Procesal, 1991, 1, pág.538.

[185] BONORINO, P.R., *Sobre las reglas de la sana crítica*, en Anuario de la Facultad de Ourense, 2003, (1), pág. 83, quien incluye esta definición como común entre los procesalistas, sin atribuirla a un autor concreto.

[186] MANRESA Y NAVARRO, J. Mª, *Comentarios a la Ley de Enjuiciamiento Civil*, t. III, ob. cit., pág. 349.

[187] MONTÓN REDONDO, A., *Valoración de la prueba e interpretación de los resultados probatorios*, en Revista de Derecho Procesal, 1978, 2-3, pág. 389.

[188] ABEL LLUCH, X., *La configuración de las reglas de la sana crítica en la LEC*, Revista Vasca de Derecho Procesal y Arbitraje, Vol. 2, Tomo XXV, 2013-2, 06/2013, págs. 135-166.

posicionaba contraria a la equiparación del documento electrónico al escrito. Por otra, el Consejo General del Poder Judicial, en su informe sobre el Anteproyecto, manifestó su disconformidad con el planteamiento doctrinal clásico de «documento» que se pretendía con la reforma. En este sentido se pronunció en su informe manifestando que: *«…Con carácter general cabe decir que el concepto de documento en el Anteproyecto se aproxima a un planteamiento doctrinal clásico, que puede estimarse superado por la realidad normativa y social, con la representación en papel de un pensamiento, voluntad o dato fáctico. Esta línea, plasmada en los artículos 368, 375 y 385 del Anteproyecto, debe ser revisada para acomodar esta concepción a una época en la que la transcripción en papel de pensamientos, ideas, informes, registro, contratos, etc., está siendo progresivamente sustituida por la generalización de las herramientas informáticas, el soporte electrónico y los medios audiovisuales. No parece, en efecto, que los medios electrónicos o informáticos tengan adecuada cabida dentro de la literal redacción del artículo 375 (ALEC), conforme al cual son documentos privados todos los que no sean enumerados como documentos públicos, ni en la expresión "otros documentos" que aparece como numerus apertus en el artículo 384 (ALEC). El Anteproyecto parece decantarse por la inclusión de estos medios y soportes técnicos dentro de la prueba de reconocimiento judicial al referirse en su artículo 403 (ALEC) al examen de lugares, "objetos" o personas. En este sentido podría hacerse referencia al concepto más avanzado que ofrece de documento el artículo 26 del vigente Código Penal, aunque ciertamente sin agotar una definición precisa, como "todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria" y precisarse aún más este concepto en el código procesal civil, siguiendo la tendencia más moderna a la extensión del concepto de documento, de acuerdo asimismo con la legislación civil sobre propiedad intelectual»*. El legislador hizo caso omiso, y el texto del Proyecto pasó sin apenas ser modificado al de la Ley definitiva. Se añadió en el art. 301.2 del Proyecto lo que sería el apartado 2 del artículo 299 de la LEC, surgiendo los art. 382 y 383 dedicados a los medios audiovisuales y el 384 sobre instrumentos de archivo (soportes informáticos)[189].

[189] Algunos países como Panamá establecen en su normativa la equivalencia en fuerza probatoria de los documentos electrónicos frente al resto de documentos. En este sentido se pronuncia la Ley 51 de 22 de julio de 2008, que define y regula los documentos electrónicos y establece en su artículo 7 que *«Los documentos electrónicos serán admisibles como medios de prueba y tendrán la misma fuerza probatoria otorgada a los documentos en el Libro segundo de procedimiento Civil del Código Judicial.//En todo caso, al valorar la fuerza probatoria de un documento electrónico se tendrá presente la confiabilidad de la forma en la que se haya generado, archivado o comunicado, y la confiabilidad de la forma en que se haya conservado la integridad de la información»*. EYNER ISAZA, H. *La prueba electrónica en Panamá y en el sistema interamericano*, ed. Universal Books, Panamá, 2013, págs. 21-22.

La Ley de Enjuiciamiento Civil, Ley 1/2000, en su redacción definitiva, enumera en su artículo 299.1 LEC los tradicionales medios de prueba: *Interrogatorio de las partes* –que sustituye a la confesión judicial-; d*ocumentos públicos*; d*ocumentos privados*; d*ictamen de peritos*; r*econocimiento judicial*; e *interrogatorio de testigos*. En el 2º párrafo del art. 299 LEC, y con intención de regular las nuevas tecnologías, efectúa una ampliación de los nuevos medios de prueba, señalando que «*También se admitirán, conforme a lo dispuesto en la Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso»*. Regulación que desarrolla en la Sección Octava, Capítulo VI, Título I, Libro II, que incluye los artículos 382 a 384 bajo la rúbrica «*De la reproducción de la palabra, el sonido y la imagen y de los instrumentos que permiten archivar y conocer datos relevantes para el proceso»*. Y finalmente, establece en su apartado tercero que *«cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre los hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias»*. Estableciendo de ese modo un *numerus apertus*.

En el apartado primero del artículo 299 de la LEC se pone de manifiesto la confusión entre *los medios* (interrogatorio, dictamen o reconocimiento) y *las fuentes* de prueba (documentos), confusión que de nuevo repite, en el apartado tercero del mismo, cuando como cláusula abierta del sistema probatorio alude a «*cualquier otro medio no expresamente previsto en los apartados anteriores»*. Dicha confusión que reaparece en la Exposición de Motivos (XI, párrafo 5º) al referirse a los cambios que afectan a la prueba cuando menciona como el primero de todos ellos: «*la apertura legal a la realidad de cuanto puede ser conducente para fundar un juicio de certeza sobre las alegaciones fácticas, apertura incompatible con la idea de un número indeterminado y cerrado de medios de prueba»*. En todos los anteriores casos debió aludir a las «fuentes de prueba» o «hechos» y no a los medios de prueba, en cuanto sólo las/los primeras/os son ilimitadas/os[190]. La regulación que efectúa la LEC de las TIC como medios de prueba independientes es errónea no sólo por los motivos ya aludidos sino porque además, a posteriori, tanto el art. 299.2 como los artículos 382 a 384 LEC no son autosuficientes, sino que precisan ponerse en conexión con el régimen específico de los medios probatorios de los que se nutren (la prueba documental, el reconocimiento judicial y la prueba pericial) y con

[190] MONTERO AROCA, J., *La prueba en el proceso civil*, 5ª ed., ed. Civitas, Madrid, 2007, pág.148.

regulación extraprocesal[191]. La regulación de la LEC 2000, por lo que respecta a la llamada «prueba electrónica» nació ya caduca y obsoleta, cuando la jurisprudencia había recogido ya el concepto de documento electrónico, era de esperar por el legislador algo más que cuatro artículos, y, por ende, un régimen jurídico más completo de la prueba electrónica o del documento electrónico.

La fuente no puede identificarse con el soporte que recoge el contenido de la información, ni el medio de prueba con su reproducción a presencia judicial. Fuente es la imagen, la palabra, los datos, las cifras, las operaciones matemáticas etc.; tales fuentes se almacenan y recogen en instrumentos de archivo, conocimiento o reproducción de datos (diskettes, flash, pendrive, DVD, disco duro, etc.); y actividad probatoria es la reproducción práctica de la prueba en el Tribunal[192]. La LEC confunde la reproducción de las palabras imágenes y sonidos captados mediante instrumentos de filmación, grabación y otros con un medio de prueba, tal y como se deduce de la lectura del artículo 382 LEC. Sin embargo, como hemos señalado, los medios de prueba son limitados, y en consecuencia la reproducción en sí misma no es medio de prueba sino una forma de practicar la prueba electrónica dado que no puede ser leída como un documento escrito. Reproducción que tendrá lugar a través de transcripción escrita de su contenido (art. 382.1 LEC) o a través medios que la parte proponente aporte o el tribunal de disponga a utilizar y le permitan su examen (art. 384.1 LEC).

La doctrina ha puesto en tela de juicio no solo la terminología empleada por la Ley de Enjuiciamiento Civil al emplear la expresión «medios e instrumentos» para regular el acceso de las vigentes tecnologías al proceso, sino también el escaso contenido de su regulación, y su ubicación sistemática[193]. Por otro lado, la proliferación de numerosas leyes regulando la realidad vigente que implican las vigentes tecnologías de la información y comunicación han dejado atrás la regulación de la LEC. Tales son: la Ley 34/2002, de 11 de julio, de Servicios en la Sociedad de la Información; Ley 59/2003, de 19 de diciembre, de Firma Electrónica[194]; Ley 25/2007 de Conservación de datos relativos a las

[191]Así lo señala ORMAZÁBAL SÁNCHEZ, G., *La prueba documental y los medios e instrumentos idóneos para reproducir imágenes o sonidos o archivar o conocer datos*, ed. La Ley, Madrid, 2000, pág. 170.

[192] En este sentido ABEL LLUCH, X. en *La prueba electrónica*, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.4, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, págs.66-67.

[193] Así lo señala NIEVA FENOLL, J. *La prueba en el documento multimedia*, en *"Jurisdicción y Proceso"*, ob. Cit., págs. 307 y 318-320.

[194] Tiene su antecedente en Real Decreto-Ley 14/1999, de 17 de diciembre. Ha sido modificada por la Ley 56/2007, de 28 de diciembre, de Impulso de la Sociedad de la Información.

Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones; Ley 11/2007, de 22 de junio, sobre el Acceso Electrónico a los ciudadanos a los Servicios Públicos, entre otras.

En lo que afecta a la regulación de la prueba electrónica a nivel internacional las Naciones Unidas, a través de UNCITRAL, recomiendan una adecuación de las legislaciones de cada país y ha emitido el documento *Legal Value of Computer Records*, en el que se expresa que las normas o reglas concernientes a las pruebas relativas a registros de computadora, no deben suponer un obstáculo para el uso de tecnologías emergentes, tanto a nivel nacional como internacional[195]. A nivel comunitario debe mencionarse la Directiva 1999/93/CE, del Parlamento de Europa y del Consejo, de 13 de Diciembre de 1999, por la cual se establece un marco unitario para la firma electrónica. También debe apuntarse que la Dirección General de Justicia, Libertad y Seguridad de la Comisión Europea, dentro del Programa Marco AGIS, aprobó un primer estudio sobre la prueba electrónica en Europa.

La rápida evolución de las Tecnologías de la Información y Comunicaciones (TIC) exige una legislación uniforme que permita el desarrollo y aplicación de las mismas en el proceso judicial con las máximas garantías. Esta legislación, y dada la complejidad del fenómeno electrónico y su globalización, debería tener ya un carácter supranacional. En la actualidad la práctica forense evidencia cierta reticencia a su admisión debido a la confusa regulación o la falta de la misma[196].

4.4 Límites de la prueba

La Constitución Española garantiza el derecho a la prueba (art. 24.2 CE), por lo que cualquier parte en el proceso tiene derecho a la admisión y práctica de los medios de prueba previstos en la Ley. No obstante, la prueba no tiene carácter ilimitado sino que está sujeta a límites. PICÓ i JUNOY clasifica dichos límites en: intrínsecos (pertinencia, utilidad y licitud) y extrínsecos. Dentro de estos últimos,

---

[195] Véase DE URBANO, E., *La valoración de la prueba electrónica*, ob. cit., pág. 50.

[196] El Magistrado del TS Marchena Manuel, «*IV Foro de las Pruebas Electrónicas*» (2008), señala que: «*los problemas de los medios de prueba electrónicos se deben a la pereza institucional para asumir compromisos normativos y los jueces no tienen un marco claro que aplicar*». Puede consultarse este artículo en la dirección electrónica http://goo.gl/ykBLR o http://goo.gl/G94u5, páginas visitadas en fecha 11 de julio de 2013. Respecto al impulso estatal pueden consultarse la Ley de Medidas de la Sociedad de la Información, Ley 56/2007 y la Ley 11/2007 de Acceso electrónico de los ciudadanos.

los extrínsecos, distingue entre genéricos, que son los requisitos legales de proposición, y específicos que son los requisitos de cada medio probatorio en particular[197].

En cuanto a lo que PICO y JUNOY denomina límites extrínsecos, se trata de aquella serie de requisitos indispensables que establece la ley para que la prueba propuesta por las partes en el juicio se admita por el juez, son los llamados «requisitos de admisión» de la prueba. Es decir, la prueba para poder acceder al proceso debe cumplir dichos criterios. En este sentido la prueba debe ser pertinente, útil y legal, y en el supuesto que no lo sea no debe ser admitida por el juez. Los anteriores son requisitos de admisión de la prueba, sin embargo, no debemos confundir «legalidad» con «ilicitud», puesto que en nuestra opinión la ilicitud no es propiamente un criterio de admisión de prueba como la pertinencia, la utilidad y la legalidad (art. 283 LEC) sino un incidente para expulsar del proceso la prueba admitida con violación de derechos fundamentales.

En primer lugar la prueba propuesta por las partes debe ser pertinente. La «pertinencia» supone que la prueba debe guardar relación con los hechos objeto del proceso. De este modo lo regula el art. 283.1 LEC al establecer expresamente que «… *No deberá admitirse ninguna prueba que, por no guardar relación con lo que sea objeto del proceso, haya de considerarse impertinente*». El Tribunal Constitucional ha perfilado la definición de pertinencia definiendo la misma como la relación entre los hechos probados y el «*thema decidendi*» (STC 26/2000, de 31 de enero, FJ 2º, SSTC 12/2004 de 12 de julio, f.j.2º y 165/2001, de 16 de julio).

En segundo lugar, la prueba debe ser «útil». La utilidad supone que deba rechazarse aquella prueba propuesta que según reglas y criterios razonables y seguros no contribuya a esclarecer los hechos controvertidos (art. 283.2 LEC). Ahora bien la garantía del derecho a la prueba determina que, en caso de duda, deba admitirse la prueba propuesta. En este sentido, no cabe declarar la inadmisión de la prueba con base en la previsión de su resultado.

Y en último lugar, la prueba propuesta debe ser «legal», es decir conforme a la ley, y debe ser «lícita». La licitud impide la permanencia en el proceso de aquella prueba obtenida vulnerando un derecho fundamental (art. 287.1 LEC y 11.1 LOPJ). Su admisión supondría, además, la infracción a un proceso con todas las garantías y a la igualdad de las partes. Tengamos presente que los derechos fundamentales son preferentes en el ordenamiento jurídico e inviolables (STC

[197] PICÓ Y JUNOY, *Problemas actuales de la prueba civil,*, en la obra colectiva del mismo título, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), J.M. Bosch, Barcelona, 2005, págs. 49 y ss.

50/2000, de 28 de febrero, f.j. 2º). Como hemos señalado anteriormente la licitud no es propiamente un criterio de admisión de la prueba sino un incidente para expulsar del proceso la prueba obtenida con vulneración de los derechos fundamentales.

En cuanto a los límites extrínsecos genéricos se incluyen los requisitos de legitimación y los temporales. La legitimación la otorga el hecho de ser parte en el proceso, y los temporales suponen que la prueba debe proponerse en el momento procesal oportuno para poder ser admitida por el órgano jurisdiccional. En cuanto a estos últimos, los límites temporales, la prueba debe solicitarse al final de la audiencia previa, en el juicio ordinario (art. 429.1 LEC) o en la vista, en el juicio verbal (art. 443.4 LEC). Por otro lado, el ejercicio de la prueba debe tener lugar en la primera instancia, teniendo la práctica de la prueba ante el órgano *ad quem* un carácter limitado al configurarse la apelación como una *revisio prioris instantiae,* por ello sólo puede solicitarse la práctica de la prueba en la segunda instancia en el escrito de interposición del recurso y por motivos tasados (art. 460.2 LEC).

4.5 Requisitos procesales para la práctica de la prueba

El Derecho a la prueba previsto en el artículo 24.2 de la CE, supone el derecho de cada parte en el proceso a practicar la prueba que estime conveniente a través de los medios de prueba previstos por la ley. No obstante, como señalábamos en el epígrafe anterior la prueba está sujeta a determinados límites, es decir, se halla modulada por la pertinencia, la utilidad y la licitud y por determinados requisitos generales de proposición de prueba previstos en la ley como la legitimación y la temporalidad. Además de todos estos requisitos que establece la ley con carácter general, existen a nivel particular requisitos procesales específicos que afectan o se aplican a la práctica de cada medio de prueba en concreto, es decir, se prevén por la ley de un modo específico para cada medio probatorio determinado. Se trata de aquellos requisitos a los que PICO y JUNOY se refiere y ha venido a llamar «límites extrínsecos específicos». Veamos, pues, brevemente algunos de los requisitos procesales que la ley exige a cada medio de prueba en concreto.

El primer medio probatorio regulado en el artículo 299.1 LEC es el interrogatorio de partes. En relación a la prueba de interrogatorio de partes la LEC prevé determinados requisitos procesales para la práctica de dicha prueba en el proceso. Nótese que el artículo 301 de la LEC prevé que «*1. Cada parte* (solo) *podrá solicitar del tribunal el interrogatorio de las demás sobre los hechos y circunstancias de los que tengan noticia y que guarden relación con el objeto del*

juicio. Un colitigante podrá solicitar el interrogatorio de otro colitigante siempre que exista en el proceso oposición o conflicto de intereses entre ambos», impidiéndose en caso contrario, lo cual supone una limitación al derecho de prueba. Por otro lado, en cuando a la capacidad para declarar en juicio de un menor la Ley exige como requisito necesario que sea asistido por su representante legal, tener más de catorce años y poseer discernimiento necesario para conocer y declarar verazmente (art. 6.1.1, 361.II, art. 7.1 LEC). La ley exige la necesaria asistencia de un representante al menor, en cuanto éste debido a su edad no está en pleno ejercicio de sus derechos civiles y por lo tanto no puede comparecer por sí solo en juicio y efectuar actos procesales válidamente. Y finalmente, la ley prevé también expresamente la forma en que debe formularse el interrogatorio, estableciendo en el artículo 302.1 que las preguntas deben ser formuladas en sentido afirmativo, con la debida claridad y precisión, sin incluir valoraciones ni calificaciones y referidas a los hechos litigiosos.

En lo referente al interrogatorio de testigos (art. 299.1.6º LEC), la LEC exige en el art. 361 LEC respecto a las personas que deben declarar idoneidad mínima, excluyendo declarar a las que se hallan permanentemente privadas de razón o uso de los sentidos respecto a hechos sólo perceptibles por los mismos. El art. 363 LEC permite al juez, una vez escuchado el testimonio de tres testigos con relación a un hecho discutido, obviar las declaraciones testificales que falten referentes a ese mismo hecho si se considera lo suficientemente ilustrado con las ya admitidas. En cuanto a las preguntas deben ser efectuadas en sentido afirmativo, con la debida claridad y precisión, y sin incluir valoraciones ni calificaciones (art. 368 LEC). Y finalmente, el artículo 371 LEC libera al testigo de declarar cuando tenga el deber de secreto por razón de estado o profesión, o sea interrogado sobre una materia legalmente declarada secreta o clasificada como de carácter reservado o secreto, salvo autorización expresa de la ley o de la persona que los ha confiado (art. 2.2 LO 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen). Por otro lado, el artículo 379.1 LEC no permite la prueba testifical para acreditar la tacha de testigo.

También se prevén determinados requisitos procesales o limitaciones específicas respecto a la prueba documental. De este modo la LEC regula expresamente el momento procesal oportuno en que debe presentarse la prueba documental, es decir, junto con la demanda, la contestación, o, en su caso, en el momento de comparecer a la vista del juicio verbal (artículos 264 y 265 LEC) precluyendo en caso contrario ese derecho (art. 269.1 LEC). No obstante, si bien la norma general es la anterior existen algunas excepciones a la misma cuya finalidad principalmente es garantizar el derecho a prueba sin crear indefensión a una de las partes.

Son excepciones a dicha norma en primer lugar los supuestos de imposibilidad previstos en el artículo 270 LEC, es decir: a.) Documentos de fecha posterior a los escritos de demanda y contestación, o en su caso, a la audiencia previa al juicio, siempre que no se hubiere podido confeccionar u obtener con anterioridad a dichos momentos procesales; b.) Documentos anteriores a la demanda o contestación o, en su caso, a la audiencia previa al juicio, cuando la parte que los presente justifique no haber tenido antes conocimiento de su existencia; c.) Documentos que no se han podido obtener con anterioridad debido a causas no imputables al litigante interesado, y siempre que éste haya hecho oportunamente la designación del archivo o lugar donde se encuentren los originales. Dichos documentos podrán aportarse antes de que concluya la vista o juicio (art. 271 LEC). En segundo lugar constituyen también una excepción a la norma general: Los documentos no esenciales o fundamentales; los que tienen por finalidad contrarrestar las alegaciones formuladas por el demandado en su contestación a la demanda (art. 265.3 in fine LEC); así como los que sirven para acreditar las aclaraciones, correcciones o modificaciones fácticas permitidas por la ley respecto a los que cabe incorporarlos al proceso durante la audiencia previa (si se trata de documentos del actor respecto a las alegaciones del demandado: art. 265 LEC) o el juicio. Y finalmente los documentos incorporados al proceso a través de las diligencias finales (art. 271.1 y 435 LEC).

La LEC establece también limitaciones al derecho a la prueba documental en los supuestos en que interviene la Agencia Tributaria. Si bien el artículo 332 LEC regula la exhibición documental de entidades oficiales (art. 332 LEC) se prevé un tratamiento privilegiado a la Agencia Tributaria, por cuanto si bien se impone el deber de exhibición documental a las entidades oficiales, ello no alcanza a los documentos de carácter reservado o secreto, por lo que aquella se ampara en el artículo 113 LGT -que establece el carácter reservado de los datos obtenidos por la Agencia Tributaria- para liberarse de la colaboración con los Tribunales.

En lo relativo a la prueba pericial es una prueba sujeta también a requisitos procesales que en ocasiones vulneran el principio de igualdad, a la defensa y a la prueba. Nótese que la parte beneficiaria de justicia gratuita no puede disponer del dictamen pericial sino una vez presentada la demanda en la que se solicita la designación correspondiente, lo cual limita las posibilidades de motivación de las alegaciones del abogado. Por otra parte, no se favorece a la parte con menos recursos puesto que de percibir más del doble del salario mínimo interprofesional deberá efectuar la provisión de fondos admitida por el juez sin audiencia de las partes quienes no podrán discutir ni importe ni forma de pago (art. 339.2.1 LEC). La obligación de presentación de dicha prueba por parte del demandado en la contestación a la demanda limita también su derecho a la defensa puesto que solo dispone de veinte días para presentarla, y

aun cuando justifique la imposibilidad de presentación pudiendo aportarla con posterioridad el abogado deberá presentar la contestación dentro de dicho plazo sin disponer de una pericial en que fundamentar sus alegaciones. Otro problema es la inclusión del gasto de dicha prueba en las costas, por lo que debe incluirse en éstas el gasto que supone el informe pericial en aras a que la parte no renuncie tácitamente a dicha prueba por el coste que supone. Por otra parte, la limitación del artículo 343.2.II LEC que establece la prohibición de la prueba testifical para acreditar la tacha del perito. Y finalmente la limitación de intervención en el proceso judicial de peritos que hayan intervenido en procesos de mediación o arbitraje sobre igual asunto (art. 335.3 y 347.1 LEC).

Por último y respecto a la prueba de reconocimiento judicial, se exige en el artículo 353 LEC al solicitante como requisito procesal necesario que exprese los extremos principales sobre los que quiere que se realice el reconocimiento judicial e indique si concurrirá al acto con alguna persona técnica o práctica en la materia, sin que sea necesario identificar a dicha persona en la audiencia previa o juicio por cuanto no aporta nada dicho dato para la admisión o no de dicha prueba.

* * *

CAPÍTULO V.- CARACTERISTICAS DEL HECHO ELECTRÓNICO

El hecho electrónico tiene peculiares características que se relacionan con los distintos ámbitos a los que se refiere. En este sentido se puede hablar de hecho electrónico desde: 1º Una dimensión técnica-científica. 2º Una dimensión social-empresarial. 3º Una dimensión jurídico-procesal. Todos estos aspectos en su conjunto conforman y definen qué sea el hecho electrónico, lo que determina su análisis detallado.

En primer lugar, desde el punto de vista científico-técnico el hecho electrónico se relaciona con los electrones que son una de las partículas que conforman la estructura atómica de la materia, y al mismo tiempo con la electrónica. De modo que podemos caracterizar el hecho electrónico como aquel fenómeno o realidad directamente originada o determinada en el entorno y con los parámetros propios de la electrónica, entendida como el ámbito físico de actuación de electrones caracterizado principalmente por el movimiento. Efectivamente, si existe electrónica y hecho electrónico es porque los electrones se mueven y producen efectos. El diccionario María Moliner define a la electrónica, en este sentido, como: «*la rama de la física y de la técnica que se ocupa del comportamiento y utilización de los electrones libres, o sea del paso de electricidad a través de gases y del vacío*». Por su parte, la Real Academia Española de la Lengua define a la electrónica como: «*el estudio y aplicación del comportamiento de los electrones en diversos medios, como el vacío, los gases y los semiconductores, sometidos a la acción de campos eléctricos y magnéticos*». Esta última definición de la Real Academia es probablemente poco explicativa del fenómeno electrónico, al centrarse en su origen básico en lugar de en la aplicación concreta de la electrónica.

El hecho electrónico está asociado indisolublemente a la electrónica que debe entenderse como la técnica que se vale, precisamente, del fenómeno físico de la circulación electrónica para obtener resultados concretos y tangibles utilizables en multitud de máquinas y dispositivos. Así, es electrónica la técnica utilizada en la transmisión, sintonización y reproducción de radio; o en los procedimientos de construcción de capas y estructuras de semiconductores de silicio que forman el cuerpo principal de los procesadores que controlan multitud de dispositivos electrónicos, incluyendo las computadoras. Es electrónico, en definitiva cualquier dispositivo que utilice, no la fuerza del agua (permítaseme la expresión), sino la fuerza de los electrones conducidos hacia un determinado propósito en multitud de máquinas y dispositivos que venimos llamando de forma genérica electrónicos.

En este punto, debemos distinguir entre la electrónica y la informática. Cabe señalar, en este sentido, que ni toda la electrónica es informática, ni toda la informática es electrónica. Así, no todos los dispositivos electrónicos tienen por finalidad el tratamiento y/o procesamiento de la información. Huelga señalar la lista interminable de dispositivos electrónicos que tienen otros fines o utilidades distintos a la informática (dispositivos de radio, dispositivos médicos, vehículos, etc.). Tampoco puede decirse que toda la informática es electrónica. Ciertamente, en el momento presente cualquier dispositivo informático está soportado por piezas y componentes electrónicos como los procesadores que, en esencia, no son más que millones de puertas lógicas de silicio que permiten el paso, o no, del flujo eléctrico. La miniaturización, la velocidad de procesamiento, las bajas tensiones eléctricas de funcionamiento y el uso de un software cada vez más sofisticado consiguen el «milagro» de poder procesar ingentes cantidades de datos en segundos. Ahora bien, téngase presente que el sistema binario tiene su origen en el álgebra de Boole que fue utilizado por primera vez en 1725 en máquinas no electrónicas que se servían de resortes y tarjetas perforadas que contenían información para el funcionamiento de máquinas de producción o de procesamiento de información .

El hecho electrónico puede ser perceptible o no por nuestros sentidos, todo depende de la clase de máquinas y dispositivos y de cómo éstas ofrezcan la información. En realidad todo hecho electrónico puede ser directamente aprehendido por los sentidos humanos ya sea en forma de señales lumínicas, sonido o píxeles en una pantalla analógica o digital. En cualquier caso, queda claro que el hecho electrónico que en esencia consiste, sencillamente, en el desplazamiento de electrones precisa de técnicas y dispositivos de captación, reproducción y/o traducción del hecho electrónico para su manifestación y percepción por nuestros sentidos. Así, el hecho electrónico se puede contener y/o, conservar en soportes de distinta clase y naturaleza (óptico, magnético) o representarse a través de un soporte (pantalla, impresora etc.).

Efectivamente, el hecho electrónico se puede manifestar de modos bien distintos, casi siempre con el denominador común del concurso del electromagnetismo que está implicado, de un modo u otro, en todos los fenómenos eléctricos y electrónicos. Así, son hechos electrónicos tanto las ondas electromagnéticas de modulación de frecuencia que nos permiten escuchar nuestra emisora preferida de radio FM, como las marcas magnéticas existentes en nuestros discos duros o memorias USB que contienen la información precisa sobre nuestros programas y datos. Finalmente, también tienen naturaleza electrónica los paquetes de información digital que circula por las redes de fibra óptica o que se almacenan en nuestros teléfonos móviles y cámaras digitales.

Al margen de lo expuesto, no cabe duda de que en la actualidad es preponderante la importancia del hecho electrónico como un sistema codificado de información, del mismo modo que lo es el alfabeto y los símbolos que lo componen. Ahora bien, el hecho electrónico no es directamente aprehensible por los sentidos como lo es el lenguaje escrito que puede ser descifrado por cualquier persona que tenga una mínima cultura que le permita leer un texto. Efectivamente, en un documento se confunde el mensaje con el soporte que lo contiene. Sin embargo, los hechos electrónicos «yacen» o se contienen en soportes técnicos a los que no se puede acceder mediante los sentidos humanos, de modo que, por lo general, se requerirá de un aparato para captar, medir o interpretar el hecho electrónico. Este sería el supuesto de los datos informáticos para cuya captación y entendimiento se requiere de software especializado y de unos aparatos técnicos (hardware). Igual sucede con las señales electromagnéticas analógicas o digitales que contienen y transportan la voz humana que precisan de aparatos sintonizadores y reproductores de radio al efecto de su escucha y entendimiento.

En segundo lugar, el hecho electrónico tiene una dimensión social que se refiere al resultado del hecho electrónico y al modo en el que se incardina en nuestra realidad diaria. Esta dimensión social es la que convierte al hecho electrónico de interés para la contienda jurídica y la prueba en el proceso. Un buen ejemplo es el documento, que ha pasado de ser un objeto claramente predeterminado y configurado como un soporte en el que contiene la voluntad y expresión humana a un objeto no claramente determinado que puede contener no sólo la expresión humana, sino también la de las máquinas y dispositivos programados que realizan tareas en nuestra sociedad. Es porque utilizamos, compramos y vendemos, alquilamos, despedimos... etc., mediante dispositivos electrónicos por lo que estos hechos pueden ser objeto de prueba en el proceso jurisdiccional.

En tercer y último lugar, el hecho electrónico actúa en el proceso jurisdiccional como tal hecho. En definitiva el adjetivo electrónico no modifica los requisitos y exigencias legales que debe cumplir cualquier hecho para ser introducido y valorado en el proceso como prueba.

* * *

CAPÍTULO VI.- EL ACCESO DEL HECHO ELECTRÓNICO AL PROCESO

6.1 Concepto de prueba electrónica

La prueba electrónica no se diferencia, en esencia, del resto de medios de prueba, ya que tiene la misma y evidente finalidad que es la de probar en el proceso jurisdiccional la certeza de los hechos sometidos a enjuiciamiento. La diferencia, por tanto, se hallaría, exclusivamente, en la fuente de la prueba que se contiene en dispositivos electrónicos, informáticos y similares. Estos son máquinas modernas que tienen la particularidad de adquirir información y procesarla por medio de lenguajes propios no accesibles para el hombre común. De este modo, podemos decir que la prueba electrónica tiene su base y fundamento en la información procedente de los citados medios o dispositivos electrónicos. Así, probablemente toda la discusión sobre el concepto y naturaleza de la prueba electrónica deba basarse en un análisis del modo en el que la información contenida en los modernos aparatos electrónicos se documente y aporte al proceso para su debida valoración.

Desde este punto de vista, cabe señalar que la discusión sobre el concepto y naturaleza de la prueba electrónica debe tener en cuenta esas dos distintas fases de generación del hecho electrónico y de su documentación y aportación al proceso. La primera fase tiene una base y fundamento netamente técnico; mientras que la segunda debe analizarse desde presupuestos básicamente jurídicos. Así, cuando utilizamos terminología procesal como la que se refiere a la «*prueba de los hechos electrónicos*» nos referimos al modo en el que debemos introducir en el proceso los hechos que se manifiestan con los perfiles propios del lenguaje electrónico o digital. A saber, como impulsos electrónicos constituidos por códigos binarios, algoritmos o sistemas de encriptación. Toda esta información, en principio no aprehensible directamente por el ser humano, puede ser almacenada en soportes (en el disco duro de un ordenador, DVD, CD-Rom, pendrive, USB flash drive) y podrá ser aportada al proceso y valorada por el tribunal una vez se haya traducido de modo que sea perceptible y comprensible. El modo en el que se documente esta información basada en hechos electrónicos no se halla predefinida en nuestro sistema jurídico que parte de la base de la libertad de prueba. Siendo así, la parte puede dar cuenta del hecho electrónico mediante cualquier clase o medio de prueba previsto por la ley, aunque no cabe duda de que la forma más usual será la prueba

documental reforzada o complementada mediante una prueba pericial técnica que dé cuenta de todos los aspectos relativos al hecho electrónico[198].

Por lo tanto, desde un punto de vista estrictamente jurídico la prueba electrónica, viene referida a aquellos medios de prueba en los que se contiene y mediante los que se pretende probar en el proceso los hechos de naturaleza electrónica constitutivos de las pretensiones de las partes. Ahora bien, ello no significa que el jurista deba prescindir, absolutamente, de las cuestiones referidas a la naturaleza técnica del hecho electrónico, ya que, indudablemente, la debida valoración del hecho electrónico como prueba en el proceso debe tener en cuenta todos los factores relativos a su génesis, almacenamiento y documentación. Sólo así el tribunal podrá valorar debidamente y con todas las cautelas y garantías el hecho electrónico y las consecuencias que deba tener para la prueba y, en definitiva, para el otorgamiento de las tutelas pretendidas. Nótese que ésta es la función y finalidad del sistema de justicia.

Sin embargo, qué sea la «prueba electrónica» es una cuestión discutida en la doctrina, no resultando fácil hallar una definición que describa con rigor y precisión las características de este medio de prueba. En este sentido, la doctrina jurídica procesal ha venido manteniendo tres posiciones distintas en cuanto al concepto y naturaleza jurídica de la prueba electrónica[199]:

Una primera teoría, denominada autónoma, mantiene que la prueba electrónica y/o digital tiene una naturaleza propia, singular y diversa respecto de la regulada por los medios de prueba tradicionales y que le corresponden criterios de valoración propios (ÁLVAREZ-CIENFUEGOS SUÁREZ o MONTÓN REDONDO). Desde mi punto de vista, esta no es una teoría correcta, por cuanto, como se ha expuesto con anterioridad, los hechos electrónicos no dejan de ser hechos caracterizados por una especial singularidad técnica, sin que de ello se pueda o deba desprender una distinta forma de introducción en el proceso y, mucho menos, una diferente valoración por el tribunal. Efectivamente, el hecho electrónico tiene una idéntica finalidad a cualquier otro tratándose de objetos representativos de un hecho de interés para el proceso. De modo que el hecho electrónico, como cualquier otro, deberá introducirse, como veremos más adelante, a través de los medios de prueba ordinarios ya existentes.

---

[198] No es habitual pero también podría probarse la manifestación de un hecho electrónico mediante una prueba testifical. Así puede suceder, por ejemplo, en el caso de la testifical sobre pantallas de ordenador u otros dispositivos electrónicos que un testigo pueda haber visto y sobre los que, naturalmente, puede declarar. Véase sobre estos supuestos el § 9.3.

[199] Véase ILLÁN FERNÁNDEZ, M. ª, La prueba electrónica, eficacia y valoración en el proceso civil. Nueva oficina judicial, comunicaciones telemáticas (Lexnet) y el expediente judicial electrónico. Análisis comparado legislativo y jurisprudencial, ed. Aranzadi, Navarra, 2009, págs. 252-260.

Una segunda teoría, denominada analógica, considera que los medios de prueba tradicionales (documental) y los nuevos medios de prueba (medios de prueba audiovisuales e instrumentos informáticos) son de naturaleza equiparable y que en los nuevos medios de prueba el soporte electrónico o digital ha sustituido al papel. Se postula la aplicación directa, o en su caso analógica, de las normas sobre prueba documental y de las normas relativas al momento procesal de aportación (art. 265,269, 270 y 399.2 LEC), a la aportación de copias para las demás partes (art. 273 a 280 LEC), a la verificación o posicionamiento en la audiencia previa (art. 427.1 LEC) y al deber de exhibición documental (art. 328 y ss LEC)[200]. A ese fin desde esta posición doctrinal se pretende una superación de la concepción estricta del documento como «escrito en soporte de papel» para llegar a la idea de documento como «representación en cualquier soporte», y de este modo, subsumir los soportes magnéticos y electrónicos en el concepto jurídico de documento[201].

Tampoco esta teoría puede ser compartida, al menos completamente, ya que el hecho electrónico puede introducirse en el proceso mediante cualquiera de los medios de prueba ya existentes que responden a una idéntica finalidad: fijar en el proceso los hechos a efectos de la prueba de las pretensiones mantenidas

---

[200] Véase ABEL LLUCH, X., *La prueba electrónica,* ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.4, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, págs. 109-110.

[201] El Tribunal Supremo ha mantenido esta tesis en sentencias como la dictada por la Sala 1ª, de 12 junio 1999, Fto. Jco. 7º (RJ 1999\4735) al afirmar que *«[…] aunque nuestro ordenamiento jurídico-civil básico, tanto sustantivo, como procesal (Código Civil y Ley de Enjuiciamiento Civil), dada la antigüedad de su redacción, no contempla como posibles medios probatorios los mecanismos o elementos derivados de importantes avances y descubrimientos técnicos de los tiempos modernos, como son las cintas magnéticas, vídeos y cualquier otro medio de reproducción hablada o representación visual del pensamiento humano, los mismos aparecen admitidos por la jurisprudencia de esta Sala [Sentencias de 30 de noviembre de 1992 (RJ 1992\9458) y 2 de diciembre de 1996 (RJ 1996\8939), debiendo ser catalogados, dentro de la enumeración contenida en los artículos 1215 del Código Civil y 578 de la Ley de Enjuiciamiento Civil, como prueba documental asimilable a los documentos privados, por cuanto que, al igual que con éstos ocurre, si la parte a quien perjudiquen no los reconoce como legítimos, habrán de ser sometidos a la correspondiente verificación o comprobación, […] en la cinta de cassette a que nos venimos refiriendo es en lo que la entidad actora funda su derecho ejercitado en este proceso […] lo procedente era su inadmisión dado el momento en que fue presentada (período de proposición de prueba), al no haber sido acompañada con la demanda, como correctamente resolvió, en su momento, la Sala de apelación […]*». En el mismo sentido, y entre otras, la STS, Sala 1ª, de 30 de noviembre de 1992, fto. jco.1º (RJ 1992\9458) que, también precisa, en relación a dos cintas de vídeo que: «*…En todo caso su utilización probatoria exige siempre la necesaria y precisa adveración y certificación de autenticidad, veracidad y fidelidad que encuentra cauce procesal adecuado mediante el reconocimiento judicial, sometido a las reglas de procedimiento y valoración previstas*». También puede verse la SAP Baleares, secc. 4ª, de 28 de enero de 2002, fto. jco. 3º (JUR 2002\98428).

por las partes en el procedimiento jurisdiccional. Siendo así, como se ha expuesto, no existe ningún óbice o impedimento para probar un hecho electrónico mediante una prueba pericial o, incluso, testifical. Cuestión distinta será que, por lo general, el hecho electrónico se documentará en soportes técnicos que pueden equipararse, sin ninguna duda, al tradicional concepto de documento.

En tercer y último lugar, la llamada teoría de la equivalencia funcional, establece que aquella tecnología que permita cumplir las mismas funciones, que una determinada institución jurídica, debe recibir los mismos efectos. Es decir, comienza a tener importancia la función que cumpla, y no el medio que se emplee[202]. Desde el punto de vista, por ejemplo, del documento electrónico en virtud de la teoría de la equivalencia funcional toda declaración de voluntad asentada en un medio informático o electrónico tiene el mismo valor jurídico que los documentos cuyo soporte sea material, es decir, producen iguales efectos jurídicos y tienen igual fuerza probatoria que los tradicionales (art. 3.8 de la LFE y 24.2 de la LSSI). Coincidimos en que no es el concepto de documento el que cambia sino la forma en que éste se representa, es decir, lo que cambia es el soporte de dicho documento. Tratándose de documento siempre que evidentemente cumpla unos mínimos caracteres de inalterabilidad, que sea legible y permanezca en el tiempo.

Esta es precisamente la tesis que mantengo en este trabajo y que he expresado al inicio de este epígrafe. Lo que caracteriza a la prueba electrónica frente a los demás tipos de prueba es que su objeto es probar un hecho de naturaleza electrónica que tenga relación con la pretensión de la parte y que pueda ser valorada por el juez. Los hechos de naturaleza electrónica pertenecen a la realidad y no pueden enumerarse son ilimitados, evolucionan con las tecnologías y se amplían en número con el tiempo. En el ámbito del derecho esos hechos de naturaleza electrónica pueden acceder al proceso mediante cualquier medio de prueba de los expresamente previstos por la ley, en cuanto los medios de prueba son tasados y son los previstos en el artículo 299.1 y 2 LEC. Y si tales hechos de naturaleza electrónica pueden cumplir iguales funciones que otras instituciones jurídicas deben suponer iguales efectos.

[202] Véase BERNING PRIETO, ANTONIO DAVID, *Derecho de la Contratación electrónica* en Artículos Doctrinales: Derecho Informático, Noticias Jurídicas, Junio 2008). Puede consultarse este artículo en la dirección electrónica http://goo.gl/CfJb1V, página visitada el 26.7.2013.

6.2 Objeto y finalidad de la prueba electrónica

El objeto principal de la prueba electrónica en el proceso serán los «hechos electrónicos» es decir, «*la información obtenida a partir de un dispositivo electrónico o medio digital*» que es introducida al proceso por la parte a través de los respectivos escritos y alegaciones[203]. La finalidad que persigue la prueba electrónica es probar o acreditar hechos o una actividad que fundamenta o tiene relación con la tutela pretendida en el proceso jurisdiccional.

La prueba electrónica no siempre se explica y define bien. Probablemente la causa de esta dificultad se halle en la complejidad de los fenómenos y actividades electrónicos frente a la multiplicidad de manifestaciones de los mismos en la vida cotidiana. Efectivamente, resulta fácil dar cuenta de la recepción de un correo electrónico que puede documentarse en un simple papel, que podrá servir como prueba documental en un proceso. Así lo hemos expuesto en el epígrafe anterior en el que se defendía que el hecho electrónico puede probarse de distintos modos y mediante los distintos medios de prueba previstos en la Ley. Ahora bien, cuestión distinta será acreditar en el proceso de forma eficaz el sistema técnico de envío y recepción del correo electrónico mediante el examen de los servidores y computadores. La prueba de estos hechos, estos sí, de carácter absolutamente técnico, sólo podrá hacerse mediante una prueba pericial informática en la que se deberán analizar y valorar hechos de naturaleza electrónica. Así, podemos decir que si bien las partes pueden dar cuenta del hecho electrónico mediante cualquier clase o medio de prueba, la prueba capaz de hacerlo en todos los aspectos relativos al hecho electrónico es una prueba pericial técnica. Por ello, incluso cuando la parte aporte prueba documental ésta usualmente vendrá reforzada o complementada mediante una prueba pericial.

6.3 Soporte material del hecho electrónico

El soporte material de un hecho electrónico puede definirse como el sustrato o base en el que éste se contiene y que puede ser objeto de prueba en el proceso jurisdiccional. Estos soportes suelen ser dispositivos de almacenamiento de datos, documentos o de registro de sucesos, que dan cuenta de la actividad

[203] Véase, en este sentido, la Decisión 2002/630/JAI del Consejo que establece que por prueba electrónica debe entenderse: «*la información obtenida a partir de un dispositivo electrónico o medio digital el cual sirve para adquirir convencimiento de la certeza de un hecho*». Decisión 2002/630/JAI del Consejo, de 22 de julio de 2002, relativa a la cooperación policial y judicial en materia penal (AGIS), Diario Oficial L 203, de 1 de agosto de 2002.

electrónica producida en un determinado tiempo. Ello sin perjuicio de poder realizar una pericia técnica en tiempo real del comportamiento de un determinado sistema informático. En cualquier caso, debemos distinguir los dispositivos técnicos que realizan las actividades programadas para cada máquina, de los dispositivos terminales que ofrecen los resultados en forma de imagen o de documento escrito. Desde este punto de vista, debemos tener clara la diferencia entre la actividad electrónica que se produce mediante fenómenos físicos de esa naturaleza y los resultados ofrecidos en los terminales de salida de datos que se ofrecen, por ejemplo, en una imagen.

En primer lugar, el principal soporte del hecho electrónico se contiene en los dispositivos de almacenamiento. Estos soportes pueden contener información esencial para fundamentar hechos de relevancia en el proceso, más allá de la que ofrece el resultado de la actividad electrónica. Así, no cabe duda de que una fotografía digital es el resultado de la aplicación de la técnica electrónica e informática al procedimiento de captación y almacenamiento de imágenes. Así hemos pasado de una técnica química, que es la tradicional de la fotografía a una técnica electrónica. Naturalmente que la fotografía digital obtenida puede servir como prueba documental sin mayores requisitos. Ahora bien, si lo que se pretende es acreditar además el tiempo exacto e incluso el lugar en el que se realizó una concreta fotografía lo indicado será obtener un análisis de los metadatos asociados a la fotografía que se pueden obtener del dispositivo que la obtuvo. Estos datos son una suerte de registros electrónicos que dan cuenta del tiempo e incluso, cuando se trate de una imagen obtenida en un teléfono móvil, del lugar donde se obtuvo la imagen. Pues bien esos metadatos sólo pueden ser captados mediante técnicas específicas de análisis pericial a partir de los soportes de almacenamiento de cada dispositivo.

El concepto de «medio o soporte de almacenamiento» debe distinguirse del concepto de «unidad o dispositivo de almacenamiento». El medio o soporte de almacenamiento es donde se escriben o leen los datos, en tanto la unidad o dispositivo de almacenamiento es la que se encarga de leer o escribir esos datos. Por ejemplo, un CD o un disquete son medios, en tanto una unidad lectora de CD o una unidad lectora de disquete son unidades o dispositivos de almacenamiento de esos medios respectivamente. Estos dispositivos realizan las operaciones de lectura o escritura de los medios o soportes donde se almacenan o guardan, lógica y físicamente, los archivos de un sistema informático.

Los soportes y dispositivos de almacenamiento pueden clasificarse en Magnéticos, Ópticos, Óptico-magnéticos y electrónicos. Con la expresión «almacenamiento óptico» nos referimos a aquellos dispositivos que son capaces de guardar datos por medio de un rayo láser en una superficie plástica,

almacenándose por medio de ranuras microscópicas (o ranuras quemadas). La información queda grabada en la superficie del soporte de manera física, por lo que solo el calor (puede producir deformaciones en la superficie del disco) y las ralladuras pueden producir la pérdida de los datos, siendo en cambio inmune a los campos magnéticos y la humedad. La principal función de los dispositivos de almacenamiento por medio óptico es almacenar archivos multimedia, como música, fotos y videos. Además de eso, son bastante utilizados para almacenar programas de computadoras, juegos y aplicaciones comerciales. Son soportes o medios de almacenamiento óptico: el *Disco óptico*, es un formato de almacenamiento de datos digital, que consiste en un disco circular en el cual la información se codifica, se guarda y almacena, haciendo unos surcos microscópicos con un láser sobre una de las caras planas que lo componen); el *Compact Disc (CD)*; el *Digital Versatile Disc (DVD)*; el *HD DVD*; el *Blu-Ray Disc*, también conocido como Blu-ray o BD, es un formato de disco óptico de nueva generación desarrollado por la BDA (siglas en inglés de Blu-ray Disc Association), empleado para vídeo de alta definición y con una capacidad de almacenamiento de datos de alta densidad mayor que la del DVD, hace uso de un rayo láser de color azul con una longitud de onda de 405 nanómetros, a diferencia del láser rojo utilizado en lectores de DVD, que tiene una longitud de onda de 650 nanómetros, esto, junto con otros avances tecnológicos, permite almacenar sustancialmente más información que el DVD en un disco de las mismas dimensiones y aspecto externo; el *Universal Media Disc (UMD,* disco universal de medios o UMD) es un disco óptico desarrollado por Sony conocido sobre todo por su uso en la PlayStation Portable (PSP) que puede contener 900 MB de datos, 1,8 GB en doble capa, pudiendo incluir juegos, películas, música, o combinaciones de estos elementos; y las *Memorias ópticas*[204].

Por otro lado, nos referimos a «almacenamiento magnético» respecto a aquellos dispositivos de almacenamiento de datos en los que se utilizan propiedades magnéticas de los materiales para almacenar información digital. La tecnología magnética consiste en la aplicación de campos magnéticos a ciertos materiales cuyas partículas reaccionan a esa influencia, generalmente orientándose en unas determinadas posiciones que conservan tras dejar de aplicarse el campo magnético. Esas imágenes representan datos (imagen, números, música). Son soportes o medios magnéticos: *la Cinta Magnética*, que está formada por una cinta de material plástico recubierta de material ferromagnético y sobre la que se registran los caracteres en formas de combinaciones de puntos, sobre pistas paralelas al eje longitudinal de la cinta - estas cintas son soporte de tipo secuencial, esto supone un inconveniente puesto que para acceder a una información determinada se hace necesario leer

[204] Información obtenida de Wikipedia. Puede consultarse este contenido en la dirección electrónica http://goo.gl/DZo9fZ (visionado el 5.8.2013)

todas las que le preceden, con la consiguiente pérdida de tiempo-; el *Disco Duro,* que es en la actualidad el principal subsistema de almacenamiento de información en los sistemas informáticos, tratándose de un dispositivo encargado de almacenar información de forma persistente en un ordenador, es considerado el sistema de almacenamiento más importante del computador y en él se guardan los archivos de los programas; *los Disquete o Disco flexible*, que es un tipo de dispositivo de almacenamiento de datos formado por una pieza circular de un material magnético que permite la grabación y lectura de datos, fino y flexible (de ahí su denominación) encerrado en una carcasa fina cuadrada o rectangular de plástico -los discos, usados usualmente son los de 3 ½ o 5 ¼ pulgadas, utilizados en ordenadores o computadoras personales, aunque actualmente los discos de 5 ¼ pulgadas están en desuso-[205].

Algunos soportes o medios combinan ambas tecnologías, es decir, son dispositivos de almacenamiento híbridos, por ej., *discos Zip*.

Finalmente podemos distinguir entre distintos dispositivos de «almacenamiento electrónico», que utilizan circuitos electrónicos para guardar la información. Entre estos dispositivos podemos citar los denominados «pendrives» y tarjetas de memoria, que se utilizan masivamente en computadoras, cámaras digitales y teléfonos celulares. Técnicamente, se pueden calificar como unidades de estado sólido (SSD, acrónimo en inglés de solid-state drive), que son dispositivos de almacenamiento de datos que usan técnicas de almacenamiento de datos basadas en hardware no mecánico, como es el caso de los platos giratorios magnéticos que utilizan los discos duros convencionales. Una memoria de estado sólido es un dispositivo de almacenamiento secundario hecho con componentes electrónicos destinada para utilizarse en equipos informáticos en lugar de una unidad de disco duro convencional, como memoria auxiliar o para crear unidades híbridas compuestas por SSD y disco duro.

Los soportes de almacenamiento de información en realidad lo que contienen son copias de información. En este sentido las huellas insertas en la memoria RAM de un ordenador son volátiles, pero terminan volcándose en el disco duro del mismo que podemos considerar como original, aunque estrictamente no dejaría también de ser una copia. Y dado que es poco operativo aportar un ordenador se suelen grabar dichas huellas en soportes como disquetes, CD, pendrive etc. Este tipo de soportes sirven para conservar el hecho electrónico que probablemente accederá al proceso como prueba documental o anexada a un dictamen pericial (art. 336.2 LEC).

[205] Información obtenida de Wikipedia.). Puede consultarse este contenido en la dirección electrónica http://goo.gl/xftUo4 y http://goo.gl/THDCRx (visionado el 5.8.2013).

En segundo lugar, el hecho electrónico también puede ser captado, analizado y ser objeto de una pericia a partir de un análisis de dispositivos en funcionamiento. En este caso, el perito podrá realizar su dictamen con base en los hechos electrónicos que se están produciendo en tiempo real y que, naturalmente, pueden ser objeto de análisis y posterior valoración en un dictamen pericial. Téngase en cuenta que la naturaleza de las partículas electrónicas tiende siempre a la estabilidad, de modo que los efectos concretos de la circulación electrónica dejaran de ser evidentes una vez se proceda a la desconexión del aparato de que se trate. Este es el caso de la memoria RAM (*random aleatory memory*) de cualquier ordenador que, naturalmente, se disipa una vez que se ha procedido al apagado del aparato.

Finalmente, y tal y como se ha expuesto con anterioridad, debemos distinguir entre el soporte y el medio de reproducción. Para poder leer o hacer aprehensible al hombre la información electrónica contenida en un soporte electrónico se requerirá una unidad lectora del mismo (por ejemplo la lectora de CD, también llamada reproductor de CD, que es un dispositivo óptico capaz de reproducir los CD de audio, de video, de datos, etc. utilizando un láser que le permite leer la información contenida en dichos discos) y otros instrumentos como por ejemplo una pantalla (hardware) o determinados programas o sistemas operativos (software). Ahora bien, una unidad lectora, un monitor o un televisor no almacenan ni contienen hechos electrónicos, salvo durante el tiempo en el que se hallan en funcionamiento y salvo, naturalmente, que el dispositivo de reproducción pueda tener integrado un sistema de registro o grabación. Ese será el caso, por ejemplo, de una cámara digital que contenga imágenes grabadas en su memoria interna. Es a estos soportes y medios de reproducción a los que se refiere el apartado 2 del artículo 299 de la LEC cuando se alude a los «*…medios de reproducción de la palabra, sonido y la imagen, así como a los instrumentos que permitan archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso*», confundiendo soporte material o medio de reproducción con medio de prueba.

La Ley de Enjuiciamiento Civil no da cuenta de la amplia realidad que supone el hecho electrónico de un modo adecuado. No tiene en cuenta que la prueba electrónica se fundamenta en hechos de naturaleza electrónica que deberán ser introducidos en el proceso mediante los medios de prueba. Y al confundir, además, la terminología lo que hace es limitar el concepto de prueba electrónica. El artículo 299 apartado segundo de la LEC pretende por una parte englobar en determinados conceptos la realidad que supone el hecho electrónico sin tener en cuenta que dicha realidad es ilimitada y que dicha terminología es inadecuada para describir los conceptos que pretende; y en segundo lugar confunde además esos conceptos con medio de prueba. Veamos

un ejemplo. Cuando la parte muestra una imagen a través de un medio de reproducción estamos ante una prueba documental, puesto que la imagen en nuestro lenguaje es «documento»; cuando lo que se ha hecho es analizar el contenido de la cámara, nos hallamos, en sentido estricto, ante una prueba electrónica.

6.4 La aportación del hecho electrónico al proceso jurisdiccional

En un primer momento pudiera pensarse que el hecho electrónico como tal únicamente pudiera acceder al proceso mediante una prueba pericial. Ahora bien, esto será así siempre que nos estemos refiriendo al hecho electrónico en su acepción más técnica, porque no cabe duda que la plasmación de hechos electrónicos en documentos o imágenes podrá acceder al proceso mediante una prueba documental[206]. Más aún, también cabe dar cuenta de la manifestación de un hecho electrónico por medio de la declaración de un testigo que puede dar cuenta de haber visto en una pantalla un determinado correo electrónico o, por ejemplo, una determinada medida o lectura en cualquier dispositivo electrónico. Ahora bien, la clave consiste en distinguir entre el hecho electrónico tal cual es en su auténtica naturaleza y su manifestación en forma de documento o imagen aprehensible para los seres humanos. En este segundo caso no podemos, *estricto sensu*, hablar de hecho electrónico, sino de documentos electrónicos.

Esta diferenciación se debe aplicar distinguiendo entre las manifestaciones del hecho electrónico que se podrán acreditar directamente mediante el art. 299.2 LEC, es decir, a través de los «*…medios de reproducción de la palabra, sonido y la imagen, así como a los instrumentos que permitan archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso*» y el mismo hecho electrónico que deberá acreditarse mediante la prueba pericial a través del dictamen de peritos (art. 299.1.4º).

En el primer caso, cuando el hecho electrónico se manifiesta a través de un resultado, como puede tratarse de una imagen, el único límite en cuanto a la forma de aportación de dicho documento electrónico al proceso lo constituye la exigencia legal que lo aportado pueda ser examinado por el tribunal y las partes con pleno respeto a las garantías de inmediación y contradicción (art. 384.1 LEC)

[206] No podemos considerar una imagen en una pantalla como prueba electrónica al igual que no consideramos la fotografía de una herida prueba médica.

principios fundamentales en un proceso judicial con todas las garantías[207]. Las partes acreditarán dicho documento en el proceso mediante la aportación de medios o soportes de almacenamiento de datos, documentos o de registro de sucesos acompañados de las unidades o dispositivos de reproducción que sean necesarios para obtener el resultado final que pretendemos visualizar y que es el objeto de aportación a juicio, es decir, el documento[208]. Ello permite que las demás partes en el proceso puedan «*…con idéntico conocimiento que el tribunal, alegar y proponer lo que a su derecho convenga*» (art. 384.1 LEC in fine), y permite al tribunal valorar en sentencia la prueba propuesta por la parte en fundamento de su pretensión. Las peculiaridades propias del hecho electrónico, que ya tratamos en el § 5, hacen necesario aportar dichos soportes de almacenamiento y dispositivos de reproducción para que dicho documento acceda al proceso y pueda ser visualizado por las partes y el tribunal[209].

---

[207] Véase al respecto PÉREZ GIL, J., *Documento informático y firma electrónica: aspectos probatorios,* en "El comercio electrónico", Echevarría Sáenz, J.A. (coord.), ed. Edisofer, Madrid, 2001, pág. 234.

[208] En derecho comparado, la Ley chilena 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, que reconoce expresamente a los documentos en formato electrónico naturaleza propiamente documental, señala que estas pruebas se acompañan con citación y establece que el juez deberá establecer cómo se debe dejar constancia en el proceso de ellas cuando requieran operaciones técnicas especiales para su producción, pudiendo para ello designar un asesor técnico. Luego señala que si la prueba fuera ofrecida por algunas de las partes y el juez lo estimare conveniente, éste deberá suministrar el personal y los instrumentos necesarios para producir prueba. Concluye el artículo señalando que de contar el tribunal con los instrumentos requeridos, y de no necesitarse la presencia de un técnico, procederá a realizar la prueba por sí mismo. CANELO, C., ARRIETA, R., MOYA, R., ROMO R. *Documento electrónico, aspectos procesales*. Revista Chilena de Derecho Informático, pág. 98. Puede consultarse en la dirección electrónica http://goo.gl/lPBXt

[209] El documento electrónico se diferencia del documento contenido en el soporte tradicional del papel, en que el documento en soporte de papel se manifiesta mediante caracteres alfabéticos, ilustraciones etc. y no puede incorporar sonidos, en él soporte y contenido se mantienen siempre unidos, siendo la estructura parte integral del documento y los metadatos del contexto y de la estructura inherentes al mismo. En cambio en el documento electrónico el soporte de almacenamiento de información electrónica puede separase de su contenido, tiene un formato determinado, susceptible de identificación y tratamiento diferenciado, y la información se halla escrita en el mismo en un lenguaje distinto del tradicional, pudiendo incorporar sonidos.

El documento creado tradicionalmente en soporte de papel posteriormente puede ser digitalizado por medio de un escáner para ser utilizado y conservado en un soporte digital. En este caso transforma una información consignada en forma analógica en una secuencia de valores numéricos, es decir, en una representación electrónica que se puede almacenar y acceder por medio de una computadora; fotografía electrónicamente una información dividiéndola en miles de elementos llamados píxeles, representados por ceros y unos. La digitalización del documento en papel permite economizar recursos, facilita el tráfico mercantil y mejora la productividad. No obstante, para la validez en el tráfico mercantil de la digitalización certificada es necesaria la autorización expresa de un proceso de digitalización de

Simplemente recordemos aquí que el hecho electrónico en esencia consiste, sencillamente, en el desplazamiento de electrones y que como tal precisa de técnicas y dispositivos de captación, reproducción y/o traducción para su manifestación y percepción por nuestros sentidos. Así, el hecho electrónico se puede contener y/o, conservar en soportes de distinta clase y naturaleza (óptico, magnético) o representarse a través de un dispositivo terminal como una pantalla, impresora etc. La necesidad de aportar tales dispositivos obedece, pues, a que los hechos electrónicos se contienen en soportes técnicos a los que no se puede acceder mediante los sentidos humanos, de modo que, por lo general, se requerirá de un aparato para captar, medir o interpretar el hecho electrónico. Este sería el supuesto, por ejemplo, de los datos informáticos para cuya captación y entendimiento se requiere de programas especializados (software) y de unos aparatos técnicos (hardware). Igual sucede con las señales electromagnéticas analógicas o digitales que contienen y transportan la voz humana que precisan de aparatos sintonizadores y reproductores de radio al efecto de su escucha y entendimiento.

La Ley de Enjuiciamiento Civil regula los soportes de almacenamiento y los medios de reproducción erróneamente como medios de prueba en la enumeración que efectúa en el artículo 299 LEC y los enumera junto a los demás medios de prueba entre los que se hallan la documental pública y la documental privada, efectuando una equiparación entre el régimen de aportación de la prueba por medios e instrumentos a la de los documentos[210]. La proposición, práctica y valoración de la prueba a través de dichos «*soportes de almacenamiento de información*» y de «*medios de reproducción*» se desarrolla en la sección 8ª del Capítulo VI del Libro II de la Ley de

---

la documentación de facturación que permite la destrucción del papel. Ello ha sido objeto de regulación, siendo normativa aplicable: el RD 1496/2003, de 28 de noviembre, Reglamento por el que se regulan las obligaciones de facturación, en su artículo 21 se refiere a la conservación de las facturas o documentos sustitutivos por medios electrónicos; la Orden EHA/962/2007, de 10 de abril, que desarrolla determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas (art. 7: Digitalización certificada de facturas recibidas); la Resolución de 24 de octubre de 2007, que regula el procedimiento de digitalización certificada de facturas; y La Orden PRE/2794/2011, de 5 de octubre, por la que se publica el acuerdo del Consejo de Ministros, de 10 de octubre de 2011, que determina el marco de ejercicio de las competencias estatales en materia de factura electrónica, se crea el Foro nacional multilateral sobre facturación electrónica y se impulsa el Servicio Central de Facturación electrónica en el ámbito de la Administración del Estado. Además la estrategia "Europa20" de la Comisión Europea incluye entre sus prioridades el desarrollo de una economía basada en el conocimiento y la innovación que haga un uso más eficaz de los recursos, siendo la digitalización y automatización de procesos administrativos un factor clave en la mejora de la productividad de la economía. En este sentido destaca en España en el sector público la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

[210] Recordemos que en realidad los documentos son fuente de prueba y no medio de prueba, aunque la Ley de Enjuiciamiento Civil los regula como medios de prueba en su artículo 299.

Enjuiciamiento Civil, cuya rubrica reza «*De la reproducción de la palabra, el sonido y la imagen y de los instrumentos que permiten archivar y conocer datos relevantes para el proceso*» (artículos 382 a 384 LEC).

La LEC distingue entre los «medios de reproducción» regulados en el artículo 382 y 383 y los «instrumentos de archivo» a los que se refiere en el artículo 384. En cuanto a los primeros establece el artículo 382 LEC que «*1. Las partes podrán proponer como medio de prueba la reproducción ante el tribunal de palabras, imágenes o sonidos captados mediante instrumentos de filmación, grabación y otros semejantes*» y en cuanto a los instrumentos de archivo regula el artículo 384 que «1. *Los instrumentos que permitan archivar, conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, que por ser relevantes para el proceso, hayan sido admitidos como prueba, serán examinados por el tribunal por los medios que la parte proponente aporte o que el tribunal disponga utilizar*…». La sistemática, la redacción y la terminología utilizada es confusa e inadecuada, como señalábamos con anterioridad, mostrando un desconocimiento de la realidad del hecho electrónico. Confunde «reproducción» con «medio de prueba», y utiliza indiscriminada e inadecuadamente los términos «medio de reproducción» y «soporte», efectuando una distinción confusa entre «los instrumentos de filmación, grabación y semejantes» y «los instrumentos que permitan archivar, conocer o reproducir palabras, cifras y operaciones matemáticas relevantes para el proceso». No insistiremos en este tema que tratamos con mayor amplitud en el § 6.3.

Lo que nos interesa en este punto es el acceso al proceso de la manifestación del hecho electrónico. En este sentido debemos precisar que dicha manifestación o resultado visible del hecho electrónico a través de una imagen, por ejemplo, se efectuará con la aportación del correspondiente medio o soporte de almacenamiento acompañado de unidades o dispositivos de reproducción que sean necesarios y que la parte proponente aporte (art. 382 y 384 LEC) o que el tribunal disponga utilizar (art. 384 LEC). Nótese que algunos dispositivos o aparatos llevaran integrado tanto el medio o soporte de almacenamiento como las unidades o dispositivos de reproducción (unidad lectora, hardware o software) y algunos otros requerirán que éstos sean aportados por las partes o como señala el propio artículo 384 LEC sea el tribunal quien acuerde «los medios» a utilizar, es decir, los dispositivos de reproducción que sean necesarios para que el hecho electrónico sea visible al ser humano y pueda ser valorado por el juez en el proceso judicial.

El legislador no ha previsto legalmente y de un modo tasado las clases de soportes de almacenamiento que pueden ser aportados ni los dispositivos o unidades de reproducción que puedan ser propuestos. Previsión legal lógica

ante la eventualidad que cualquier enumeración devendría obsoleta un poco tiempo. Es evidente, que por comodidad y en la medida de lo posible las partes intentarán aportar soportes o medios de almacenamiento de pequeño formato (CD, DVD, pendrive), aunque nada impide que se aporte, por ejemplo, el disco duro de un ordenador.

En el supuesto el hecho electrónico se manifieste formalmente «en palabras» la ley permite a la parte con carácter facultativo aportar únicamente el soporte informático sin transcripción de su contenido o bien acompañar transcripción escrita de las palabras contenidas en el soporte de que se trate y que resulten relevantes para el caso (art 382.1). Este será el caso de las filmaciones o grabaciones en las cuales se contienen declaraciones verbales que pueden ser aprehendidas directamente por el juzgador. En el acta de reproducción y custodia el tribunal también podrá acordar mediante providencia la transcripción siempre que sea relevante para el caso, y que se unirá al acta (art 383.1 segundo párrafo). Será necesaria la reproducción o «lectura» por el secretario judicial a efectos de su constancia en las actuaciones. Dispone el artículo 383.2 LEC que « 2. *El material que contenga la palabra, la imagen o el sonido reproducidos habrá de conservarse por el Secretario Judicial, con referencia a los autos del juicio, de modo que no sufra alteraciones*».

Por otro lado, si bien un documento electrónico puede ser visualizado a través del «pantallazo» en una computadora u otro dispositivo lo cierto es que en muchas ocasiones resulta mucho más cómodo el volcado de la información electrónica a través de la «impresión» en un soporte de papel. Tal posibilidad, cada vez más frecuente en la práctica forense, se ha sugerido en alguna resolución de la jurisprudencia menor con fundamento en permitir una «mayor accesibilidad» al contenido del documento en soporte electrónico (SAP Santa Cruz de Tenerife de 18 de noviembre de 2009[211]). Sin embargo, en este caso la jurisprudencia viene dando a dicha impresión el valor *de copias o reproducciones fotostáticas*, quedando sometidas al artículo 326 LEC. Conforme a dicho artículo, sólo harán prueba plena en el proceso si no han sido impugnadas por la parte a quien perjudiquen. En otro caso, siendo impugnada su autenticidad y no previendo dicho artículo más que el cotejo pericial de letras u otra prueba en el supuesto de documento tradicional en papel, manuscrito y firmado de forma autógrafa, serán de aplicación las reglas de la sana crítica[212].

---

[211] La SAP de Santa Cruz de Tenerife, secc.4ª, de 18 de noviembre de 2009, en su fto. jco.2º (JUR 2010\77692) afirma: «*…se podría precisar que la copia del documento multimedia debe aportarse con ese soporte (y a través del medio adecuado –pendrive, por ejemplo-) y no en papel, pero su traslado a éste puede representar, de igual modo y para permitir una mayor accesibilidad, una transcripción adecuada en ese soporte del mismo documento*».

[212] MONTÓN REDONDO considera que la «impresión» es una reproducción escrita del instrumento informático que hace las veces de simple documento, de modo que, de ser

En el segundo caso, es decir, el acceso al proceso del hecho electrónico en sentido técnico solo podrá tener lugar a través de la prueba pericial, regulada en la Sección 5ª del Capítulo VI, Título I del Libro II, rubricada «*Del dictamen de peritos*». La prueba pericial es la única prueba capaz de documentar el hecho electrónico en sí en el proceso y hacerlo accesible a las partes o al tribunal, explicar su génesis, la actividad electrónica producida y su resultado. El perito será con sus conocimientos técnicos la única persona cualificada para estudiar el fenómeno físico de la circulación electrónica en cada uno de sus resultados concretos utilizados en multitud de máquinas y dispositivos ya tengan por finalidad el tratamiento y/o procesamiento de la información o no y hacerla accesible a las partes y al tribunal. Lo más frecuente es que se trate de periciales efectuadas sobre dispositivos que procesen información. En tal caso el perito realizará un estudio sobre los dispositivos implicados siguiendo una rutina de investigación consistente en el análisis preliminar, la adquisición de datos y el análisis forense que le llevarán a formular las correspondientes conclusiones debidamente contenidas en el dictamen pericial. Precisamente junto al mismo acostumbrará a acompañar tal y como prevé el artículo 336.2 LEC «*los demás documentos, instrumentos o materiales adecuados para exponer el parecer del perito sobre lo que haya sido objeto de pericia*». Lo que en prueba electrónica incluye los soportes de almacenamiento con datos de interés. Resaltar que, en concreto, respecto a la pericial informática cuando el perito deba realizar para la adquisición de datos copias espejo de otro medio o soporte a los efectos de poder efectuar el análisis forense, realizará un resumen digital o «hash» para garantizar la no alterabilidad de los hechos electrónicos copiados y contenidos en el soporte. Todo ello constará anexado y descrito en su dictamen pericial, permitiendo que a través de dicho medio de prueba la parte haga llegar al proceso esos hechos electrónicos poniéndolos en conocimiento de las demás partes y del juez a los efectos de que puedan ser valorados por este último.

* * *

reconocido, haría innecesaria la reproducción directa del contenido a presencia judicial. Véase MONTÓN REDONDO, A., *Medios de reproducción de la imagen y del sonido*…, ob. cit. pág.196.

CAPÍTULO VII.- LA PRUEBA PERICIAL ELECTRÓNICA

7.1 Concepto

La prueba pericial puede definirse en general como aquella actividad procesal, en virtud de la cual personas expertas transmiten al juez conocimientos especializados en determinados campos de la ciencia, el arte, la técnica o prácticos para que aquél pueda valorar hechos o circunstancias relevantes en el asunto sobre el que versa el pleito o adquirir certeza sobre los mismos[213].

Cuando dicha actividad procesal transmite al juez conocimientos científicos, técnicos o prácticos para que éste pueda valorar o adquirir certeza sobre hechos electrónicos podemos hablar de «*prueba pericial electrónica*».

La Ley de Enjuiciamiento Civil no emplea la expresión «prueba pericial» sino que regula el «dictamen de peritos» en la Sección 5ª dentro del Capítulo VI del Título I del Libro II de dicho cuerpo legal como medio de prueba (art. 299.1.4º). Ello probablemente porque el conocimiento científico, artístico, técnico o práctico de que disponen determinadas personas consideradas expertas en un determinado campo constituye «*fuente de prueba*», mientras que el modo a través del cual dicho conocimiento llega al proceso es el dictamen de peritos, que constituye «*medio de prueba*».

La pericial electrónica versa sobre hechos electrónicos. Tales hechos se manifiestan con los perfiles propios del lenguaje electrónico o digital, es decir, como impulsos electrónicos constituidos por códigos binarios, algoritmos o sistemas de encriptación. Toda esta información, en principio no aprehensible directamente por el ser humano, puede ser almacenada en soportes (en el disco duro de un ordenador, DVD, CD-Rom, pendrive, USB flash drive) electrónicos o no y podrá ser aportada al proceso y valorada por el tribunal una vez se haya traducido de modo que sea perceptible y comprensible. El hecho electrónico no puede verse, ni puede interpretarse sin conocimientos técnicos. El conocimiento, estudio e interpretación de la actividad electrónica, entendida no solo como el hecho electrónico en sí sino todo aquello relacionado con su actividad como, por ejemplo, el estudio de los metadatos que quedan registrados en determinados dispositivos electrónicos como consecuencia de dicha actividad electrónica, requiere de conocimientos técnicos, científicos y prácticos específicos que probablemente excedan del conocimiento medio general de un juez. Por lo tanto, la única prueba capaz de acreditar estos hechos

[213] Existen muchísimas definiciones de prueba pericial ABEL LLUCH efectúa una síntesis reciente de dichas definiciones. Véase ABEL LLUCH, X., Derecho Probatorio, J. M. Bosch editor, Barcelona, 2012, nota a pie de página núm.2048, en págs. 653-654.

en todos sus aspectos técnicos, y entendidos como la actividad electrónica producida, es la prueba pericial, capaz de identificar, analizar, acreditar y explicar los datos generados como consecuencia de la actividad electrónica. El dictamen pericial facilitará al juez el estudio sobre la existencia de determinada actividad electrónica en medios y dispositivos de igual naturaleza, a la vez que podrá acreditar la autenticidad, inalterabilidad e integridad del hecho electrónico de la manifestación de éste (art. 382.2 y 384.2 LEC)[214]. A través del dictamen pericial el experto trasladará sus conocimientos técnicos y científicos al juez, su aplicación práctica al caso concreto y los razonamientos que le llevan a alcanzar determinadas conclusiones, acompañándose de los «*…documentos, instrumentos o materiales adecuados para exponer el parecer del perito sobre lo que haya sido objeto de pericia»* (art. 336.2 LEC). El juez obtendrá valorada dicha prueba sus conclusiones, tratándose las reglas de la experiencia técnica de un instrumento de integración del juicio lógico del juez.

La prueba pericial electrónica pretende, pues, acreditar la actividad electrónica que se genera. De este modo cuando visualizamos la imagen en la pantalla de un ordenador dicha prueba no acredita la actividad electrónica generada, ya que solo somos capaces de visualizar el resultado de un proceso electrónico anterior, sin saber cuál es, ni de dónde procede, ni de qué información ha partido el ordenador para poder procesar y ofrecer ese resultado a través de ese periférico. Para que el juez pueda efectuar una valoración de dicha actividad debería tener conocimientos informático-forenses y llevar a cabo un análisis del proceso seguido por el ordenador y de los datos informáticos obrantes e el mismo, por lo tanto si el objeto de la prueba es la actividad electrónica generada será necesario que la parte proponente acuda a la prueba pericial.

---

[214] La LEC prevé la posibilidad de aportar prueba pericial con el objeto de acreditar la autenticidad o exactitud del hecho electrónico reproducido (art. 382.2 y 384.2 LEC), con fundamento en ello doctrinalmente viene distinguiéndose por algunos autores entre la llamada «pericial instrumental», es decir, aquella pericial cuya finalidad es hacer conocer el contenido o sentido de una prueba o su acertada valoración (art. 352 LEC) -por ejemplo para determinar si la firma digital corresponde a una determinada persona; y la llamada «pericial autónoma», es decir, aquella que no resulta supeditada a otros medios -por ejemplo, aquella que se aporta para acreditar el número de visitas de una página Web-. La denominada «pericial instrumental» ha sido denominada por GUASP prueba secundaria o de segundo grado, dicho autor la definía como aquélla que tiene por objeto convencer al juez de la verdad o falsedad de otra prueba practicada en el mismo proceso anteriormente. MUÑOZ SABATÉ quien cita al anterior la denomina «prueba sobre la prueba». MUÑOZ SABATÉ, Ll., *Fundamentos de la Prueba judicial civil LEC 1/2000,* J.M. Bosch Editor, Barcelona 2001, pp. 95 y ss. Dicha distinción entre pericial «autónoma» e «instrumental» nos parece inadecuada por cuanto si bien es cierto que una prueba pericial puede «complementar» a otra prueba como una documental por ejemplo, ello no significa que sea «complementaria» a la misma.

Un correo electrónico impreso no es prueba electrónica, es prueba documental. Cuando el experto en informática-forense efectúa un análisis del correo enviado en un ordenador, su análisis consiste en una serie de datos en un archivo informático, que no sólo contienen el texto del mensaje, sino un «encabezado de Internet», que contiene gran cantidad de información relevante, incluyendo el recorrido que ha hecho por Internet desde el emisor hasta el receptor (hora y fecha de envío, dirección electrónica de envío y de destino, asunto del mensaje, protocolo informático etc.), todos ellos datos que verifican la autenticidad del correo. A su vez, además de los «*logs*» (registros) que archivan los correos electrónicos analizaría otras fuentes como las copias de seguridad para asegurar que no han sido objeto de manipulación, ya que la copia puede quedar archivada en los servidores por los que pasa, además del ordenador del emisor y receptor final. Y de tener un buen sistema implantado el formato de archivo incluiría en la copia los documentos adjuntos[215].

El experto obtiene prueba en la máquina de la parte que ha contratado sus servicios, conjuntamente con toda la información pública disponible (en Internet, esto implica incluir datos públicos obrantes respecto de la contraparte). Además esa actividad del experto en informática-forense es importante que venga acompañada de una medida aseguratoria adoptada judicialmente a instancia de parte para resguardar la información obrante en las máquinas de la contraparte y de terceros relacionados, así como de la solicitud de prueba de informes al ISP, para que nos diga si los mensajes obtenidos o capturados coinciden en fecha, hora, origen y destino, con los que ya se han obtenido, así como idéntica constatación por informes respecto a los alojamientos de información propia y de la contraparte (alocación de páginas web, reservorios externos de información, mecanismos de comunicaciones, cuentas de correo públicas, empresariales, privada, etc.). Estas actuaciones dificultarán que se falsifique no sólo el mensaje de correo electrónico sino también los datos obrantes en el servidor del ISP, para que coincidan hora GMT, origen y destino[216]. El análisis y conclusiones llevadas a cabo por un perito a través del medio de prueba que es el dictamen pericial constituirán prueba electrónica. Prueba electrónica en sentido estricto solo lo es la pericial, única prueba capaz de acreditar dichos extremos.

Nótese, no obstante, que existe una figura híbrida que se asemeja mucho a la figura del perito como es la del testigo-perito. Se trata de aquella persona que

[215] Véase PASAMAR, A., en *Empresa y prueba informática*, en el libro del mismo título "Empresa y Prueba informática", ob. cit. pág. 32.

[216] Véase DARAHUGE, M.E Y ARELLANO GONZALEZ, L.E. *Manual de Informática Forense (Prueba Indiciaria Informático Forense).* Ed. Errepar, 2012, pág. 45.

posee también conocimientos técnicos y que mediante su intervención judicial facilita el acceso del hecho electrónico al proceso, pudiendo también considerase, en su caso, como prueba electrónica –aunque limitada a los hechos en los que históricamente participó-. Se hallaría en este caso el supuesto de un profesional que trabaja en el Departamento de Seguridad de una empresa y detecta fuga de información, realiza investigación y seguimiento y emite un informe. Analizaremos dicha figura en el § 8.

7.2 Naturaleza jurídica

La prueba pericial electrónica, como en general cualquier prueba pericial, contribuirá a formar la convicción del juez respecto a la certeza de las afirmaciones de los litigantes referidas a los hechos en los que funden sus pretensiones, y como tal constituye un «medio de prueba». El proceso civil es un proceso regido por el principio dispositivo, y con arreglo al mismo, como norma general, la iniciativa de dicho medio de prueba corresponde exclusivamente a las partes, aunque excepcionalmente se atribuye al juez (art. 282 LEC), se trata en este caso de supuestos especialmente regulados por la ley como en el caso de procesos no dispositivos. En este sentido se pronuncia la Ley de Enjuiciamiento Civil en el párrafo 14º del epígrafe XI de la Exposición de Motivos al señalar que «…*Con las excepciones obligadas respecto de los procesos civiles en que ha de satisfacerse un interés público, esta Ley se inclina coherentemente por entender el dictamen de peritos como un medio de prueba en el marco del proceso, en el que, salvo las excepciones aludidas, no se impone y se responsabiliza al tribunal de la investigación y comprobación de la veracidad de los hechos relevantes…».*

La Ley de Enjuiciamiento Civil regula dentro de los «medios de prueba» el dictamen de peritos (art. 299.1.4º) y se pronuncia expresamente sobre la naturaleza de la prueba pericial como «medio de prueba» en el párrafo 14º del epígrafe XI de la Exposición de Motivos al manifestar que *«…Así, la actividad pericial, cuya regulación decimonónica reflejaba el no resuelto dilema acerca de su naturaleza –si medio de prueba o complemento o auxilio del juzgador-, responde ahora plenamente a los principios generales que deben regir la actividad probatoria, adquiriendo sentido su libre valoración*».

La naturaleza de la prueba pericial como medio de prueba, tesis que sostenemos, la comparten autores como DE LA OLIVA, MONTERO AROCA, FONT SERRA[217], RIFA SOLER y RICHARD GONZÁLEZ, ha sido recogida en

[217] Véase FONT SERRA, E. *La prueba de peritos en el proceso civil español*. Ed. Biblioteca hispano europea de ciencias sociales, 1974, págs. 7-11.

resoluciones del Tribunal Supremo como en las Sentencias de fecha 7 de abril de 1995, 11 de octubre de 1994, 30 de marzo de 1998 y 23 de octubre de 2000.

No obstante, algunos autores disienten de dicha posición doctrinal defendiendo la naturaleza del perito como un «auxiliar de juez». Desde este punto de vista, el perito emite, con fundamento en sus conocimientos técnicos, un dictamen pericial que facilita el juicio de hecho del juez. De modo que el perito no introduciría hechos nuevos en el proceso, sino que dictamina sobre los ya aportados, proporcionando al juez máximas de experiencia para completar su capacidad de juicio. Es decir, se trataría de aportar al juez un elemento de valoración de hechos o circunstancias que ayudarán a formar su opinión sobre elementos de los que carece de formación o preparación, que serán libremente valorados por el mismo, no proporcionando dichos argumentos prueba alguna. Esta postura centra la función del perito en el auxilio jurisdiccional, apartándola de la influencia de las partes, y configura el dictamen pericial como la aportación al proceso de conocimientos técnicos especializados que facilitan el juicio de hecho del juez[218]. Dicha doctrina cuyo impulso se encuentra en CARNELUTTI, ha sido recogida por autores como PRIETO CASTRO, GÓMEZ ORBANEJA, SERRA DOMÍNGUEZ, GÓMEZ COLOMER, PICO y JUNOY o ABEL LLUCH[219]. Y por su parte, en la jurisprudencia dicho punto de vista se halla en diversas resoluciones como las SSTS 6 de febrero de 1987, 23 de abril de 1987, 18 de febrero de 1988, 10 de noviembre y de 10 de febrero de 1994. En otros ordenamientos jurídicos como Alemania, Italia, Francia, Bélgica e Inglaterra, se sigue esta misma posición, y también en textos supranacionales –Principles and

---

[218] Véase sobre este tema PRIETO CASTRO, L., *Derecho Procesal Civil*, 5ª ed, ed. Tecnos, Madrid, 1989, pág. 179 y SERRA DOMÍNGUEZ, M., *La prueba pericial*, en "*Instituciones del nuevo proceso civil. Comentarios sistemáticos a la Ley 1/2000",* vol. II, Alonso-Cuevilles Sayrol, J (coord.) edit. Difusa, Barcelona 2000, pág. 787.

[219] Véase CARNELUTTI, *Sistema de Derecho Procesal Civil*, Trad. Alcalá Zamora y Sentís Mellado, Buenos Aires, 1944, t. II, págs. 147 y 209 y ss. Por otro lado, SERRA DOMÍNGUEZ señala que el perito completa al Juez, pero no lo sustituye, y que si un perito declara como han ocurrido los hechos después de haber analizado el material probatorio, no aporta nuevas afirmaciones al proceso, sino que valora o aprecia las ya aportadas, siendo su actuación no tanto probatoria como jurisdiccional. La concepción del dictamen pericial como aportación al proceso de conocimientos técnicos especializados que facilitan el juicio de hecho del juez es la que según dicho autor cumple mejor las exigencias teóricas y prácticas de la pericia, ya que sobre explicar su fundamento y función, permite obtener su desarrollo dinámico e imparcial al apartarla de la influencia de las partes y centrarla en el auxilio a la función jurisdiccional a la que proporciona los materiales que podrán servir de base a la decisión judicial y que hubieran podido ser seleccionados directamente por el juez. SERRA DOMÍNGUEZ, Manuel. *La prueba pericial*, en "*Instituciones del nuevo proceso civil. Comentarios sistemáticos a la Ley 1/2000*", vol. II, Alonso-Cuevilles Sayrol, J (coord.) ed. Difusa, Barcelona 2000, págs. 288-289.

Rules Transnational of Civil Procedure y Código Procesal Civil Modelo para Iberoamérica- [220] .

Por otro lado, existe también un sector doctrinal que mantiene una posición mixta o ecléctica atribuyendo a la prueba pericial una naturaleza dual, considerando que la prueba pericial es un medio de prueba y a la vez el perito es auxiliar del juez. Respaldan esta opinión autores alemanes entre los que se encuentran BINDING, SCHONKE, GUASP, DEVIS ECHANDIA y VIADA[221]. Se sigue esta posición, por ejemplo, en el ordenamiento jurídico colombiano[222].

Por otra parte, y en nuestra opinión, no debe confundirse la naturaleza de la pericia como medio de prueba con la función que desempeña el perito en el proceso. Efectivamente, la naturaleza de la prueba pericial debe quedar

---

[220] Véase PICÓ i JUNOY, J., *La prueba pericial en el proceso civil español*, JM Bosch editor, Barcelona, 2001, págs. 43-46.

[221] DEVIS ECHANDIA y VIADA reconocen que el perito es un auxiliar técnico del juez pero de las tres funciones principales que tiene asignadas: verificar la existencia y características de los hechos técnicos; aplicar las reglas técnicas a los hechos verificados, y proporcionar al juez únicamente las reglas técnicas, sólo en el último supuesto, en la práctica muy poco frecuente, no actuaría como medio de prueba. DEVIS ECHANDÍA, *Teoría general de la prueba*, pág. 305 y 319, y VIADA, *Naturaleza jurídica de la pericia*, en "Anuario de Derecho Penal", 1951, pág. 48.

[222] Sobre la naturaleza dual de la prueba pericial en Colombia se pronuncia la Sentencia C-124/11 de 11 de marzo de 2011 de la CORTE CONSTITUCIONAL DE COLOMBIA al señalar: « *(…)Es por esta última razón que los ordenamientos procedimentales como el colombiano, prevén que el dictamen pericial, en su condición de prueba dentro del proceso correspondiente, debe ser sometido a la posibilidad de contradicción de las partes, mediante mecanismos como las aclaraciones, complementaciones u objeciones por error grave. Este carácter dual es confirmado por autores como Silva Melero, quien sostiene que el dictamen pericial cumple una doble función. De un lado «… llevar al proceso conocimientos científicos o prácticos que el juez podría conocer, pero que no está obligado a ello, y que son precisos para adoptar la decisión». Por otro lado, el dictamen también opera como «concepto de pericia de constatación de hechos», o lo que es lo mismo«… constataciones objetivas, que pueden ser independientes a la persona del inculpado». A idéntica conclusión arriba la jurisprudencia constitucional. Sobre el particular, en la sentencia T-796/06 (M.P. Clara Inés Vargas Hernández), se pone de presente cómo el dictamen pericial responde a una naturaleza jurídica dual. De un lado, es comprendido como «…un verdadero medio de prueba, debido a que el dictamen pericial se dirige a provocar la convicción en un determinado sentido, esto es, la actividad que realiza el perito tiene finalidad probatoria, ya que tiende a la fijación de la certeza positiva o negativa de unos hechos» De otro, la experticia también es comprendida como «…un mecanismo auxiliar del juez, ya que mediante el dictamen pericial no se aportan hechos distintos de los discutidos en el proceso sino que se complementan los conocimientos necesarios para su valoración por parte del juez. Mientras los medios de prueba introducen en el proceso afirmaciones fácticas relacionadas con las afirmaciones iniciales de las partes, con interés exclusivo para el proceso concreto, la pericia introduce máximas de experiencia técnica especializadas de validez universal para cualquier tipo de proceso».* Véanse tales sentencias en la página web http://goo.gl/bFLz7.

desvinculada de la forma en que la ley regula la designación del perito, en cuanto se trata de dos cosas distintas y que a veces se confunden. Es decir, el hecho de que el perito sea designado por las partes o por el juez de oficio responde al reparto de facultades entre el juez y las partes en cada ordenamiento jurídico, pero no afecta a la naturaleza de la prueba pericial ni a la condición de su actividad. Así mientras en la concepción española predominan los poderes de las partes, en la italiana, por ejemplo, se parte del aumento de los poderes del juez, respondiendo a concepciones políticas diferentes, que no alteran la naturaleza del perito y su actividad[223].

Tampoco afecta a la naturaleza de la prueba pericial la circunstancia de que el perito se considere como medio de prueba o bien como auxiliar del Juez. Es decir, ya sea que el perito efectúe un análisis o reconocimiento de un hecho u objeto, como la pericia sirva de complemento de los conocimientos del Juez para la valoración de la prueba y decisión del asunto. En este último caso los hechos aportados por el perito tienen por finalidad arrojar certeza sobre los hechos controvertidos facilitando al Juez su comprensión intelectual. Pero, en cualquiera de los casos la naturaleza y esencia de la pericia serán la misma que no es otra que verificar mediante criterios técnicos los hechos relevantes del proceso sirvan a los intereses de parte o, más ampliamente, a los intereses y fines de la justicia encarnada en la sentencia. En este sentido, se pronuncia DE LA OLIVA SANTOS que señalar que*: «incluso en aquellos dictámenes que se limitan a transmitir principios o reglas generales de índole experimental se ponen en relación con datos fácticos concretos (de lo contrario no serían pertinentes) con el fin de arrojar certeza sobre dichos datos, facilitando su más completa comprensión intelectual, lo que inexorablemente supone un enriquecimiento de su conocimiento (enriquece, por ejemplo, el conocimiento de un hecho saber qué denominación le corresponde)*»[224] .

7.3 Finalidad y Objeto de la pericia

La prueba pericial electrónica persigue aportar hechos, argumentos, conclusiones, verificaciones para acreditar en el proceso las afirmaciones sobre

[223] Véase sobre este punto MONTERO AROCA, J., *La prueba en el proceso civil*, 5ª ed., ed. Civitas, Madrid, 2007, págs. 349 y 350; y SERRA DOMINGUEZ *La prueba pericial, en "Instituciones del nuevo proceso civil.* Comentarios sistemáticos a la Ley 1/2000", vol. II, Alonso-Cuevilles Sayrol, J (coord.) edit. Difusa, Barcelona 2000, pág. 291.

[224] Véase DE LA OLIVA, A y FERNÁNDEZ, M.A., *Derecho Procesal civil II, Objetos, Actos y Recursos del proceso civil. El proceso civil de declaración, e*d. Centro de Estudios Ramón Areces, Madrid 1993, pág. 346.

los hechos de naturaleza electrónica aportados por las partes en sus escritos de demanda y contestación y determinar la certeza de los hechos controvertidos. Se trata de una actividad desplegada generalmente por las partes, y excepcionalmente de oficio por el juez (art. 282 LEC) que cumple con la finalidad de servir para acreditar las pretensiones de cada una de las partes en el proceso. Dicha prueba deberá versar sobre hechos que deben haber sido introducidos por las partes en el proceso no pudiendo versar sobre hechos nuevos[225]. En este sentido se pronuncia el Tribunal Supremo señalando que *« (…) la prueba pericial ha de recaer sobre unos hechos o datos aportados al proceso para ser valorados y apreciados técnicamente, constituyendo lo antedicho la regla de oro de la prueba pericial en el área jurisdiccional civil*» (La STS, Sala 1ª, de 12 de abril de 2000, Fdo. Jco. 1º, RA 1826). Por otro lado, el dictamen pericial debe limitarse o ceñirse a los extremos que la parte, o en su caso, el juez haya propuesto.

El hecho electrónico, en la mayoría de los casos, suele ser en realidad «accesorio» al hecho fundamental que se pretende probar en el juicio. La prueba pericial electrónica persigue probar o acreditar hechos o una actividad de naturaleza electrónica que fundamenta o tiene relación con la tutela pretendida en el proceso jurisdiccional. Sin embargo, nótese que si bien existen supuestos en que la finalidad es acreditar un hecho electrónico en sí mismo, la mayor parte de las veces la finalidad perseguida con la aportación de la prueba pericial al proceso es la de acreditar o valorar la certeza de una actividad humana de naturaleza electrónica. Es decir, en un juicio la parte propone prueba pericial a los efectos de acreditar en el proceso que tal persona remitió un correo electrónico a otra, lo cual es relevante a los efectos de la pretensión objeto de juicio. La finalidad perseguida en este caso es acreditar la actividad o comportamiento humano consistente en el envío de un correo electrónico. Para poder probar la existencia de tal envío, actividad o comportamiento humano, el perito estudiará la actividad electrónica producida, es decir, el hecho electrónico propiamente dicho. Para ello, como hemos visto en el capítulo anterior, el perito analizará una serie de datos en un archivo informático, registros o *logs*, así como

[225] En este sentido SERRA DOMINGUEZ afirma que dicha ampliación de facultades del perito -introducción de hechos nuevos- no está autorizado por la Ley, ha sido criticada por la jurisprudencia, y se presta a serios abusos en la práctica, tanto por la absoluta falta de garantía con que dichos hechos se introducen al proceso, como por entrañar la sustitución del necesario reconocimiento judicial por la pericia, cuanto, por último, por dificultar el control crítico del Juez sobre los resultados de la pericia. SERRA DOMINGUEZ, M., *La prueba pericial, en Instituciones del nuevo proceso civil. Comentarios sistemáticos a la Ley 1/2000*, vol. II, Alonso-Cuevilles Sayrol, J (coord.) edit. Difusa, Barcelona 2000, pág. 294. Véase también PICÓ Y JUNOY, *La prueba pericial en el proceso civil español*, JM Bosch editor, Barcelona, 2001, págs. 50 y 51.

copias de seguridad y los contrastará con la información pública de la que disponga.

La pericial electrónica, por lo general, suele ser prueba relevante en procesos en que se discuten actitudes o comportamientos humanos que desde un punto de vista jurídico constituyen actividades ilícitas, ya sean penales o civiles, tales como: el envío de mensajes que constituyen amenazas, injurias o información confidencial a través de correos electrónicos o su publicación a través de Internet; el uso malintencionado de los sistemas de la empresa como el borrado masivo o sobreescritura de información, sabotaje de los sistemas, modificación no autorizada de páginas Web, suplantación de identidad, etc.; el fraude económico o contable, la fugas de información, la competencia desleal, el espionaje empresarial o industrial; el uso no autorizado de los privilegios de administración informática; el bajo rendimiento laboral, el uso indebido de los sistemas etc. en conflictos laborales.; conflictos en proyectos de desarrollo de software o implementación de sistemas informáticos entre cliente y fabricante o instalador, entre muchos otros[226].

En el ámbito de la prueba pericial informática suelen diferenciarse aquellos supuestos en que el objeto perseguido por las partes en el proceso al proponer prueba pericial es probar un hecho directamente relacionado con un sistema informático de aquellos otros en que se pretende probar hechos relacionados o para cuya comisión se emplean sistemas informáticos. En este sentido, y desde un punto de vista técnico, los expertos suelen diferenciar entre: «*Computer forensics*» entendido como aquel análisis forense relacionado con la investigación de situaciones donde está implicado el uso de un sistema informático o de una evidencia digital, siendo el ilícito cometido de cualquier tipo, no sólo de los propios sistemas de información (p.ej. delito a la propiedad intelectual); y «*Instrusion forensics*» que puede definirse como aquel análisis forense relacionado con la investigación de ataques o comportamientos sospechosos contra sistemas informáticos o ilícitos cometidos únicamente sobre los mismos como pueden ser intrusiones o ataques Dos[227].

[226] Enumeración obtenida en página comercial. Puede consultarse en la siguiente dirección electrónica: http://goo.gl/jtJRO.

[227] Un ataque de denegación de servicio en seguridad informática, también llamado ataque DoS (de las siglas en inglés *Denial of Service*), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le denomina «denegación», pues hace que el servidor no dé abasto a la cantidad de solicitudes. Esta técnica es usada por los llamados Crackers para dejar fuera de servicio a servidores objetivo. Una ampliación del ataque Dos es el llamado ataque distribuido de denegación de servicio, también llamado ataque DDoS

La prueba pericial podrá consistir, o tener por objeto, en verificar un hecho, y/o determinar la causa o el cómo se produjo, así como, en su caso, determinar sus efectos. En el supuesto de verificación se pretende adquirir certeza sobre la existencia de un hecho afirmado por una parte y negado por la contraria. El perito verifica la existencia o las características de los hechos técnicos o científicos, los/las constata e ilustra al juez. Esta clase de dictamen es, indudablemente, un medio para la comprobación de hechos (*percipiendi)*. En otros supuestos el perito valorará hechos ya probados en el proceso o de los que no se duda de su existencia. Estas peritaciones tienen por finalidad aplicar las reglas técnicas o científicas de la experiencia especializada de los expertos, a los hechos verificados en el proceso, por cualquier medio de prueba, para deducir de ellos las consecuencias, las causas o las calidades o valores que se investigan. El perito llega a una conclusión, que infiere en un proceso racional y lógico, tras la aplicación de las reglas técnicas -valor económico, perjuicio causado etc.- *(deduciendi)*.

Así, la pericial electrónica puede tener por objeto reconstruir datos destruidos en un ordenador. Se trata en este supuesto de lo que los técnicos en el ámbito informático llaman «*análisis post-mortem»*, es decir, análisis una vez acaecido el hecho objeto de prueba. Se realiza con un equipo dedicado específicamente para fines forenses para examinar discos duros, datos o cualquier tipo de información recabada de un sistema que ha sufrido un incidente. Se utilizan herramientas de laboratorio para el análisis de discos duros, archivos de logs[228] o de firewalls [229] o IDS[230], etc. Otro ejemplo, fuera del campo de la informática,

---

(de las siglas en inglés *Distributed Denial of Service*) el cual lleva a cabo generando un gran flujo de información desde varios puntos de conexión. La forma más común de realizar un DDoS es a través de una botnet, siendo esta técnica el ciberataque más usual y eficaz por su sencillez tecnológica. Véase Wikipedia, disponible en http://goo.gl/g9Ccd9, página consultada el 8.8.2013.

[228] El término *log* puede hacer referencia a: Un Log, un registro de algo; un web log, es decir, Blog; o log, Logaritmo.

[229] Un *cortafuego (firewall* en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuegos a una tercera red, llamada *Zona desmilitarizada* o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior. Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente.

lo sería la determinación de la causa que produjo un accidente ferroviario a través del análisis del funcionamiento del Sistema de Anuncio de Señales y Frenado Automático ferroviario (ASFA) y de la caja negra del tren o registrador de eventos[231].

Por otro lado, la pericial puede tener por objeto la verificación de un hecho, cuando como, por ejemplo, el perito efectúa una comprobación de la existencia de una página Web y determina el origen de la información colgada en la misma. Conviene en estos supuestos la práctica simultánea del reconocimiento judicial y el pericial (art. 356 LEC), por cuanto el juez visualizará personalmente la página y el perito realizará el análisis técnico. En este supuesto se englobarían los casos llamados técnicamente de «*análisis en caliente*». Es decir, aquellos en que el análisis se lleva a cabo sobre un sistema que se presume está sufriendo un incidente de seguridad. En este último caso se suele emplear un CD con las herramientas de respuesta ante incidentes y análisis forense compiladas de

---

La seguridad informática abarca más ámbitos y más niveles de trabajo y protección. Véase sobre este tema Wikipedia. Disponible en *http://goo.gl/bmHOqa* . Página visionada el 8.8.2013.

[230] Un sistema de detección de intrusos (o IDS de sus siglas en inglés *Intrusion Detection System*) es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.
El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas. Puede consultarse esta información en la página web de Wikipedia.

[231] En el ámbito ferroviario el Sistema de Anuncio de Señales y Frenado Automático ferroviario (ASFA) es un sistema en el que se sitúan balizas en el eje de una vía de tren, entre los carriles, cinco metros antes de una señal y protegidas por una cuña de madera a cada lado. Dichas balizas transmiten pasivamente una radiofrecuencia determinada según el estado de la señal a la que acompañan. Las balizas tienen capacidad de transmitir en nueve frecuencias diferentes, cada una de las cuales indica un estado de la señal adyacente. El tren dispone bajo el bastidor de un captador, situado en la parte delantera, que a su vez dispone de un oscilador que oscila a determinada frecuencia, y que al pasar sobre la baliza pasa a oscilar a la frecuencia de resonancia del circuito de la baliza. La frecuencia obtenida se envía a un armario de control, activándose en la cabina una señal luminosa y en ocasiones acústica que indica el estado de la señal. El conductor debe confirmar en menos de tres segundos que ha entendido la señal. Si la señal indica alguna limitación el tren debe comenzar a adaptarse a la limitación en un tiempo determinado o se produce una frenada de emergencia. El Asfa está conectado al equipo de frenado, al tacógrafo, al tacómetro y al registrador de eventos o caja negra del tren, donde queda constancia de todas las indicaciones presentadas por las señales y las actuaciones del maquinista. En relación al sistema ASFA. Véase *Así funciona el ASFA, Anuncio de señales y Frenado automático*, en Vía Libre, La Revista del Ferrocarril, 31 de julio de 2013, puede consultarse este artículo en la dirección electrónica http://goo.gl/zCrI2o; Y el sistema ASFA en la página web de Wikipedia en la siguiente dirección electrónica http://goo.gl/iKkSv8. Páginas consultadas el 6.8.2013.

forma que no realicen modificaciones en el sistema. Una vez efectuado este análisis, y confirmado el incidente, se realiza el llamado técnicamente *«análisis post-mortem*».

Finalmente la pericial electrónica también podrá tener por objeto determinar los efectos de un hecho electrónico no controvertido, se trataría del caso en que el perito estudia los daños derivados de la descarga de una página Web, por ejemplo posibles daños causados por un trabajador a una empresa por introducción de virus al abrir páginas de contenido pornográfico.

En general, el análisis forense, puede tener por objeto distintos extremos y su finalidad puede consistir, entre muchas otras, por ejemplo en: Localizar y extraer documentos, actividad que debe ser realizada siempre respetando los derechos a la intimidad y al secreto de las comunicaciones de las personas implicadas; determinar la autoría de un documento o una acción en un entorno digital, como, por ejemplo, averiguar quién ha creado un página Web determinada; analizar la actividad, o determinación de la cadena de hechos previa o posterior a un suceso en un entorno digital; recuperar archivos e información borrada, incluso después de varios formateados y reinstalaciones del sistema; certificar la información técnica, como procedencia de correos electrónicos o autoría de información publicada en Internet; revelar información oculta en un sistema digital, accidental o malintencionadamente; investigar hechos y recopilar información en entornos digitales; o realizar periciales de programas y sistemas informáticos[232].

* * *

[232] Enumeración obtenida en la página web a que responde la dirección electrónica http://goo.gl/6CT0g. Página comercial.

CAPÍTULO VIII.- EL PERITO TECNOLÓGICO Y EL DICTAMEN PERICIAL

8.1 El perito

8.1.1 La figura del experto como asesor técnico

El extraordinario avance de la ciencia y la tecnología supone en la actualidad que jueces con conocimientos generales deban, cada vez en mayor medida, hacer frente a cuestiones técnicas complejas que exceden de su experiencia. Las peculiaridades y la extrema complejidad de las evidencias digitales, como en cualquier otro ámbito tecnológico o científico, resulta un reto de enorme dificultad para los ciudadanos, que necesitan acreditar los hechos en el proceso y para los jueces que deben resolver las peticiones de los ciudadanos con relación a materias cada vez más complejas técnicamente. Esta dificultad afecta tanto al planteamiento de las demandas como a la resolución de las cuestiones que se planteen en el proceso en medidas de aseguramiento o cautelares o diligencias, preliminares y, por supuesto, a la hora de dictar sentencia. En estos supuestos de asuntos relacionados con la ciencia y/o la técnica resultará imprescindible la aportación y valoración de informes elaborados por expertos técnicos en la materia cuyo contenido será instrumento de integración del juicio lógico del juez[233]. Dicho supuestos en que está presente la tecnología han pasado de la excepcionalidad a ser cada vez más numerosos, dada la mayor presencia de los medios digitales en nuestro cotidianeidad, por lo que se han reabierto debates no solo a nivel nacional sino también internacional sobre el modo en que las partes, el sistema de justicia y, en definitiva, los jueces deben hacer frente a tales cuestiones técnicas y científicas[234].

---

[233] En supuestos de medidas de aseguramiento de prueba o de diligencias preparatorias en asuntos tecnológicos o en los que interviene la tecnología, acordadas en muchas ocasiones «inaudita parte» dada la probabilidad que la contraria haga desaparecer la evidencia electrónica, podrán solicitarse clonaciones de la información, para lo cual el juez para valorar si lo solicitado es ajustado a derecho o excede del objeto de demanda deberá tener a su disposición informes periciales que le permitan efectuar una valoración de lo solicitado por la parte. Se trataría, por ejemplo, del supuesto en que a petición de parte se solicita el clonado de toda una ERP en una empresa.

[234] Sobre este particular puede verse el interesante artículo de MIRANDA DE VÁZQUEZ, C. *¿Es realmente el juez el "peritus peritorum"? (Propuesta de reformulación del brocardo y análisis del alcance efectivo de la valoración judicial de la prueba pericial)*, en "Derecho Probatorio contemporáneo. Prueba científica y técnicas forenses", Bustamante Rúa, M. (coord.), Universidad de Medellín, 2012, pág. 293-310, quien propone permitir al juez «*a través de las leyes procesales que pueda designar un perito, siempre que lo precise, para que le proporcione máximas de experiencia técnicas, de naturaleza epistemológica, específicas del área de conocimiento que sea*

En Estados Unidos, por ejemplo, la extrema complejidad de casos científicos y tecnológicos y las limitaciones de los jueces para poder dirigir estos procesos ha hecho que se postule por el nombramiento de expertos asesores del juez. Así lo defendió el Juez del caso MICROSOFT VS APPLE, en una conferencia celebrada en Neuquen en 2005[235]. Ello pese a que hasta dicho momento y a pesar de la existencia de dicha figura los jueces americanos eran reticentes al nombramiento de tales expertos, puesto que en los sistemas de derecho occidentales rige, con carácter general, el «adversary system» concebido como principio jurídico natural del proceso que garantiza la autonomía de las partes (principio de instancia de parte) e imparcialidad judicial.

La figura del experto como consejero del juez o «*technical advisor*» coexiste en Estados Unidos junto a otras figuras distintas como los «*court-appointed experts*» (expertos nombrados por las partes) y de «*specials master*». Se trata de una figura que no emite un dictamen pericial, sino que ilustra al juez de como es el conflicto, permitiéndole conocer el problema y guiar el proceso con mayor idoneidad técnica. Dicho experto no aporta evidencia, no investiga fuera del caso, no ofrece su opinión sobre el mismo y se nombra con fundamento en el poder inherente del juez. En el proceso civil ambas partes presentan o aceptan, si lo presenta el Juez, un reconocido perito que informa al juez de la base del litigio en términos técnicos. El experto consejero del juez es considerado como empleado público y cobra por sus servicios. En Estados Unidos, como anteriormente hemos indicado, pese a la existencia de esta figura del consejero del juez o «*technical advisor*», durante mucho tiempo han existido reticencias por parte de los jueces americanos al nombramiento de estos asesores ya que ello supone asumir un poder tradicionalmente reservado a las partes en dicho sistema.

Sin ningún ánimo exhaustivo veamos unas pinceladas de los cuatro hitos importantes a los cuales ha estado vinculada dicha figura. Ello nos permitirá comprender el nacimiento de la figura del asesor técnico en los Estados Unidos de América, aunque teniendo presente que el sistema americano es diferente al nuestro y que en dicho país la admisión de la prueba es una fase procesal previa

---

objeto del litigio» (p.308). Esta sugerencia también se recoge en la monografía de ABEL LLUCH, X., *La valoración de la prueba en el proceso civil*, ed. La Ley, Madrid, 2014, pag.130. Desde el punto de vista de la epistemología, se puede consultar el interesante artículo HAACK, S. *Irreconciliable diffferences? The troubled marriage of science and law*, en Law and contemporary problems, vol.72, núm.1, 2000, pag.12.

[235] Véase sobre este punto VAZQUEL VILLAR, AIDEE, *Las medidas cautelares en el proceso penal por delitos ambientales. Fallos y doctrina de la Patagonia*. Alveroni Ediciones, Revista trimestral, Año II-núm. 2, marzo de 2007, pág. 13. Puede consultarse en la página web http://goo.gl/eL8o8.

al juicio[236]. En 1823 *FRY V. UNITED STATES* estableció que la admisibilidad de la prueba científica debía dejarse en manos de la comunidad científica a través del llamado «test de Frye». Esta postura fue muy criticada al delegar la decisión de admisión de la prueba científica a los expertos. El comentarista Bert Black mantuvo que debía diferenciarse entre, por un lado, el razonamiento y la metodología que debían dejarse en manos de expertos, y por el otro, la toma de decisión sobre la admisión de la conclusión del experto que correspondía al juez. Sin embargo, los jueces aplicaron el test tanto a la tecnología como a las conclusiones admitiendo la prueba científica si estaba aceptada por la comunidad científica.

En 1975 *The Federal Rules of Evidence* establecieron dos nuevos test: el «test de relevancia» y el «test de fiabilidad». Los defensores del test de la relevancia sostenían que cualquier conclusión relevante apoyada en el testimonio de un experto cualificado debía ser en principio admitida porque las diferencias sobre fiabilidad afectaban al contenido de la evidencia y no a la admisibilidad. Esta postura fue criticada en cuanto si no hay control judicial y el juez no se implica cualquier prueba científica es admitida independientemente de su relevancia. Según dicha posición doctrinal crítica los jueces deben examinar las pruebas científicas y razonar la admisibilidad.

En 1988 en el caso *REILLY V. UNITED STATES* la Corte Suprema Americana aprobó el nombramiento por parte del juez de un asesor. No obstante, en dicho caso la Corte Suprema a pesar de ratificar el nombramiento de dicho experto, reconoció que las partes debían estar más protegidas procesalmente. Afirmó que en un futuro las partes debían estar informadas del nombramiento por parte del juez del «*technical advisor*» y debían tener derecho a oponerse a su nombramiento. También señaló que el juez debía exponer por escrito el ámbito de los deberes de dicha figura, es decir, en qué consistiría su actuación, y el experto debía presentar una declaración jurada conforme cumplía las especificaciones requeridas por el juez. El tribunal de apelación rechazó la necesidad de presentar informe escrito y no se pronunció acerca de si las partes debían tener acceso directo al asesor[237].

---

[236] Sobre la figura del «technical advisor» americano pueden consultarse: *Improving judicial gatekeeping: Technical advisors and scientific evidence*. Full Text Available Harvard Law Review. Feb97, Vol. 110 Issue 4, pág. 941. 18p.; Hess, Robert L., *Judges cooperating with scientists: A proposal for more effective limits on the federal trial judge's inherent power to appoint technical advisors*, V. II. Vanderbilt Law Review 54. 2 (Mar 2001), págs. 547-590; Connelly, Michael; Muir, John, *Special Masters, Court-Appointed Experts and Technical Advisors in Federal Court*. Full, Defense Counsel Journal. Jan2009, Vol. 76 Issue 1, págs. 77-90. 14p.

[237] En el caso HEMSTREET Vs. BURROUGHS CORP (1988) la Corte Suprema exigió que el «technical advisor» presentara informe escrito.

Y finalmente en 1993 en el conocido caso *DAUBERT* la Corte Suprema afirmó que el juez debe asegurarse que los testigos científicos o las evidencias deben ser relevantes y fiables. Los jueces deben revisar el razonamiento y la metodología. Y para ello la Corte recomendó cuatro criterios básicos que los jueces deben considerar para admitir prueba: si la teoría o técnica es testable o ha sido testada; si ha estado sujeta a revisión o ha sido objeto de publicaciones científicas; la tasa de error conocida o potencial de la técnica empleada; y la existencia y mantenimiento en los standards de control de la técnica[238]. Dada la dificultad se sugirió a los jueces que nombraran sus propios expertos al amparo de la federal Rule of Evidence 706 para examinar la evidencia científica. Sin embargo, la Corte Federal no detalla cómo deben ser nombrados dichos expertos, ni si han de actuar como testigos o solo informar al juez, y si bien afirma que los jueces no pueden delegar la toma de decisiones a los expertos no precisa como impedirlo.

En Estados Unidos si bien existe todavía incertidumbre sobre la normativa por la que deben regularse los «*technical advisors*» cada vez se realza más la necesidad de su nombramiento, dado los complejos casos tecnológicos que se plantean en dichos Tribunales y la frecuente crítica de que la práctica de peritos nombrados a instancia de parte es una práctica poco fidedigna e ineficiente de utilizar los conocimientos técnicos o científicos. Según las resoluciones que se vienen dictando deben establecerse límites a su designación y actuación para impedir vulnerar la imparcialidad judicial. Para facilitar el nombramiento de dichos expertos nació el Proyecto CASE. The Court Appointed Scientific Experts (CASE), es una organización creada por la «*American Association for the Advancement of Science*» (AAAS). A grandes rasgos dicha organización, que goza de prestigio internacional, propone un listado de expertos de acuerdo con los expresos requerimientos del juez para el caso en concreto y habiéndose

---

[238] La cita literal inglesa es la siguiente: «1) Testability: whether it (the evidence, theory or technique) can be (has been) tested; 2) Error Rate: the known or potential rate of error; 3) Peer review: whether the theory or technique has been subjected to peer review and publication; 4) General aceptante: the explicit identifications of a relevant scientific community and an express determination of a particular degree of acceptance within that community» (Daubert at 594). Sobre esta fundamental sentencia, cuya influencia ha traspasado las fronteras del common law, se pueden ver, entre otros muchos, los siguientes comentarios: TARUFFO, M., *La aplicación de estándares científicos a las ciencias sociales y forenses*, en "Estándares de prueba y prueba científica", ed. Marcial Pons, 2013, pág.204; y en la literatura anglosajona, y entre otros muchos, GIANNELLI, P.C., *Daubert and forensic science: the pifalls of law enforcement control of scientific research*, University of Illionois Law Review, 2011, pág. 60; GODDEN, D.M. y WALTON, D., *Argument form Expert Opinion as Legal Evidence: Criticual Questions and Admissibility Criteria of Expert Testimony in the American Legal System, Ratio Juris*, Vol.19, núm.3, septiembre 2006, pág.271.

analizado con carácter previo las necesidades del caso específico, el experto es nombrado por el juez a partir de dicho listado. Anteriormente al Proyecto CASE los jueces americanos que optaban por dicha designa la efectuaban entre personas conocidas de su entorno o bien debían destinar un notable empleo de tiempo y esfuerzo en encontrar personas lo suficientemente preparadas. Es por este último motivo por el que muchos jueces desistían de efectuar dichos nombramientos debido a la sobrecarga de trabajo que ello suponía[239].

En otros países como Italia se otorgan históricamente mayores poderes al juez que a las partes en las designas de perito. En dicho país la institución del consultor técnico aparece por primera vez en el Codice di Procedura Penale italiano de 1930, si bien su antecedente se encuentra en el Proyecto de CARNELUTTI de 1925; y se halla también en el Cod. Proc. Civ. Italiano 1940. En el primero de estos Códigos, de MANZINI, el consultor técnico entronca con el perito de parte, y se contrapone al perito designado por el juez, al que se le conserva el nombre de perito. Mientras que la pericia se acuerda por el juez, que dirige su práctica (art. 314 y 317 Cod. Proc. Pen. Italiano), el consultor técnico es la persona, nombrada por las partes –asesor o defensor técnico del litigante- para examinar los informes y dictámenes del perito oficial y hacerle las observaciones oportunas (art. 323 a 325 Cod. Proc. Italiano). En cambio en el Cod. Proc. Civ. De 1940 se denomina consultores técnicos tanto al perito designado por el juez como a los elegidos por las partes, sustituyendo así, de un modo total, el tradicional nombre de perito (medio de prueba) y dando a los expertos una misión de asesoramiento[240].

En nuestro país, dado el notable incremento de los casos en que interviene la tecnología, por parte de algunos sectores del mundo jurídico vienen reclamándose soluciones entre las que se hallan una mejor formación a los miembros de la judicatura, la creación de lo que llaman «perito tecnológico», o la creación de Juzgados especializados[241]. Respecto a dichas propuestas y en cuanto a la formación de los jueces nada que objetar en cuanto la formación siempre es imprescindible no solo en esta materia sino en todas las demás. Está mejor formación no solo debería limitarse al ámbito de la tecnología o informática forense, sino particularmente, al ámbito de la epistemología, como

[239] Puede consultarse información sobre «The Court Appointed Scientific Experts» en la dirección electronica http://goo.gl/XURpY

[240] Véase FONT SERRA, E. *La prueba de peritos en el proceso civil español*. Ed. Biblioteca hispano europea de ciencias sociales, 1974, págs. 99-101.

[241] Véase el artículo de El País "*Tecnología*" donde por parte de miembros de la judicatura y la policía se reclama una mejor formación en tecnologías y la creación de la figura del «perito tecnológico». Puede consultarse este artículo en la página web http://goo.gl/mzi8l

herramienta metodológica que permite el sometimiento del dictamen pericial científico a las reglas de la sana crítica[242].

Respecto al «perito tecnológico» no acaba de quedar clara la figura que proponen, pues si bien aluden a la misma no he hallado descripción de la misma y de su función. Y finalmente respecto a los juzgados especializados si bien es cierto que la creación de dichos juzgados permitiría la acumulación de experiencia y conocimientos por parte de los jueces adscritos a los mismos, no lo es menos que la tecnología en la actualidad forma parte de todos los ámbitos constituyendo no solo objeto sino medio para cualquier fin. Y aunque podamos deslindar a efectos prácticos determinados delitos en el ámbito penal y determinadas materias en el ámbito civil, como propiedad intelectual e industrial, en que las tecnologías actuales constituyen principal centro de debate, lo cierto es que la tecnología forma parte de la cotidianeidad de cualquier sujeto individual o corporativo y puede aparecer en cualquier tipo de procedimiento, siendo patente tanto en una estafa informática como en la remisión de un correo electrónico en cualquier tipo de procedimiento civil. Indicar, además, que con la actual Planta Judicial sería muy difícil y costosa económicamente la creación de juzgados especializados en las distintas jurisdicciones, mayormente cuando las reformas judiciales se orientan por la supresión de Juzgados y la creación de Juzgados provinciales.

En cualquier caso el juez no tiene porqué convertirse en un experto técnico puesto que no es esa su función en el proceso, sino que al juez le corresponde efectuar una valoración mediante el razonamiento de los informes de expertos que son quienes deben aportar sus conocimientos y sus conclusiones. Por lo tanto, la solución debería pasar en nuestro ordenamiento por facilitar procesalmente al juez la posibilidad de acudir a la pericial en aquellos supuestos que necesite conocimientos técnicos, científicos o prácticos en la materia y las partes no los hayan aportado o de aportarlos no fueran suficientes para poder adoptar una resolución.

Las facultades directivas que corresponden al juez en la obtención de la certeza de los hechos controvertidos ha sido en nuestro país desde siempre objeto de debate[243]. Frente a posturas doctrinales que sostienen que la iniciativa

[242] Dicha mejor formación de los jueces debería tener ya su reflejo en el programa de Oposiciones para el Ingreso en la Carrera Judicial y en los programas de Formación Inicial y Continua en la Escuela Judicial.

[243] Certeza como estado de conocimiento individual o configuración subjetiva de la verdad, según SENTÍS MELENDO, S., la verdad es inasequible, pero se puede alcanzar la certeza, ya que «pretender la creación de una verdad ficticia roza los límites de lo absurdo». SENTÍS MELENDO, S, *Naturaleza de la prueba, en "*La prueba. Los grandes temas del derecho probatorio*"*, ed. EJEA, Buenos Aires, 1979, págs. 42-43 y 89.

probatoria corresponde exclusivamente a las partes, ya que de lo contrario podría vulnerarse la imparcialidad de los órganos judiciales[244], otros autores sostienen la necesidad de combinar los principios oficial y dispositivo, otorgando mayor protagonismo al juez en el esclarecimiento de los hechos, siendo necesario por parte de éste un completo conocimiento del asunto[245]. Actualmente, la mayor parte de la doctrina sostiene el modelo intermedio, en el que el juez interviene cuando existen abusos o desviaciones evidentes de las partes en el proceso. Es decir, el principio dispositivo debe quedar intacto en el proceso civil pero el principio de aportación de parte está sujeto al equilibrio entre el poder de las partes y la del juez, quien debe verificar, esclarecer y completar tal actividad[246].

Lo que sí es evidente, como ha puesto de manifiesto la práctica forense, son los defectos o fallos en el sistema vigente. Así por ejemplo el principio de aportación de parte en los supuestos de evidencia científica o tecnológica puede llevar a situaciones en las que se ofrezcan conclusiones dispares en los dictámenes periciales presentados por cada una de las partes. En esta situación, los peritos presentados sustentarán y fortalecerán las alegaciones de las partes proponentes, que naturalmente defienden sus propios intereses, mientras que los letrados contribuirán «oscurecer» las cuestiones mediante la defensa de los argumentos aducidos por su propio perito. En esta tesitura el juez puede carecer de criterio para adoptar una sentencia con el debido fundamento. Téngase en cuenta, que nuestro sistema presume la igualdad entre las partes, aunque en realidad los recursos y el talento de los letrados que actúan en el juicio no sean iguales. La solución lógica para esta cuestión sería la de que el Juez pudiera nombrar un perito dirimente que resolviera entre las conclusiones

---

[244] Véase CARRERAS LLANSANA, J., *Facultades materiales de dirección*. Estudios de Derecho Procesal, Librería Bosch, Barcelona, 1962, pág.258.

[245] Véase FAIREN GUILLÉN, V., *El Proyecto de la Ordenanza Procesal Civil Austríaca visto por Franz Klein*, Estudios de Derecho procesal, Revista de Derecho Privado, Madrid, 1955, pág.315; y PRIETO-CASTRO Y FERRÁNDIZ, L., *Derecho procesal Civil,* Revista de Derecho Privado, Madrid, 1968, pág..230. Sobre este particular puede verse también ampliamente MONTERO AROCA, J. (coord.), *Proceso civil e ideología. Un prefacio, una sentencia, dos cartas y quince ensayos*, ed. Tirant lo Blanch, Valencia, 2006, destacando particularmente dentro de esta obra el artículo PICÓ I JUNOY, J., *El derecho procesal entre el garantismo y la eficacia un debate mal planteado*, pág.109-127 y su interesante conclusión tercera en la que se afirma "[…] *Por ello, para evitar enfrentamientos más ideológicos que técnicos, debe hacerse siempre una lectura garantista de las normas procesales en orden a la máxima eficacia de las mismas. Y esta lectura, como se ha podido comprobar, no es incompatible con el hecho de atribuir cierta iniciativa probatoria al juez civil, o permitirle el control de la buena fe procesal de las partes"* (pág.126).

[246] En este sentido véase CORDÓN MORENO, *Entorno a los poderes de dirección el juez civil*, Revista de Derecho Privado, 1979, nº 9, págs. 809, 816, 817.

dispares de los peritos de parte. Pero, esta posibilidad únicamente puede adoptarse mediante una interpretación amplia del art. 435 respecto a la posibilidad de que el Juez pueda acordar de oficio diligencias finales.

Nuestro actual código procesal recoge los principios dispositivo y de aportación de parte. Tal y como señala el art. 216 LEC «*Los tribunales civiles decidirán los asuntos en virtud de las aportaciones de los hechos, pruebas y pretensiones de las partes, excepto cuando la ley disponga otra cosa en casos especiales*». El «principio dispositivo» rige en derecho privado frente al proceso penal, que tiene carácter inquisitivo. Conforme a dicho principio corresponde a la parte el ejercicio de la acción en protección a sus derechos. En palabras de SERRA DOMÍNGUEZ el principio dispositivo «*comprende todas aquellas facultades procesales derivadas de la titularidad afirmada en el proceso de los derechos sustanciales*»[247]. Por otro lado, el «principio de aportación de parte» supone la atribución por parte de la ley a las partes de aducir y traer al proceso el material de hecho, limitando básicamente la función del juez a recibirlo, para valorarlo después[248]. No obstante, el Juez debe poder disponer de medios para poder acceder a la certeza de los hechos o circunstancias relevantes en el asunto sobre el que versa el pleito pudiendo decidir cuando la prueba presentada no es suficiente o es inadecuada.

En este sentido la vigente LEC le otorga al Juez ciertas facultades directivas del proceso en la proposición, admisión y práctica de la prueba, reforzando su papel directivo del proceso aunque limitando en nuestra opinión dicho papel en exceso. Nuestro sistema como regla general otorga la iniciativa probatoria a las partes (art. 282 LEC) no obstante admite excepciones en aquellos casos en que expresamente lo determine la ley. En fase de proposición de prueba la LEC faculta al juez a intervenir advirtiendo a las partes de la insuficiencia de la prueba propuesta por las partes para obtener la certeza de los hechos controvertidos e incluso la facultad de sugerir medios de prueba necesarios para probar los hechos (art. 429.II y III LEC). Mayores facultades probatorias se otorgan al juez en los procedimientos especiales no dispositivos sobre capacidad, filiación, matrimonio y menores (art. 752.1.II, 759.1 y .3, 763.3 LEC, 767.2 y .4 y 771.3, 770.4ª y 774.2, 777.4 LEC). La facultad directiva del proceso por parte del juez se manifiesta también en el juicio de admisibilidad, definiéndose la pertinencia, la utilidad y la legalidad, y se regula también la declaración de ilicitud de una prueba. Rige un sistema de inmediación judicial

[247] Véase SERRA DOMÍNGUEZ, M., *Liberalización y socialización del proceso civil*, Revista de Derecho Procesal Iberoamericana, 1972, nº 2 y 3, págs. 520-521.

[248] Sobre la delimitación de los principios dispositivo y de aportación de parte puede verse ABEL LLUCH, X., *Iniciativa probatoria de oficio*, ed. Bosch, 2005, págs. 56-63.

(art.137.1 y 289.2 LEC), el juez que presencia la prueba falla el asunto (art 194 LEC). Se deduce también de la regulación una mayor participación del juez, según su propio criterio, en la práctica de la prueba (art. 302, 304, 306, 307,371.2, 372, 373.1, 381, 339, 338.2, 347.2, 327, 329.1, 354.1, 383.1.11, 384.1 LEC).

A pesar de ello, la vigente LEC debilita la iniciativa judicial en materia probatoria al regular las diligencias finales (art. 435) en contraposición a las diligencias de mejor proveer que regulaba la anterior Ley de Enjuiciamiento Civil de 1981 (art. 340 a 342). Si bien mantiene el carácter facultativo y discrecional del juez, la iniciativa en cuanto a la práctica de dichas diligencias corresponde a las partes, con la excepción tasada de iniciativa de oficio recogida en el apartado segundo de dicho artículo. La Exposición de Motivos de la LEC es bien clara al respecto fundamentando tal regulación en la restricción de la actividad previa a la sentencia a aquello que sea estrictamente necesario y en la improcedencia de llevar a cabo nada de cuanto se hubiera podido proponer y no se hubiera propuesto, así como de cualquier actividad del tribunal que, con merma de la igualitaria contienda entre las partes, supla su falta de diligencia y cuidado. En cuanto a las diligencias finales ex oficio, reguladas en el apartado segundo del artículo 435, el supuesto legal comprende exclusivamente la reiteración de pruebas practicadas pero que no han deparado el resultado esperado por unas circunstancias no imputables a la parte y que han desaparecido. Así se desprende de la literalidad del precepto, siendo una interpretación extensiva incoherente con la redacción del mismo y los requisitos exigidos por éste[249]. Existe, no obstante, un sector doctrinal que entiende que dicho precepto permite practicar pruebas que las partes hubieran podido proponer en tiempo y forma, aun cuando no lo hicieron. En este sentido, MIRANDA VÁZQUEZ plantea la posibilidad de que el juez pueda designar un perito, siempre que lo precise, para que le proporcione máximas de la experiencia técnicas, de naturaleza epistemológica, específicas del área de conocimiento que sea objeto de litigio[250].

[249] A favor de tal interpretación se pronuncian autores como SACRISTÁN REPRESA, TAPIA FERNÁNDEZ y VÁZQUEZ IRUZUBIETA. Véanse: SACRISTÁN REPRESA, G., *La prueba documental en la nueva ley de enjuiciamiento civi*l, Cuadernos de derecho judicial, en "La prueba", CGPJ, Madrid, 2000, VII, pág. 319; TAPIA FERNÁNDEZ, I., *Comentarios a la ley de enjuiciamiento civil*, Vol.I, Aranzadi, Elcano (Navarra), 2001, pág1483; VÁZQUEZ IRUZUBIETA, C., *Comentarios a la nueva ley de Enjuiciamiento Civil. Doctrina y jurisprudencia de la ley 1/2000, de 7 de enero*, Dijusa, Madrid, 2000, pág.628.

[250] Véase MIRANDA VÁZQUEZ, Carlos. *¿Es realmente el Juez el "peritus peritorum"? (Propuesta de reformulación del brocardo y análisis del alcance efectivo de la valoración judicial de la prueba pericial)* en "Derecho Probatorio Contemporáneo. Prueba científica y técnicas forenses", Bustamante, M.M. (coord.), Universidad de Medellín, 2012, págs. 293-309.

Desde mi punto de vista no cabe duda de que existe un problema respecto a la ausencia, deficiencia o contradicción de la prueba pericial que debe resolverse atendiendo a la finalidad pública del proceso y al deber y obligación de los jueces de dictar sentencia conforme a derecho para garantizar el derecho de tutela judicial efectiva de las partes en el proceso. En este punto, comparto la opinión conforme a la que la regulación debiera facultar, de algún modo, al juez para acordar diligencias de prueba con la finalidad de permitirle decidir en justicia el asunto planteado. Ahora bien, también entiendo que la actual regulación no permite esta posibilidad, ya que impide al Juez acordar prueba de oficio, excepto en los procesos no dispositivos, limitándose la ley a otorgar facultades directivas del juez[251].

Ahora bien, podemos realizar un ejercicio de lectura «creativa» de la Ley para considerar admisible la posibilidad de que el Juez pueda designar una suerte de asesor técnico. Esta posibilidad se fundamentaría en la circunstancia, que ya hemos señalado, de que nuestro sistema ya efectúa excepciones al principio de aportación de parte otorgándole al juez facultades de dirección del proceso, incluso muchos autores sostienen facultades probatorias por parte del juez en artículos de la LEC como en el supuesto de las diligencias finales (art. 435 LEC). Pero, esta solución plantea muchas objeciones como se exponen en el párrafo siguiente. En cualquier caso, y al margen de las objeciones que se expondrán, resulta claro que la designación judicial del experto debería ir acompañada de garantías para las partes como la notificación de la decisión del juez de nombrar un experto y del motivo de su nombramiento, así como de los extremos sobre los que debiera informar al juez. Por último, debería regularse la participación de las partes en la designación de dicho experto y la presentación por escrito del correspondiente informe con traslado a las partes, o en su caso, de ser factible la convocatoria de una vista. Todo ello podría servir, eventualmente, para poder legitimar la intervención de tal experto en el proceso.

Ahora bien, como decía, la designación por el juez de un asesor técnico es contraria tanto a lo establecido por la ley, que no prevé específicamente esta posibilidad, como al principio de aportación de parte. Además se plantean otras objeciones: que el juez podría acabar delegando su papel en dichos expertos; que puede incluso que el experto sostenga conocimientos o teorías en que la propia comunidad científica está dividida; y finalmente podría alegarse también una enorme dificultad para encontrar y designar a tales expertos. En definitiva, hemos de tener en cuenta que el sistema judicial presupone la integridad e

[251] En sentido contrario, puede verse ABEL LLUCH, X. y PICÓ i JUNOY, J., *Viabilidad de las diligencias finales de oficio en la segunda instancia*, en Especial Cuadernos de Probática y Derecho Probatorio, núm.3/2010, Diario La Ley, núm.7494, de 22 de octubre de 2010, págs.14 y 15.

independencia de los jueces y su capacidad para ejercer su función. El juez sabe que no debe delegar su función. Y si bien es cierto que un experto puede sostener una posición concreta en una teoría en que la comunidad científica esté dividida, lo cierto es que la función del experto sería la de exponer al juez ambas teorías, es decir, informarle. Debiéndose adoptar medidas que garanticen e impidan extralimitaciones. Medidas que pueden pasar por mantener informadas a las partes sobre las peticiones del juez y las posibilidades de futuro recurso en el supuesto que para la adopción de una resolución el juez se hubiera basado en el informe de dicho experto y dicho informe fuera impreciso. En cuanto al hecho que los científicos y expertos en tecnología reconocidos son reacios a la participación como peritos en los procesos judiciales, el hecho de que dichos expertos no tengan vinculación con ninguna de las partes podría hacer más atractiva para ellos su participación, elevándose cualitativamente el papel de ciencia y tecnología en los tribunales.

En cualquier caso, el problema existe, ya que los jueces están obligados a servir al fin constitucionalmente previsto de otorgar tutela judicial. Es por ello que conforme al art. 11 LOPJ no pueden abstenerse de dictar sentencia sobre el fondo del asunto planteado. Y al mismo tiempo es claro que la solución obtenida por el juez no puede ser tomada con base en otro criterio que no sea el del convencimiento de que la decisión adoptada en conforme a derecho, ya que los jueces no pueden otorgar tutelas infundadas. Es por ello que considero que, de algún modo, debe preverse un cauce procesal para que los jueces puedan solucionar los problemas de prueba, especialmente en los asuntos en los que se debaten complejas cuestiones de ciencia y/o tecnología. Esta solución pasa por facultar a los tribunales para acordar con carácter excepcional una prueba pericial en los supuestos que la prueba de oficio resulte necesaria ante la insuficiencia o contradicción de las pruebas practicadas por las partes. De ese modo, el Tribunal podría atender a sus obligaciones constitucionales, que no son solo con las partes, sino que también lo son con el sistema entero de justicia. El propio artículo 353.2 LEC en sede de reconocimiento judicial refiere la posibilidad de que el juez practique el reconocimiento judicial asistido de «personas técnicas o prácticas en la materia». A ese fin considero que la solución más adecuada sería una modificación del art. 435 de la LEC para establecer, expresamente, la posibilidad de que en los casos apuntados de insuficiencia o contradicción de la prueba, el Juez pueda acordar prueba de oficio, como un modo de adquirir conocimientos técnicos, científicos o prácticos como instrumento de integración de su juicio lógico.

8.1.2 El perito informático

8.1.2.1 Introducción. Titulaciones en informática

La «profesión Informática», en España, está extraordinariamente difuminada, conviviendo, en la práctica profesional, personas poseedoras de una multiplicidad de títulos, tanto públicos como privados, a los que hay que añadir una larga relación de diplomas públicos proporcionados en la modalidad de enseñanza no reglada. La profesión carece de regulación y titulación oficial unificada, existiendo gran cantidad de titulaciones en informática. Los estudios universitarios de informática han adoptado una gran variedad de soluciones en el panorama universitario español. En algunas universidades el primer ciclo de la carrera superior coincidía con la ingeniería técnica, de forma que no existía como tal el primer ciclo de la superior. En otras universidades se podía estudiar tanto la carrera técnica como la superior, manteniendo un amplio abanico de posibilidades, que iban desde un cierto *numerus clausus* para el acceso al segundo ciclo hasta aquellas que habían desarrollado una política activa en sus planes de estudios para no facilitar el acceso de los ingenieros técnicos al segundo ciclo. Y finalmente algunas universidades optaron por la existencia de un único título, evitando las complicaciones que suponían la convivencia de los tres. La falta de clarificación ha llegado a la actividad profesional, siendo ya indistinta la solicitud de un ingeniero técnico o superior, erosionando el papel de ambos.

Los titulados en Informática pertenecen al área de las Tecnologías de la Información y Comunicaciones (TIC), bajo cuya denominación se reúnen todas aquellas enseñanzas que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de datos e informaciones contenidos en señales de naturaleza acústica, óptica o electromagnética. Estas disciplinas son las siguientes: Tecnologías físico- eléctricas básicas; circuitos y equipos electrónicos; tecnología de software; arquitectura y tecnología de computadores; ingeniería telemática; radio-comunicaciones; y automatización y control industrial. Examinando sólo los títulos oficiales existentes en el sistema educativo español se aprecia una triplicidad de los mismos: 1. Ciclos formativos de FP; 2. Ingeniería Técnica, con dos especialidades: Gestión y Sistemas; y 3. Ingeniería Informática. Aunque la duración y contenido de todos ellos no ha dado lugar a confusión, no queda definida su diferenciación profesional. A esta multiplicidad de títulos se añade la presencia de la Ingeniería de Telecomunicaciones que presenta, además de una Ingeniería Superior, cuatro Ingenierías Técnicas. Por otro lado, en el sector de la informática, se desenvuelven entre otros, titulados universitarios procedentes de la Ingeniería Industrial así como Licenciados en Ciencias Físicas y en Matemáticas.

A lo anterior hay que añadir titulaciones procedentes del sector empresarial. Éste ha venido ofertando diplomas en forma de título de carácter profesional (que se adapta en principio a cada una de sus demandas locales), o en forma de certificación, como mecanismo tanto de negocio interno como para reforzar su presencia en el mercado. Son ejemplos las compañías Microsoft, SUN, Oracle o Cisco. Como consecuencia de la globalización de estas herramientas, las facilidades de aprendizaje y la demanda surgida, se están convirtiendo en vías alternativas a los títulos oficiales para el ingreso en la profesión. Finalmente, existen también titulaciones no regladas que se han impulsado desde las entidades responsables de la educación. Ejemplos de ello son la «Iniciativa Form@tic» de la Generalitat de Cataluña (para reciclar a licenciados próximos a la informática hacia empleos relacionados con la Sociedad de la Información), y otros títulos que se han planteado por la propias Universidades.

A raíz de dicha diversidad, en marzo de 2005 la Agencia Nacional de Evaluación de la Calidad y Acreditación (ANECA) editó el Libro Blanco de la Titulación para el Grado en Ingeniería Informática, remitiéndolo una vez concluido a la Dirección General de Universidades (MECD) y al Consejo de Coordinación Universitaria para su consideración. Dicho libro fue el resultado del trabajo llevado a cabo por una red de universidades españolas con el objetivo explícito de realizar estudios y supuestos prácticos útiles en el diseño de un Título de Grado adaptado al Espacio Europeo de Educación Superior (EEES). Dicho Libro recoge todos los datos anteriores[252]. Frente a las tres titulaciones universitarias de Informática existentes en España (una de dos ciclos, Ingeniería Informática, y dos de un único ciclo, Ingeniería en Informática de Gestión e Ingeniería Técnica en Informática de Sistemas), la propuesta efectuada por el Libro Blanco fue la reducción del catálogo de titulaciones a una única titulación de grado: la «Ingeniería en Informática» . Dicho grado englobaría contenidos generales y básicos, que permitieran posteriormente llegar a las especializaciones acordes con los diferentes ámbitos de aplicación de la informática y permitir una rápida adaptación a la constante evolución de las TIC. Se reduce por lo tanto el nuevo espectro de la TIC a las titulaciones europeas de: «Ingeniería en Informática» e «Ingeniería de Telecomunicación». Una vez obtenido el grado (primer ciclo) se daría acceso al Máster que supondría la especialización profesional de los ingenieros en informática o bien a su preparación para la investigación. El Máster debería permitir el acceso a la realización de la tesis doctoral con el objeto de obtener el grado en doctor.

Según definición del Libro Blanco el ingeniero en informática debe ser un experto en tecnología software, en arquitectura y tecnología de los

[252] *Libro Blanco de Titulación de Grado en Ingeniería Informática*. Ed. Agencia Nacional de Evaluación de la Calidad y Acreditación, Madrid, marzo 2005, págs. 81, 150-152.

computadores, en tecnología de las redes de computadores y en equipos electrónicos, conocimientos que le capacitan para trabajar en todo tipo de empresas y en todos los departamentos de la empresa, aunque fundamentalmente se agrupen en el departamento de Informática[253]. Distinguiéndose tres perfiles profesionales: Perfil profesional de «Desarrollo Software» (se trata de un perfil de gran capacitación tecnológica que, aunque está orientado principalmente al desarrollo de soluciones software, requiere conocimientos tanto de hardware –porque en ciertas áreas de aplicación, las soluciones de software se ven influidas por la naturaleza del hardware- como de los sistemas empotrados); perfil profesional de «Sistemas»; y perfil profesional de «Gestión y Explotación de Tecnologías de la Información». Sin embargo, las recomendaciones del Libro Blanco no se han aplicado de modo uniforme en las Universidades españolas. Y la aplicación del Plan Bolonia por parte de las universidades ha comportado además la aparición de más de 300 titulaciones distintas en el campo de la ingeniería (120 títulos de grado y 250 Masters frente a las 15 titulaciones en ingeniería que existían en España).

Pese a los constantes requerimientos de regulación de la profesión y titulaciones oficiales de Colegios y Asociaciones hasta el momento sólo se ha publicado en el BOE de fecha 4 de agosto de 2009 la Resolución de fecha 8 de junio de 2009 de la Secretaría General de Universidades, por la que se da publicidad al Acuerdo del Consejo de Universidades. En dicho Acuerdo se establecen recomendaciones para la propuesta por las universidades de memorias de solicitud de títulos oficiales en los ámbitos de la Ingeniería Informática, Ingeniería Técnica Informática e Ingeniería Química. Ello hasta tanto se establezcan las oportunas reformas de la regulación de las profesiones con carácter general en España y, en concreto, la actualización del listado de las mismas previsto en la normativa vigente, atendiendo a la petición formulada por la Comisión de Ingeniería y Arquitectura del Consejo de Universidades en su sesión del día 4 de diciembre de 2008. Sin embargo, actualmente la variedad de titulaciones universitarias sigue siendo manifiesta. Así la Universidad Politécnica de Cataluña ofrece grado en ingeniería informática y grado en ingeniería de sistemas TIC; en la UPC de Madrid se imparten desde el grado en informática en la Universidad de Informática hasta el grado de ingeniería de Computadores o grado de ingeniería de software en la Escuela Universitaria Informática; en la Universidad Autónoma de Madrid se imparte en la Escuela Politécnica Superior la ingeniería informática -alertando que se extinguirá por el grado en ingeniería informática- y el grado de ingeniería informática etc.
A raíz de la diversidad de titulaciones nacieron para la protección de los intereses de sus miembros las primeras organizaciones profesionales. La

[253] *Véase el Libro Blanco de Titulación de Grado en Ingeniería Informática*. Ed. Agencia Nacional de Evaluación de la Calidad y Acreditación, Madrid, marzo 2005, pág. 163.

primera tomó el nombre de ATI (Asociación de Técnicos en Informática). Más adelante se creó ALI (Asociación de Licenciados en Informática) a medida que se iban incorporando al mercado del trabajo lo nuevos titulados en informática. Posteriormente aparecieron las AI2 (Asociaciones de Ingeniería en Informática), normalmente de carácter autonómico, que han desarrollado un papel muy activo en la creación de los Colegios Profesionales, en su doble versión de Ingeniería Técnica Informática e Ingeniería Informática. Recientemente se ha creado ANTPJI (Asociación Nacional de Tasadores y Peritos Judiciales Informáticos) y ASPEI (Asociación Profesional de Peritos Informáticos). Dichas Asociaciones vienen denunciando la falta de regulación y el intrusismo profesional.

Por otro lado, existen diferentes colectivos de ingenieros –industriales, caminos, telecomunicaciones, agrónomos e informáticos- agrupados en diversos colegios. Y a su vez existen Colegios de ingenieros informáticos y el Colegio de ingenieros técnicos informáticos. Sin embargo, la entrada en vigor de la ley ómnibus 25/2009 del 22 de diciembre, que elimina la obligatoriedad de la mayoría de visados de proyectos en ingeniería junto a la aplicación del Plan Bolonia por parte de las universidades y la multiplicación de títulos en ingeniería, ha puesto en cuestión el modelo actual de los colegios profesionales técnicos de nuestro territorio, por lo que las Asociaciones se han movilizado en busca del nivel de acreditación profesional y formación continuada de sus afiliados. El ejercicio profesional liberalizado deja a los colegios tradicionales sin los ingresos de los visados y ante una previsible pérdida de miembros y a los ingenieros de las nuevas titulaciones sin una masa crítica para constituir sus propios colegios. Ante este panorama han nacido nuevas propuestas como la del Col·legi d'Enginyers Industrials de Catalunya (AEIC) que ha iniciado un proceso para liderar la consolidación de todos los ingenieros, sea cual sea su especialidad, en una única Asociación, a semejanza de las existentes en Alemania o Reino Unido. Dichas Asociaciones clasifican a sus miembros según su especialidad y su capacidad individual, asignándoles un cierto nivel de acreditación –que puede ir creciendo a lo largo de los años– que se vincula a diversos aspectos como, por ejemplo, su «prestigio profesional», los «títulos académicos» que posee o su «experiencia profesional». Si bien en Alemania y Reino Unido no es preceptiva la afiliación a dichos colegios, sólo los ingenieros que forman parte de estas asociaciones obtienen la confianza de las empresas en dichos países.

8.1.2.2 El perito informático-forense

El perito tecnológico es una persona experta con conocimientos especializados en determinados campos de la ciencia y conocimientos técnicos o prácticos, que transmite al juez a través del dictamen pericial para que aquél pueda valorar hechos o circunstancias relevantes en el asunto sobre el que versa el pleito o adquirir certeza sobre los mismos. El perito debe, pues, tener conocimientos especializados de interés para el proceso. Dichos conocimientos deberán acreditarse mediante «títulos profesionales oficiales», es decir, tal y como establece el artículo 340.1 LEC «*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»*.

Las condiciones profesionales son exigibles tanto para los peritos nombrados de forma directa por las partes como para los designados judicialmente. Resultaría un contrasentido permitir una afirmación pericial, aun a las partes, que fuera llevada a cabo por un sujeto que no posee el grado de conocimientos mínimo que exige en todo caso el artículo 340 LEC, ya que no existe constancia de que el informe se elabore de forma adecuada. Por lo tanto, si el informe técnico presentado no reuniera estos requisitos, el mismo debería rechazarse y tomarse como inexistente, al no poder ser calificado como dictamen pericial[254]. Sostenemos tal opinión pese a que cuando la Ley de Enjuiciamiento Civil regula el perito nombrado directamente por las partes en su artículo 335.1 LEC alude de modo genérico a los «*peritos que posean los conocimientos correspondientes»,* sin hacer referencia expresa a la titulación oficial.

No obstante, parte de la doctrina mantiene que las explícitas condiciones exigidas por el artículo 340 LEC sólo son aplicables a los peritos designados judicialmente al no ser exigidas para el perito de parte en el art. 335 LEC. Lo anterior no excluye una mayor credibilidad en la valoración de los dictámenes o informes de especialistas en la materia, en cuanto el Tribunal tomará en consideración la formación y aptitud del perito a la hora de valorar el dictamen[255]. No compartimos dicha opinión por cuando ello supondría que el

[254] Véase ASENCIO MELLADO, J.M, *Proceso civil práctico*, Gimeno Sendra., V. (dir), t. IV, ed. La Ley, Madrid, 2005, págs. 672-673; RIFA SOLER, J.M. *Comentarios a la nueva Ley de Enjuiciamiento Civil*, Fernández Ballesteros, M.A., Rifa Soler, J.M., y Valls Gombau, JF (coord..), ed. Atelier, Barcelona, 2000, pág. 1578; ILLESCAS RUS, V. *El dictamen de peritos*, "*La prueba en la nueva Ley de Enjuiciamiento Civil*", jornada monográfica, A Coruña, 4 de mayo de 2001, organizada por Enfoque XXI y el Ilustre Colegio Provincial de la Coruña, págs. 8-9.

[255] Véase MONTERO AROCA, J., *La prueba en el proceso civil*, 4ª ed., ed. Civitas, Madrid, 2005, págs. 356 y 396 y ss.

dictamen pericial pudiera ser emitido por personas sin título ni cualificación alguna, que solo manifiesten tener conocimientos en la materia en aquellas ocasiones en que las partes aportaran sus respectivos dictámenes periciales sin solicitar designa judicial de perito. Algunos autores matizan que pese a que los requisitos profesionales exigidos en el artículo 340 LEC no son formalmente exigibles al perito de parte no existe inconveniente en que las partes acudan a los criterios e indicaciones que se establecen en dicho artículo, siendo evidente que las partes litigantes por su propio interés elegirán peritos con preparación o titulación adecuada al objeto de la pericia[256].

Especial mención debemos efectuar a la pericia corporativa, en la misma las Academias e instituciones culturales y científicas gozan de una «habilitación general» para emitir dictámenes siempre que *«se ocupen del estudio de materias correspondientes al objeto de pericia»* (art. 340.2 LEC), mientras que se exige una «habilitación legal» para el resto de personas jurídicas. Las personas que dentro de la persona jurídica efectúen el dictamen deberán estar en posesión de la titulación profesional oficial o, en su caso, ser personas entendidas en la materia, por aplicación analógica de la normativa relativa al perito individual.

El problema que se plantea en general en toda Europa y en concreto en España en el ámbito de la informática-forense es la falta de normativa que precise las características que debe reunir un experto en Informática Forense, y las subdisciplinas que debieran formarse dentro de la misma. En Europa en general no existe formación universitaria en materia de análisis forense de medios digitales, aunque sí existen formaciones de postgrado en informática forense en países como Francia y en investigación de ciberdelitos, por ejemplo en Irlanda. Sólo Rumania exige una certificación o autorización oficial del Estado para poder actuar como experto[257].

En España, tal y como hemos explicado en el epígrafe anterior, carecemos de regulación de la profesión informática, y por lo tanto también carecemos de normativa que regule una titulación oficial en «informática forense» como especialidad dentro de la informática en general. Por otro lado, tampoco existe normativa específica que determine un plazo de experiencia profesional que acredite a una persona con conocimientos informáticos como «experto» a los efectos de que pueda declarar en juicio como perito en informática-forense.

---

[256] Está de acuerdo con dicha opinión GUZMAN FLUJA, V., en *El proceso civil,* V. III, Escribano Mora, F. (coords.), ed. Tirant Lo Blanch, Valencia, 2001, pág. 2474.

[257] Véase sobre este extremo: INSA, F., LÁZARO, C. y GARCÍA, N. (2008). *Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad. Un proyecto europeo*. Enl@ce: Revista Venezolana de Información, Tecnología y Conocimiento, 5 (2), págs.139-152.

Dicha situación supone que en la actualidad cualquiera que acredite algún tipo de relación con el amplísimo campo de la informática puede actuar como perito informático y en concreto como perito informático forense en juicio con la falta de garantías que ello supone. Ni siquiera los cursos impartidos por Colegios y Asociaciones son obligatorios. Tratándose, además, de cursos de duración muy limitada y por lo tanto de contenidos insuficientes.

Es evidente que la falta de normativa y la confusión actual entre titulaciones, así como la falta de titulación oficial en informática forense dificulta notablemente la designación del perito judicial para el objeto de pericia y conlleva la actuación en juicio de personas que actúan como peritos expertos pero carecen de la formación necesaria en la disciplina informático forense. Ello reviste especial gravedad en cuanto puede conllevar la pérdida de valor de la prueba presentada por la parte (en el supuesto de obtención mediante métodos inapropiados, por ejemplo el no uso de bloqueadores de escritura al acceder a los repositorios de información, la contaminación de la misma etc.) e incluso la apreciación de su ilicitud si no se han respetado derechos constitucionales en su obtención. La falta de verdaderos expertos titulados universitarios oficiales en informática-forense y con experiencia acreditada supone la actuación de personas no cualificadas que pueden cometer graves errores en el tratamiento de la prueba informática por desconocimiento y que avocan a una prueba sin valor alguno por infracción de la legalidad vigente o bien por falta de conocimientos técnicos y prácticos suficientes.

Es por ello que resulta fundamental el reconocimiento de la existencia de la informática forense como disciplina y la necesidad de una titulación oficial en dicha especialidad para poder ejercer como perito, pero además es necesario que se garantice para poder ejercer como perito en dicha disciplina experiencia suficiente, actualización científica y solvencia profesional. Como afirmaba Thomas Penfield Jackson, Juez Federal de Estados Unidos «(…) e*n definitiva, es importante implementar un sistema que garantice que los peritos que van a intervenir en un proceso, además de imparcialidad, tengan experiencia, actualización científica y solvencia profesional*» [258] .

La informática forense es una disciplina que se compone de diversas especialidades[259] y requiere no solo tener conocimientos técnicos y prácticos

[258] Véase las declaraciones de THOMAS PENFIELD JACKSON, Juez Federal de Estados Unidos, en la página web con la dirección electrónica http://goo.gl/OOmBm.

[259] DARAHUGE y ARELLANO efectúan la siguiente clasificación: 1.- Computacional, dentro de la que distinguen entre fija, móvil, Integrada al atuendo (vestimenta), de base (sistemas operativos) y de aplicación (programas ejecutados en un determinado sistema operativo); 2.-Conectividad; 3.-Telefonía forense; 4.-Sistemas de posicionamiento global GPS; 5.-Archivos documentales digitalizados (tratamiento de imágenes, video y audio); 6.-Residuos informáticos (tratamiento de

sino también conocimientos legales. El perito informático forense debe ser un especialista capaz de ejercer actividad probatoria en entornos informatizados. Desde un punto de vista técnico el experto en informática forense para poder llevar a cabo su labor con plena eficacia y garantías debe no sólo tener conocimientos específicos informáticos o de telecomunicaciones sino experiencia en el manejo de evidencias digitales. Es decir, el perito informático-forense debe tener una cualificación superior a un experto informático, que instala, configura, repara, formatea o efectúa copias de seguridad, con el que sólo comparte una formación básica en informática[260]. Necesita tener conocimientos sobre las herramientas y los procesos específicos que se requieren en cada caso concreto dentro de un entorno informatizado. Lo anterior incluye, por ejemplo, conocimientos sobre las herramientas y procesos de reconstrucción de archivos destruidos o sobre las herramientas y procedimientos de extracción de archivos.

Pero además debe estar formado en «informática forense» –también denominada «*computer forensics*» o análisis forense de dispositivos digitales-. El llamado «*computer forensic*» o «informático forense» debe ser experto en identificar, analizar, preservar y saber presentar las evidencias digitales en forma que sean aceptadas en el proceso judicial. Necesita no sólo conocimientos del hardware y el software informático sino también de correctas técnicas que eviten que se destruyan o comprometan las evidencias digitales. Por ello debe actuar con absoluto rigor y siguiendo los estándares de investigación forense, garantizando un correcto tratamiento de datos, y la no alteración de la evidencia electrónica, así como garantizando la cadena de custodia de los elementos que constituirán la prueba digital que se presente en el proceso judicial. Para ello se requiere conocer los protocolos de cadena de custodia para que dichas evidencias electrónicas puedan tener valor probatorio en el proceso judicial. Pero además necesita tener conocimientos legales fundamentales a nivel procesal y constitucional. El informático-forense necesita reunir en su persona tanto «conocimientos» como «competencias». Refiriéndose el primer término a la asimilación de información a través de cualquier acción formativa, y el segundo a la habilidad demostrada para aplicar este conocimiento en la resolución de tareas y problemas específicos.

---

residuos físicos y lógicos). Véase DARAHUGE, M.E Y ARELLANO GONZALEZ, L.E. *Manual de Informática Forense (Prueba Indiciaria Informático Forense)*. Ed. Errepar, 2012, pág. 15.

[260] En la obra de DARAHUGE, M.E Y ARELLANO GONZALEZ, L.E. *Manual de Informática Forense (Prueba Indiciaria Informático Forense)*. Ed. Errepar, 2012, los autores realizan una comparativa entres los conocimientos y capacidades del perito experto en informática forense y el experto en informática/computación. págs. 11-14.

La Asociación Española de Normalización y Certificación (AENOR,) a través del Proyecto del Comité Técnico de Normalización AEN/CTN 197, Norma 71506, *Tecnología de las Información, Metodología para el análisis forense de las evidencias electrónicas,* determina una serie de categorías con que ha de contar el personal involucrado en análisis forense, clasificándolas en técnicas, profesionales y personales. Desde un punto de vista «técnico» se distinguen: El conocimiento de la legislación vigente en lo concerniente a la relevancia digital de las evidencias forenses y de cómo éstas han de ser tratadas en todo su ciclo de vida para no perder validez; el conocimiento de software y hardware forense existente en la industria actual; entrenamiento adecuado en labores de manejo de la evidencia digital; conocimientos en labores de identificación de la información forense; conocimientos sobre los métodos existentes de extracción de contraseñas; conocimientos sobre los diferentes elementos de Internet que pueden ser almacenados en un sistema; conocimientos sobre las diferentes técnicas y herramientas usadas en el fraude informático; y conocimientos sobre los principales métodos usados por los intrusos informáticos.

A nivel «profesional» se requiere tener experiencias previas en las tareas a desempeñar en las diferentes fases de análisis forense y una formación continua en el ámbito forense. Y finalmente a nivel «personal» se exige: Honestidad, discreción y cumplimiento del oportuno código de práctica profesional; espíritu crítico e independiente, de mente abierta para tomar en consideración diferentes opiniones y puntos de vista; perseverancia, autodisciplina, con capacidad de aprendizaje y adaptación a nuevos escenarios; capacidad de observación, análisis y extracción de conclusiones basadas en el razonamiento y análisis lógico; y capacidad de describir situaciones y fenómenos complejos en términos comprensibles[261].

Los especialistas o expertos en informática forense necesitan conocimientos técnicos que deberán actualizar de modo permanente dado la rapidez de evolución de los mismos en este ámbito. De igual modo necesitarán recursos tecnológicos suficientes, debido a la complejidad de las nuevas tecnologías y su rápida evolución, es decir, contar con un laboratorio profesional con *know how* suficiente, y actualizado con tecnología puntera disponiendo de los medios necesarios y más novedosos para la realización de todas las fases de investigación necesarias. Tener no sólo conocimientos técnicos sino también conocimientos jurídicos para garantizar la legalidad de la prueba y su admisión en juicio. Y disponer de facilidad para exponer los resultados obtenidos de un modo claro y entendible para personas no técnicas en la materia. El informático forense deberá tener conocimientos técnicos, legales y prácticos

[261] Estas recomendaciones se amplian en la Guía «*CEN/Guide 14 Common policy guidance for addressing standardisation on qualification of professions and personnel*».

suficientes para diseñar una estrategia de investigación pericial que culmine con la presentación inteligible ante el juez[262]. Algunos autores vienen señalando la conveniencia que la titulación mínima necesaria para un informático-forense sea una licenciatura universitaria, preferentemente en Informática, Ingeniería o Matemáticas, y contar como mínimo con dos años de experiencia[263].

En España sería aconsejable la unificación de las titulaciones oficiales en un único grado de ingeniería informática en todas las universidades y la existencia de especialización en «*informática forense*» cursando un máster que daría lugar a un título oficial universitario. Este último título incluiría no sólo conocimientos técnicos sino también jurídicos. Siendo requisito indispensable para poder ejercer como perito la necesidad de contar con una experiencia acreditada de entre dos y cinco años, como vienen señalando los expertos.

La tenencia de un título universitario oficial en ingeniería informática forense y la experiencia podría acreditarse a través de una única Asociación que agrupara toda la ingeniería informática en semejanza la *Verein Deutscher Ingenieure* (VDI) en Alemania asociación que goza de prestigio y es centro de referencia, fomentando una formación continuada de sus miembros[264]. Existen otras iniciativas que han resultado también eficaces, como la creación en Estados Unidos de América por parte de la Asociación Americana para el Avance de la Ciencia (AAAS) de la llamada Corte de Expertos Científicos (CASE). Servicio que ayuda a los jueces federales y estatales, jueces y árbitros de derecho administrativo en la designa de expertos que intervengan en los procesos judiciales. Dicha organización facilita la identificación de científicos altamente calificados, ingenieros y profesionales de la salud para que puedan ser designados como expertos científicos. Originalmente concebido como un proyecto de estudio, se limitó a los jueces federales de distrito, recibiendo sus primeras peticiones por parte de los jueces en febrero de 2001. No obstante,

---

[262] Véase sobre el tema FREDESVINDA INSA, *Procedimiento de obtención y análisis forense de dispositivos electrónicos*, en "las Jornadas sobre Prueba electrónica, obtención, admisibilidad y jurisprudencia" organizadas por la Sección de Derecho de las Tecnologías de Información y Comunicación del Colegio de Abogados de Barcelona en fecha 26 de enero de 2011.

[263] Sobre el particular véase BEVILACQUA, M., *¿Qué es el computer forensics?,* en e-newsletter Cybex, septiembre, 2008, núm. 41, págs. 21-24; y INSA MÉRIDA, F; LÁZARO HERRERO, C; GARCÍA GONZÁLEZ, N., *Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad. Un proyecto europeo*, en Revista Venezolana de Información, Tecnología y Comunicación, año 5, mayo-agosto, 2008, página 149.

[264] Se recoge dicha propuesta en algunos artículos publicados en el periódico La Vanguardia, en concreto en la página 22 de la edición del día 27.02.2011, y en la página 49 de la edición del día 5.7.2011. Pueden consultarse dichos artículos en la hemeroteca de La Vanguardia.com página web http://goo.gl/0ThgU y http://goo.gl/Oj1DM.

dado el éxito del proyecto, en septiembre de 2004 se amplió para incluir a los tribunales estatales de prueba, los tribunales de derecho administrativo y de arbitraje. CASE elige y recomienda a los expertos basándose en el caso concreto judicial y a los requerimientos fijados por parte del juez. En dicha organización se utilizan varios métodos y recursos para identificar a los expertos adecuados, incluyendo asociaciones profesionales y otras instituciones o sociedades científicas. El grupo está compuesto por personas reconocidas y respetadas en sus respectivas disciplinas científicas y de ingeniería. Y las personas que lo componen tiene dos funciones principales: La primera es ayudar a identificar a los científicos, ingenieros y médicos altamente calificados en el área de especialización buscada por un juez que ha solicitado la asistencia del proyecto; y la segunda investigar a los científicos recomendados, ingenieros o médicos en cuanto a su méritos científicos, su reputación y su capacidad de comunicar en las audiencias información muy técnica a personas legas en dichos conocimientos[265] .

8.1.3 Pericial individual y pericial corporativa

La vigente Ley de Enjuiciamiento Civil regula la pericial individual –emitida por una persona física- y pericial corporativa –emitida por una persona jurídica- como alternativas posibles a la emisión de un dictamen pericial. En este segundo supuesto «*Podrá (….) solicitarse dictamen de Academias e Instituciones culturales y científicas que se ocupen del estudio de las materias correspondientes al objeto de la pericia. También podrán emitir dictamen sobre cuestiones específicas las personas jurídicas legalmente habilitadas para ello*» (art. 340.2 LEC).

La pericial corporativa pierde en la actual regulación el carácter de excepcional con que venía regulándose en la anterior Ley de Enjuiciamiento Civil de 1881 (art. 631.1), en la cual sólo se permitía pedir pericial corporativa cuando el dictamen pericial exigía operaciones o conocimientos científicos especiales, pues si los conocimientos precisos se podían proporcionar por los peritos individuales, la pericia colegiada era improcedente (STS, entre otras, de 5 de marzo y 16 de octubre de 1956, y 29 de septiembre de 1.998). Por otro lado, la vigente LEC permite acudir a «personas jurídicas privadas», siempre que se hallen legalmente «habilitadas para ello». La anterior regulación sólo permitía la emisión de dictámenes periciales a Academias, Colegios o Corporaciones

[265] Puede obtenerse información sobre la «*American Association for the Advancement of Science*» en la página web http://goo.gl/N4jAi. También puede obtenerse información sobre «*The Court Appointed Scientific Experts*» en la página web http://goo.gl/XURpY.

oficiales con exclusión de instituciones privadas y Cátedras universitarias -*al no tener éstas entidad corporativa, ni asociativa, ni colegial y no debiendo confundirse con quien ejerce el cargo de catedrático*- (STS 21 de junio de 1999). La habilitación requerida por la vigente LEC debe proceder de una norma jurídica expresa o de la autoridad administrativa competente. Suscita duda si la «habilitación» debe considerase general, es decir, que la persona jurídica privada esté legalmente reconocida como poseedora de conocimientos específicos, o por el contrario precisará que esté habilitada para emitir dictámenes[266].

La pericia podrá aportarse por las partes junto a los escritos de alegaciones. En el supuesto de conformidad de las partes en una misma «entidad» podrá efectuarse designa judicial (art. 339.4 LEC). Sin embargo, a falta de acuerdo, no existe norma que permita acudir a la misma, por cuanto aún cuando podría ser de aplicación el sistema de lista corrida (art. 341.1 LEC) previsto para peritos individuales, no existe en la práctica –al menos en Cataluña- listado alguno remitido por Colegios profesionales o entidades análogas, ni de Academias e Instituciones culturales y científicas de institutos o instituciones, cátedras etc. que permita llevarlo a la práctica[267]. A falta de regulación si el juez considera dicha prueba pericial corporativa pertinente y útil procederá a la designa judicial directa. Siendo pocos en la práctica forense los supuestos en que se proponga pericial corporativa en el ámbito de evidencia electrónica.

En lo referente al procedimiento la pericial corporativa se rige por el correspondiente al dictamen de peritos estando por lo tanto sujeta a preclusión. A diferencia del artículo 631 LEC 1881 que excluía la preclusión de la pericia corporativa permitiendo su incorporación a los autos incluso después de transcurrido el término de prueba. La institución a la que se encargue el dictamen expresará a la mayor brevedad qué persona o personas se encargarán directamente de prepararlo, a las que se exigirá el juramento o promesa previsto en el apartado segundo del artículo 335 (art. 340.3 LEC). Los sujetos individuales podrán ser objeto de recusación, puesto que se les aplican las normas correspondientes a los peritos individuales. Y en los supuestos de incumplimiento del deber que les corresponde se originará una responsabilidad solidaria entre institución e individuo designado. La regulación en la Ley de Enjuiciamiento Civil de la pericial corporativa es bastante breve e incompleta, no constando, por ejemplo, siquiera un específico trámite de aclaraciones. Ello no puede suplirse por analogía de todos los preceptos relativos a la pericial individual en cuanto algunos son inaplicables.

---

[266] Se plantea dicha cuestión ABEL LLUCH, X. en *Derecho probatorio*. Ed. Bosch, 2012, pág. 668.

[267] Información obtenida mediante consulta formulada al Colegio de Ingeniería Informática de Cataluña y a la Subdirección General de Soporte Judicial de la Generalitat de Cataluña.

En nuestros Tribunales no se hace apenas uso de la pericial corporativa en el ámbito de la evidencia electrónica. Probablemente ello es debido a la falta de Institutos o Instituciones informático-forenses de estudio e investigación de carácter público o privado y de cátedras específicas universitarias. Lo que va íntimamente ligado a la falta y a la inminente necesidad de regulación de estudios y titulaciones universitarias oficiales en informática forense. Y por otro lado, tampoco existen grupos de estudio e investigación dentro de los colegios oficiales, que pudieran emitir dichos dictámenes. La existencia de dichos Institutos o Instituciones públicos o privados, cátedras, y grupos de estudio e investigación en colegios oficiales, que gozaran de conocimiento, estudio, experiencia y reconocimiento nacional e internacional por trabajos y publicaciones, facilitaría la designa de las mismas para emisión de dictámenes corporativos, y una mayor garantía de certeza en la evidencia científica o técnica que llega a nuestros tribunales. En la actualidad existe alguna iniciativa al efecto en emisión de dictámenes informático-forenses, como el Instituto de Ciencias Forenses de la Universidad Autónoma de Madrid[268].

En lo referente a los Colegios profesionales no se conoce grupo alguno de estudio o investigación. Y si bien en sus estatutos no se hace mención expresa a la pericial corporativa los fines definidos en ellos habilitan o permiten el cumplimiento de encargos bajo la tutela del artículo 340.1 de la LEC. Así «e*l Colegio Oficial de Ingeniería en Informática de Cataluña tiene los fines propios de las corporaciones profesionales y, como finalidad última, la tutela del correcto ejercicio de la profesión como garantía de los derechos de los ciudadanos/nas. En particular, a título enunciativo y no limitativo, tienes las siguientes finalidades: (…) 8. Ejercer todas las funciones que le sean encomendadas por las Administraciones públicas y asesorar Organismos del Estado de la Comunidad Autónoma y las Corporaciones locales, las personas y entidades públicas y privadas, y los mismos colegiados, emitiendo informes, resolviendo consultas, o actuando en arbitrajes técnicos y económicos a instancia de las partes; 9. Cooperar con la Administración de Justicia y otros organismos Oficiales o particulares en la designación de ingenieros en informática que deban intervenir como peritos en los asuntos judiciales, y en otros, y que deban realizar informes, dictámenes, tasaciones u otras actividades profesionales…*» (artículo 7 de los estatutos vigentes del Colegio de Ingeniería en Informática de Cataluña ubicado en el Capítulo II rubricado «*De los fines y de las facultades*»). Por otro lado, los estatutos aprobados por la asamblea del Consejo de Colegios de Ingeniería Informática, pendientes de aprobación y publicación en el BOE, establecen en el Título III «*Sobre el Consejo General de Colegios*», Capítulo I «*Disposiciones Generales*», *artículo 26 lo siguiente:* « *1. Son funciones del Consejo General de Colegios Oficiales de Ingeniería en Informática, cuando tengan ámbito o repercusión*

[268] Puede consultarse información relativa al Instituto de Ciencias Forenses y de la Seguridad (ICFS) de la Universidad Autónoma de Madrid en la página web www.icfs.uam.es

nacional, las que a continuación se citan, siempre y cuando no entren en conflicto con las competencias de los distintos Colegios profesionales y Consejos Autonómicos (…) b) Ejercer cuantas funciones les sean encomendadas por la Administración y colaborar con ésta mediante la realización de estudios, emisión de informes, elaboración de estadísticas y otras actividades relacionadas con sus fines que puedan serles solicitadas o acuerden formular por propia iniciativa…».

Las instituciones científicas en la actualidad pueden ser determinantes para la emisión de dictámenes en cuanto pueden facilitar en ámbitos muy complejos científica y tecnológicamente conocimientos actualizados y experiencia práctica. La pericial corporativa persigue que en supuestos de especial complejidad del hecho objeto de prueba el perito disponga de los medios necesarios para realizar los informes solicitados. Por ello, adquiere mayor relevancia en la prueba informática forense, ya que en la actualidad los peritos informáticos forenses que actúan individualmente y firman un dictamen en numerosas ocasiones necesitan acudir a laboratorios de análisis por no disponer de los medios propios necesarios.

Esta prueba podría ser también la solución a la desigualdad generada en el proceso según los medios económicos de las partes. La existencia de un organismo público adscrito al órgano jurisdiccional, técnicamente preparado y que ofreciera garantías de imparcialidad, y que emitiera un informe sin coste inmediato para la parte sin recursos económicos, sin perjuicio de lo que con posterioridad se fijara en costas, ayudaría a garantizar la emisión de informes y paliar las diferencias creadas entre las partes por motivos económicos en el proceso, lográndose que éste fuera más justo e igualitario. Sin embargo ello requeriría de un nuevo coste económico para el Estado algo ahora al parecer inasumible.

8.1.4 La confección de listas de peritos informáticos

Los peritajes pueden ser solicitados privadamente, es decir extrajudicialmente, por la parte o bien puede tratarse de una designa judicial a petición de la parte y ya dentro del proceso. En el caso de peritajes privados, las partes pueden solicitar un perito a los Colegios o Asociaciones o pueden solicitar un peritaje a un profesional concreto según su propio criterio.

Los Colegios y Asociaciones mantienen ciertas listas que gestionan según el Reglamento de Peritajes vigente. Así, por ejemplo, en el Colegio de Ingenieros Informáticos de Cataluña la parte interesada solicita un perito a la Secretaria de Comisión de peritajes de dicho Colegio oficial. La Secretaria solicita información

a la parte para determinar la especialidad idónea que debe tener ese perito y elabora un listado específico de peritos para el caso solicitado incorporando sólo aquellos peritos idóneos que hayan confirmado su disposición a efectuar el encargo. La parte elige el perito que considera oportuno, poniéndose las partes de acuerdo para la aceptación del cargo. La provisión de fondos se tramita a través de la Secretarias de la Comisión de Peritos. Y una vez satisfecha la provisión, el perito realiza y entrega el informe, cobrando el Colegio un porcentaje por gastos de administración[269].

Por otro lado, las partes podrán solicitar en el proceso la designación judicial de un perito. Tratándose de designación judicial de peritos en los procesos jurisdiccionales podemos diferenciar su aspecto jurisdiccional y su aspecto gubernativo. Desde un punto de vista «jurisdiccional», la designa concierne a la designación de la persona concreta que habrá de actuar como perito en un proceso determinado. «*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*» (artículo 340 LEC).

Cuando hablamos de la designa judicial desde su aspecto meramente «gubernativo», su alcance o contenido no es sino el puramente instrumental de establecer el elenco de personas al que habrá de acudir para realizar tal designación (STS 30 de marzo de 2010)[270]. En este sentido «*1. En el mes de enero de cada año se interesará de los distintos Colegios profesionales o, en su defecto, de entidades análogas, así como de las Academias e instituciones culturales y científicas (*a que se refiere el art. 340.2 LEC*) el envío de una lista de colegiados o asociados dispuestos a actuar como peritos. La primera designación de cada lista se efectuará por sorteo realizado en presencia del Secretario Judicial, y a partir de ella se efectuarán las siguientes designaciones por orden correlativo. 2. Cuando haya de designarse perito a persona sin título oficial, práctica o entendida en la materia, previa citación de las partes, se realizará la designación por el procedimiento establecido en el apartado anterior, usándose para ello una lista de personas que cada año se solicitará de sindicatos, asociaciones y entidades apropiadas, y que deberá estar integrada por al menos cinco de aquellas personas. Si, por razón de la singularidad de la materia de dictamen, únicamente se dispusiera del nombre de una persona entendida o práctica, se*

[269] Información obtenida en la página web del Colegio Oficial de Ingenieros Informáticos de Cataluña.

[270] Sentencia del Tribunal Supremo, Sala de lo Contencioso, de fecha 3 de marzo de 2010 (recurso 299/2008).

recabará de las partes su consentimiento y sólo si todas lo otorgan se designará perito a esa persona» (art. 341 LEC). En el ámbito de la pericial informática los diferentes Colegios y Asociaciones -Colegios de Ingenieros Informáticos, Colegio de Ingenieros Técnicos Informáticos, ATI, ALI, APTI, A12 etc.- remiten listados de colegiados o asociados dispuestos a actuar como peritos para la elaboración de las listas judiciales[271]. La gran diversidad de las titulaciones en informática es patente en dichas listas judiciales, por lo que sería oportuno establecer algunos criterios orientadores para que el juez pudiera efectuar la designación del perito con un mínimo de «garantías»[272]. Es fundamental reseñar que la actuación jurisdiccional de la designación judicial en ningún caso debe quedar constreñida por la disponibilidad de la lista.

En Cataluña, el Departamento de Justicia, dentro de las competencias que le corresponden en materia de provisión de medios materiales y económicos para el funcionamiento de la Administración de Justicia, en el ámbito de periciales judiciales gestiona los listados de peritos y efectúa el pago de dichas periciales en los supuestos previstos por la ley. En el mes de enero de cada año el Departamento de Justicia actualiza las listas de peritos judiciales de acuerdo con la información que previamente han validado los colegios profesionales o entidades del sector, por lo tanto si un perito está interesado en formar parte de dichas listas debe solicitarlo al colegio profesional o entidad correspondiente facilitándoles sus datos actualizados. Dichos datos se incorporan a una aplicación informática para que todos los órganos judiciales puedan visualizarla en el buscador de peritos de la intranet de la Administración de Justicia.

Desde el año 2006 el Departamento de Justicia dispone de una aplicación informática de búsqueda de peritos judiciales de uso exclusivo para los órganos

---

[271] Con referencia al ámbito penal, puede verse la SAP Barcelona, secc. 7ª, de 29 de enero de 2008, fto. jco. 1º (ARP 2008\317) en la que el Juez de Instrucción, para el examen de unos archivos informáticos incautados, efectúa un nombramiento de perito judicial, optando por una de las tres posibilidades dadas por la denunciante: lista de peritos judiciales; Asociación de Doctores, Licenciados e Ingenieros en Informática (ALI); o Asociación de Técnicos en Informática (ATI).

[272] En la lista judicial de Cataluña 2012 aparece la siguiente clasificación: Ingenieros de telecomunicaciones con la subespecialidad de sistemas informáticos; ingenieros e ingenieros técnicos en informática sin subespecialidad o con diversas subespecialidades como consultaría, asesoramiento y dirección de proyectos, creación y mantenimientos de programación, ERP´s y sistemas de gestión integrada, grandes instalaciones (sistemas host), instalaciones de maquinaria (hardware) especializado, instalaciones de maquinaria (hardware) general, internet, creación y mantenimiento de páginas web, internet, tráfico legal y delitos en internet y propiedad intelectual de productos informáticos; ingenieros industriales con subespecialidad en informática; ingenieros técnicos informáticos con subespecialidad en informática (maquinaria y programación); informáticos de ámbito general sin subespecialidad; y tasadores en bienes muebles y otros con subespecialidad en electrónica e informática.

judiciales. La consulta puede efectuarse por partido judicial, especialidad y subespecialidad, permitiendo ver también los peritos dispuestos a actuar según las disposiciones de la Orden JUS/419/2009, de 17 de septiembre, relativa al pago de las periciales judiciales a cargo del Departamento de Justicia[273]. Los datos que se visualizan, entre otros, son titulaciones, especialidad, partidos judiciales donde quieren actuar y colegio profesional o entidad a la que pertenecen[274]. La libre decisión por parte de los peritos del lugar en que quieren actuar supone uno de los principales problemas que surgen en la práctica forense para la designa de peritos dada la falta de éstos en partidos judiciales pequeños, lo que supone una nueva grieta en un sistema igualitario y con plenas garantías a las partes, principalmente en supuestos en que una de éstas carece de recursos.

La principal deficiencia del sistema es que las listas no garantizan la profesionalidad ni experiencia de quienes forman parte de las mismas. El artículo 341 de la LEC, a la hora de establecer la preferencia de las listas remitidas por los Colegios Profesionales, no efectúa distinción alguna sobre el carácter obligatorio o voluntario de la colegiación en aquéllos, como tampoco equipara la colegiación con la posesión de título oficial correspondiente a la materia objeto de dictamen y a la naturaleza de éste, ni regula la cualificación profesional exigida a los peritos en el artículo 340.1 de la LEC (STS 21 de septiembre de 2011)[275]. En informática-forense ello se complica por cuanto no existe siquiera normativa que regule tal profesión. El ejercicio de la función pericial en el ámbito informático forense no ofrece ninguna garantía, en cuanto cualquiera puede ejercer en los tribunales como perito. La situación planteada ha provocado que algunos Colegios oficiales hayan planteado la necesidad de exigir determinados requisitos para que dichos profesionales puedan acceder a las listas de peritos y actuar como tales ante los Tribunales. Acción que ha sido coartada con fundamento en el derecho a la libertad de competencia.

---

[273] Orden JUS/419/2009, de 17 de septiembre, relativa al pago de las periciales judiciales a cargo del Departamento de Justicia, Diario Oficial de la Generalitat de Catalunya (DOGC), num. 5474, de 30 de septiembre de 2009. En cuanto al coste por parte del Estado de los peritajes judiciales puede consultarse el Informe sobre peritajes judiciales correspondiente a los años 2010 y 2011 en la página web stat.pnj.cgpj.es., en formato pdf.

Véase el artículo de ORELLANA CASTRO, R., *Lo que vale un perito,* publicado en Cuadernos de Probática, Diario La Ley 1260/2011, 8 de febrero de 2011, págs. 14-15, en el que se reflexiona acerca del coste del informe pericial desde la óptica del perito.

[274] Puede consultarse la página web de la Administración de Justicia de Cataluña en la dirección http://goo.gl/Y6PyH.

[275] STS 6211/2011, Sala de lo Contencioso, de fecha 21 de septiembre de 2011, F. Jco. 5º.

En el marco de la remisión a los órganos jurisdiccionales de las listas de profesionales para su designación como peritos, el Pleno del Consejo General del Poder Judicial dictó en fecha 28 de octubre de 2010 un Acuerdo por el que se modificaba la Instrucción 5/2001 de 19 de diciembre, publicado en el BOE de 18 de noviembre de 2010. Esta modificación consistió principalmente en la introducción del siguiente párrafo: «*Para los casos en que la prueba pericial requerida exija una titulación de colegiación obligatoria, los Presidentes de los Tribunales Superiores de Justicia y Jueces Decanos procurarán recabar los listados de todos aquellos Colegios Profesionales existentes en la demarcación vinculados a una profesión cuya titulación pudiera guardar relación directa y resultar idónea para el ejercicio del peritaje judicialmente requerido. Para los casos en que la colegiación no constituya requisito imprescindible para el ejercicio profesional o existan distintas titulaciones y/o profesiones susceptibles de realizar de forma adecuada la práctica pericial solicitada, los Presidentes de los Tribunales Superiores de Justicia y los Jueces Decanos procurarán solicitar los listados de los peritos de todas las asociaciones profesionales, corporaciones, y colegios no oficiales que existan en la demarcación*».

Ante tal reforma, la Asociación Intercolegial de Colegios Profesionales de Cataluña formuló consulta ante los principales organismos de competencia dadas las dudas interpretativas en relación a la exigencia de «idoneidad» que según la misma generaba dicha reforma, entendiendo que facultaba a los colegios de profesionales para que se requiriera a los colegiados que acreditaran determinados requisitos para su inclusión en las listas de peritos. Dicha interpretación resultaba contradictoria con la normativa existente, en concreto la Ley 15/2007, de 3 de julio, de defensa de la competencia (LDC). Y por lo anterior entendían que debía aplicarse el artículo 6 LDC que recoge la posibilidad de considerar inaplicable el artículo 1 LDC por «afectar al interés público». Sin embargo las posiciones sostenidas por organismos como la Comisión Nacional de la Competencia (CNC) y la Autoridad Catalana de la Competencia (ACCO) son de modo unánime contrarias a tal planteamiento. Dichos órganos resuelven que la introducción de requisitos adicionales a los previstos legalmente a las listas a partir de las cuales se efectuarán las designaciones de peritos constituye una práctica contraria a las normas en materia de defensa de la competencia.

La Comisión Nacional de la Competencia (CNC) en su resolución de fecha 23 de diciembre de 2011 señala que « *(…) el que el CGPJ considere que los listados de peritos que deben facilitar los Colegios profesionales deban tener relación directa y resultar idóneos para el ejercicio del peritaje judicialmente requerido, no permite deducir que pueda corresponder a los colegios profesionales una labor de discriminación entre los profesionales por dos razones: Primero, porque de acuerdo con el CGPJ, a quien corresponde valorar el cumplimiento de los*

principios de relación directa e idoneidad es a los Tribunales Superiores de Justicia y Jueces Decanos, y es a ellos a quienes se dirige la Instrucción 5/2001[276] *y a quienes se dan las instrucciones diferentes según la titulación requerida para los profesionales que compongan las listas de peritos sea de colegiación obligatoria o no; y segundo, porque de acuerdo con el CGPJ el cumplimiento de los principios de «relación directa» e «idoneidad» depende exclusivamente de la titulación de los profesionales y no de otra clase de consideraciones*».

Por otro lado, según señala la Autoridad Catalana de la Competencia (ACCO), en su Resolución de fecha 13 de enero de 2012, por «titulación» debe entenderse la que habilita expresamente para la profesión correspondiente. No debiendo confundirse «titulación» con «formación». Así, debe estar relacionada directamente con el objeto de pericia. Debe ser «idónea» por cuanto en los supuestos que exista más de una titulación directamente vinculada con el objeto de pericia debe elegirse aquella titulación y por tanto profesión más idónea para el trabajo a desarrollar, o bien en los supuestos en los que existan diferentes niveles de titulación habilitantes relativos a una misma profesión (por ejemplo arquitectos técnicos y superiores) se requiera aquella titulación más adecuada a las exigencias que plantea la pericia. Todo ello sin perder de vista que son los Tribunales Superiores de Justicia y los Jueces Decanos quienes deben determinar en primer lugar cual es la profesión que se adecua a la necesidad del peritaje requerido. La conclusión es que «idoneidad» no se refiere a requisitos adicionales a la titulación habilitante, sino a la selección de dicha titulación/profesión adecuada al objeto de la pericia.

La propia Exposición de Motivos del citado Acuerdo precisa que el objetivo de la modificación es adaptar la Instrucción 5/2001 a la jurisprudencia del Tribunal Supremo, que considera que sólo puede exigirse como requisito para la designación de peritos la titulación adecuada al peritaje: «*Sin embargo, el eficaz ejercicio de la potestad jurisdiccional presupone la disponibilidad de las relaciones deducibles del artículo 341 de la Ley de Enjuiciamiento civil, por tanto, este Consejo General del Poder Judicial, que consideró oportuno coordinar de modo uniforme la actividad gubernativa desarrollada en este ámbito al aprobar la Instrucción 5/2001, y el protocolo de ella derivado, aborda ahora la necesidad de introducir algunas precisiones en la Instrucción 5/2001 y en el Protocolo subsiguiente, a la luz de la jurisprudencia del Tribunal Supremo en la materia, que únicamente exige como requisito para la designación de peritos la titulación*

[276] Se refiere al párrafo segundo del apartado tercero de la Instrucción 5/2001, dada por el apartado primero del Acuerdo de 28 de octubre de 2010, del Pleno del CGPJ. En la Exposición de Motivos de dicho Acuerdo se precisa: *«(…) este Consejo General del Poder Judicial…aborda ahora la necesidad de introducir algunas precisiones en la Instrucción 5/2001 y en el Protocolo subsiguiente, a la luz de la jurisprudencia del Tribunal Supremo en la materia, que únicamente exige como requisito para la designación de peritos la titulación adecuada al peritaje requerido…*».

adecuada del peritaje requerido, de las diferentes exigencias y especificidades que presenta y plantea la realidad de la práctica pericial en cada proceso, de la diversidad de titulaciones existentes en la actualidad, de las Leyes 17/2009, de 23 de noviembre, sobre libre acceso a las actividades de servicios y su ejercicio, y 25/2009, de 22 de diciembre, de modificación de diversa leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios y su ejercicio en transposición de la directiva 2006/123/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, y de la propia práctica de este Consejo en su actividad gubernativa».

La tendencia política actual es permitir que cualquier profesional, en los supuestos de profesiones de colegiación voluntaria, pueda apuntarse a las listas para poder ejercer de peritos judiciales. En este sentido parece orientarse el Anteproyecto de Ley de Servicios Profesionales de 2012, distanciándose de un sistema que asegure que los peritos sean personas realmente expertas en la materia, con conocimientos suficientes y de prestigio reconocido como los profesionales que designa CASE en Estados Unidos o que forman parte de la *Verein Deutscher Ingenieure* (VDI) en Alemania. En Alemania y Reino Unido dichas Asociaciones clasifican a sus miembros según su especialidad y su capacidad individual, asignándoles un cierto nivel de acreditación –que puede ir creciendo a lo largo de los años– que se vincula a diversos aspectos como, por ejemplo, su «prestigio profesional», los «títulos académicos» que posee o su «experiencia profesional». En Estados Unidos The Court Appointed Scientific Experts (CASE), es una organización creada por la «*American Association for the Advancement of Science*» (AAAS), que goza de prestigio internacional y propone un listado de expertos de acuerdo con los expresos requerimientos del juez para el caso en concreto y habiéndose analizado con carácter previo las necesidades del caso específico, siendo el experto nombrado por el juez a partir de dicho listado. Véase § 8.1.2.

Frente al sistema de listas otra propuesta, aunque considero que poco viable y eficaz, sería que las designas judiciales se efectuaran sobre funcionarios públicos. En este caso se concretaría en la creación de un *«experto informático forense»* propiamente dicho como funcionario auxiliar del Juez o el Tribunal. Es lo que podríamos llamar «ciencia informática legal» por el símil con la «medicina legal» y que debería englobar: 1.- Por una parte «el informático forense» propiamente dicho cuyo ejercicio dependería y se desarrollaría exclusivamente en el ámbito de la Administración de Justicia, auxiliando al Juez; 2.- y por el otro, las cátedras universitarias de informática legal y el ejercicio privado como profesionales autónomos. Se trataría de la creación de un Cuerpo Nacional de Informáticos Forenses que dependerían orgánicamente del Ministerio de Justicia o de la CCAA que tuviera transferidas dichas competencias. Funcionarios públicos con acceso a través de oposición o a través

del modo que en su caso se regulara, y sujetos a un Reglamento Orgánico. Trabajarían directamente en los Institutos de Informática Legal, cuyas principales funciones se concretarían en auxiliar a Tribunales, Jueces y Fiscales de los partidos judiciales de su ámbito y debieran preverse normativamente; y asimismo llevarían a cabo actividades de docencia e investigación en las distintas áreas de las ciencias informáticas forenses que permitirían la actualización constante, indispensable dada la rapidez de evolución de las nuevas tecnologías[277].

En la actualidad, desde la Administración Pública sólo se dispone de equipos de delitos informáticos de las fuerzas del orden público quienes además se auxilian en algunos casos en empresas privadas. Se acude también en el ámbito civil a la policía judicial con específicos conocimientos en materia de tratamiento de datos informáticos. La evidencia electrónica tiene frecuente acceso al debate judicial por lo que al igual que se crearon cuerpos de funcionarios como en el caso de los médicos forenses (art. 479 LOPJ) y equipos psicosociales integrados en los Juzgados de Familia, en materia de evidencia electrónica se crearía un cuerpo de funcionarios, personal adscrito o regulación específica que permitiera un correcto funcionamiento judicial.

En España, el Servicio de Modernización y Racionalización de la Oficina Judicial del CGPJ viene solicitando la creación de la figura del que denomina «perito

[277] Puede consultarse la siguiente normativa relacionada con medicina forense: Ley orgánica 19/2003, de 23 de diciembre, de modificación de la Ley Orgánica 6/1985, de 1 de julio del Poder Judicial. Tít. I. Cap. I. Art. 470 y ss.; Real Decreto 2003/2008, de 5 de diciembre, sobre traspaso a la Comunidad Autónoma del Principado de Asturias de las funciones y servicios de la Administración General del Estado en materia de provisión de medios personales y económicos para el funcionamiento de la Administración de Justicia, BOE 31/12/2008; Decreto 37/2006, de 4 de mayo, del Consejo de Gobierno, por el que se crea el Instituto de Medicina Legal de la Comunidad de Madrid y se aprueba su Reglamento, BOCM 09/05/2006; Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género, BOE 29/12/2004; Real Decreto 441/1996, de 1 de marzo, sobre traspaso de funciones y servicios de la Administración del Estado a la Generalidad de Cataluña en materia de medios personales al servicio de la Administración de Justicia, BOE 10/14/1996; Real Decreto 296/1996, de 23 de febrero, por el que se aprueba el Reglamento Orgánico del Cuerpo de Médicos Forenses, BOE 01/03/1996; Real Decreto 386/1996, de 1 de marzo, por el que se aprueba el Reglamento de los Institutos de Medicina Legal, BOE 09/03/1996; Ley Orgánica 7/1992, de 20 de noviembre, por la que se integra diverso personal médico en el Cuerpo de Médicos Forenses, BOE 21/11/1992.

tecnológico», uniéndose a la nueva corriente innovadora de otros países que supone la creación de nuevas figuras y perfiles profesionales que mejoren la Administración de Justicia. La Ley Orgánica 19/2003 establece entre otros como principios básicos de la Nueva Oficina Judicial (NOJ): la coordinación interna entre distintas unidades a través de soportes informáticos y de modernas tecnologías; la adaptación en el funcionamiento de la Administración de Justicia a las nuevas tecnologías; y la creación de nuevos sistemas de gestión basados en la agilidad, eficacia, eficiencia y racionalización del trabajo. Con fundamento en dichos principios están previstas dentro de las nuevas oficinas judiciales (NOJ) las llamadas Unidades Administrativas (UA). Unidades que sin estar integradas en la oficina judicial forman parte de la Administración de Justicia y dentro de las cuales se prevé incluir entre otras funciones las peritaciones para el juez. Dichas unidades dependerán de las Comunidades Autónomas con competencias en la materia y dentro de las mismas podrán crearse oficinas comunes de apoyo a una o varias oficinas judiciales, para la prestación de servicios, cuya naturaleza no exija la realización de funciones encomendadas como propias por la LOPJ a los funcionarios de los Cuerpos de Administración de Justicia convenientes o necesarios para el buen funcionamiento de las mismas (art. 439 LOPJ). Cada Administración en su propio ámbito territorial deberá diseñar, crear y organizar las mismas. El equipo multidisciplinar de evidencias electrónicas o, en su caso, las unidades de peritos tecnológicos formarían parte de las Oficinas de Apoyo de las Unidades Administrativas (UA) de la Nueva Oficina Judicial.

En nuestra opinión un sistema de designación judicial de expertos sobre funcionarios públicos es poco viable en cuanto el coste de mantenimiento de un nuevo sector de funcionarios públicos incrementaría en exceso el gasto, sin perjuicio de que además la práctica forense indica que los médicos forenses suelen ser médicos con conocimientos generalistas y que carecen de formación específica para casos concretos. Un sistema contractual, resulta a nuestro juicio más indicado. Primero porque implica un menor coste, ligado también a la mayor o menor complejidad del caso para el que es nombrado; y segundo, porque de estar bien regulado y gestionado ofrece mayores garantías científicas y técnicas. El sistema contractual, de estar bien gestionado, garantizaría expertos realmente cualificados para emitir dictamen en el caso concreto. La agilidad y eficacia de dicho sistema dependería evidentemente también de la existencia de una organización de prestigio e igualmente eficaz como CASE en el ejemplo americano o de la pertenencia a una asociación que controle la titulación, formación continua de sus miembros y experiencia, como en el caso de Alemania o Reino Unido.

8.1.5 Designación

La Ley de Enjuiciamiento Civil vigente establece en nuestro proceso civil como norma general la pericia extrajudicial convirtiendo en subsidiaria y eventual la pericia de designa judicial. Las partes en el proceso designan perito, determinaran el objeto y la oportunidad de su aportación (art. 336 a 338 LEC), o solicitan, en su caso, la designación judicial del perito (art. 339 LEC) determinando el contenido del dictamen de designación judicial (art. 342.3, III LEC), y pudiendo incluso dejar sin efecto la pericia dejando de consignar el importe requerido para la provisión de fondos. La designación del perito informático puede efectuarse, en primer lugar, por las partes. Por cada una de ellas en los dictámenes acompañados a los escritos de alegaciones (art. 265.1.4º y 336.1 LEC) y en caso de conformidad de las partes en la persona o entidad mediante designación judicial (art. 339.2 LEC). Aunque la LEC omite pronunciarse sobre el procedimiento necesario para obtener dicho acuerdo[278].

La primera crítica a efectuar a este sistema principalmente en el que prima la pericial extrajudicial es que el «carácter privado» de la prueba pericial aminora su valor. Ello por cuanto son las partes quienes efectúan la designación y remuneración, seleccionan los extremos que evidentemente le son más favorables, y entregan para la emisión de dictamen material e instrumentos sin intervención de la parte contraria. Asimismo es un hecho que las partes nunca aportarán un dictamen desfavorable a sus pretensiones. La propia LEC parece desconfiar del perito de parte, por ejemplo, en el art. 759.1 al exigir pericial de oficio en los procesos de incapacitación. Por otro lado, se favorece a la parte económicamente más poderosa, ya que puede disponer de mejores y más acreditados peritos frente al que carece de medios económicos[279].

Por otro lado, la vigente regulación limita en exceso las facultades directivas del juez. Nótese que si bien se permite al juez formular preguntas a los peritos y requerir de ellos explicaciones sobre los que sea objeto del dictamen aportado no se le permite acordar la ampliación del dictamen pericial, salvo que se trate de peritos designados de oficio en procesos no dispositivos –declaración o impugnación de la filiación, paternidad y maternidad, capacidad de las

[278] Los art. 614 a 616 LEC 1881 establecían una forma mixta de designación de peritos atendiendo en primer lugar al acuerdo entre las partes, de no existir acuerdo entre las partes, a la insaculación mediante sorteo entre un número de peritos triple, por lo menos, al que debe ser designado, y de ser insuficiente el número de peritos a insacular, el propio Juez designaba directamente los peritos.

[279] Véase sobre las principales críticas efectuadas a la vigente regulación en la LEC: RIFA SOLER, J.M. *Comentarios a la nueva Ley de Enjuiciamiento Civil,* Fernández Ballesteros, M.A., Rifa Soler, J.M., y Valls Gombau, JF (coord..), ed. Atelier, Barcelona, 2000. pág. 1576.

personales o procesos matrimoniales- (art. 347.2 y 339.5 LEC). Dicha facultad resulta necesaria en supuestos como el de existencia de dictámenes contradictorios de las partes que generan dudas al Tribunal al tiempo de valorarlos. La norma tampoco permite la adopción de un dictamen pericial de oficio, y a salvo de los procesos no dispositivos (art. 339.5 LEC), teniendo difícil encaje al amparo del artículo 429.1. II y III LEC y tampoco parece posible como diligencia final de oficio al amparo del artículo 435.2 LEC, aun cuando algunos autores sostienen su viabilidad partiendo de una lectura constitucional y flexible de las normas probatorias[280].

No obstante, autores como MAGRO SERVET siguen defendiendo la prueba pericial de parte frente a la de designa judicial en el actual proceso: En primer lugar, por razones de aportación directa con la demanda de la prueba pericial sobre la que descansan las razones técnico-jurídicas que alegan las partes; y en segundo lugar, por la agilidad en la proposición de la prueba, ya que sólo requiere de su aportación directa y su práctica en el juicio de su ratificación del informe. Según dicho autor, la pericial judicial distorsiona la tramitación procedimental, al tener el juez que proceder a la designación del perito, aceptación posterior del cargo y más tarde la emisión del dictamen, una vez se le hayan comunicado las razones y temas sobre los que debe girar la emisión del dictamen[281]. En mi opinión, si bien es cierto que procesalmente la prueba pericial de parte implica dar una mayor celeridad al proceso, la igualdad de armas en el proceso en la medida que ello sea posible, la objetividad de la prueba pericial y la necesidad de que el juez disponga de medios suficientes para poder adoptar una resolución son razones que priman sobre aquella.

La designa judicial de perito puede ser instado por una de las partes (art. 339.2 LEC), por ambas *ab initio* (art. 339.2 párrafo 3º LEC) o a consecuencia de alegaciones o peticiones complementarias acaecidas durante el proceso (art. 339.3 LEC). En este último supuesto se exige: que el dictamen sea útil y pertinente; que ambas partes se muestren conformes con el objeto de la pericia; y que se comprometan ambas partes a aceptar el dictamen del perito designado (no en el contenido del mismo ya que si no sería prueba tasada, sino en la materia sobre la que debe versar, en que sea designado un único perito y que la designación la efectúe el tribunal). La designa *ex officio* queda reservada en nuestra LEC para procesos de carácter no dispositivo, declaración o

[280] Sobre este extremo véase ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.*), La prueba pericial, Serie estudios prácticos sobre los medios de prueba*, núm.3, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, pág. 30.

[281] MAGRO SERVET, Vicente. *La reforma de la prueba pericial en el proceso civil en la Ley 13/2009*. Revista de Jurisprudencia, núm. 4, 28 de julio de 2011. El Derecho.com/civil/

impugnación de la filiación, paternidad o maternidad, capacidad de las personas o procesos matrimoniales (art. 339.5 LEC).

La solicitud de pericial por designación judicial debe ir acompañada de los extremos sobre los que debe pronunciarse el dictamen y motivar su solicitud, razonando la pertinencia y utilidad de la prueba pericial (art. 339.2 LEC). Aun cuando la determinación de los extremos no se precisa en la regulación legal difícilmente el juez podrá valorar la pertinencia o utilidad de la misma a que se refiere la ley si no constan los mismos.

En cuanto al sistema de designación judicial de peritos en nuestro ordenamiento rige el sistema de «lista corrida» como supuesto normal. El sistema de lista corrida, regulado en el artículo 341 LEC, parte, como ya explicamos en el § anterior, de unas listas remitidas en el mes de enero de cada año por los Colegios Profesionales, Academias e Instituciones culturales y científicas. Se efectúa la primera designación por sorteo en presencia del Secretario Judicial, y las siguientes por orden correlativo. En el supuesto de designación de perito sin título oficial en la materia, se procederá a la insaculación entre una lista de personas proporcionada por sindicatos, asociaciones y entidades apropiadas, que deberá estar constituida por un mínimo de cinco personas. Si únicamente se dispusiera del nombre de una persona se recabará de todas las partes su consentimiento y sólo si éstas lo otorgan se designará perito a esta persona. Como hemos reiterado a lo largo de este trabajo el sistema de lista corrida no asegura ni competencia profesional ni imparcialidad. Véase sobre dicho extremo el § 8.1.2.

En el supuesto de disfrutar del derecho a la asistencia jurídica gratuita la designación se produce «ex lege». Recae en personal técnico adscrito al órgano jurisdiccional o, en su defecto, en funcionarios técnicos dependientes de la Administración de Justicia (art. 339.1 LEc en relación art. 6.6 Ley de Asistencia Jurídica Gratuita). El art. 6.6.2 de dicha ley establece que excepcionalmente y cuando por inexistencia de técnicos en la materia de que se trate, no fuere posible la asistencia pericial de peritos dependientes de los órganos jurisdiccionales o de las Administraciones públicas, ésta se llevará a cabo, si el Juez o el Tribunal lo estima pertinente, en resolución motivada, a cargo de peritos designados de acuerdo a lo que se establece en las leyes procesales, entre los técnicos privados que correspondan. Ante la inexistencia de personal o funcionarios en la demarcación judicial se admite la designación directa por el juez en procesos no dispositivos (SAP Málaga de 24 de junio de 2006). Sin embargo, pese a lo previsto en la ley la designa de técnicos privados para emitir un informe genera en la práctica muchos problemas dada la demora que para los mismos supone el cobro de dichos informes, presentando continuamente excusas que deben resolverse y demorándose el procedimiento, lo que

distorsiona el procedimiento y muestra las deficiencias en el principio de una justicia igualitaria para todos[282]. Ténganse en cuenta las normas contenidas en el artículo 45 y 46 del RD 996/2003 de 25 de julio, por el que se aprueba el Reglamento de asistencia jurídica gratuita, que prevén que el coste de los informes periciales se asumirán por el Ministerio de Justicia, excepto cuando exista condena en costas a favor del titular del derecho, o bien cuando venciendo en el pleito el titular del derecho a justicia gratuita y no existiendo en la sentencia pronunciamiento expreso sobre costas los beneficios obtenidos por éste en el proceso supere en tres veces las costas de su defensa. En el supuesto de que el titular del derecho a justicia gratuita fuera condenado en costas quedará obligado a abonar las peritaciones efectuadas por técnicos privados, si dentro de los tres años siguientes a la terminación del proceso viniese a mejor fortuna.

La designación judicial de perito deberá realizarse en el plazo de cinco días desde la presentación de la contestación a la demanda, con independencia de quien haya solicitado dicha designación, o en el plazo de dos días a contar desde la presentación de la solicitud en los supuestos de juicio verbal sin contestación escrita. Cuando ambas partes la hubiesen pedido inicialmente, el Tribunal podrá designar, si aquéllas se muestran conformes, un único perito que emita el informe solicitado (art. 339.2 párrafo segundo).

8.1.6 Aceptación

La aceptación del cargo por parte del perito es voluntaria en los supuestos de designación unilateral y obligatoria en los supuestos de designación judicial, salvo alegación y aceptación de justa causa (art. 342.2 LEC) que determina la sustitución del perito por el siguiente de la lista. El perito puede, no obstante, eludir el nombramiento del cargo no concurriendo a la diligencia de aceptación de cargo en cuyo caso deberá nombrarse sustituto (art. 342.2 LEC), o bien exigiendo una provisión de fondos que no sea asumida por las partes, en cuyo caso no puede procederse a nueva designación (art. 342.3, II LEC), quedando el perito eximido de emitir el dictamen y el juez privado de perito[283].

---

[282] Véase el comentario que efectúa el perito MARTÍNEZ DE CARVAJAL HEDRICH, en su libro *Informática Forense, 44 casos reales*, julio 2012, ed. Ernesto Martínez de Carvajal Hedrich, pág. 150, al señalar: «*…Es importante que antes de aceptar el cargo de perito judicial, conozca si se trata de un caso de justicia gratuita ya que, en caso afirmativo, quien paga es la Administración de justicia, aplicando unos criterios subjetivos que apenas cubren las fotocopias*».

[283] La posibilidad de que el perito solicite una provisión de fondos es una mera facultad del mismo, y es el Secretario quien decide sobre su corrección, de forma que puede disminuir la cantidad exigida como provisión.

No existe previsión legal para el supuesto de incomparecencia de perito a la aceptación de cargo, pues no fue aceptada una enmienda del Grupo Parlamentario Socialista en el Congreso, y después en el Senado que imponía la obligación de aceptar el cargo a las personas incluidas en las listas remitidas por los Colegios y las Asociaciones Profesionales, bajo advertencia de exclusión de las listas[284].

8.1.7 Imparcialidad

En el ámbito civil el perito tecnológico, ya sea de parte o designado judicialmente, garantizará su imparcialidad mediante el juramento o promesa de actuar con objetividad (art. 335.2 LEC). Dicho juramento supone objetividad tanto en la aplicación de conocimientos y técnicas, como en relación a la emisión de la opinión o criterio propio (SAP Álava, de 24 de julio de 2006)[285]. Asimismo, a través del mismo se pone de manifiesto que dicho perito comprende y tiene conocimiento de las sanciones penales si incumpliere su labor como perito (art. 335.2 LEC), previniéndole sobre la posible comisión de los delitos de falso testimonio (art. 459 y 460 CP), cohecho (art. 421 CP) y negociaciones y actividades prohibidas a peritos (art. 440 CP).

El juramento deberá efectuarse en el momento de «emitir el dictamen» (art. 335.2 LEC). Su omisión es un defecto subsanable, que no impide la valoración de la prueba. En supuestos de omisión una vez verificada la ratificación y subsanación del juramento debe considerarse como prueba pericial con valor probatorio pleno (SAP Madrid de 28 de junio de 2006). Aunque en ocasiones se valora como prueba documental el dictamen escrito y la ratificación del perito como testigo (SAP Segovia, de 29 de diciembre de 2006), e incluso con excesivo rigor en otras ocasiones se le ha negado eficacia probatoria (SAP Tarragona, de 3 de noviembre de 2006)[286]. En el supuesto que no se subsane y el perito no sea llamado a juicio solo podrá valorase dicha prueba como documental.

Otras mecanismos que garantizan la imparcialidad son respecto al perito designado judicialmente la «abstención» (art. 105 LEC) y la «recusación» (arts.

---

[284] Enmienda núm. 358, BOCD, de 26 de marzo de 1999.

[285] SAP Álava, secc. 1ª, de 24 de julio de 2006, fto. Jco 3º.

[286] SAP Madrid, secc. 12, de 28 de junio de 2006, fdo. Jco 6º; SAP Segovia, secc. 1ª, de 29 de diciembre de 2006, Fdo. Jco 5º y SAP Tarragona, secc 3ª, de 3 de noviembre de 2006, Fdo. Jco. 1º.

124 a 128 y 343.1 LEC), y respecto al perito de parte la «tacha» (art. 343.1.II LEC) –siendo una de las novedades más destacadas de la vigente LEC puesto que en la LEC de 1881 sólo se tachaba a los testigos-.

La tacha del perito no impide que este rinda su dictamen y que el juez lo valore en sentencia (art. 344.2), sino que supone una advertencia al juzgador de la falta de fiabilidad del mismo. La LEC excluye la prueba testifical para acreditar la tacha, y establece una causa amplia en exceso para la introducción de la misma «*cualquier otra circunstancia, debidamente acreditada, que les haga desmerecer en el concepto profesional*» (art. 343.1.5º). Para dejar a salvo el prestigio del perito, éste puede solicitar del Juzgado que, una vez emitida sentencia, mediante providencia declare que «la tacha carece de fundamento».

Las tachas no podrán formularse después del juicio o de la vista, en los juicios verbales. Si se tratare de juicio ordinario las tachas de los peritos autores de dictámenes aportados junto a la demanda y contestación deberán formularse en la audiencia previa al juicio (art. 344.2 LEC). No existe trámite procesal específico para la formulación de tachas respecto a dictámenes periciales aportados con posterioridad, pudiendo formularse mediante escrito independiente, bien oralmente en el acto de juicio o de la vista, pero siempre con anterioridad a la terminación de ambos (art. 343.2.1). La LEC no regula el procedimiento a seguir para la práctica de la prueba de tacha, debiendo entenderse que se efectuará en el acto de juicio o vista junto a la prueba principal. El artículo 343.2.2 se limita a indicar que «*al formular la tacha de peritos se podrá proponer prueba conducente a justificarla, excepto, la testifical*» y el art. 344 señala que «*cualquier parte interesada podrá dirigirse al tribunal a fin de negar o contradecir la tacha, aportando los documentos que consideren pertinentes la efecto*». No se prevé plazo, ni se prevé la posibilidad de practicar prueba distinta a la documental. Y tampoco se ha previsto la audiencia del perito en torno a la tacha alegada como sería conveniente[287].

En primer lugar, la tacha a diferencia de la recusación no impide valorar los conocimientos técnicos en sentencia del perito tachado y no aparta a éste del procedimiento, remitiéndose la resolución de la misma a una cuestión de valoración probatoria (art. 344 LEC), al margen de la providencia que el tribunal pueda dictar al término del proceso declarando que la tacha carece de fundamento. No se requiere, por lo tanto, resolución expresa destinada a resolver la tacha, sino que se podrá aludir a la misma en la valoración de la prueba pericial que se efectúe en sentencia. Sin embargo, el perito debería

[287] En este sentido se pronuncia SERRA DOMÍNGUEZ, M, en *La prueba pericial, en* "Instituciones del nuevo proceso civil. Comentarios sistemáticos a la Ley 1/2000", vol. II, Alonso-Cuevilles Sayrol, J. (coord.) edit. Difusa, Barcelona 2000, pág. 305.

poder ser reemplazado por otro ya que a diferencia del testigo es sustituible, aunque evidentemente ello no podrá aplicarse mientras la valoración se efectúe en sentencia[288]. Por otra parte, si bien es cierto que el demandado ha formulado su denuncia antes del tiempo reseñado en el artículo 343.2 de la LEC, y que lo ha realizado por escrito, frente al sistema oral que impone la LEC, el cambio de pericial por el mero planteamiento de la tacha altera la necesidad de aportación con la demanda y la contestación de los dictámenes elaborados por peritos designados por las partes, a que se refiere el artículo 336 de la LEC, sin concurrir realmente la imposibilidad a que alude el artículo 337 de la ley procesal. No se cumple ninguno de los presupuestos requeridos por este último artículo para la aportación posterior de dictámenes: que no les fuese posible a las partes aportarlos y que se expresen aquéllos de que en su caso pretendan valerse[289].

La «abstención» supone la sustitución por un suplente si se reproduce en el momento de la designación, y en el caso que se produzca con carácter posterior a la aceptación del cargo se remite a la decisión del Juez o Tribunal que conozca del asunto (art. 105 LEC). La «recusación» se prevé en el art 124 de la LEC exclusivamente para aquellos peritos designados por sorteo, aunque es pacífica la doctrina que considera que es aplicable a cualquier perito designado judicialmente, por cuanto dicha limitación a los peritos designados por sorteo se debe a un error de tramitación parlamentaria de la LEC. Las causas de abstención y recusación son comunes (art. 99.2 LEC)

8.1.8 Derechos y Deberes

El perito tecnológico en el ejercicio de su actividad es titular de derechos y de igual modo está sujeto a determinados deberes u obligaciones, la mayor parte de ellos expresamente reconocidos y regulados en la ley y otros implícitos a la profesión y a la diligencia con la cual debe actuar. Entre los derechos en primer lugar la ley garantiza al perito mediante el auxilio judicial y sanciones en supuestos de mala fe procesal el «acceso» a los medios necesarios para que éste pueda desarrollar su actividad de un modo adecuado. El perito tiene derecho a acceder a los medios adecuados para el estudio de las cuestiones que se hayan planteado. En el ámbito de la pericial electrónica el perito solicitará el acceso al dispositivo o medio que incorpore información digital como pueden

[288] En este sentido véase SERRA DOMÍNGUEZ, M. *La prueba pericial*, en "Instituciones del nuevo proceso civil" Ob. Cit. pág. 305.

[289] VELÁZQUEZ VIOQUE, D., *Dictamen por perito designado a instancia de parte* en "La prueba pericial", ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.3, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, pp. 309-316.

ser ordenadores personales y portátiles, teléfonos móviles, agendas electrónicas (PDA's), smartphones etc. En el supuesto que una de las partes negare injustificadamente al perito de la adversa o al de designación judicial el acceso al ordenador u otro dispositivo electrónico objeto de pericia se deberá dejar constancia de tal incidencia, preferiblemente mediante acta notarial, y recabar la pertinente autorización judicial para tener acceso a tal dispositivo, y que el perito pueda elaborar el dictamen y aportarlo al proceso, sin perjuicio, de que de estimarlo procedente el juez podrá sancionar a la parte obstruccionista con una multa por infracción de la buena fe procesal (art. 247 LEC).

En segundo lugar, la actividad pericial es una «actividad remunerada». Es decir, el perito tiene derecho a una remuneración por su trabajo, tanto si es perito de parte como por designación judicial. El perito tiene la potestad de solicitar la provisión de fondos que considere necesaria a modo de anticipo a cuenta de la liquidación final. Lo puede hacer directamente a la parte que le ha designado o bien de la parte o partes que hubieran solicitado su designación judicial y no tuvieran derecho a la asistencia de justicia gratuita (art. 342.3 LEC). *«El perito designado podrá solicitar, en los tres días siguientes a su nombramiento, la provisión de fondos que considere necesaria, que será a cuenta de la liquidación final. El Secretario judicial, mediante decreto, decidirá sobre la provisión solicitada y ordenará a la parte o partes que hubiesen propuesto la prueba pericial y no tuviesen derecho a la asistencia jurídica gratuita, que procedan a abonar la cantidad fijada en la Cuenta de Depósitos y Consignaciones del Tribunal, en el plazo de cinco días. Transcurrido dicho plazo, si no se hubiere depositado la cantidad establecida, el perito quedará eximido de emitir el dictamen, sin que pueda procederse a una nueva designación. Cuando el perito designado lo hubiese sido de común acuerdo, y uno de los litigantes no realizare la parte de la consignación que le correspondiere, el Secretario judicial ofrecerá al otro litigante la posibilidad de completar la cantidad que faltare, indicando en tal caso los puntos sobre los que deba pronunciarse el dictamen, o de recuperar la cantidad depositada, en cuyo caso se aplicará lo dispuesto en el párrafo anterior» (art.* 342.3 LEC*).*El perito informático podrá incluir sus honorarios en la tasación de costas ya sea perito de designación de parte o judicial, ya que el artículo 241.14º LEC no distingue entre ambos. En el supuesto que el perito deba reclamar por falta de pago acudirá al proceso declarativo, aun cuando de *lege ferenda* se ha postulado que el perito pudiera acudir al procedimiento de jura de cuentas (art. 35 LEC) frente a la parte que hubiera interesado su nombramiento o frente a la parte condenada en costas.

En cuanto a los deberes que vinculan al perito, en primer lugar, le corresponde la obligación deontológica de actuar de forma veraz y objetiva, con conocimiento de que en el supuesto de incumplimiento puede incurrir en delito penal (delito de falso testimonio, art. 459 y 460 CP). Tiene el deber de

manifestar, bajo juramento o promesa de decir la verdad, que ha actuado y, en su caso, actuará con la mayor objetividad posible, tomando en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a cualquiera de las partes, y que conoce las sanciones penales en las que podría incurrir si incumpliere su deber como perito (art. 335.2 LEC).

Son deberes implícitos a la propia actividad pericial aun cuando no se hallan regulados normativamente los relacionados con su formación, experiencia y diligencia. En este sentido el perito informático forense en el ejercicio de su actividad tiene el deber de tener conocimientos y experiencia suficientes, de preservar la información obtenida, de respetar y proteger la cadena de custodia y el deber de conocer y aplicar la normativa jurídica. Esto último implica tener conocimientos legales no sólo a nivel procesal sino también constitucional. Debe conocer la normativa vigente, ya que su actuación podría vulnerar derechos constitucionales como el derecho a la intimidad o a las comunicaciones. Por ejemplo, si accediera sin autorización judicial a un *chat* cuando se emplea la opción que limita la comunicación a dos interlocutores. Debe tener conocimientos técnicos suficientes, por ejemplo, para acceder a la información y copia de la misma de modo que no se produzca alteración de la información obtenida. En estos casos, el perito que intervenga con posterioridad deberá poder tener acceso a dicha información de forma inalterada y a los modos de acceso a efectos de poder emitir un dictamen pericial.

Entre los deberes del perito se halla también el guardar «secreto profesional». Deber regulado en la normativa profesional y deontológica de los Colegios Profesionales[290] cuya infracción implica sanción disciplinaria colegial. El perito tecnológico y en concreto el informático-forense en el ejercicio de la pericia informática tras efectuar la adquisición de datos de medios o dispositivos electrónicos y proceder al análisis forense accederá en muchas ocasiones a información confidencial respecto a la que deberá guardar secreto. Nótense los temas relacionados con *know how* de las empresas, datos de proveedores, de clientes, datos económicos etc., que de hacerse públicas pudieran perjudicar económicamente a las empresas implicadas.

Por otro lado, la participación del perito en procesos de mediación o arbitraje imposibilitará su participación en procedimientos judiciales que traten sobre igual asunto, salvo acuerdo en contrario de las partes. Ello en atención al principio de protección a la confidencialidad en la mediación y su contenido (art. 335.3 y 347.1 LEC reformados por el RD 56/2012 de mediación en asuntos civiles y mercantiles, así como art. 9 de este último).

[290] La Asociación de Peritos judiciales colaboradores con la Administración de Justicia recogen dicho deber en el artículo 6 de sus Principios deontológicos y de buenas prácticas.

Tratándose de perito designado judicialmente éste tiene la obligación de «aceptar el cargo», salvo en supuestos en que concurra justa causa (art. 341.2 LEC). Y para poder llevar a cabo su actividad pericial debe dar aviso a las partes, con una antelación de cuarenta y ocho horas, del día, hora, y lugar en que tendrán lugar las operaciones periciales (art. 345.2 LEC).

Es obligación del perito «aportar el dictamen pericial». En el supuesto de designa de parte el incumplimiento supone preclusión probatoria para las partes y el incumplimiento de un contrato de arrendamiento de servicios entre parte y perito que, en su caso, podría dar lugar a responsabilidad civil. En el supuesto de designa judicial deberá presentar el dictamen en el plazo señalado (art. 346 LEC) para el cual se le requiere normalmente en la diligencia de aceptación del cargo. Fuera de los supuestos de imposibilidad o presentación tardía, en el caso de incumplimiento queda sujeto a responsabilidad civil por incumplimiento de los deberes contraídos con su aceptación, y también a responsabilidad penal.

Por otro lado, el perito debe «comparecer al acto de juicio» si así es solicitado por las partes ya sea perito de designación de parte o judicial (337.2 y 346 LEC). En el supuesto de designa judicial, por parte del juez podrá acordarse de oficio su comparecencia si la considera necesaria para comprender y valorar mejor el dictamen realizado. Su incomparecencia puede suponer la suspensión del señalamiento (art.183.4 LEC) o la interrupción de la vista (art. 193.1.3 LEC) si el juez estima imprescindible su presencia. La incomparecencia injustificada será sancionada con una multa, y hecho el requerimiento por segunda vez el perito podrá incurrir en un delito por desobediencia a la autoridad (art. 292 LEC). En su comparecencia en el juicio o vista debe tener un comportamiento adecuado y correcto, guardando consideración a las partes, al público y al tribunal (art. 193 y 194 LOPJ). La infracción de dicho deber se sanciona con una multa (art. 193 LOPJ), con constancia documental en el acta del hecho que motiva la sanción, las explicaciones dadas, en su caso, por el sancionado y el acuerdo que se adopte por el juez (art. 194.1 LOPJ). Fijándose el límite máximo de la cuantía de la multa en «*la cuantía de la multa más elevada prevista en el Código Penal como pena correspondiente a las faltas*» (art. 192 LOPJ).

El incumplimiento de los deberes del perito supondrá no solo una posible responsabilidad ante los tribunales sino también podrá provocar sanciones dada su pertenencia a un colegio profesional. Es decir, la responsabilidad disciplinaria es autónoma e independiente de la responsabilidad civil o penal en que incurra el perito. En cuanto a la responsabilidad penal (art. 459 y 460 CP) se impone al perito que «faltare a la verdad maliciosamente en su dictamen» las penas del falso testimonio en su mitad superior añadiendo, además, la inhabilitación especial para profesión u oficio, empleo o cargo público, por

tiempo de seis a doce años. Cuando el perito sin faltar sustancialmente a la verdad, la alterare con reticencias, inexactitudes o silenciando hechos o datos relevantes que le fueran conocidos, será castigado con la pena de multa de seis a doce meses y, en su caso, de suspensión de empleo o cargo público, profesión u oficio, de seis meses a tres años. La inexactitud debe ser consciente y voluntaria no derivándose responsabilidad criminal del mero error o equivocación.

En cuanto a la responsabilidad civil del perito podrá exigirse por vía ordinaria, al no existir procedimiento específico. La responsabilidad derivada de su actuación es contractual y no extracontractual al proceder de un arrendamiento de servicios. Matizar, no obstante, que un sector doctrinal sostiene que respecto al perito de designación judicial la responsabilidad es extracontractual[291]. Lo anterior es importante a efectos de prescripción. Por otro lado, frente a la discusión de si una ulterior discusión sobre la corrección o incorrección del dictamen pericial podría afectar a la autoridad de cosa juzgada estimamos que es precisamente la existencia de cosa juzgada lo que origina el perjuicio cuya indemnización se solicita frente al perito; y que al igual que ocurre con la responsabilidad civil del Juez, la responsabilidad civil del perito no afecta a la invariabilidad de la sentencia[292].

8.2 El dictamen pericial

8.2.1 Forma del dictamen pericial

El dictamen pericial es el medio a través del cual el experto transmite al juez sus conocimientos especializados en determinados campos de la ciencia, el arte, la técnica o prácticos para que este último pueda valorar hechos o circunstancias relevantes en el asunto sobre el que versa el pleito o adquirir certeza sobre los mismos. En el ámbito de la prueba electrónica el perito transmitirá a través de su dictamen conocimientos científicos, técnicos o prácticos sobre hechos de naturaleza electrónica. Dado que el dictamen pericial constituye un medio de prueba (art. 299 LEC) que será objeto de valoración por el juez resulta fundamental que emplee un lenguaje de fácil comprensión, que se estructure

[291] Véase ABEL LLUCH, X., *La prueba pericial*, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.3, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, pág. 89.

[292] SERRA DOMÍNGUEZ, M. *La prueba pericial*, en *"Instituciones del nuevo proceso civil"* Ob. Cit. pág. 307.

de una forma clara y que contenga todos los elementos e información necesarios para que el juez pueda conocer y entender las operaciones y razonamientos llevados a cabo por el perito y a través de los cuales formula finalmente sus conclusiones. Lo anterior incluye tanto los exámenes, métodos, experimentos e investigaciones efectuadas por el perito como los fundamentos técnicos y científicos en que se basa.

La Ley de Enjuiciamiento Civil no detalla la forma y contenido que debe revestir el dictamen pericial sino que se limita a exigir el dictamen por escrito y la posibilidad de acompañar o identificar los documentos, instrumentos o materiales adecuados para exponer el parecer del perito sobre lo que haya sido el objeto de la pericia (art. 346 y 336.2). La actual regulación se diferencia de la de 1881 al exigir el dictamen por escrito ya que la regulación anterior permitía la emisión del dictamen tanto en forma oral como escrita. A pesar de la falta de normativa vinculante, existen algunas iniciativas de ámbito nacional destinadas a establecer directrices en la presentación de la información ante los Tribunales como el proyecto PNE 71056 llevado a cabo por el Comité técnico de normalización (AEN/CTN 197) de la Asociación Española de Normalización y Certificación (AENOR). A nivel europeo puede destacarse el Centro Europeo de Normalización en el CEN/PC 405 «*European standard on Expertise Services*», y a nivel internacional la «*American Society for Testing and Materials*» (ASTM9). Aunque ninguna de las anteriores normas es de obligado cumplimiento. Pese a la necesidad de regulación muchos peritos no comparten esta idea argumentando que la existencia de normas vinculantes de obligado cumplimiento relativas a la forma y contenido del dictamen pericial puede volverse en contra de los mismos, por cuanto la falta de cumplimiento en alguno de sus extremos podría ser utilizada en juicio como arma arrojadiza para menoscabar su dictamen. Un argumento por cierto bastante pobre ya que en nuestra opinión no puede haber conocimiento científico sin metodología.

La Ley de Enjuiciamiento Criminal describe cómo debe ser o presentarse dicho dictamen, a diferencia de la falta de regulación de la forma y contenido que debe revestir el dictamen pericial en el ámbito civil, indicando que: «e*l informe pericial comprenderá, si fuere posible: 1.Descripción de la persona o cosa que sea objeto del mismo, estado o del modo en que se halle. El Secretario extenderá esta descripción, dictándola los peritos y suscribiéndola todos los concurrentes. 2.Relación detallada de todas las operaciones practicadas por los peritos y de su resultado, extendida y autorizada en la misma forma que la anterior.3.Las conclusiones que en vista de tales datos formulen los peritos, conforme a los principios y reglas de su ciencia o arte» (*artículo 478 de la Lecrim.). Podemos afirmar, pues, que con carácter general el dictamen de un perito deberá comprender la descripción del objeto de dictamen, las operaciones periciales

llevadas a cabo, el resultado de dichas operaciones periciales y finalmente las conclusiones obtenidas.

El dictamen pericial tecnológico puede ser de parte o bien de designación judicial. En ambos casos, el dictamen deberá revestir igual forma y contenido, respetarse la cadena de custodia que garantiza la integridad, conservación e inalterabilidad de los hechos electrónicos. Ello incluye su obtención, custodia, transporte y presentación en los tribunales hasta su disposición final por orden judicial. Dicho ésto nos ceñiremos en la forma y contenido que, a nuestro parecer, debe reunir un dictamen pericial.

El dictamen pericial con carácter general debe ser claro, preciso, exhaustivo y detallado. Se trata de un medio probatorio dirigido al juez y a las partes que no tienen por qué ser personal técnico ni entender en profundidad las nuevas tecnologías, de ahí la necesidad de compaginar los términos técnicos con un lenguaje de fácil comprensión[293]. Por otro lado, el perito puede acompañarse en su comparecencia a la vista o juicio de cualquier medio o instrumento que sea necesario para una mejor comprensión de su dictamen pericial. Recordemos que los dictámenes irán «*…acompañados, en su caso, de los demás documentos, instrumentos o materiales adecuados para exponer el parecer del perito sobre lo que haya sido objeto de pericia*». No podemos olvidar que tan importante como el dictamen escrito es la contradicción del dictamen en el acto del juicio o de la vista y las respuestas del perito a las preguntas de los letrados y del propio juez (art. 347 LEC).

En cuanto a su contenido, en primer lugar conviene dejar constancia del número de autos y Juzgado, si se dispusiere ya de dicha información, e identificar a la persona que ha efectuado el encargo. En segundo lugar, el dictamen pericial debiera estructurarse en una parte inicial relativa al perito o peritos intervinientes, es decir, a los datos identificativos y profesionales relacionados con el mismo y su obligación de actuar con objetividad, y una segunda, que sería el cuerpo del dictamen pericial. Finalmente el dictamen

[293] En cuanto a la necesidad de emplear un lenguaje fácil y comprensible por personas no técnicas en la materia se refiere el artículo 9 del PNE 71506. Dicho proyecto pretende determinar la forma en que deben presentarse los dictámenes periciales informáticos. Se trata de un proyecto que está siendo elaborado en España por el Comité técnico de normalización AEN/CTN 197, AENOR (Asociación Española de Normalización y Certificación) cuyo objetivo es la normalización de criterios generales para la elaboración de informes de actuaciones periciales en todas las áreas existentes incluidas las TIC, que den respuesta a las necesidades de Justicia y a los profesionales que elaboran los informes periciales. Dicho proyecto remite en la confección de la parte general del mismo a la Norma UNE 197001, con la particularidad que en este caso, su contenido versa sobre aspectos técnicos propios de las tecnologías de la información.

debiera acompañarse del correspondiente anexo de documentos e instrumentos necesarios para elaboración y su comprensión.

La parte inicial del dictamen pericial electrónico contendría, en primer lugar, los datos relativos a la persona del perito o peritos que lo emiten y de quienes han participado en su elaboración. Ello englobaría, por un lado, los datos meramente identificativos como su nombre, dirección, el número de teléfono, número de identificación y los demás datos que faciliten la localización del perito. De tratarse de pericial corporativa deberían de igual modo hacerse constar los datos identificativos de la entidad y también la de aquellas personas físicas que han intervenido y emitido el dictamen pericial.

Por otro lado, junto a los datos meramente identificativos deberían hacerse constar aquellos datos relacionados con la profesión, experiencia y prestigio profesional del perito o peritos que emiten el dictamen e intervinientes. Comprenderían dichos datos la reseña de su profesión, oficio o actividad especial ejercida, así como los títulos académicos y los documentos que certifiquen la respectiva experiencia profesional o técnica y que le habilitan para su ejercicio. Los documentos acreditativos de tales extremos irían anexados al dictamen. También podría dejarse constancia de la lista de las últimas publicaciones del perito o de aquellas publicaciones de mayor impacto o aceptación en la comunidad científica, si las tuviere[294].

Una vez finalizada la parte relativa a los datos identificativos y profesionales del perito, éste a continuación asumirá la obligación de actuar de forma objetiva conociendo las responsabilidades que puedan derivarse de la infracción de tal obligación. En este sentido debe «2. … *manifestar, bajo juramento o promesa de decir verdad, que ha actuado y, en su caso, actuará con la mayor objetividad posible, tomando en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a cualquiera de las partes, y que conoce las sanciones penales en las que podría incurrir si incumpliere su deber como perito»* (art. 335.2 LEC). Tal indicación puede efectuarse también en la parte final del

[294] La reseña de tales circunstancias se recoge en los apartados 1 a 5 del artículo 226 del Código Procesal Colombiano, Ley núm. 1564, de fecha 12 de julio de 2012. En dicho Código el apartado 4 limita la lista de publicaciones, relacionadas con la materia del peritaje, que el perito haya realizado a los últimos diez (10) años, si las tuviere, y en su apartado 5 la lista de casos en los que haya sido designado como perito o en los que haya participado en la elaboración de un dictamen pericial a los últimos cuatro (4) años. Dicha lista incluiría el juzgado o despacho de abogados en donde se presentó, el nombre de las partes, de los apoderados de las partes y la materia sobre la cual versó el dictamen.

dictamen[295]. La falta de constancia de dicha mención es subsanable (SAP Burgos, Sec. 3ª, de 11 de noviembre de 2003; Orense, Sec. 1ª de 12 de febrero de 2004; Tarragona, Sec. 1ª, de 8 de marzo de 2005). Aunque algunas resoluciones de los tribunales, más rigurosas, entienden que la ausencia de juramento o promesa en el dictamen le priva de la condición de prueba pericial y le convierte en una prueba documental (SSAAPP Zamora, Sec. 1ª, de 30 de diciembre de 2004; Murcia, Sec 5ª, de 16 de mayo de 2006). Tratándose de perito designado judicialmente el juramento o promesa de decir verdad y las demás manifestaciones de la norma se efectúan en el momento de aceptar el cargo. Debería, asimismo, manifestar si fueren peritos de designa de parte si se encuentran incursos en alguna de las causas de tacha (artículos 343 y 344 LEC) o tratándose de peritos judiciales manifestar que no se hallan incursos en causa de abstención o recusación (arts. 105, 124 a 128 y 343.1 LEC).

El cuerpo del dictamen pericial se inicia con una descripción detallada de cada uno de los extremos solicitados por el abogado de la parte. De tratarse de diversas cuestiones deberán numerarse y separarse solicitando con claridad y precisión lo que se pida. Éste es uno de los elementos más importantes del dictamen pericial y su fundamento por cuanto el dictamen es un medio de prueba que propondrá la parte, y en su caso el juez, y por lo tanto el perito nunca debe extralimitarse en sus funciones usurpando el lugar que le corresponde a quien lo solicita -parte o juez-. Es decir, quien determina los extremos es la parte no el perito. Si bien ello parece evidente lo cierto es que en la práctica forense hallamos peritos que se erigen en partes determinando sobre qué debe versar el dictamen pericial. También debemos hacer hincapié en que la determinación con claridad de cada uno de los extremos solicitados debe hacerse constar no solo en el dictamen emitido en el proceso sino también en los informes técnicos emitidos con carácter preprocesal, lo que a veces parecen olvidar algunos letrados.

Se dejará constancia de la fecha de inicio y fin del examen o análisis pericial. A continuación conforme al sistema de cadena de custodia se reseñarán e identificarán todas las fuentes de prueba recibidas y su estado así como se dejará constancia de las precauciones adoptadas para que no exista pérdida de datos. Se documentarán fotográfica o videográficamente el lugar y los soportes, medios o dispositivos sobre los que se ejercerá el estudio y/o componentes objeto de análisis.

Después se entrará en el cuerpo del informe pericial propiamente dicho que contendrá todos los estudios efectuados sobre el hecho electrónico. Contendrá

[295] En este sentido se pronuncia ABEL LLUCH, X; ARIMANY-MANSO, J; GÓMEZ DURÁN, E.L.; *El dictamen médico-legal en supuestos de responsabilidad profesional médica: fuentes y contenido*, artículo inédito y facilitado por los autores.

en su caso, captura de la información, copia y preservación (fase de adquisición de datos) y fase de análisis forense, es decir, clasificación, identificación, individualización y asociación de la información o datos electrónicos obtenidos. El Proyecto PNE 71506 del Comité técnico de normalización (AEN/CTN 197) de la Asociación Española de Normalización y Certificación (AENOR) cuyo objetivo es dar unos criterios básicos y generales para la elaboración de informes de actuaciones periciales establece en su anexo A apartado tercero o c) una descripción de lo que vendría a incluirse en este apartado del dictamen y que consiste en «*… todos los análisis previos descritos en la Norma 71506 así como en detalle, el apartado correspondiente al análisis de los datos, reflejándose, por lo tanto, los siguientes subapartados: Descripción del proceso de clonado bit a bit de la información original o procedimiento seguido para obtener los datos copia que han servido para el estudio de las evidencias correspondientes; análisis de las particiones y sistemas de ficheros; proceso de recuperación de archivos borrados, si ha lugar; estudio del sistema operativo y usuarios del mismo; estudio de la seguridad implementada; y análisis detallado e individualizado, para cada soporte digital, de los indicios encontrados de interés de las distintas evidencias electrónicas. Deben reseñarse a lo largo de este análisis, en los anexos correspondientes, los indicios encontrados perfectamente clasificados, con sus rutas de ubicación en los soportes originales*»[296].

Es fundamental la constancia de cada una de las diligencias practicadas, documentando e identificando las fuentes, identificando las personas que hayan intervenido, haciendo constar los métodos y herramientas utilizadas, así como las posibles incidencias que hayan ocurrido. Entendiendo en la prueba pericial informático forense por «herramientas empleadas» aquellos programas informático forenses que ayudan al experto en su labor de captura de la evidencia digital y por «método técnico empleado» el conjunto de operaciones técnicas informáticas empleadas por el experto informático-forense desde el mismo momento de la identificación del hecho electrónico hasta la finalización de todo el proceso. Precisamente en cuanto a las técnicas y herramientas entendemos fundamental que exista un apartado en el dictamen pericial que no solo las identifique sino que informe sobre aquellos elementos que las validan científicamente.

En cuanto a los elementos integrantes del dictamen pericial que sirvan para la validación científica de los métodos y herramientas seguidos por el perito forense en su análisis podemos acudir al Test de DAUBERT, nacido a partir de la Sentencia del Tribunal Supremo de los Estados Unidos de América de 1993 en el caso DAUBERT Vs MERRILL DOW PHARMACEUTICALS, INC., en que la Corte

[296] El contenido de las normas de AENOR nos ha sido facilitada por el Colegio de Ingenieros Informáticos de Cataluña.

recomendó los criterios básicos que los jueces deben considerar para admitir prueba pericial científica en un procedimiento judicial: a) Si la técnica ha sido comprobada o refutada; b) si ha sido objeto de examen y publicación en el ámbito científico que procede; c) la tasa de error conocida o potencial de la técnica empleada; d) la existencia y mantenimiento de normas y controles en cuanto a su práctica; y e) el grado de aceptación de la técnica en el marco de la comunidad científica[297]. Dichos elementos servirán para que el juez efectúe una valoración del dictamen como medio de prueba sujeto a sana crítica. Y para ello es relevante que el perito haga también constar en su dictamen si los exámenes, métodos, experimentos e investigaciones efectuados son diferentes respecto de los que ha utilizado en peritajes rendidos en anteriores procesos que versen sobre las mismas materias. Y en el caso de que sean diferentes explique cómo justifica la variación. Así como que explique si los exámenes, métodos, experimentos e investigaciones efectuados son diferentes respecto de aquellos que utiliza en el ejercicio regular de su profesión u oficio. Y en el caso que sean diferentes también será necesario que explique cómo justifica dicha variación[298]. En definitiva, es recomendable que el dictamen pericial contenga como elementos integrantes una explicación de los criterios científicos en que se fundamente, y la mayor o menor acogida por la comunidad científica de los mismos así como el fundamento de ello. Ya que como afirma RICHARD GONZÁLEZ «… *la conclusión científica es siempre, por esencia, refutable y está sujeta a crítica y revisión*»[299].

El cuerpo del dictamen pericial finalizará con las «conclusiones finales» obtenidas tras los estudios efectuados sobre los hechos electrónicos y los medios o soportes que los contienen y/o sobre los dispositivos a través de los

[297] Véase: Improving judicial gatekeeping: Technical advisors and scientific evidence. Full Text Available Harvard Law Review. Feb 97, Vol. 110 Issue 4, pág. 945-946; Hess, Robert L., Judges cooperating with scientists: A proposal for more effective limits on the federal trial judge's inherent power to appoint technical advisors, V. II. Vanderbilt Law Review 54. 2 (Mar 2001), pág. 564; H.T. Greely y A.D. Wagner, Reference Manual on Scientific Evidence, Third Edition, federal Judicial Center, National Academic Press, Washington D.C. 2011, págs. 772 y ss.

[298] El artículo 226 del Código Procesal Colombiano, Ley núm. 1564, de fecha 12 de julio de 2012, recoge en sus apartados 8. y 9. como elementos integrantes mínimos que debe recoger el dictamen pericial: «… *8. Declarar si los exámenes, métodos, experimentos e investigaciones efectuados son diferentes respecto de los que ha utilizado en peritajes rendidos en anteriores procesos que versen sobre las mismas materias. En caso de que sea diferente, deberá explicar la justificación de la variación; 9. Declarar si los exámenes, métodos, experimentos e investigaciones efectuados son diferentes respecto de aquellos que utiliza en el ejercicio regular de su profesión u oficio. En caso de que sea diferente, deberá explicar la justificación de la variación*».

[299] RICHARD GONZÁLEZ, MANUEL., *Admisibilidad, eficacia y valoración de las pruebas neurológicas en el proceso penal*, Revista Iuris, Probática, Coord. Instituto de Probática y Derecho del Proceso de la Facultad de Derecho ESADE-URL, 2ª enero de 2014, págs. 36- 41.

cuales se manifiestan. Las conclusiones deben dar respuesta a los extremos solicitados por las partes o el juez. Es fundamental que sean claras, comprensibles, concisas y sin ambigüedades. Las conclusiones serán «*evaluativas*»[300] y de acuerdo con el *«paradigma de la verosimilitud*» (probabilidad como grado de creencia no de arbitrariedad) y no el habitual «*paradigma de la individualización*» (infalibilidad de la prueba científica), al perito sólo le compete ilustrar sobre lo que dicen los datos resultantes de la prueba y éstos han de expresarse científicamente en términos de verosimilitud.

Es decir, lo único que el perito puede (y debe) hacer es expresar los resultados de la prueba de un modo científicamente riguroso y que al mismo tiempo permita al juez comprender el alcance exacto de los mismos de cara a realizar su valoración ponderándolos con el resto de pruebas. Es por ello incorrecto el uso de las *escalas verbales de la probabilidad*, muy utilizadas, y que reproducen el *paradigma de la individualización* indicando no lo que dicen los datos sino lo que se debe creer[301]. La toma de conciencia de que el riesgo de errores judiciales por mala interpretación de datos obrantes en las conclusiones periciales es alto ha conducido en Reino Unido a adoptar un acuerdo sobre el modo científicamente riguroso de formular las conclusiones de los informes. Se trata del estándar en conclusiones denominado «*Standards for the Formulation of Evaluative Forensic Science Expert Opinion,* creado por la *Association of Forensic Science Providers»*[302]. También el Laboratorio Nacional de ciencia Forense Sueco (SKL) anunció en la V Conferencia de la Academia Europea de Ciencia Forense celebrada en Glasgow en septiembre de 2009, su decisión de unificar la forma de expresar las conclusiones de los informes periciales con independencia de la disciplina científica[303].

---

[300] Se suele distinguir entre conclusiones factuales, investigativas y evaluativas. Las «factuales» no requieren ninguna interpretación entendida como ejercicio de injerencias, las «investigativas» se relacionan con los informes de peritos que se aportan a Unidades de Investigación, y las «evaluativas» que requieren ejercicio de inferencias. Véase Association of Forensic Science Providers-Unid Kingtom (AFSP), Standards for the formulation of evaluative forensic science expert opinion, págs.161-164.

[301] Véase sobre este tema GASCÓN ABELLÁN, Marina, LUCENA MOLINA, José Juan y GONZÁLEZ RODRÍGUEZ, Joaquín. *Razones científico-jurídicas para valorar la prueba científica: una argumentación multidisciplinar.* Diario La Ley, Nº 7481, Sección Doctrina, 4 oct. 2010, Año XXXI, Ref. D-292, Ed. La Ley, pág.14.

[302] Véase *Standards for the Formulation of Evaluative Forensic Science Expert Opinion*, Association of Forensic Science Providers-United kingdom (AFSP), Science & Justice 49 (3), Septiembre, 2009. págs. 161-164.

[303] A. Norgaard et. Al., Ordinal scales of conclusion for de value of evidence, Interpretation and Evaluation Session of the V Conference of the European Academy of Sciences held in Glasgow (Scotland), University of Strathclyde, 8-11, Septiembre, 2009.

La cadena de custodia obliga a que una vez finalizados los estudios por parte del perito se especifique «*…el destino final que se dará a las evidencias una vez concluido su análisis, reseñando para todas ellas el medio utilizado para la puesta a disposición del organismo o entidad solicitante de la pericial*»[304]. Se remitirá al organismo solicitante del estudio los equipos y soportes digitales estudiados, acompañados del correspondiente recibo o documento de control de evidencias. Dicho recibo debidamente cumplimentado, debe devolverse al organismo u empresa que lo emite, una vez haya llegado el informe y las muestras objeto de estudio al organismo o entidad que lo solicitó, dando así por finalizado la trazabilidad y el proceso de custodia de las evidencias objeto de análisis forense.

El informe pericial será firmado por los peritos y otros responsables del entorno de análisis forense que lo emiten, según el plan de calidad instaurado en el mismo, o bien, se puede firmar digitalmente por los mismos actores anteriores.

Anexados al dictamen pericial se acompañarán, de conformidad a lo previsto en el artículo 336.2 LEC, los documentos, instrumentos o materiales adecuados para exponer el parecer del perito sobre lo que haya sido objeto de la pericia. Lo cual ayudará notablemente la comprensión por las partes y el juez de los extremos que conforman el dictamen. Este artículo permite anexar, por ejemplo, al dictamen pericial informático-forense la copia de la información obtenida de un ordenador y efectuada en un CD con el correspondiente hash –soporte de los datos informáticos obtenidos- y que permitiría una contrapericia. En aquellos supuestos en que no fuese posible o conveniente aportar estos materiales e instrumentos, el escrito de dictamen contendrá sobre ellos las indicaciones suficientes. Podrán, asimismo, acompañarse al dictamen los documentos que se estimen adecuados para su más acertada valoración (336.2 LEC)[305].

[304] Así lo recoge el apartado cuarto de la norma 71056 de AENOR: «*…Una vez finalizados los estudios reflejados en el apartado anterior, debe especificarse el destino final que se dará a las evidencias una vez concluido su análisis, reseñando para todas ellas el medio utilizado para la puesta a disposición del organismo o entidad solicitante de la pericial*».

[305] La posibilidad de anexar dichos documentos aparece en también regulado en códigos procesales como el colombiano que regula en el apartado 10 del artículo 226 como requisito mínimo del dictamen la necesidad de «*10. Relacionar y adjuntar los documentos e información utilizados para la elaboración del dictamen*». Código Procesal Colombiano, Ley núm. 1564, de fecha 12 de julio de 2012.

8.2.2 Compatibilidad de dictámenes periciales

La normativa actual no ofrece una respuesta clara al hecho de que cualquiera de las partes litigantes en un juicio pueda aportar como prueba al litigio un dictamen pericial de parte y uno realizado por designación judicial (art. 339.2.II y .3 y art 427.3 y .4 LEC). Dicha posibilidad revestirá, por ejemplo, relevancia en supuestos de prueba dirimente en que existen en el proceso dos dictámenes contradictorios. A nuestro modo de ver la respuesta a esta cuestión pasa por una interpretación flexible del artículo 335 LEC en el sentido más favorable al ejercicio del derecho de prueba de conformidad a la constitucionalización de este derecho en el artículo 24 de la Constitución Española, por lo que estamos a favor de la compatibilidad entre ambas periciales. Parte de la doctrina sustenta tal posición doctrinal como en el caso de FONT SERRA, RIFÁ, GUZMÁN FLUJA, GARBERÍ LLOBREGAT y BUITRÓN RAMIREZ, DÍAZ FUENTES, MONTERO AROCA y PICO i JUNOY. Dicha posición doctrinal viene también apoyada jurisprudencialmente en resoluciones como el auto del Juzgado de primera Instancia número 4 de la Coruña de 14 de junio de 2006, el auto del Juzgado de Primera Instancia núm. 1 de Cantabria de 4 de diciembre de 2002, y el auto del Juzgado de primera Instancia número 9 de la Coruña de 7 de julio de 2001[306].

Frente a la anterior posición doctrinal, otros autores como ASENCIO MELLADO, SERRA DOMÍNGUEZ, MUÑOZ SABATÉ, GARCIANDÍA GONZALEZ y FLORES PRADA, sostienen la incompatibilidad de ambas periciales[307]. Entre estos últimos

[306] A favor de la compatibilidad entre dictámenes véanse: FONT SERRA, E., *El dictamen de peritos y el reconocimiento judicial en el proceso civil,* edit. La Ley, Madrid, 2000, págs. 66, 126-127; RIFA SOLER, J.M., *Comentarios a la nueva Ley de Enjuiciamiento Civil,* M.A. Fernández-Ballesteros, J.Mª. Rifa Soler y J.F. Valls Gombau (coords.), edit. Atelier, Barcelona, 2000, pág. 1577; GUZMAN FLUJA, V., *El proceso Civil,* Vol. II, F. Escribano Mora (coord..) edit. Tirant Lo Blanch, Valencia, 2001, págs. 2465 y 2466; GARBERÍ LLOBREGAT, J. y BUITRON RAMIREZ, G, *La prueba civil,* edit. Tirant lo Blanch, Valencia 2004, pág. 415; DÍAZ FUENTES, A., *La prueba en la nueva Ley de Enjuiciamiento Civil,* 2ª edit. Bosch, Barcelona, 2004, pág.250; y MONTERO AROCA, J., *La prueba en el proceso civil,* 4ª edic., edit. Civitas, Madrid, 2005, pág. 333; PICO y JUNOY, *Dictamen por perito designado a instancia de parte,* en "La prueba pericial", ABEL LLUCH, X. y PICO y JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.3, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, págs.299 a 306.

[307] A favor de la incompatibilidad de dictámenes se pronuncian: ASENCIO MELLADO, JM., en *AAVV, Proceso Civil Práctico*, T. IV, director V. Gimeno Sendra, edit. La Ley, Madrid, 2001, págs. 646 y 647; SERRA DOMÍNGUEZ, M., *La prueba pericial*, en "Instituciones del nuevo proceso civil: comentarios sistemáticos de la Ley 1/2000, coord. J. Alonso-Cuevillas, vol. II, edit. Difusión Jurídica, Barcelona, 2000, pág. 310; MUÑOZ SABATÉ, Ll., *Fundamentos de la Prueba judicial civil LEC 1/2000*, J.M. Bosch Editor, Barcelona 2001, pág. 341; GARCIANDÍA GONZALEZ, P., *Del dictamen de peritos*, en "Comentarios a la Ley de Enjuiciamiento Civil", F. Cordón Moreno, T. Armenta Deu, J. Muerza Esparza y T. Tapia Fernández (coord..), edit. Aranzadi, Navarra, 2001, pág. 1147; y FLORES PRADA, I., *La prueba pericial de parte en el proceso civil*, edit. Tirant Lo

autores que defienden la incompatibilidad de las pericial de designación judicial y la de parte, también existe división de criterios en cuanto a si es posible elegir entre una u otra o la pericial de designación judicial es subsidiaria a la de parte. Por la aplicación subsidiaria de la pericial judicial aboga SERRA DOMÍNGUEZ, GÓMEZ COLOMER, CREMADES MORANT Y RODRÍGUEZ ACHÚTEGUI. Sostiene la aplicación alternativa y por lo tanto el reconocimiento a la posibilidad de optar entre una u otra pericial, PINAZO OSUNA[308].

Volviendo a la cuestión principal sobre la compatibilidad de la prueba pericial privada y de designa judicial presentadas por una misma parte veamos de modo general un resumen de los argumentos esgrimidos en contra y a favor. Entre quienes sostienen que nos hallamos ante dictámenes incompatibles (ASENCIO MELLADO), por lo que la opción por el dictamen de parte excluye la posibilidad de otro efectuado por un perito judicialmente designado, postura electiva y excluyente, se esgrimen los siguientes argumentos: 1º) El uso de la conjunción disyuntiva «o» en el artículo 335 LEC, según el cual: «… *Las partes podrán aportar al proceso el dictamen de peritos que posean los conocimientos correspondientes o solicitar, en los casos previstos en la ley, que se emita dictamen por perito designado por el tribunal».* Así, se afirma que si el legislador hubiese querido conferir a dicha conjunción naturaleza copulativa hubiera utilizado la «y» como hace en otros preceptos a los que quiere conferir dicha función; 2º) La propia configuración procedimental que la LEC ha diseñado de la prueba pericial, de la que puede deducirse la voluntad de excluir dictámenes periciales dirimentes. Se afirma que si el legislador hubiese deseado que las partes pudieran acudir a una tercera opinión, lo lógico hubiese sido que la proposición del dictamen emitido por un perito judicialmente designado se hubiera llevado al momento oportuno de proposición de prueba, esto es, a la audiencia previa, una vez deducidas la demanda y la contestación y aportados los informes periciales contradictorios y no antes, en los citados escritos iniciales de alegaciones; 3º) Carece de lógica permitir que sobre una misma materia litigiosa la parte pretenda articular dos pruebas con el mismo contenido, siendo la segunda –la referente a la pericial elaborada por un perito judicialmente designado- del todo inútil, por lo que debe inadmitirse atendiendo al art. 283.2 LEC; 4º) Sencillez. La finalidad anunciada en la Exposición de Motivos de una mayor sencillez, quedaría inmediatamente frustrada si se produjeran una

---

Blanch, Valencia, 2005, pág. 234. En esta línea SAP Barcelona, secc. 14ª, de 24 de marzo de 2006, Pte. Ilmo. Sr. D. Francisco Javier Pereda Gámez, Fdo. Jco. 1º.

[308] CALVO GONZÁLEZ, Susana, *Compatibilidad entre la pericial de parte y la pericial judicial en la LEC 2000*, en Problemas actuales de la prueba civil, en la obra colectiva del mismo título, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), J.M. Bosch, Barcelona, 2005, p. 103 y ss.

pluralidad de dictámenes[309]; y 5º) Economía procesal. Con la opción de la subsidiariedad, se incumpliría la que parece finalidad principal de la ley, es decir, alcanzar un procedimiento ágil, careciendo de sentido exigir primero la presentación de dictámenes periciales con los escritos iniciales y después, abrir a todos los supuestos la posibilidad de solicitar la designación judicial de perito, dando lugar de nuevo a la situación de la LEC de 1881 en la que la prueba pericial dilataba los procesos de modo ineludible[310].

Frente a los anteriores argumentos la doctrina proclive a la compatibilidad de ambas periciales alega: 1º) Que la conjunción «o» no solo denota «diferencia, separación o alternativa» sino también puede denotar «equivalencia» según el Diccionario de la Real Academia Española; 2º) Si bien es cierto que la LEC no ha previsto dictámenes periciales dirimentes, no lo es menos que no hay ninguna norma expresa que los prohíba, por lo que la eficacia de un derecho fundamental a la prueba no puede limitarse en méritos de una norma prohibitiva que expresamente no aparece en la ley, por lo que tampoco este argumento resulta convincente; 3º) Una interpretación conjunta de todo el articulado regulador de la prueba pericial. La lectura aislada de los artículos 336 y 338 LEC puede llevar a la conclusión de incompatibilidad y el juego de la pericial judicial sólo excepcionalmente. Sin embargo en dichos artículos no hace sino regularse el momento procesal de la aportación de los informes traídos por la parte, estableciendo un régimen de incorporación y preclusión similar al de los documentos. Si la parte aporta su pericial en dichos momentos, no se ve privado de la posibilidad de pedir designación judicial de perito si lo entiende conveniente o necesario para sus intereses; el artículo 339.2 LEC no condiciona tal posibilidad a la circunstancia de no haberse presentado dictamen escrito; 4º) En el supuesto que el dictamen extraprocesal no fuera suficiente a efectos probatorios de haberse inadmitido el dictamen de perito designado judicialmente podría alegarse indefensión por denegación de dicha pericia, por cuanto el rechazo sólo debe producirse por razones de impertinencia o utilidad no simplemente por el obstáculo de que ya obre en autos; y 5º) El segundo dictamen puede obedecer a la intención de la parte de dar mayor solidez a las conclusiones del dictamen ya aportado inicialmente con una segunda opinión,

[309] Véase SUÁREZ GONZÁLEZ, C., *Introducción al nuevo régimen jurídico del dictamen de peritos. Aportación al proceso, tacha, recusación y régimen económico*, en "La prueba pericial, el perito y la nueva Ley de Enjuiciamiento Civil", Jornada del Colegio de Abogados del Ilustre Señorío de Bizkaia, Bilbao, 2001, pág.5.

[310] Véase GARCÍA GONZÁLEZ, C. *El nuevo régimen de peritos designados judicialmente*, en "La prueba pericial, el perito y la nueva Ley de Enjuiciamiento Civil", Jornada del Colegio de Abogados del Ilustre Señorío de Bizkaia, Bilbao, 2001, pág. 49.

obteniendo el juez un mayor material probatorio que le permitirá alcanzar una mayor efectividad de la tutela judicial [311].

Suscribo los argumentos a favor de la compatibilidad de dictámenes. A mi modo de ver, ni existe norma que lo impida atendiendo a los razonamientos anteriores, ni puede restringirse el derecho a la prueba de la parte proponente, pudiendo la segunda pericial aportar nueva información al juez en que fundamentar su valoración. Sin perjuicio que de no aportar la segunda pericial nada nuevo y tratándose de una simple reiteración el juez la excluya expresamente de la condena en costas, debiendo asumir su coste la parte proponente.

* * *

[311] Véase CALVO GONZÁLEZ, Susana, *Compatibilidad entre la pericial de parte y la pericial judicial en la LEC 2000*, en Problemas actuales de la prueba civil, en la obra colectiva del mismo título, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), J.M. Bosch, Barcelona, 2005, pág. 100.

CAPÍTULO IX.- LA PRÁCTICA DE LA PRUEBA SOBRE EL HECHO ELECTRÓNICO EN EL PROCESO JURISDICCIONAL

9.1 Introducción

La Constitución Española garantiza el derecho a la prueba (art. 24.2 CE), por lo que cualquiera de los litigantes tiene derecho a la admisión y práctica de cualquier fuente de prueba. La práctica de la prueba garantiza, además, la intervención de la contraparte, quien podrá utilizar la prueba propuesta por la contraria para lograr el convencimiento del juez mediante una actitud activa en su desarrollo, lo cual constituye una manifestación del genérico derecho a la prueba[312].

El derecho a la práctica de la prueba es un derecho que siempre viene modulado por la pertinencia, la necesidad y los requisitos de admisión previstos por la ley (STC 30 de enero de 2003, entre otras). Como norma general recae en las partes la carga de la prueba, salvo en algunos casos excepcionales en que la ley procesal permite acordarla de oficio (art. 282 y 216 LEC)[313]. Los litigantes deberán averiguar las fuentes que servirán para acreditar las afirmaciones de los hechos alegadas y controvertidas (281.3 de la LEC). Dichas fuentes accederán al proceso a través de los medios de prueba propuestos por las partes, previa admisión por parte del Juez, y a través de los mismos serán objeto de valoración a los efectos de motivar la sentencia (art. 218.2 de la LEC y 24.2 y 120.3 de la CE).

La prueba que propongan las partes debe ser una prueba autorizada por el Ordenamiento jurídico, es decir, no pueden proponer pruebas ilegales, prohibidas por el Ordenamiento Jurídico, o ilícitas, obtenidas con vulneración o infracción de los derechos fundamentales (art. 283, 287 de la LEC y 11 LOPJ). La prueba debe ser pertinente, es decir, debe tener relación con el *thema decidendi*, y debe proponerse en tiempo y forma (art. 284, 414.1, 429.1, 435.1, 444.4 y 460.2 LEC). Debe ser útil, es decir, debe inadmitirse aquella prueba que según reglas y criterios razonables y seguros, en ningún caso pueda contribuir a esclarecer los hechos controvertidos (art. 283.2 LEC).

---

[312] En este sentido se pronuncian ABEL LLUCH, X y PICO I JUNOY, J. en *Problemas actuales de la prueba civil,* J.M Bosch Editor, 2005, pág. 40.

[313] Recogen la iniciativa probatoria de oficio los artículos 429.1, 435.2, 752.1, 759.1, 763.3, 770.4ª, 339.5, 306.1.II y 372.2 LEC. Tratamiento específico merecen el derecho extranjero y el derecho consuetudinario (art. 281.2 LEC) y la dispensa de prueba relativa a los hechos notorios (art. 281.4 LEC) y dispensa absoluta a los hechos respecto a los que exista conformidad (art.281.3 LEC).

La prueba sobre el hecho electrónico presentada por cada parte procesal podrá ser «impugnada» por las restantes. «Impugnación» entendida en sentido amplio no sólo como la interposición de recursos sino también como el posicionamiento en juicio por parte de la adversa sobre la prueba presentada. Es decir, las partes pueden formular alegaciones relacionadas con el juicio de admisión o valoración probatoria de la prueba electrónica presentada, o aportar medios de prueba que la desvirtúen[314]. En relación a las alegaciones relacionadas con el juicio de admisión las partes podrán fundamentarlas en la presentación de los medios de prueba fuera del momento procesal oportuno determinado legalmente (criterio de temporalidad) o por incumplir los requisitos establecidos legalmente (criterio de legalidad). Cuando la impugnación consista en aportar medios de prueba que desvirtúen la aportada de contrario, tratándose de prueba pericial las partes podrán aportar medios de prueba que desvirtúen las máximas de la experiencia técnica o conclusiones del dictamen pericial adverso; y tratándose de prueba documental la parte contraria podrá aportar pruebas con el objeto de desvirtuar el contenido de un documento adverso.

Una vez propuesta la prueba el Juez dictará resolución admitiendo o inadmitiendo la misma. Debe razonar la inadmisión sin que dicha resolución pueda ser irrazonable o arbitraria (STC de 14 de enero de 2004)[315]. Una vez admitida la prueba debe ser practicada (STC de 14 de febrero de 2000 y STC de 12 de diciembre de 2005)[316].

Las pruebas deben practicarse contradictoriamente en vista pública, o con publicidad y documentación similares si no se llevan a efecto en sede del tribunal (art. 289.1 LEC), siendo inexcusable la presencia judicial en el interrogatorio de partes y de testigos, en el reconocimiento de lugares, objetos o personas, en la reproducción de palabras, sonidos e imágenes y, en su caso, cifras y datos, así como en las explicaciones, impugnaciones, rectificaciones o ampliaciones de los dictámenes periciales (art. 289.2 LEC). Tal y como recoge el artículo 384.1 de la LEC, los instrumentos serán examinados por el tribunal por

[314] ABEL LLUCH utiliza en este sentido un concepto amplio del término «impugnación», es decir, no circunscrito a la interposición de recursos sino entendiendo por «impugnar» el hecho de formular alegaciones o aportar medios de prueba que desvirtúen la prueba presentada por la parte contraria. ABEL LLUCH, X. *Derecho probatorio*. Ed. Bosch, 2012, págs. 749-753.

[315] Véase sobre la necesidad de que el juez razone su resolución la STC 14 enero 2004, fto. jco.2º, (EDJ 2004/389).

[316] STC de 12 de diciembre de 2005, fto. jco.4º (EDJ 2005/213561), la cual, a su vez, cita las SSTC de 17 de enero de 2005 (EDJ 2005/3244), de 26 de marzo de 2001 (EDJ 2001/2656), de 16 de octubre de 2000, (EDJ 2000/31691), y 24 de febrero de 2000 (EDJ 2000/1145).

los medios que la parte proponente aporte o que el tribunal disponga utilizar, asegurando el derecho a la práctica de la prueba en el supuesto de que el Juzgado no disponga de medios técnicos suficientes al efecto. Es evidente que en la prueba del hecho electrónico existirán mayores dificultades cuando se aporte directamente mediante soporte electrónico sin volcado en papel dado que el juez ignora su contenido, por lo que deberá procederse a su reproducción en la propia audiencia previa o juicio lo cual supondrá una mayor duración de dicho trámite procesal.

La prueba electrónica podrá practicarse como prueba anticipada, cuando existe temor fundado de que las pruebas puedan desaparecer o perder su objeto por el transcurso del tiempo (art.295 LEC); o como diligencia final (art. 434 a 436 LEC).

9.2 Prueba electrónica: Prueba pericial.

9.2.1 Momento procesal de aportación del dictamen pericial

9.2.1.1 Con los escritos iniciadores del proceso

La regla general inicial en el proceso judicial, si las partes optan por la prueba pericial de designa de parte, es que el actor deberá aportar el dictamen pericial junto con la demanda y el demandado junto a la contestación a la misma (art. 265.1.4º y 336.1 LEC). Es decir, el actor debe esperar a disponer del dictamen pericial para presentar la demanda. Solo excepcionalmente cuando la defensa de su derecho no permita demorar la interposición de aquella podrá aportarlo con posterioridad, en cuyo caso deberá anunciarlo en la demanda y justificarlo «cumplidamente». Dicho dictamen deberá aportarse, para su traslado a la parte contraria, en cuanto se disponga del mismo y, en todo caso, cinco días antes de iniciarse la audiencia previa al juicio ordinario o de la vista al juicio verbal (art. 336.3 y 337.1 LEC)[317]. Deberá, asimismo, indicarse la solicitud de comparecencia de los peritos a fin de que exista pronunciamiento judicial al efecto (art. 337.2 LEC). De igual modo, en los juicios verbales con contestación escrita el demandado que no pueda aportar el dictamen junto con la contestación a la demanda deberá justificar la imposibilidad de pedirlos y obtenerlos dentro del plazo para contestar, y aportarlo para traslado a las partes con cinco días de

[317] El artículo 337 fue modificado por la Ley 13/2009, de 3 de noviembre, introduciendo el plazo de cinco días, terminando con las presentaciones sorpresivas de dictámenes periciales antes del inicio de la audiencia previa en el juicio ordinario y en la vista en el juicio verbal.

antelación a la vista del juicio (art. 336.4 y 337.1 LEC). Este último caso puede resultar más habitual en supuestos de mayor complejidad dado el plazo vinculante para la contestación a la demanda, y deja abierta la cuestión de indefensión para el demandado dado que se ve obligado a contestar por escrito sin disponer del dictamen pericial.

En el juicio verbal sin contestación escrita el dictamen pericial por parte del demandado se aportará el mismo día de la vista de juicio de conformidad a lo previsto en los artículos 265.1.4º y 336 LEC (Sentencia del Tribunal Supremo, Sala Segunda, en sentencia de fecha 26 de marzo de 2007). Si como consecuencia de lo alegado en la contestación a la demanda, fuera necesario para el actor aportar un dictamen pericial, deberá interrumpirse la vista a tenor del artículo 193 LEC. El artículo 265 .1.4º de la LEC establece expresamente que el dictamen pericial deberá acompañarse a la contestación a la demanda. No es posible aplicar analógicamente el artículo 338 de la LEC, que regula los dictámenes cuya necesidad o utilidad se ponga de manifiesto a causa de alegaciones del demandado en la contestación a la demanda o de las alegaciones o pretensiones complementarias admitidas a tenor del art. 426, ni el artículo 337 LEC, que prevé, tras la reforma 13/2009, un plazo de cinco días para poder presentar el dictamen antes de iniciarse la vista del juicio verbal en el supuesto que no pueda aportarse junto a la contestación. Lo contrario supondría crear indefensión a la parte y dejar a discreción del juez exigir dichos plazos, puesto que la propia LEC no prevé el mismo de un modo expreso.

No obstante, la norma procesal es confusa en su redacción. De hecho si bien el artículo 265 LEC establece una norma al parecer general, no parece desprenderse lo mismo del artículo 336.1 el cual señala expresamente que habrán de aportarse dichos dictámenes junto con la demanda o contestación «*si ésta hubiera de realizarse en forma escrita*» de lo que *a «sensu contrario»* se deduce que no es así en el supuesto que la contestación no sea escrita. Siendo a nuestro modo de ver contradictorio que la LEC insista en que los dictámenes periciales consten en autos con carácter previo a la vista de juicio cuando no se han podido aportar junto a la contestación, o bien cuando obedecen a pretensiones o alegaciones posteriores a la demanda o contestación, e incluso determine en su artículo 339.1 -que regula la pericial de designa judicial en los casos de derecho de asistencia jurídica gratuita- un plazo de diez días de solicitud a «*fin de que la pericial conste aportada antes de la vista de juicio*», y por el contrario no regule expresamente la aportación de dicho dictamen con carácter previo al juicio en el juicio verbal sin contestación escrita a la demanda y en la designa judicial sin la excepción de quien les asiste el derecho de justicia gratuita.

La aportación simultánea a la contestación a la demanda en el juicio verbal sin contestación escrita obliga al letrado de la parte contraria a dar lectura de forma apremiante a un dictamen en ocasiones complejo técnicamente y extenso lo que obliga a la suspensión del juicio en aras a no crear indefensión a la parte, provocando demora en el procedimiento y satura más a nuestros tribunales, o le obliga a una improvisación que vulnera el derecho a la defensa de su representado. De igual modo también provoca interrupción en los supuestos de solicitud de pericial complementaria por parte de la actora. Realmente el legislador debiera plantearse si realmente los juicios verbales sin contestación escrita aportan mayores beneficios que inconvenientes, y si a la larga no repercute esa mayor celeridad en retrasos y suspensiones innecesarias en nuestros tribunales, y una menor preparación por parte de los letrados en la vista de juicio al desconocer cuáles serán las alegaciones del demandado. Todo ello sin perjuicio de que dada la agenda de muchos juzgados siquiera es posible acordar interrupciones en los juicios respetando los plazos establecidos por la ley dada la agenda de señalamientos de los mismos y la carga que soportan.

Tratándose del caso del demandado declarado en rebeldía, éste no tiene la posibilidad de aportar un dictamen pericial de parte, y no puede tampoco solicitar la designación judicial de perito, en virtud del principio de preclusión, más allá de los limitados supuestos previstos en el artículo 426 LEC, en relación con el artículo 338.1 LEC. Ello salvo en el supuesto previsto en el último apartado del artículo 339.3 LEC. Lo contrario supondría hacer de mejor derecho al demandado que no comparece y no contesta a la demanda, sin conocerse los motivos de esa incomparecencia, que aquél que sí lo ha hecho. Además causaría evidente indefensión a la parte actora, que desconocería hasta la audiencia previa el contenido del dictamen pericial en el caso de que sea de parte y presentado en dicho acto.

En el supuesto que las partes soliciten la designación de un perito judicial para emitir el dictamen deberán pedir dicha designación en los escritos de alegaciones iniciales, es decir, en los escritos de demanda y contestación. En el juicio verbal en el que no exista trámite de contestación a la demanda el demandado deberá realizar la solicitud de designa judicial de perito con al menos diez días de antelación al que se hubiera señalado para la celebración del acto de la vista (art. 339 LEC)[318].

La ley prevé expresamente el supuesto en que cualquiera de las partes fuese titular del derecho de asistencia jurídica gratuita. En tal caso, el titular del derecho a la asistencia de justicia gratuita no está obligado a acompañar

[318] Redacción dada según el apartado 161 del artículo decimoquinto de la Ley 13/2009, de 3 de noviembre.

dictamen pericial junto a la demanda o a la contestación a la demanda, sino que simplemente deberá anunciarlo en dichos escritos a los efectos de que se proceda a la designación judicial de perito, conforme a lo que se establece en la Ley de Asistencia Jurídica Gratuita. Si se tratara de juicios verbales sin trámite de contestación escrita, el demandado beneficiario de justicia gratuita deberá solicitar la designación judicial de perito al menos con diez días de antelación al que se hubiera señalado para la celebración del acto de la vista, a fin de que el perito designado pueda emitir su informe con anterioridad a dicho acto (art. 339.1 LEC).

La desigualdad en oportunidad de armas del demandado titular del derecho a justicia gratuita respecto al que disponga de recursos económicos es evidente, puesto que mientras este segundo está en condiciones de fundamentar su pretensión en la demanda mediante asesoramiento técnico del que puede hacer uso con gran antelación, al primero se le veda dicha posibilidad o se le concede un escaso plazo para obtener un dictamen pericial en orden a rebatir el presentado por el actor (veinte días de contestación a la demanda ex artículo 404 LEC). Por otra parte, el titular de justicia gratuita no podrá tampoco elegir perito de confianza frente a la posibilidad de que dispone la otra parte. La solución ante tales desigualdades lleva a afirmar la necesidad de autorizar, pese, al silencio legal al respecto, la suspensión del plazo para contestar a la demanda en orden a la elaboración por el perito judicial del dictamen, permitiendo que la parte demandada pueda formular sus alegaciones iniciales, disponiendo, al igual que el actor, de conocimientos técnicos requeridos para el adecuado ejercicio del derecho de defensa, en cumplimiento de las garantías reconocidas en el artículo 24 de la CE. Podría apoyarse dicha tesis desde un punto de vista procesal en el artículo 134.2 de la LEC, en cuanto prevé la interrupción de los plazos y su reanudación en los supuestos de fuerza mayor. A tenor de dicho artículo, que alude al momento en que hubiera cesado la causa determinante de la interrupción o demora como tiempo referencial a los efectos de reanudación del proceso, debemos concluir que en todo caso, una vez elaborado y aportado el informe pericial a las actuaciones no deberían rebasarse los 20 días previstos legalmente para la contestación a la demanda. Debiendo suspenderse el plazo de tiempo prudencial que requiera la elaboración de la pericial propuesta (considerando igualmente el contenido del art. 132.2 de la LEC, al preceptuar que cuando no se fije plazo ni término, se entenderá que han de practicarse las actuaciones del juicio sin dilación) en cuanto ha sido su necesidad de valoración la causa determinante de la suspensión alegada por la parte[319].

[319] Véase: VELÁZQUEZ VIOQUE, D., *Dictamen por perito por designación judicial,* en "La prueba pericial", ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.3, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch,

La no presentación del dictamen pericial o, en su caso, solicitud de designa judicial en el tiempo legalmente establecido se sanciona con preclusión probatoria (arts. 269, 265.1.4º, 336.1, 337.1, 338.2, 339.2 II LEC,). En el supuesto de perito de designa judicial la pericial debe aportarse por el perito «en el plazo que se le haya señalado» del cual el Secretario dará traslado a las partes por si quieren someterlo a contradicción, por lo que, en todo caso, deberá efectuarse con anterioridad a la vista o al acto de juicio oral (art. 346 LEC).

9.2.1.2 Aportación de dictámenes periciales una vez iniciado el proceso

La Ley de Enjuiciamiento civil regula la posibilidad de aportar dictámenes periciales de designación de parte o judicial en función de actuaciones posteriores a la demanda. En este sentido la norma permite aportar prueba pericial que verse sobre alegaciones o pretensiones complementarias durante el transcurso del proceso –suscitados por la contestación a la demanda- y durante la audiencia previa al juicio. Dichos dictámenes deberán aportarse, en el supuesto de designa de parte, para su traslado a las contrarias, con al menos cinco días de antelación a la celebración del juicio o de la vista en los juicios verbales con trámite de contestación escrita y en la designa judicial en «el plazo señalado» (art. 338.2, 339.2 párrafo segundo y 427.4 LEC).

La pericial por designa judicial podrá, asimismo, ser acordada de oficio por el juez «*cuando así lo establezca la ley*» (art. 282 LEC). Regulación acorde con el sistema actual en que domina la iniciativa probatoria de parte (art. 282 LEC). La Exposición de Motivos de dicho cuerpo legal así lo ratifica al señalar que «*no se impone y se responsabiliza al tribunal de la investigación y comprobación de la veracidad de los hechos relevantes en que se fundamentan las pretensiones de tutela formuladas por las partes, sino que es sobre éstas sobre las que recae la carga de alegar y probar*». La LEC prevé que se acuerde por parte del juez la pericial en los procesos no dispositivos (art. 339.5 LEC), la posibilidad de «sugerir» prueba pericial para paliar la insuficiencia de la prueba propuesta por las partes a los efectos que las partes puedan completar o modificar sus proposiciones de prueba (art. 429.1.II LEC), y la de acordar una prueba pericial como diligencia final de oficio (art. 435.2 LEC).

El supuesto de sugerencia por parte del juez en los casos de insuficiencia de las pruebas propuestas por las partes (art. 429.1.II) obedece al ejercicio de sus poderes de dirección del proceso y no implica en ningún caso que pueda

---

págs. 345-352; y MUÑOZ SABATÉ, Ll., *Fundamentos de la Prueba judicial civil LEC 1/2000*, J.M. Bosch Editor, Barcelona 200, pág. 342.

acordar prueba de oficio, dado que ésta sólo se prevé para los supuestos expresamente previstos en la ley (art. 282 y 339.5 LEC) y porque el propio art. 429.1 LEC, en su párrafo tercero, dispone, que a la vista de la indicación de insuficiencia probatoria efectuada por el juez, las partes podrán completar o modificar sus proposiciones iniciales de prueba. En todo caso las indicaciones efectuadas por el juez a los abogados no son vinculantes, y si bien por lo general los abogados, cuando su asistencia sea preceptiva, aceptarán tal sugerencia por temor a perder el pleito por prueba insuficiente, ello no implica que tengan obligación de seguir tales indicaciones, pudiendo desoírlas, sin perjuicio de que, en su caso, pudiera exigirse responsabilidad al abogado por negligencia profesional si causara un total vacío probatorio[320].

La facultad prevista en el artículo 429.1.11 LEC está sujeta a una serie de presupuestos: 1º) La existencia de hechos controvertidos, porque en su defecto no se abre el periodo probatorio; 2º) la previa proposición de las partes, porque la normativa del art. 429.1.2º LEC no puede suplir la inactividad de las partes ni subsanar pruebas no propuestas o propuestas indebidamente por las partes; y la existencia de un juicio eventual de insuficiencia probatoria (STSJ Cataluña, Sala Civil y Penal, de 17 de diciembre de 2012). Además el juez no puede introducir hechos distintos de los alegados por las partes, respetando el principio dispositivo. Y no puede utilizar fuentes probatorias distintas de las existentes en las actuaciones, respetándose así la debida imparcialidad judicial[321].

Uno de los temas más polémicos del art. 429.1.II LEC es si, al amparo de dicha normativa, el juez puede proponer un medio de prueba –en este caso un dictamen pericial- cuyo momento procesal ya ha precluido. Si bien una parte de la doctrina y de la jurisprudencia sostienen la no preclusión probatoria con fundamento a que ésta vincula a las partes pero no al juez[322], otro sector

---

[320] Véase FERNÁNDEZ LÓPEZ, M., *Las facultades probatorias del juez civil previstas en el art. 429.1.11 LEC*, artículo publicado en la revista jurídica "Práctica de Tribunales. Revista de Derecho Procesal Civil y Mercantil", núm. 21, noviembre de 2005. Puede visualizarse en formato PDF en la página web rua.ua.es.

[321] Pueden consultarse: PICÓ y JUNOY, J., *El derecho a la prueba*, J.M. Bosch, Barcelona, 1996, págs. 267 a 271; y del mismo autor *El juez y la prueba*, J.M. Bosch, Barcelona, 2007, págs. 117 a 119.

[322] Respecto a la no vinculación probatoria del juez véase PICO PICÓ i JUNOY *La iniciativa probatoria del juez civil. A propósito de un caso, en* "Los poderes del Juez Civil en materia Probatoria", ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), J.M. Bosch, Barcelona, 2003, págs. 159-160; y DE LA RUA NAVARRO, J, *La facultad del art. 429.1, II y III LEC y la preclusión probatoria. ¿Puede el juez proponer medios de prueba cuyo momento procesal ha precluído (ej. Dictámenes y documentos)?,* en "Problemas actuales en la prueba civil", Abel Lluch, X y Picó i Junoy, J (coords), J.M. Bosch, Barcelona, 2005, págs. 253 y ss.

jurisprudencial y doctrinal, entre el que nos incluimos, entiende con acierto que existe preclusión probatoria y por lo tanto el juez no puede proponer dicho medio de prueba (SAP Rioja de 31 de enero 2005y AP Murcia de 15 de febrero de 2002)[323]. Es decir, la facultad del artículo 429.1.II LEC debe efectuarse con respeto a la legalidad probatoria de manera que no pueden proponerse medios de prueba sometidos a un estado anterior de preclusión.

Fundamentan dicha posición doctrinal la sumisión de la solicitud y aportación de los dictámenes a unos estrictos momentos preclusivos, sea con los escritos de alegaciones (art. 265.1.4 y 336.1 LEC), sea con la necesidad de formular su solicitud en tales momentos (art. 339.2. LEC), así como la normativa del art. 429.1 de la LEC que no permite la subsanación de pruebas no propuestas o propuestas indebidamente por las partes. Es decir, solo cabe indicación y propuesta de una prueba pericial, al amparo de la normativa del artículo 429.1.2º en los supuestos legalmente previstos. Y habida cuenta de lo previsto en el artículo 265.1.4 y 336 LEC –carga procesal de aportación de los dictámenes de parte en los escritos de alegaciones- y del ar. 339.2.II LEC –solicitud de dictamen judicial en los escritos de alegaciones salvo alegaciones o «pretensiones no contenidos en la demanda»- el juez solo podrá efectuar tal «sugerencia» respecto a las alegaciones o pretensiones complementarias (art. 427.3 en relación con el art. 426.1, 2 y 3 LEC) de hechos nuevos o de nueva noticia (art. 286.3 LEC). Si no se trata de estos supuestos y ante la existencia de dictámenes contradictorios solo podrá también sugerir la conveniencia de intervención del perito en el acto del juicio o de la vista[324].

---

[323] La SAP Rioja, Secc. 1ª, de 31 de enero 2005, F.J. 1º indica que *«(…) el juez no puede subsanar, al amparo de la facultad que le confiere el artículo 429.1 de la Ley Civil Adjetiva, la omisión de los informes periciales que deben acompañarse con la demanda (art. 336 LEC), la omisión del anuncio del dictamen cuando no se pueda aportar con la demanda (art. 337 LEC) y la falta de solicitud en el escrito de demanda de la designación judicial del perito (art. 339 LEC»)*. En igual sentido se pronuncia la SAP Murcia, Secc. 3ª, de 15 de febrero de 2002, F.J. 2º. Véase también CHICO FERNÁNDEZ, T, *La facultad del juez de indicar la insuficiencia de la prueba propuesta y la preclusión probatoria. A propósito del art. 429.1.II y III LEC,* en "Aspectos Prácticos de la Prueba civil", Abel Lluch, X y Picó i Junoy, J (dirs), J.M. Bosch editor, Barcelona, 2006, págs. 264-271; *ABEL LLUCH, X. Iniciativa probatoria de oficio en el proceso civil,* ed. Bosch, Barcelona, 2005, págs. 111 y ss.

[324] Véase ABEL LLUCH, X., *III. ¿Puede el juez al amparo del artículo 429.1.11 Ley de Enjuiciamiento Civil sugerir la práctica de una prueba pericial?*, en "Jurisprudencia sobre derecho probatorio", Diario La Ley, Año XXXIV, Núm. 8187, 8 de noviembre de 2013, págs. 26-28, disponible en www.diariolaley.es.

9.2.1.3 La aportación de dictámenes periciales como diligencia final. Pericial dirimente

La Ley de Enjuiciamiento Civil prevé en su artículo 435.2 la posibilidad con carácter «excepcional» de que el tribunal pueda acordar, de oficio o a instancia de parte, que se practiquen «de nuevo» pruebas sobre hechos relevantes oportunamente alegados con la condición de que los actos de prueba anteriores no hubieran resultado conducentes «*a causa de circunstancias ya desaparecidas e independientes de la voluntad y diligencia de las partes*». Con fundamento en dicho artículo parte de la doctrina entiende que la LEC abre la posibilidad al juez de acordar una pericial dirimente en aquellos supuestos de concurrencia de dictámenes contradictorios.

La prueba pericial electrónica es aquella actividad procesal que transmite al juez conocimientos científicos, técnicos o prácticos para que éste pueda valorar o adquirir certeza sobre hechos electrónicos. Es decir, como prueba tiene como finalidad la convicción judicial. En supuestos en que existen dos dictámenes periciales dispares, cuyas contradicciones no han podido salvarse por la vía de la contradicción del art. 347 LEC, es claro que las pruebas anteriores «*no han resultado conducentes*» –empleando los términos del artículo 435.2 LEC- para el esclarecimiento de los hechos controvertidos, es por ello que se plantea por parte de la doctrina la posibilidad de adopción por parte del juez de un dictamen pericial como diligencia final de oficio (art. 435.2 LEC). Respecto a la anterior posibilidad la doctrina está dividida. La mayor parte de la misma niega la subsistencia del llamado «peritaje judicial dirimente» argumentando que el dictamen pericial tiene unos momentos de aportación previstos específicamente en la regulación legal y ninguno de ellos hace referencia a su aportación como diligencia final, y por otra parte, que no tiene encaje en el artículo 435.2 LEC, pues no existen «*circunstancias ya desaparecidas e independientes de la voluntad y diligencia de las partes*» que hubieran impedido en su momento la práctica de la pericial, que normalmente ya se realizó y cuyos resultados constan en los autos (BANACLOCHE PALAO, SAP Barcelona de 31 de marzo de 2006)[325]. Únicamente se exceptúa aquel supuesto en que una imposibilidad natural hubiera impedido practicar una operación determinada y relevante.

Frente a la anterior posición doctrinal otro sector doctrinal, hoy minoritario, entiende que puede adoptarse una pericial dirimente, con base a que no existe prohibición expresa, y que debe efectuarse una interpretación no restrictiva de las normas que limiten la eficacia del derecho a la prueba. En este sentido se pronuncian autores como ABEL LLUCH, recogiéndose dicha doctrina en

[325] Véase BANACLOCHE PALAO, J, *La pericia: claves para un planteamiento eficaz de la prueba,* en rev. Iuris, núm. 71, abril 2003, págs. 4 y 5.

sentencias como la SAP Málaga de 25 de febrero de 2005 y la SAP Cáceres de 27 de enero de 2003[326]. Ante la inexistencia de prohibición legal para acordar una pericial dirimente, recuerdan que la constitucionalización del derecho a la utilización de los medios de prueba pertinentes (art. 24.2 CE) comporta la necesidad de efectuar una lectura amplia y flexible de las normas probatorias, tendente a permitir la máxima actividad probatoria de las partes, así como igualmente una interpretación restrictiva de los preceptos que limiten la eficacia del derecho a la prueba[327]. Y además, alegan también que existiendo dos periciales contradictorias no se ha obtenido lo conducente a obtener la convicción del juez por lo que se requiere un tercer dictamen dirimente[328].

En mi opinión la vigente regulación no permitiría el nombramiento por parte del juez de un perito dirimente en el supuesto de periciales contradictorias, ya que el art. 435.2 exige claramente para practicar «de nuevo» pruebas sobre hechos relevantes oportunamente alegados que los actos de prueba anteriores no hubieran resultado conducentes «*a causa de circunstancias ya desaparecidas e independientes de la voluntad y diligencia de las partes*». No obstante, como ya se expuso en el § 8.1.1, soy del parecer que debiera regularse de modo expreso en la ley la posibilidad por parte del juez de nombrar un perito dirimente en casos de dictámenes contradictorios. Nuestro ordenamiento debiera facilitar procesalmente al juez la posibilidad de acudir a la prueba pericial en aquellos supuestos que necesite conocimientos técnicos, científicos o prácticos en la materia y las partes no los hayan aportado o de aportarlos no fueran suficientes para poder adoptar una resolución al no disponer de los elementos suficientes para formar su convicción, como en el supuesto de periciales contradictorias.

---

[326] Véase ABEL LLUCH, X., *La prueba pericial,* ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.3, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, pág. 123. Y SAP Barcelona, secc. 14ª, de 31 de marzo de 2006, fdo. Jco 2º; SAP Málaga, secc. 5ª, de 25 de febrero de 2005, fdo. Jco. 2º; y SAP Cáceres, secc 1ª, de 27 de enero de 2003, fdo. Jco. 1º.

[327] Véase PICÓ Y JUNOY, *Problemas actuales de la prueba civil,*, en la obra colectiva del mismo título, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), J.M. Bosch, Barcelona, 2005, págs. 31-34.

[328] Véase PICÓ i JUNOY, J., *Cuestiones de Procedimiento* en "*La prueba pericial*", ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.3, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, pág.126.

9.2.2 Posición de las partes sobre la prueba pericial electrónica presentada de contrario con anterioridad a la valoración en la sentencia.

Las partes podrán posicionarse ante la prueba presentada de contrario. Es decir, el dictamen pericial aportado por una de las partes puede ser objeto de impugnación en el sentido amplio del término por las demás partes en el proceso. Dicha impugnación podrá efectuarse en tres fases del juicio: en la fase de alegaciones, en la audiencia previa al juicio y en la fase de juicio oral y conclusiones. En la fase de alegaciones, el demandado podrá en su escrito de contestación a la demanda o bien efectuar las alegaciones que rebatan las conclusiones del dictamen aportado por el actor junto con la demanda, bien aportar un dictamen contradictorio, bien solicitar la designación judicial de perito. Y lo mismo puede hacer el actor con respecto al dictamen aportado por el demandado al amparo del artículo 338 LEC.

En la audiencia previa (del juicio ordinario) o en la vista (del juicio verbal) cada parte se posicionará sobre los dictámenes de contrario. «*…Las partes, si fuere el caso, expresarán lo que convenga a su derecho acerca de los dictámenes periciales presentados hasta ese momento, admitiéndolos, contradiciéndolos o proponiendo que sean ampliados en los extremos que determinen (*art. 427.2 LEC)…». La «admisión» del dictamen pericial de adverso no impedirá que la parte aportante solicite la presencia del perito al acto de juicio o de la vista (art. 347 LEC), ni exime al juez de su valoración conforme a la sana crítica (art. 348 LEC). La admisión del dictamen pericial tampoco comporta la admisión de hechos, de modo que estos se conviertan en no controvertidos y exentos de prueba (art. 281.3 LEC).

Por otro lado, la «contradicción» del dictamen pericial es una simple manifestación de parte de disconformidad con el contenido del dictamen, que traslada el debate sobre el contenido del dictamen al acto de juicio o vista, donde tiene lugar la verdadera contradicción, respondiendo el perito a las preguntas que le sometan lo letrados y el propio juez (art. 347 LEC)[329]. La manifestación de contradicción no significa necesariamente el llamamiento del perito contrario a los efectos de explicación de su informe (SAP Alicante, 1 de octubre de 2002), pudiendo ser contradicho el dictamen pericial con otras pruebas destinadas a desvirtuarlo. Dicha contradicción puede operar de forma

[329] Véase ALONSO-CUEVILLES SAYROL, J. *La audiencia previa,* en "Instituciones del nuevo Proceso Civil. Comentarios sistemáticos a la Ley 1/2000", pág.163.

expresa, mediante manifestación al efecto, o bien tácita, mediante la presentación de un dictamen pericial contradictorio[330].

Finalmente la «ampliación» del dictamen pericial en la fase de audiencia previa es una posibilidad ya prevista en la fase del juicio o de la vista (art. 347.1.4º LEC). Si el demandado quiere ampliar el dictamen aportado por el actor con la demanda, le basta con aportar un dictamen en la contestación a la demanda o solicitar una pericial de designación judicial. Y si es el actor, puede hacer lo mismo al amparo del art. 338 LEC. En todo caso, la ampliación debe concretarse a puntos conexos a los que han sido objeto de pericia, no pudiendo hacerse extensivo a nuevos hechos o datos que, siendo conocidos de antemano, pudieron y debieron ser objeto de pericial en el informe inicial, aportado por la propia parte (SAP Toledo, 18 d octubre de 2005)[331]. Las partes «*…También se pronunciarán sobre los informes que se hubieran aportado al amparo del número 5 del apartado 1 del artículo 265»* (art. 427.2 in fine LEC). En este último caso, -art. 265.1.5º LEC- se refiere a los informes elaborados por profesionales de la investigación legalmente habilitados sobre hechos relevantes para las pretensiones de las partes. «*…Sobre estos hechos, si no fuesen reconocidos como ciertos, se practicará prueba testifical*».

Los letrados podrán impugnar críticamente el dictamen pericial sujetándose a los parámetros de valoración del dictamen pericial finalmente también en la fase de juicio oral, donde los abogados tienen oportunidad de cuestionar, criticar e intentar refutar los informes de contrario mediante las preguntas al perito. Finalmente, las conclusiones a las que debiera llegarse, al parecer de cada abogado, se formularán en el trámite de conclusiones.

En prueba pericial electrónica la contradicción o la impugnación crítica de la prueba pericial presentada de contrario versará principalmente sobre las herramientas y métodos empleados por el perito y/o sobre el respeto de la cadena de custodia, aunque la impugnación crítica de los letrados podrá versar también sobre criterios de menor entidad como la falta de cualificación profesional, contradicciones, concurrencia de algún motivo de tacha etc. Es fundamental que el informe pericial sea completo y detallado tal y como veíamos en el § 8.2.1 incluyendo cada uno de los apartados que concretamos en dicho capítulo. Especial relevancia cobra el apartado relativo a la descripción de los elementos integrantes del dictamen pericial que sirven para la validación

[330] Véase DE LA RÚA, J., *El "posicionamiento" ante documentos y dictámenes en la audiencia previa,* en "Aspectos prácticos de la prueba civil". Abel Lluch, X., y Picó y Junoy. (dirs.), ed. J.M Bosch editor, Barcelona, 2006, pág. 237.

[331] SAP Toledo, secc. 1ª, de fecha 18 de octubre de 2005, Fdo. Jco. 1º.

científica de los métodos y herramientas seguidos por el perito forense en su análisis.

Y por ser también uno de los motivos generales de impugnación es importante también que el dictamen pericial reseñe todas y cada una de las diligencias practicadas y personas intervinientes desde la captura de la información electrónica hasta su análisis y puesta a disposición judicial, para que no pueda alegarse ruptura de la cadena de custodia tanto preprocesal como procesal. Imaginemos en este último caso el supuesto de un informe pericial cuyo objeto es la revisión de los contenidos del disco duro de un ordenador personal, en el que el perito basa su análisis en las copias efectuadas y que le han sido entregadas por el familiar de una de las partes en el proceso sin adoptar ninguna garantía al efecto[332]. En este caso será difícil acreditar la procedencia e integridad de la información. Es decir, los letrados principalmente impugnarán la prueba pericial contraria alegando: La falta de validez técnica y la falta de validez de la cadena de custodia entendida como sistema que garantiza la integridad, conservación e inalterabilidad de los hechos electrónicos incluyendo su obtención, custodia, transporte y presentación en los tribunales hasta su disposición final por orden judicial. Podrán también alegar la ilicitud de la prueba por haber sido obtenida vulnerando derechos constitucionales. Como tratamos anteriormente el experto informático-forense o perito nunca debe acceder a datos o hechos que forman parte de la «esfera privada» del individuo sin una autorización judicial y de hacerlo no intencionadamente debe apartarse inmediatamente de dichos contenidos que evidentemente no pueden entrar a formar parte de su informe o dictamen pericial. En caso contrario nos hallaríamos ante una prueba ilícita que no puede acceder al proceso y que exigiría un incidente contradictorio entre las partes conforme al artículo 287 LEC. Véase sobre este tema el § 3[333].

---

[332] Este es uno de los casos reales –caso 43- citado por el perito informático MARTÍNEZ DE CARVAJAL HEDRICH, Ernesto, en su libro *Informática Forense, 44 casos reales*. Julio 2012, págs. 201-209.

[333] DARAHUGE y ARELLANO aluden a los tres aspectos a que hemos hechos referencia – técnico, cadena de custodia y constitucional- empleando los términos «validez técnica informática», «validación técnica criminalística» y «validación técnica legal». La primera implica, según dichos autores, el control, revisión y auditoría de todas las operaciones técnicas informáticas, realizadas desde el momento de la identificación de la prueba documental informática capturada hasta el presente, de análisis considerado (el momento en que se realiza dicha evaluación técnica). Debiéndose tener en cuenta los recursos involucrados integrados en dicha tarea (edilicios, instrumentales, lógicos, humanos). La segunda, «validación técnica criminalística», engloba el control, revisión y auditoria de todas las operaciones técnicas criminalísticas, realizadas desde el momento de la toma de contacto, de los actores participantes de la tarea analizada. Se extiende más allá de la revisión especificada en el apartado anterior, ya que implica la interacción multi y transdisciplinaria de todos los participantes (peritos, expertos o no) en la preservación de la prueba. Y finalmente refieren también «la validación técnica legal» referida a la preservación de

9.2.3 Juicio de admisión

Una vez propuesta la prueba el Juez dictará resolución admitiendo o inadmitiendo la misma. El juez estará sujeto a los criterios de admisión de cualquier prueba, pertinencia, utilidad y legalidad (art. 283 LEC). La prueba debe ser pertinente, es decir, debe tener relación con el *thema decidendi*, y debe proponerse en tiempo y forma (art. 284, 414.1, 429.1, 435.1, 444.4 y 460.2 LEC). Debe ser útil, es decir, debe inadmitirse aquella prueba que según reglas y criterios razonables y seguros, en ningún caso pueda contribuir a esclarecer los hechos controvertidos (art. 283.2 LEC). En el supuesto que el juez decida inadmitir una prueba debe razonar la inadmisión sin que dicha resolución pueda incurrir en incongruencia, irrazonabilidad o arbitrariedad (STC de 14 de enero de 2004)[334].

La prueba pericial electrónica requiere, pues, para su admisibilidad de dos exigencias: «pertinencia» y «utilidad». La «pertinencia», como hemos señalado, determina su relación con el objeto del proceso. Dentro de este concepto se incluye la necesidad de que dicha prueba verse sobre hechos alegados por las partes y controvertidos por las mismas en el proceso[335]. El artículo 335.1 LEC acoge de modo genérico la «pertinencia» de la prueba *«Cuando sean necesarios conocimientos científicos, artísticos, técnicos o prácticos para valorar hechos o circunstancias relevantes en el asunto o adquirir certeza sobre ellos, las partes podrán aportar al proceso el dictamen de peritos que posean los conocimientos correspondientes o solicitar, en los casos previstos en esta ley, que se emita dictamen por perito designado por el tribunal»*.

Sin embargo el artículo 336.1 LEC centra la aportación del dictamen pericial sobre el criterio de «conveniencia» de las partes al establecer *«Los dictámenes de que los litigantes dispongan, elaborados por peritos por ellos designados, y que estimen necesarios o convenientes para la defensa de sus derechos, habrán de aportarlos con la demanda o con la contestación, si ésta hubiere de realizarse en forma escrita, sin perjuicio de lo dispuesto en el artículo 337 de la presente Ley»*. Criterio que de nuevo repite el artículo 339.2 LEC cuando al tratar la solicitud de designación de perito judicial en el escrito de demanda establece: «*El*

---

derechos constitucionales. DARAHUGE, M.E Y ARELLANO GONZALEZ, L.E. *Manual de Informática Forense (Prueba Indiciaria Informático Forense)*. Ed. Errepar, 2012, pág. 67.

[334] STC 14 enero 2004, fto. jco.2º, (EDJ 2004/389).

[335] PICO i JUNOY incluye la propuesta por las partes de un medio de prueba con el fin de probar hechos no controvertidos como supuesto de inadmisión por impertinencia. PICÓ Y JUNOY, *Problemas actuales de la prueba civil*,, en la obra colectiva del mismo título, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), J.M. Bosch, Barcelona, 2005, págs. 49 y ss.

demandante o el demandado, aunque no se hallen en el caso del apartado anterior, también podrán solicitar en sus respectivos escritos iniciales o el demandado con la antelación prevista en el párrafo segundo del apartado anterior de este artículo, que se proceda a la designación judicial de perito, si entienden conveniente o necesario para sus intereses la emisión de informe pericial (…)». No obstante, en este último supuesto al tratarse de pericial de designación judicial y al contrario de la pericial de parte queda sujeta a «rogación», además de pertinencia y utilidad. De modo que dicho precepto continúa diciendo « (…) *En tal caso, el tribunal procederá a la designación, siempre que considere pertinente y útil el dictamen pericial solicitado. Dicho dictamen será a costa de quien lo haya pedido, sin perjuicio de lo que pudiere acordarse en materia de costas (…)».* Es decir, si el juez considera que los dictámenes periciales aportados junto a los escritos de alegaciones son suficientes podrá denegarla[336]. El tribunal, de admitir la solicitud, dictará auto, pronunciándose sobre su admisión (art. 285,206.2.2 y 339.2.3 LEC), y designado perito (art. 341 LEC).

La prueba pericial informática debe ser «útil», es decir, contribuir a esclarecer los hechos controvertidos (283 LEC). En cuanto a la «necesidad», el juez no debería inadmitir una prueba pericial informática propuesta por alguna de las partes con fundamento a su conocimiento individual, porque los conocimientos que tenga privadamente un juez de primera instancia no han de tenerlos necesariamente los magistrados en segunda instancia[337].Y, a su vez, porque la prueba pericial complementará sus conocimientos técnicos y ayudará al mismo a efectuar una mejor y más fundada valoración. Por otro lado, el momento en que el juez debe aplicar dichos conocimientos técnicos, de tenerlos, es en la fase de valoración de la prueba, una vez practicada íntegramente la misma, no en la fase de admisión. La admisión debe fundarse en parámetros objetivos.

El artículo 338.1 LEC en relación a las actuaciones procesales posteriores a la presentación de la demanda alude a los criterios de necesidad y utilidad: «L*o dispuesto en el artículo anterior no será de aplicación a los dictámenes cuya*

[336] En este sentido se pronuncia la SAP León, secc. 3ª, de 12 de abril de 2007, fto. Jco 3º (EDJ 2007/121506). En la práctica forense viene admitiéndose la designa judicial con carácter prácticamente automático, lo cual ha contribuido a que muchos abogados prefieran no acompañar a sus escrito de alegaciones periciales de parte, con la creencia de que un perito designado judicialmente gozará de mayor credibilidad ante un juez.

[337] En este sentido se pronuncia la SAP Madrid, de 18 de octubre de 2003 y STS de 7 de abril de 1995. En contra SSTS de 30 de marzo de 1984 (RJ 1984,1472) y 7 de abril de 1995. Véase también sobre este tema RIFA SOLER, J.M. *Comentarios a la nueva Ley de Enjuiciamiento Civil*, Fernández Ballesteros, M.A., Rifa Soler, J.M., y Valls Gombau, JF (coord..), ed. Atelier, Barcelona, 2000. pág. 1597.

necesidad o utilidad se ponga de manifiesto a causa de alegaciones del demandado en la contestación a la demanda o de las alegaciones o pretensiones complementarias admitidas en la audiencia, a tenor del artículo 426 de esta Ley. // 2. Los dictámenes cuya necesidad o utilidad venga suscitada por la contestación a la demanda o por lo alegado y pretendido en la audiencia previa al juicio se aportarán por las partes, para su traslado a las contrarias, con al menos cinco días de antelación a la celebración del juicio o de la vista, en los juicios verbales con trámite de contestación escrita, manifestando las partes al tribunal si consideran necesario que concurran a dichos juicio o vista los peritos autores de los dictámenes, con expresión de lo que se señala en el apartado 2 del artículo 337. El tribunal podrá acordar también en este caso la presencia de los peritos en el juicio o vista en los términos señalados en el apartado 2 del artículo anterior».

En primer lugar, en lo referente a los dictámenes periciales de parte, como hemos señalado con anterioridad, éstos se aportarán al proceso con la demanda y la contestación (art. 336 LEC), serán anunciados con los escritos de alegaciones (art. 337 LEC), o bien serán consecuencia de actuaciones procesales posteriores a la demanda (art. 338 LEC)-. El legislador equipara tales dictámenes –al menos a los aportados junto con la demanda y contestación- a los documentos fundamentales sujetándose a la obligación de aportación inicial (art. 265.1.4º) y a idéntico régimen de preclusión (art. 269 LEC). Si bien dichos documentos acceden al proceso en un momento inicial al mismo, por considerarse fundamentales y con ello garantizar un legítimo derecho a la defensa en plano de igualdad de armas entre las partes, ello no significa a nuestro parecer y a diferencia de lo que han señalado algunos autores, que no exista un juicio de admisión respecto a los mismos. La admisión a trámite de la demanda por parte del Secretario Judicial no obsta a que exista un juicio de admisión de la prueba, que es función exclusivamente jurisdiccional. Dicho juicio de admisión tendrá lugar en la audiencia previa, en el supuesto de juicio ordinario, o en la propia vista, en el juicio verbal, pues estrictamente el trámite de admisión o rechazo de la prueba tiene lugar en dicho momento procesal (art. 285.1, 443.4, 429.1y 445 LEC). El juez debe abstenerse de devolver el dictamen pericial a la parte que lo aporta *a limine,* esto es, junto a la demanda o a la contestación y esperarse a la audiencia previa o vista[338].

[338] Véase sobre ello y a favor de tal posición: PICÓ i JUNOY, J. , *Admisibilidad de la prueba pericial* en "La prueba pericial", ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.3, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, pág. 251; ILLESCAS RUS, A *La prueba pericial en la Ley 1/2000 de Enjuiciamiento Civil,* ed. Aranzadi, Pamplona 2000, pág. 245; y YAÑEZ VELASCO, R, *El peritaje en el proceso civil,* ed. Grupo Difusión, Madrid 2005, pág. 58. En contra se pronuncia FLORES PRADA, sosteniendo la inadmisión *a limine*, es decir en el momento de la aportación.

No obstante, se ha sostenido que en los dictámenes a instancia de parte no cabe impugnación del juicio de admisión al equipararse a los documentos fundamentales y estar sujetos a preclusión. Entendiéndose que dichos dictámenes no están sujetos a un juicio de pertinencia y utilidad como los restantes medios de prueba (art. 283 y 285 LEC), y alegando que la única intervención que se prevé del juez en el art. 336 y 337 LEC es el llamamiento de los peritos al juicio (SAP Asturias, de 1 de septiembre de 2005)[339].

A nuestro parecer los citados artículos regulan única y exclusivamente el momento en que los dictámenes periciales deben acceder al proceso, no existiendo regulación alguna que les exima de un juicio por parte del juez de pertinencia y utilidad al igual que las demás pruebas que acceden al mismo (arts. 285.1, 443.4, 429.1y 445 LEC). El derecho a la admisión y práctica de la prueba debe estar siempre modulado por la pertinencia, la necesidad y los requisitos de admisión, como señala la doctrina constitucional, existiendo momentos procesales expresamente determinados por la LEC al efecto. Por otro lado, el decreto de admisión efectuado por el Secretario judicial se limita a constatar el cumplimiento de los requisitos y las causas de inadmisión establecidas en el artículo 403 LEC, sin que el juez efectúe una valoración de los mismos, salvo en los supuestos previstos en el artículo 404 de dicho Cuerpo legal. La atribución de competencias al Secretario judicial para admitir la demanda se justifica en la propia Exposición de Motivos de la LEC porque salvo los casos especiales previstos en el artículo 404 LEC, la ley sólo exige la comprobación de requisitos formales y el examen de la jurisdicción y competencia objetiva y territorial, es decir, una mera comprobación material. Ello justifica aún más el posterior juicio de admisión de la totalidad de la prueba en la fase procesal expresamente prevista por la Ley de Enjuiciamiento Civil al tratarse de una función exclusivamente jurisdiccional. Asimismo, supondría una contradicción la diferencia de trato entre los dictámenes de parte y los de designación judicial en estos términos cuando la propia LEC pretende la equiparación de ambos.

En los dictámenes anunciados pero no aportados el juez deberá verificar la justificación de no aportación inicial y su presentación antes de los cinco días anteriores a la audiencia previa o de la vista en el juicio verbal (art. 337.1 LEC). Y en los dictámenes que sean consecuencia de alegaciones posteriores a la vista, el juez deberá verificar su aportación con al menos cinco días de antelación a la celebración del juicio o de la vista (art. 338.1 LEC), así como que la presentación

[339] En este sentido se pronuncian la SAP Asturias, secc. 5ª, de 1 de septiembre de 2005, Fdo. Jco. 3º (EDJ 20036/151856) y ABEL LLUCH, X., en *Derecho probatorio.* Ed. Bosch, 2012, págs. 747-749 y en *La prueba pericial*, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), *Serie estudios prácticos sobre los medios de prueba*, núm.3, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, págs.166 y ss.

del dictamen obedece a desvirtuar las alegaciones del demandado en la contestación o las alegaciones o pretensiones complementarias admitidas en la audiencia previa, y no se trata de una aportación extemporánea de un dictamen pericial.

La incorporación de la pericial de parte a las actuaciones no impide que la adversa pueda impugnar la idoneidad del perito designado por la parte aportante o la correlación entre los extremos del dictamen y los hechos que fundamentan la demanda (o, en su caso, la contestación) en la audiencia previa al juicio, pues como hemos dicho es estrictamente en dicho trámite en el que debe procederse a la admisión o rechazo de la prueba. La parte también podrá impugnar la aportación cuando sea extemporánea –fuera de los plazos preclusivos- o cuando sea innecesaria- cuando los dictámenes no versen sobre aspectos tan simples que no precisen conocimientos técnicos-, sin perjuicio de la posibilidad de manifestar la contradicción o solicitar la ampliación del dictamen pericial en la audiencia previa (art. 427.2 LEC) o de impugnarlo en el trámite de conclusiones (art. 433.2 LEC).

Frente a la admisión o, en su caso, inadmisión del dictamen de parte en el decreto de admisión a trámite de la demanda o de la contestación a la demanda cabe recurso de reposición ante el Secretario judicial de trámite escrito y general (art. 451 LEC). En el juicio ordinario, frente a la admisión o, en su caso, inadmisión del dictamen de parte que tiene lugar durante la audiencia previa cabe recurso de reposición de interposición, substanciación y resolución oral (art. 285.2 LEC) y si se desestimare, la parte perjudicada podrá formular protesta a los efectos de hacer valer el dictamen en la segunda instancia. En el juicio verbal, frente a la inadmisión de una prueba electrónica o la admisión de una prueba electrónica de las que se denunciara como obtenidas con violación de derechos fundamentales, las partes podrán formular protesta a los efectos de hacer valer sus derechos en segunda instancia (art. 446 LEC). En el juicio verbal, pues, no cabe protesta contra la admisión de una prueba electrónica que la parte considera impertinente, inútil o que infringe la legalidad del procedimiento.

En segundo lugar, en lo referente a los dictámenes de designación judicial éstos se hallan sujetos a un juicio de pertinencia y utilidad y a la necesidad de ser solicitados en el momento procesal oportuno, es decir, junto con la demanda o la contestación, o en el caso de juicios verbales sin contestación por escrito al menos con diez días de antelación al que se hubiera señalado para la celebración del acto de la vista (art. 339.2 LEC). Se podrá impugnar los dictámenes que sean impertinentes –por no guardar relación con los hechos controvertidos-; inútiles –por no contribuir en ningún caso al esclarecimiento de los hechos controvertidos- (art. 339.2 LEC); y extemporáneos –por haberse

solicitado con posterioridad a los escritos de demanda o contestación o fuera del plazo de diez días previos a la vista en los juicios verbales con contestación escrita-, a salvo que se refieran a alegaciones o pretensiones no contenidas en la demanda (art. 339.3 LEC). Y a pesar del silencio legal, también se podrán impugnar los extremos del dictamen propuestos por la parte solicitante. Cabe también impugnar la designación judicial del perito del litigante con derecho de asistencia jurídica gratuita por ser impertinente, inútil o extemporánea, ya que el artículo 339.1 LEC se refiere a la forma de designación del perito y no al juicio de admisión, como pudiera deducirse de la dicción legal. Tratándose de alegaciones o pretensiones complementarias permitidas en la audiencia previa (art. 339.3 LEC) la designación judicial podrá impugnarse por tres razones: 1ª) Falta de pertinencia o utilidad; 2ª) falta de acuerdo de las partes en el objeto de la pericia; y 3ª) falta de conformidad de las partes en el perito nombrado por el tribunal.

Frente a la admisión, o en su caso, inadmisión, del dictamen de designación judicial en el juicio ordinario cabrá un recurso de reposición, y si se desestimare, la parte perjudicada podrá formular protesta al efecto de hacer valer sus derechos en la segunda instancia. En el juicio verbal, frente a la inadmisión o la admisión de una prueba electrónica de las que se denunciara como obtenidas con violación de derechos fundamentales, las partes podrán formular protesta a los efectos de hacer valer sus derechos en segunda instancia (art. 446 LEC). En el juicio verbal, como hemos señalado no cabe protesta contra la admisión de una prueba electrónica que la parte considera impertinente, inútil o que infringe la legalidad del procedimiento.

Si se deniega la prueba pericial anticipada, pese al silencio legal (art. 294 LEC), cabe interponer el recurso de reposición. Siquiera algún autor ha defendido que si la solicitud de la pericial anticipada es anterior al inicio del proceso en la medida en que todavía este no existe, contra la resolución que deniega la prueba y que pone fin a las actuaciones solo cabe recurso de apelación (art. 455.1 LEC). En el supuesto que la pericial fuera adoptada al amparo del artículo 429.1, II y III LEC cabrá recurso de reposición no contra la «indicación o sugerencia» judicial –que no es una resolución- sino contra la resolución que admite la prueba pericial a raíz de la citada «indicación o sugerencia». Y finalmente en el supuesto que la pericial se adopte como diligencia final –ordinaria o extraordinaria-, y frente al auto de admisión o, en su caso inadmisión, cabe recurso de reposición de trámite escrito y general.

En segunda instancia la parte podrá solicitar la prueba pericial inadmitida en la instancia o no practicada en el escrito de interposición del recurso (art. 460.2 LEC) o en el de impugnación de la sentencia (art. 461.3 LEC), o la prueba admitida pero que por cualquier causa no imputable al recurrente, no se haya

podido practicar, ni como diligencia final (art. 460.2.2º LEC). Si la prueba pericial solicitada en segunda instancia es denegada, la parte gravada podrá interponer recurso de reposición (art. 206.2, 451 y 464 LEC), que constituye, a su vez, el presupuesto para que en el supuesto que la Audiencia confirme su decisión e inadmita la prueba pericial, poder interponer un recurso de casación por infracción procesal (art. 469.1 LEC) o eventualmente un recurso de amparo (art.44 LOTC).

9.2.4 La práctica de la prueba pericial electrónica en el juicio oral

9.2.4.1 El experto en informática forense: perito, testigo-perito o figura afín

El experto en informática forense puede desempeñar distintas funciones. Es decir, un experto en informática forense puede desarrollar su actividad profesional en una empresa dentro del Departamento de Seguridad de la misma, puede tratarse de un investigador digital externo a la misma y contratado cuando se ha detectado un incidente en concreto, habilitado o no como detective privado (art. 19.1 de la Ley 23/1992, de 30 de julio, de Seguridad Privada (LSP), o puede tratarse de un experto al que se le encargue un informe pericial privado o bien que forme parte de las listas de peritos para designa judicial.

La función que desempeña cada uno es diferente y por lo tanto es importante determinar en qué calidad prestarán declaración en un posible juicio. Si bien *a priori* las diferencias parecen claras, las funciones en ocasiones se confunden y la línea divisoria entre ellas se difumina. Así por ejemplo, el investigador experto en informática forense que es contratado por una empresa ante sus sospechas de sustracción de información privilegiada acaba en muchas ocasiones declarando en juicio en calidad de perito, tras investigar, hallar y redactar un informe que confirma aquellas meras sospechas iniciales de la empresa. El experto redacta un informe que suele acompañar a la demanda de la empresa como dictamen pericial contra el presunto sustractor. En la práctica forense en este supuesto quien era investigador inicialmente se trasforma con posterioridad en perito que actuará en juicio.

En este sentido, podemos analizar la figura del experto en informática forense según la función que desarrolla atendiendo a las similitudes y diferencias entre

el perito y el testigo-perito. Para ello partiremos de la diferenciación que ABEL LLUCH realiza entorno a estas dos últimas figuras[340]:

1º *Fungibilidad. El perito es sustituible por otro que posea los mismos conocimientos especializados, el perito-testigo es insustituible porque tuvo un conocimiento personal de los hechos. El testigo-perito posee un saber subjetivamente infungible –tercero conocedor de los hechos con relevancia procesal- y objetivamente fungible –su conocimiento científico, técnico o artístico o práctico lo puede poseer cualquier otro técnico de la misma rama del saber humano-.*

En evidencia electrónica el experto que lleva a cabo la investigación de los hechos, ya sea individuo contratado al efecto y externo o trabajador de un Departamento de seguridad, tiene un conocimiento histórico previo al proceso. Efectúa un clonado o bien realiza el análisis en una fecha y en unas condiciones determinadas. No obstante, por regla general si actúa de modo eficiente y efectúa una copia de la información sin incidencias las posteriores actuaciones de investigación sobre la información obtenida pueden ser repetidas por un tercero con su cualificación. Posee conocimientos técnicos con carácter objetivamente fungibles.

2º *Relación histórica con los hechos. El criterio diferencial entre el testigo-perito y el perito radica «en la forma de ponerse en relación con los hechos enjuiciados, de modo histórico (testigo) o por la circunstancia de ser requerido para valorar un hecho con trascendencia para un eventual proceso sin previo conocimiento (perito)»* (*SAP Coruña, 31 de mayo de 2006 y AP Asturias de 19 de noviembre de 2007, y SAP Tarragona de 10 de diciembre de 2010).*

El experto en evidencia digital tendrá un conocimiento histórico de los hechos derivado de su propia función en la empresa en el supuesto que trabaje en el Departamento de seguridad de la misma, o bien como consecuencia de ser requerido para «investigar» no para «valorar» un hecho con trascendencia para un eventual proceso sin previo conocimiento. La «valoración» de la metodología y de las conclusiones a que ha llegado e incluso la comprobación de los hechos referidos en dicho informe, hechos objeto del procedimiento, corresponde a la figura del perito.

3º *Llamada al proceso y proposición. El perito es llamado al proceso por sus conocimientos especializados, el testigo-perito por haber presenciado los hechos. El perito recibe un encargo –de la parte o del juez- para que realice un trabajo de investigación sobre unos hechos normalmente presentes. El testigo es propuesto por las partes para que declare sobre unos hechos pasados.*

[340] Véase ABEL LLUCH, X., *Derecho Probatorio,* Ed. Bosch, 2012. págs. 675-677.

El experto será llamado al proceso por haber presenciado los hechos ya se trate de hechos iniciales (se produce la incidencia) o hechos derivados de los primeros (constata indicios consecuencia de unos hechos), cuando dicha investigación forme parte de su cometido dentro de una empresa. También puede darse el supuesto de que reciba un encargo de la parte o del juez para que realice un trabajo de investigación sobre la existencia de unos hechos, con carácter previo a la demanda. En ambos casos tiene conocimientos especializados.

4º *Deber, forma y modo de declaración. El perito puede no aceptar el cargo, mientras el testigo-perito tiene la obligación de declarar. El perito emite dictamen escrito, con anterioridad al periodo de práctica de la prueba (art. 346 LEC). El testigo- perito presta su declaración oral en el periodo de práctica de la prueba (370.4 LEC). El perito somete su dictamen a contradicción de los Letrados, pudiendo incluso recibir la crítica de otros peritos. El testigo-perito se somete al interrogatorio de los Letrados, debiendo responder a sus preguntas conforme a los requisitos del interrogatorio de testigos.*

El experto investigador externo contratado emitirá informe escrito. El perito informático forense emitirá dictamen escrito. Y posiblemente el experto que trabaja en un Departamento de seguridad en una empresa emitirá también un informe escrito. Las diferencias entre unos y otros informes radicarán en si hubo encargo y en el contenido de los mismos. En los tres casos posiblemente los informes contengan consideraciones técnicas apoyadas en conocimientos técnicos.

5º *Juramento y objetividad. El perito debe prestar juramento de decir verdad y actuar con la mayor objetividad posible, tomando en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a cualquiera de las partes (ART. 335.2 LEC), mientras el testigo- perito solo tiene que prestar juramento o promesa de decir verdad (art. 365 LEC).*

6º *Garantías de imparcialidad. La parcialidad del perito se protege a través de la recusación –si es designado judicialmente- (art 343.1 y 124.1 LEC) o la tacha (art. 343.1 LEC) –si es designado a instancia de parte-; mientras la parcialidad del testigo-perito solo se pone de manifiesto mediante la tacha (art. 370.4.II LEC).*

7º Remuneración. El perito recibe unos honorarios por la emisión del dictamen pericial (art. 342.3 LEC), mientras el testigo-perito puede percibir una indemnización por los gastos y perjuicios derivados de su declaración (art. 375 LEC y SAP León, 4 de junio de 2009).

El experto que actúe por encargo cobrará honorarios por la emisión del informe, si fuese posible llamarle a juicio a declarar probablemente cobraría también honorarios a la parte proponente por ello por lo que parece inaplicable el artículo 375 LEC relativo a la indemnización percibida por el testigo-perito. Distinto es el caso en que se trata del personal del Departamento de Seguridad de una empresa, puesto que éste sí podrá acceder a la indemnización citada en cuanto su actuación forma parte de sus funciones en la empresa donde presta servicio.

8º *El testigo-perito puede entrar en conocimiento de los hechos de modo accidental –Ej. El médico que presencia un accidente y presta labores de auxilio- o puede tener conocimiento de los hechos por su profesión –Ej. Médico que trató habitualmente al enfermo de alzhéimer y es llamado al juicio de impugnación del testamento por falta de capacidad del testador-, pero en ambos casos tiene un conocimiento preprocesal.*

El experto puede tener conocimiento de los hechos también con carácter accidental o por su profesión. Su conocimiento es preprocesal cuando se le encarga la investigación de los hechos por la parte propietaria de los dispositivos, tratándose de información privada o de información pública de una Web, siempre que no se requiera clave para ingresar, o cuando trabaja en un Departamento de seguridad; procesal, cuando se solicita una investigación como actos preparatorios y se requiere autorización judicial, o cuando se trata de elaborar un informe pericial antes o una vez iniciado el proceso pero con la finalidad de aportarlo en el mismo. El conocimiento histórico adquirido puede ser o no accidental. Puede adquirirlo por su análisis a través de encargo como «investigador» con miras a la posible interposición de una demanda si encuentra hechos que lo fundamenten, o bien ser inherente a su propia profesión, tratándose del experto informático-forense que trabaja en el departamento de Seguridad de la empresa e inicia la investigación tras constatar la incidencia.

La valoración de lo anteriormente expuesto nos lleva a la conclusión que la figura del empleado formado en informática-forense que trabaja en el Departamento de Seguridad de una empresa, detecta el incidente y abre una investigación emitiendo un informe, puede incardinarse en la figura del testigo-perito regulada en el artículo 370.4 LEC por remisión del artículo 380.2 del mismo Cuerpo legal. Recuerda en este caso al médico que por su profesión trata al enfermo y con posterioridad es citado a juicio. A tenor del artículo 380.2 LEC si se hubieren aportado como prueba documental informes sobre hechos, que no hubiesen sido reconocidos como ciertos por todas las partes a quienes pudieran perjudicar, y dichos informes contuvieren también valoraciones fundadas en conocimientos científicos, artísticos, técnicos o prácticos de sus

autores, se interrogará como testigos-peritos a los autores de dichos informes. En este sentido, el experto es una persona con conocimientos técnicos o científicos sobre la que se efectúa un interrogatorio sobre los hechos que ha conocido históricamente.

Mayor dificultad plantea la figura de un tercero ajeno a la empresa y contratado a efectos de realizar una investigación informático-forense. En este caso puede tratarse de un investigador privado (detective privado) con la correspondiente autorización administrativa que le habilita para ofertar y prestar servicios profesionales[341] o no. El artículo 19.1 de la Ley 23/1992, de 30 de julio, de Seguridad Privada (LSP) establece entre las funciones de los detectives privados el «obtener y aportar información y pruebas sobre conductas o hechos privados» e «investigar delitos perseguibles solo a instancia de parte por encargo de los legitimados en el proceso penal». Como resultado de una investigación la parte podrá aportar un soporte grabado, como por ejemplo un CD, con la información obtenida o bien un informe en el que consten las operaciones efectuadas y el resultado obtenido. El Tribunal Supremo se ha pronunciado en varias sentencias afirmando que ni la declaración del investigador privado en juicio ni el informe emitido por el mismo son pruebas documentales o periciales sino que se trata de testifical documentada o lo que es lo mismo manifestaciones testificales manifestadas por escrito (SSTS de 2 de octubre de 1989, Azdi. 7092, 13 de marzo de 1991, Azdi. 1851). A su vez, recordemos que el artículo 265.1.5º LEC establece que a toda demanda o contestación deberán aportarse los informes, elaborados por profesionales de la investigación privada, legalmente habilitados, sobre hechos relevantes en que aquellas apoyen sus pretensiones. Sobre estos hechos, si no fuesen reconocidos como ciertos, se practicará prueba testifical. Y, en este caso, teniendo en cuenta que el testigo dispone de conocimientos técnicos actuaría en calidad de testigo-perito (art. 370.4 LEC). Si bien es cierto que se asemeja al perito en que su informe constará de consideraciones técnicas apoyadas en conocimientos técnicos y que al igual que el perito existe un encargo previo[342], entendemos que no podemos considerarlo como tal puesto que su función no es la de

[341] La autorización administrativa y el diploma acreditativo de haber superado los módulos formativos exigidos para la obtención de la misma no son desde un punto de vista jurídico procesal «título oficial».

[342] Véase las diferencias entre perito y testigo-perito en PICÓ I JUNOY., *La prueba pericial en el proceso civil español,* J.M. Bosch editor, Barcelona, 2001, págs. 54-55. Por otro lado RIFA SOLER señala respecto al testigo-perito que «se trata de un testigo, porque se pone en relación directa, histórica y natural con los hechos; pero en ningún caso su relación con los hechos deriva de encargo alguno, sea de parte o del tribunal». RIFA SOLER, J.M., en *Comentarios a la nueva Ley de Enjuiciamiento Civil,* Fernández-Ballesteros, M.A., Rifa Soler, J.M., Valls Gombau J.F. (coord..), ed. Iurgium, Barcelona, pág. 1717.

efectuar una valoración de los hechos, ni investigar para verificar un hecho ya conocido, sino la de investigar para descubrir o confirmar sospechas que de verificarse y convertirse en hechos, en su caso, pudieran fundamentar la demanda. Lo cual nos plantea la duda también de si una vez las sospechas se transforman en hechos electrónicos que pueden acreditarse, el propio investigador puede emitir informe como perito y actuar en juicio como tal. Entendemos que no existe impedimento en tal sentido siempre que reúna los requisitos exigidos por la LEC y haya sido propuesto por las partes y el tribunal como perito[343].

9.2.4.2 Solicitud, citación y comparecencia en el juicio de los peritos

La prueba pericial en general, y la prueba pericial electrónica en particular, constituyen una prueba compleja en la que la comparecencia de los peritos en el juicio resulta esencial para que el juez pueda comprender y efectuar una razonada valoración de la prueba pericial en sentencia. La presencia física del perito en juicio permitirá la exposición de su dictamen, en su caso, o la formulación de preguntas por las partes o el tribunal, así como las aclaraciones que al efecto sean necesarias. Ello obedece, a su vez, a los principios de publicidad, contradicción e inmediación que rigen en general para toda la prueba en nuestra norma procesal (art. 289, 431 y 137 LEC).

Las partes, aportados los informes periciales a los autos, habrán de manifestar si desean que los peritos autores de los dictámenes comparezcan en el juicio del procedimiento ordinario, o en su caso, en la vista del juicio verbal, expresando si deberán exponer o explicar el dictamen o responder a preguntas, objeciones o propuestas de rectificación o intervenir de cualquier otra forma útil para entender y valorar el dictamen en relación con lo que sea objeto del pleito (art. 337.2 y 338.2 LEC). Tratándose de perito de designa judicial, una vez emitido por éste el dictamen, se dará traslado por el Secretario judicial a las partes por si consideran necesario que el perito concurra al juicio o a la vista a los efectos de que aporte las aclaraciones o explicaciones que sean oportunas (art. 346 LEC). La posibilidad de solicitud de comparecencia del perito al juicio o vista es congruente con los principios de contradicción y publicidad que rigen en nuestro procedimiento, sin embargo se contradice con la facultad discrecional

[343] SEGOVIA ARROYA concluye que quien esté habilitado por el Ministerio del Interior como detective privado podrá actuar en el marco de un proceso judicial como perito sólo si reúne las condiciones que la LEC establece para esta figura y ha sido designado en tal concepto por el Juez o Tribunal, pudiendo emitir entonces el correspondiente dictamen pericial. Véase SEGOVIA ARROYA, J.A, *¿Es el informe profesional del detective privado equivalente a un dictamen pericial?*, Derecho.com, 15 de febrero de 2003, http://goo.gl/iSHW0q, página web visualizada en fecha 6 de octubre de 2013.

que el artículo 347.1 segundo párrafo de la LEC otorga al juez para denegar las solicitudes de intervención que, por su finalidad y contenido, hayan de estimarse impertinentes o inútiles.

El Tribunal también podrá acordar, de oficio, la intervención de los peritos en el acto del juicio ordinario o en la vista del juicio verbal para poder comprender y valorar mejor el dictamen realizado, y ello se prevé tanto respecto a los dictámenes periciales emitidos por peritos de designa de parte (art. 338.2.2 LEC), como los designados judicialmente (art. 346 LEC).

Dada la importancia de la comparecencia del perito en juicio a los efectos señalados resulta criticable que la ley no prevea la necesidad de la comparecencia del mismo en juicio y lo establezca de un modo potestativo.

En resumen, las partes podrán interesar la presencia del perito al acto del juicio o la vista para someter a contradicción el dictamen (art. 337.2 y 346 LEC), pudiendo también el tribunal interesar la comparecencia del perito (art. 338.2.II y 346 LEC). Tratándose de dictámenes a instancia de parte, la petición de comparecencia de perito la podrá realizar tanto la parte que aportó el dictamen como la adversa (art. 337.2 LEC), del mismo modo que ambas partes pueden interesar la comparecencia del perito de designación judicial (art. 346 LEC) aun no habiendo interesado su designación (SAP Madrid, 26 de septiembre de 2006[344]).

En lo referente a la citación de los peritos a juicio, en el juicio ordinario las partes deberán indicar en la audiencia previa los peritos que se comprometen a presentar en juicio y los que deben ser citados por el tribunal. El tribunal acordará las citaciones que procedan que se practicarán con la antelación suficiente (art. 429.5 LEC). La citación se efectuará de conformidad a lo previsto en los artículos 159, 160 y 161 LEC. En el juicio verbal la LEC no prevé la citación judicial de los peritos para su intervención en el acto de la vista por lo que tanto actor como demandado deberán presentar en la vista al perito que hubiera elaborado el dictamen pericial.

La infracción del deber de comparecencia en el juicio o vista se sancionará por el tribunal, previa audiencia de cinco días, con multa de ciento ochenta a seiscientos euros, y apercibimiento de desobediencia a la autoridad (art. 292.1.y 2 LEC). Cuando sin mediar previa excusa el perito no compareciera al juicio o vista, el tribunal, oyendo a las partes que hubiesen comparecido, decidirá mediante providencia, si la audiencia ha de suspenderse o debe continuar (art.

[344] SAP Madrid, secc. 25ª, de 26 de septiembre de 2006, fto. Jco. 6º (EDJ 2006/356674). En el mismo sentido, STSJ Navarra, de 17 de mayo de 2006, fdo. Jco. 2º (EDJ 2006/98933).

292.3 LEC). En el supuesto de imposibilidad de asistencia el día señalado, por causa de fuerza mayor u otro motivo de análoga entidad, lo manifestará de inmediato al Tribunal, acreditando cumplidamente la causa. El tribunal, oídas las partes acordará si deja sin efecto el señalamiento y efectúa uno nuevo, o bien si cita al perito para la práctica del medio de prueba antes del acto del juicio, o bien acuerda rechazar la excusa y mantener el señalamiento (art. 183.4 LEC). En el caso de acordarse la práctica de la pericia en acto aparte, se deberá celebrar antes del juicio según dispone el artículo 290.1 LEC.

La ratificación de los peritos se realizará en la sede del Juzgado o tribunal que esté conociendo del asunto de que se trate, aunque su domicilio se encuentre fuera de la circunscripción correspondiente. Sólo cuando por razón de la distancia, dificultad del desplazamiento, circunstancias personales o por cualquier otra causa de análogas características resulte imposible o muy gravosa la comparecencia de las personas citadas en la sede del Juzgado o tribunal, se podrá solicitar el auxilio judicial para la práctica de dicho acto de prueba (art. 169.4 LEC). El artículo 429.5.2 LEC no hace referencia a la posibilidad de practicarse la prueba pericial mediante auxilio judicial. El artículo 169 LEC sólo hace referencia a la ratificación pero no a todas las cuestiones que refiere el artículo 347 LEC. Precisamente por su complejidad no se prevén en la regulación de la prueba de peritos normas sobre la práctica de la prueba mediante auxilio judicial, como sí se prevé para el supuesto de la declaración de testigo que no pudiera comparecer en juicio por las razones previstas en el art. 169.4 LEC, donde se establece la posibilidad de presentar un interrogatorio por escrito (art. 364 LEC). Actualmente, no obstante, existen medios de comunicación con imagen que permiten practicar dicha prueba con inmediación del juez que lleva el asunto aunque el perito se halle en el juzgado de otro partido.

9.2.4.3 Intervención del perito en juicio

La declaración del perito en juicio se realiza tras el interrogatorio de las partes y de los testigos, aunque dicho orden puede ser alterado por acuerdo del tribunal, de oficio o a instancia de parte cuando sea necesario (art. 300 LEC). La Ley de Enjuiciamiento Civil no regula cómo será el trámite de la intervención del perito en juicio limitándose a señalar en qué consistirá la intervención del mismo (art. 347 LEC). Pero en la práctica forense en el acto del juicio suele darse cuenta del perito que comparece y en qué calidad comparece. A continuación el Juez pregunta al perito por su cualificación profesional y sobre la existencia de alguna relación con alguna de las partes o su defensa o representación. Le recuerda el juramento o promesa que realizó al emitir el dictamen de actuar con

la mayor objetividad, (art. 335.2 LEC) y las penas establecidas en el Código Penal para el supuesto de faltar maliciosamente a la verdad (art. 440, 459 y 460 CP).

La comparecencia del perito obedecerá a los extremos declarados útiles y pertinentes por el juez en conformidad a lo previsto en el artículo 347 LEC, teniendo en cuenta que la misma no supone una reiteración literal del dictamen por escrito ya aportado, sino que su intervención obedece a una finalidad aclaratoria o explicativa del dictamen, crítica con el dictamen de otros peritos o bien declarativa respecto a su tacha. El ámbito de intervención del perito podrá consistir (art. 347 LEC), sin que dicha enumeración sea un «número clausus», en:

1º La exposición completa del dictamen, cuando esa exposición requiera la realización de otras operaciones, complementarias del escrito aportado, mediante el empleo de los documentos, materiales y otros elementos a que se refiere el apartado 2 del artículo 336 LEC;

2º La explicación del dictamen o de alguno o algunos de sus puntos, cuyo significado no se considerase suficientemente expresivo a los efectos de la prueba;

3º Respuestas a preguntas y objeciones, sobre método, premisas, conclusiones y otros aspectos del dictamen;

4º Respuestas a solicitudes de ampliación del dictamen a otros puntos conexos, por si pudiera llevarse a cabo en el mismo acto y a efectos, en cualquier caso, de conocer la opinión del perito sobre la posibilidad y utilidad de la ampliación, así como del plazo necesario para llevarla a cabo. Es decir, existe la posibilidad de que las partes soliciten que el perito amplíe el dictamen en el propio acto del juicio, o bien, de no poder llevarse a efecto en el mismo acto, que el juez acuerde la interrupción de la vista de juicio por considerar dicha ampliación del dictamen pericial útil y pertinente (347.4º y 193 LEC), o acordar la ampliación como diligencia final (art 435.2 LEC). Con carácter previo el juez preguntará al perito su opinión sobre la utilidad y posibilidad de la ampliación y el plazo en que puede llevarse a efecto. El tribunal no puede acordar, de oficio, que se amplíe el dictamen pericial, salvo que se trate de peritos designados de oficio en procesos sobre declaración o impugnación de la filiación, paternidad y maternidad, sobre capacidad de las personas o en procesos matrimoniales (art. 339.5 y 347.2 LEC). Coincidimos con ABEL LLUCH en que resulta censurable que se permita la ampliación del dictamen a puntos conexos a instancia de cualquiera de las partes (art. 347.1.4º LEC) y, por el contrario, se prohíba –salvo en los procesos no dispositivos- la ampliación del dictamen por el juez de oficio (art. 347.2 LEC), pues siendo el juez destinatario de la prueba pudiera estar interesado en su ampliación para formar mejor su convicción judicial, tal y como

admitía la derogada LEC de 1881 (arts. 340 y 634 LEC) y se producía en la práctica forense sin oposición en el foro ni en la doctrina[345];

5º Crítica del dictamen de que se trate por el perito de la parte contraria;

6º Formulación de las tachas que pudieran afectar al perito. (347.6 LEC). Recordemos que sólo pueden ser objeto de tacha los peritos designados por las partes ya que los peritos designados judicialmente quedan sujetos a posible recusación. Por otra parte, las tachas no podrán formularse después del juicio o la vista en los juicios verbales, y tratándose de juicio ordinario las tachas de los peritos cuya dictamen fue aportado en la demanda o contestación tuvo que efectuarse en la audiencia previa al juicio (art. 343.2 LEC).

En cuando al orden de intervención en juicio, en primer lugar formulará las preguntas la parte proponente, a continuación la parte o partes contraria y finalmente el Juez. El tribunal podrá también, pues, formular preguntas a los peritos y requerir de ellos explicaciones sobre lo que sea objeto del dictamen aportado (art. 347.2 LEC), ello conforme al principio de inmediación. Tratándose del supuesto en que el perito hubiese sido designado judicialmente a petición de ambas partes, primero preguntará la parte demandante y después la parte demandada.

Las preguntas y aclaraciones que efectúe el perito son fundamentales a efectos de formar la convicción del juez. Será en las mismas donde las partes podrán preguntar en prueba pericial electrónica sobre la cadena de custodia de la prueba, sobre las herramientas utilizadas y su consideración en el ámbito científico en cuanto a fiabilidad, y sobre los hechos que han llevado a las conclusiones del informe pericial. También servirán para aclarar conceptos excesivamente técnicos para las partes y el Juez y hacerla más entendible a legos en la materia.

9.2.4.4 Rectificación del dictamen pericial

En lo referente a la posibilidad de rectificar el dictamen pericial emitido, la doctrina está de acuerdo en que si el perito descubre eventuales errores en el dictamen, antes de que el Juez haya dictado sentencia, debe manifestarlos al Juez, a fin de que éste lo valore adecuadamente, bien para prescindir del

[345] Véase ABEL LLUCH, X. *La prueba pericial,* ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.3, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, pág. 117.

dictamen emitido. En España se mantenía la opinión contraria con el doble fundamento de la preclusión de los plazos probatorios y de la prohibición de repetir el dictamen pericial recogida en el artículo 630 LEC de 1881. Ello no obstante, autores como SERRA DOMÍNGUEZ estimaban que la rectificación debía ser posible en todo caso bien antes de la ratificación del dictamen, bien como consecuencia de las aclaraciones solicitadas por las partes; y que incluso con posterioridad siendo el Juez libre para aceptar o rechazar el dictamen pericial, con mayor razón podría prescindir del mismo cuando haya sido rechazado por el propio autor. Desaparecidos los plazos preclusivos en la LEC 1/2000 así como la prohibición de repetir el dictamen pericial, consideramos que no debe estimarse existente actualmente ningún obstáculo que impida dicha rectificación[346].

9.2.4.5 Careo entre peritos

El careo entre peritos con la finalidad de aclarar contradicciones entre los dictámenes periciales, pese a su evidente utilidad, no está prevista en la Ley de Enjuiciamiento Civil. Sin embargo en el proceso penal sí que se prevé y permite el careo entre peritos cuando tratándose de peritos de una misma disciplina declaren sobre los mismos hechos (artículo 724 LEcrim). La LEC regula en el artículo 373 el careo entre testigos, y partes y testigos al incurrir éstos en graves contradicciones, no obstante en relación a los peritos la Ley se limita a señalar en el artículo 347.1.5º la posibilidad de que el perito efectúe una crítica del dictamen de que se trate por la parte contraria.

Algunos autores como MAGRO SERVET dada la vigente regulación sostienen que no puede practicarse careo entre los peritos[347], otros autores, sin embargo, como ABEL LLUCH admiten el careo de peritos de cualificación similar o idéntica bajo el fundamento de que puede realzar o disminuir la credibilidad de los informes ya aportados[348], y PICÓ JUNOY admite una suerte de careo bajo el doble argumento de que el perito, al igual que el testigo, es un tercero y que

---

[346] Véase SERRA DOMÍNGUEZ, M. *La prueba pericial,* en "Instituciones del nuevo proceso civil. Comentarios sistemáticos a la Ley 1/2000", Vol. II, Alonso-Cuevilles Sayrol, J (coord.) edit. Difusa, Barcelona 2000, pág. 315.

[347] Véase MAGRO SERVET, Vicente, La Prueba pericial civil en la LEC y en la Ley de Ordenación de la edificación, La Ley, 2007, pág. 56.

[348] Véase ABEL LLUCH, X. La prueba pericial, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), *Serie estudios prácticos sobre los medios de prueba*, núm.3, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, pág. 155.

«*la contradicción de conocimientos entre personas de similares características profesionales permitirá valorar mejor el contenido del dictamen pericial*»[349]. La jurisprudencia se halla también dividida, en contra de su admisión podemos citar entre otras la SAP Granada de 3 de marzo de 2006[350] o la SAP Málaga, de 11 de marzo de 2004[351]. Esgrimen argumentos a su favor: la SAP Madrid de 11 de noviembre de 2005[352], SAP Coruña, de 14 de julio de 2005[353], SAP Barcelona de 15 de junio de 2004[354], SAP Asturias de 13 de julio de 2004[355], SAP Alicante de 5 de mayo de 2005[356] entre otras. Entendemos con dichos autores que pese a la falta de expresa regulación el careo entre peritos debe admitirse.

9.3 Prueba sobre la manifestación del hecho electrónico

9.3.1 Prueba documental

9.3.1.1 Momento procesal de aportación de la prueba documental

La prueba documental por medios e instrumentos queda sujeta como cualquier otra prueba a límites temporales, es decir, debe ser aportada en el momento procesal oportuno y dentro de los plazos señalados por la ley. En este sentido dispone la Exposición de Motivos de la LEC en su epígrafe X, párrafo 12º que «*...En los momentos iniciales del proceso, además de acompañar a la demanda o personación los documentos que acrediten los presupuestos procesales, es de gran importancia, para información de la parte contraria, la presentación de los documentos sobre el fondo del asunto, a los que la regulación de esta Ley añade medios e instrumentos en que consten hechos fundamentales (palabras, imágenes*

[349] Puede consultarse PICÓ Y JUNOY, *La prueba pericial en el proceso civil español*, JM Bosch editor, Barcelona, 2001, pág. 158.

[350] SAP Granada, secc. 3ª, de 3 de marzo de 2006, fdo.jco 3º (EDJ 2006/90463).

[351] SAP Málaga, secc. 4ª, de 11 de marzo de 2004, fdo. Jco. 2º (EDJ 2004/146969).

[352] SAP Madrid, secc. 21ª, de 11 de noviembre de 2005, fdo. Jco 5º (EDJ 2005/221662).

[353] SAP Coruña, secc. 4ª, de 14 de julio de 2005, fdo.jco 3º (EDJ 2005/216110).

[354] SAP Barcelona, secc. 13ª, de 15 de junio de 2004, fdo. Jco. 2º (EDJ 2004/84907).

[355] SAP Asturias, secc. 5ª, de 13 de julio de 2004, fdo. Jco. 2º (EDJ 2004/75849).

[356] SAP Alicante, secc. 5ª, de 5 de mayo de 2005, fdo. jco 4º (EDJ 2005/180891).

o cifras) para las pretensiones de las partes, así como los dictámenes escritos y ciertos informes sobre hechos». Es decir dicha prueba, como regla general, cuando tenga relación con el fondo del asunto deberá ser aportada por las partes junto con la demanda o la contestación en el juicio ordinario (art. 265.1.2º y 299) y tratándose de juicio verbal el demandado deberá aportarla en el acto de la vista (art. 265.4 LEC). Excepcionalmente también regula la ley la posibilidad de presentarla en momentos posteriores a la presentación de los escritos de demanda y contestación en que se basa su pretensión, se trata de supuestos especiales tales como imposibilidad de disponer de los mismos al presentar la demanda o contestación, alegaciones efectuadas en contestación a la demanda etc., se trata de los supuestos regulados en los arts. 265.2 y 3, 270, 271 y 435 LEC.

la Ley de Enjuiciamiento Civil contiene normas específicas relativas a la prueba documental electrónica a la que alude con los términos «medios» e «instrumentos» entre las que figuran las siguientes: a) Los «medios e instrumentos» que sean fundamentales deberán aportarse con los escritos de alegaciones (art. 265.1.2º LEC) y si siendo fundamentales se intentaran aportar con posterioridad con el carácter de complementarios deberán inadmitirse; b) los «medios e instrumentos» relativos al fondo del asunto podrán aportarse también en un momento no inicial en los supuestos excepcionales expresamente previstos por la ley en este caso podrán impugnarse por ser de fecha anterior a la demanda y contestación o haberse podido confeccionar con anterioridad (art. 270.1 LEC), por no justificarse su desconocimiento (art. 270.2 LEC), o por no acreditarse la falta de disponibilidad inicial del mismo (art. 270.3 LEC); c) los «medios e instrumentos» no podrán aportarse con posterioridad a la vista (en el juicio verbal) o al acto del juicio (en el juicio ordinario) (art. 271.1 LEC); d) los «medios e instrumentos» pueden aportarse por vía de diligencias finales en los supuestos previstos en el art. 435.1, regla 3ª LEC (art. 271. 1 LEC), en este caso podrán ser impugnados por no referirse a hechos nuevos o de nueva noticia o por no ser anteriores al momento de formular conclusiones o no ser decisivos en términos del fallo (art. 271.2 LEC); e) los «medios e instrumentos» requeridos de exhibición se podrán impugnar por falta de los requisitos previstos para la exhibición entre partes (art. 328 LEC) –como puede ser, por ejemplo, la falta de disponibilidad del medio o instrumento-, por falta de los requisitos para la exhibición por terceros (art. 329 LEC) –como puede ser, por ejemplo, que el medio o instrumento no tiene el carácter de trascendente para dictar sentencia-, o por falta de requisitos para la exhibición por las entidades oficiales (art. 333 LEC) –como puede ser, por ejemplo, que se trate de medios o instrumentos de carácter reservado-.

Teniendo en cuenta cada una de las normas que determinan el momento procesal en que deben aportarse dichos documentos, es decir, atendiendo al

«criterio de temporalidad» podemos clasificar los documentos en: 1) documentos acompañados, que son los aportados junto con los escritos de alegaciones y que fundamentan las alegaciones que se vierten en los mismos; 2) documentos aportados, que son los presentados aisladamente del cuerpo de alegaciones y comprensivos de a) los documentos llamados complementarios, b) los documentos cuyo interés o relevancia se puso de manifiesto a consecuencia de las alegaciones del demandado al contestar la demanda (art. 265.3 LEC), c) los documentos que se pueden aportar en un momento no inicial del proceso (art. 270 LEC), d) los documentos que se pueden aportar como diligencia final en sustitución de otros actos de prueba fallidos (art. 435.2 LEC) y e) los documentos que se pueden presentar excepcionalmente frente a la regla de la preclusión definitiva (art. 271 LEC); y finalmente 3) documentos *requeridos*, que son aquellos que se solicitan o requieren a las otras partes o a un tercero para que proceda a su debida exhibición en el proceso (arts. 328, 329 y 333 LEC)[357].

Por otro lado, atendiendo al «criterio de la legalidad», es decir, atendiendo a si cumplen o no con los requisitos que el legislador ha fijado para su admisión, podemos distinguir: a) documentos fundamentales, que son los que fundan la causa de pedir de las partes o, en la terminología legal «el derecho a la tutela judicial que pretenden» (art. 265.1.1º LEC); b) documentos complementarios, que son los documentos accesorios o auxiliares o aquellos destinados a combatir las alegaciones de adverso (SAP Madrid, de 17 de octubre de 2007[358]); c) documentos que se pueden aportar en un momento no inicial del proceso, por ser fecha posterior a la demanda y contestación y no haberse podido confeccionar con anterioridad (art. 270.1 LEC) o por ser documentos que la parte justifica no haber conocido con anterioridad a la demanda y contestación (art. 270.3 LEC)[359]; d) documentos que se pueden aportar por vía de diligencias finales, por ser documentos referidos a hechos nuevos o de nueva noticia (art. 271.1 LEC) o sentencias o resoluciones judiciales o de autoridad administrativa anteriores a la fase de conclusiones y decisivas en términos del fallo (art. 271.2 LEC); e) y finalmente documentos requeridos a las partes, terceros, o

[357] Véase MUÑOZ SABATÉ, LL., *Fundamentos*..., ob. cit. págs. 295-304.

[358] La SAP Madrid, secc. 21ª, de 17 de octubre de 2007, fto. jco.2º (AC 2008\70) razona que un libro de comercio aportado por la actora en la audiencia previa debe admitirse, sin que pueda ser tachado de extemporáneo, porque no se trata de un libro que genera la causa de pedir de la parte actora en la litis, sino lo que pretende es desvirtuar determinadas alegaciones efectuadas por la parte demandada en su escrito de contestación a la demanda.

[359] Con referencia al derogado art. 506 LEC 1881, similar al actual art. 270 LEC, puede verse MONTERO AROCA, J., *Presentación de documentos materiales con la demanda y contestación*, en Revista Poder Judicial, núm. 17, Madrid, 1990, pág. 53, donde efectúa un análisis de distintos pronunciamientos del Tribunal Supremo.

Administraciones, en cuyo caso deberán concurrir, respectivamente, los requisitos de los artículos 329, 330 y 333 LEC.

En segunda instancia, la aportación de nueva prueba documental se circunscribe a *«los documentos que se encuentren en alguno de los casos previstos en el artículo 270 y que no hayan podido aportarse en la práctica de la instancia»* (art. 460.1 LEC). Recordemos que el artículo 270 recoge los supuestos de aquellos documentos: que son de fecha posterior a la demanda o a la contestación o, en su caso, a la audiencia previa al juicio, siempre que no se hubiesen podido confeccionar ni obtener con anterioridad a dichos momentos procesales; anteriores a la demanda o contestación o, en su caso, a la audiencia previa al juicio, cuando la parte que los presente justifique no haber tenido antes conocimiento de su existencia; y finalmente aquellos que no han podido ser obtenidos con anterioridad por causas que no sean imputables a la parte, siempre que haya hecho oportunamente la designación a que se refiere el apartado 2 del artículo 265, o en su caso, el anuncio al que se refiere el número 4.º del apartado primero del artículo 265 de la presente Ley.

9.3.1.2 Posición de las partes sobre la prueba documental electrónica. La firma electrónica como garantía.

La prueba documental aportada por una de las partes implicará respecto a las restantes el posicionarse sobre los documentos presentados de adverso. Es decir, podrán: reconocer como auténtico el documento suscrito por ellas; admitir el documento, la parte no ha suscrito el documento pero lo reconoce como auténtico; o impugnar el documento, considerando que el documento no es auténtico o la copia, certificación o testimonio no es exacto (art. 427.1 LEC).

El documento puede ser objeto de impugnación en fase de alegaciones, en fase de audiencia previa o vista, y en fase de conclusiones, todo ello con anterioridad a la valoración judicial en sentencia. La impugnación documental tiene lugar en el juicio ordinario en fase de audiencia previa (art. 427.1 LEC) y en el juicio verbal en la vista (433 LEC). Dichas normas generales se aplican en defecto de expresa regulación procesal respecto a la prueba electrónica, puesto que el artículo 382.2 LEC, al que remite el artículo 384.2 LEC, se limita a permitir la aportación de dictámenes y medios de prueba instrumentales «*cuando se cuestione la autenticidad de lo reproducido*».

Pueden ser objeto de impugnación: *la «autenticidad»* del documento, esto es, la concordancia del autor aparente con el autor real; *la «exactitud»*, esto es la concordancia de la copia, testimonio o certificación con el original; y *la*

«certeza», esto es, la concordancia de las declaraciones o testimonios contenidos en el documento con la realidad[360]. *La valoración de la certeza* de un documento, es decir, la concordancia entre la información que contiene y la realidad, corresponde a la fase de dictado de la sentencia.

En cuanto a la «exactitud» solo indicar que entre las técnicas más comunes para garantizar el control de la integridad o exactitud de un documento electrónico se hallan, en primer lugar, la verificación de la utilización correcta del código secreto PIN (*Personal Identificación Number*) y que consiste en una combinación de cifras y/o letras que el sujeto conoce y digita sobre el teclado del sistema que va a utilizar. Habitualmente de forma complementaria se recurre a combinar el uso del PIN con la introducción, dentro de la misma máquina, de una carta o pista magnética, o de una carta a memoria, que verifica la validez del código dado, sin que sea necesario poner en juego el cerebro central del sistema. En segundo lugar la desencriptación del documento cuando aparece encriptado, rastreando quien conoce el sistema de codificación empleado. La criptografía se utiliza para hacer efectivos numerosos mecanismos de seguridad informática y consiste en la codificación del texto a transmitir con la ayuda de claves y de algoritmos, de modo que la información así tratada deviene ininteligible para toda persona que no posee la clave de desciframiento. Y en tercer y último lugar una técnica común es también la aplicación de la biometría (iris del ojo, huella dactilar) que permite validar un documento así signado. La biometría es una ciencia que estudia características mesurables de los seres humanos. Está constatado que cada ser humano posee un cierto número de rasgos absolutamente exclusivos que permiten identificarlo. La mayoría de sus métodos (reconocimiento del iris, de la voz, tipología de sangres y tejidos, etc.), aún están en fase de experimentación y es una técnica con alto coste económico[361].

La «autenticidad» de un documento, es decir, la concordancia entre autor aparente y autor real, dependerá de elementos del propio documento, principalmente en el documento electrónico de la firma[362]. La existencia de firma en el documento y del tipo de firma electrónica afectará a la autenticidad

---

[360] Véase ABEL LLUCH, X. *La prueba documental*, en la obra colectiva del mismo título, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.4, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, pág. 173.

[361] Véase SANCHÍS CRESPO, C., *La prueba por medios audiovisuales*, ob. cit., págs .90 y 91. Dicha autora sigue en las descripciones de dichas técnicas a CARRASCOSA LÓPEZ, V., *La Informática y la prueba*, La Ley, nº 4696, 18 de diciembre de 1998, pág. 16.

[362] La doctrina enumera como elementos que deben integrar la noción de documento: el soporte, el contenido y el autor. Discutiéndose si la firma es elemento esencial del documento.

del mismo[363]. La firma en el documento electrónico cobra especial relevancia por cuanto su autenticidad determina el contenido auténtico del documento. La autenticidad de la firma electrónica, al contrario de la firma manuscrita, no es disociable de la valoración de los datos cifrados. Puede suceder que la firma manuscrita de un documento tradicional sea auténtica pero que, ello no obstante, no lo sea el contenido del documento, puesto que su texto, una vez firmado puede ser adulterado, falsificado o alterado. En el caso de la firma electrónica, por el contrario, fijada la autenticidad de la firma queda excluida cualquiera duda sobre la autenticidad de la información documentada, concluyendo con certeza que el contenido del documento es también auténtico, es decir, que no ha sufrido falsificación o alteración posterior a la firma[364]. Resulta, pues, hoy más factible asegurar la identidad y fiabilidad de un documento firmado electrónicamente que de un documento manuscrito en soporte tradicional por resultar este segundo medio de más fácil manipulación. En una firma tradicional aparece el nombre y apellidos de su autor junto con la rúbrica, que sirve de impronta a la hora de vincular a la persona que firma el documento con su contenido, mientras que, en la firma electrónica, se acentúa más la identidad entre el autor con el contenido, resumiendo una parte esencial del mismo, cifrándolo posteriormente, con la fecha y la hora de emisión, por lo que la menor variación del algoritmo, así obtenido, supondría una prueba de manipulación externa que derivaría a la existencia de un tercero no querido, y posiblemente malintencionado, entre las partes en cuestión[365].

Frente a la firma manuscrita contenida en el documento tradicional, la firma electrónica presenta particularidades propias como: precisar de un acto relevante de asunción como mecanismo de suscripción de declaraciones de voluntad, mientras que la firma autógrafa no precisa de una manifestación específica para adjudicarle la virtualidad de representar la voluntad del firmante; resulta separable de su titular a diferencia de la firma manuscrita que está indisolublemente unida a un sujeto; y finalmente tiene una vigencia cronológica limitada, dado que es posible escindir entre sujeto y mecanismo de creación de firma (clave privada), a diferencia de la firma manuscrita acompaña al individuo durante toda su vida. Cuestión distinta es la relativa a su eficacia probatoria, esto es, que la firma electrónica reconocida tenga respecto de los

[363] Véase en este sentido la SAP Cádiz, secc. 2ª, de 25 de febrero de 2008, fto. jco. 4º (JUR\2008\235221).

[364] Véase ORMAZÁBAL SÁNCHEZ, G., *Informática y prueba judicial. Especial referencia a la firma electrónica* en "*Empresa y prueba informática*", Colección de Formación continuada Facultad de Derecho de ESADE, ed. Bosch Educación, Barcelona 2006, págs. 65 y ss.

[365] Véase ELÍAS BATURONES, JJ. *La prueba de documentos electrónicos en los Tribunales de Justicia*, ed. Tirant Lo Blanch, Valencia, 2008, págs. 48-49.

datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel[366].

La firma electrónica es aquel «*…conjunto de datos, en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante*» art. 3.1 LFE). *E*n ningún caso debe confundirse la «firma electrónica» con la «firma manuscrita digitalizada» que no es una firma electrónica, sino una forma de trasvasar o escanear una firma escrita a un soporte informático, con muy poco valor y utilidad. La firma electrónica se regula en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, que sustituía al Real Decreto Ley 14/1999, de 17 de septiembre, y que fue promulgada tras la Directiva 1999/93/CE, del Parlamento de Europa y del Consejo, de 13 de Diciembre de 1999, por la cual se establece un marco unitario para la firma electrónica. Posteriormente la LFE ha sido modificada por la Ley 56/2007 de medidas de impulso de la Sociedad de la Información, de 28 de diciembre de 2007[367].

Los documentos electrónicos pueden clasificarse entre «firmados» y «no firmados». A su vez dentro de los documentos electrónicos firmados podemos distinguir aquellos que se hallan firmados con firma electrónica simple, con firma electrónica avanzada y con firma electrónica reconocida. La firma electrónica «simple» se describe como el conjunto de datos en forma electrónica, consignados junto a otros o asociados a ellos, que pueden ser utilizados como medio de identificación del firmante (art. 3.1 LFE). Se admite como prueba documental el documento aportado a través de un soporte en que se hallen los datos con firma electrónica simple (art. 3.8 LFE). Su eficacia probatoria – a diferencia de la firma electrónica reconocida- no viene tasada en la LFE, pero al establecer que se admite como prueba documental, debemos entender que tendrá la eficacia propia del documento -público o privado- a través del cual se aporte al proceso, y que su autenticidad, de ser impugnada, puede acreditarse a través de un dictamen pericial.

La firma electrónica «a*vanzada*» es aquella que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados (art. 3.2 LFE) está vinculada al firmante de forma única y a los datos a los que se refiere y ha sido

[366] Véase BORNARDELL LOZANO, R*., La firma electrónica. Especial consideración de sus efectos jurídicos, Notariado y contratación electrónica*, Consejo General del Notariado, Madrid, 2000, págs. 59 y ss.

[367] Sobre el concepto de firma electrónica y sus clases puede consultarse GARCIA MAS, F.J., *El documento público electrónico*, en "Nuevas tecnologías en la contratación: sociedad, nueva empresa e hipoteca electrónica", Seminario organizado por el Consejo General del Notariado en la UIMP en julio de 2003, Escolano Navarro, J.J. (dir.), ed. Civitas, 2005, págs.124 y ss.

creada por medios que el firmante puede mantener bajo su control. Está basada en un *certificado reconocido* y generada con un dispositivo seguro de creación de firma. La LFE no le otorga reconocimiento probatorio específico, por lo que deberá equipararse a la firma simple. Y finalmente la firma electrónica «r*econocida*», es aquella firma electrónica avanzada basada en un certificado reconocido y generado mediante un dispositivo de firma segura. Su eficacia probatoria se equipara a la de la firma manuscrita (arts. 3.3. y 3.4, LFE). La firma electrónica reconocida precisa la concurrencia de los siguientes requisitos: a) debe tratarse de una firma electrónica avanzada, es decir, la que cumple los requisitos del artículo 3.2 LFE, relativos a la autenticidad e integridad del mensaje y que se reconducen a la firma digital basada en la criptografía simétrica; b) dicha firma electrónica avanzada ha de estar basada en un certificado reconocido, es decir, que cumpla los requisitos de los artículos 11, 12 y 13 LFE (en particular, las exigencias en materia de comprobación de la identidad del solicitante, que se realizará, de forma general, con personación física del mismo ante el prestador de servicios de certificación o entidad delegada) y que haya sido expedida por un prestador que cumple los requisitos del artículo 20 LFE; y c) finalmente dicha firma electrónica avanzada, además, ha de haber sido producida por un dispositivo de creación de firma, que es aquel que cumple las exigencias legalmente establecidas[368].

La firma electrónica avanzada usa la criptografía con un sistema de claves asimétricas. Se pueden definir como una pareja de claves criptográficas, una privada y una pública, relacionadas entre ellas y que se utilizan en el ámbito de la validación. La clave privada está constituida por un código alfanumérico, y sólo la conoce el titular. Su correspondiente clave pública también está constituida por un código de letras y números, pero se diferencia de la clave privada en que su conocimiento es de dominio público, puesto que aparece en unas guías puestas al día y custodiadas por una entidad de certificación. Esta entidad garantiza la validez de la clave, pues la vincula a un sujeto determinado de forma segura, emitiendo para ello un certificado en el que confiarán aquellos terceros que contraten por medios electrónicos a ese sujeto[369]. Las dos claves asimétricas, pública y privada, se identifican mutuamente si se pone en relación una con la otra. Esto sucede por medio de un especial procedimiento informático de control. Quien posea una pareja de tales claves asimétricas puede firmar un documento informático, de tal modo quien acceda a aquél tendrá certeza respecto a la paternidad e integridad del documento, para lo que

[368] Véase MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003, de firma electrónica*, 2ª ed., ed. Civitas, 2009, pág.90.

[369] El Anexo II de la Directiva 1999/92/EC, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica dispone los requisitos que deben cumplir estos proveedores de servicios de certificación.

sólo tendrá que proceder a la verificación de la correspondencia entre la clave pública asociada al nombre del firmante y la clave privada con la que el documento está firmado. Siguiendo el ejemplo citado por SANCHIS CRESPO, si Ticio después de haber firmado digitalmente un documento con su clave privada lo transmite a Cayo a través de una red o disquete, Cayo, para controlar que efectivamente aquel documento ha sido firmado digitalmente por Ticio, deberá primero controlar en la guías públicas la composición de la clave pública de Ticio, para después aplicarla al documento. Si la clave pública se corresponde con la privada el documento será legible para Cayo quien además tendrá la absoluta seguridad de que Ticio es su autor. En caso contrario, es decir, si la clave pública no se corresponde con la privada, el documento permanecerá ilegible y Cayo sabrá que Ticio no es su autor[370].

Un documento electrónico con certificado reconocido es un juego de claves, encriptaciones o algoritmos que atestiguan de forma fehaciente que la clave pública pertenece a un determinado individuo, de tal manera que la función huella propia de estos certificados detecta cualquier alteración en el documento. La clave pública con la que se firma un documento electrónico es el conjunto de hardware, software, personas, políticas y procedimientos necesarios para crear, gestionar, almacenar, distribuir y revocar certificados digitales basados en criptografía de clave pública. La información encriptada mediante clave pública sólo puede recuperarse mediante la clave privada complementaria. Se entenderá con el siguiente ejemplo: si un procurador quiere remitir un documento a un abogado para que ningún hacker u otra persona pueda acceder a su contenido, lo primero que hace es cifrar o codificar el mensaje con una clave de forma tal que aunque otra persona intercepte el documento no pueda descifrarlo. A su vez el abogado debe disponer de la clave usada por el procurador y de una clave asimétrica que sólo tenga él para que el procurador tenga seguridad que nadie más pueda acceder a su contenido. Como el procurador tiene que remitir muchos documentos a diversos abogados y éstos no pueden tener la misma clave, lo que se hace es que el procurador tenga una clave pública (que puede conocer cualquier abogado) y cada abogado destinatario tenga una clave privada[371].

Conviene también precisar a efectos de una mayor comprensión sobre el tema que cuando el legislador español en la LFE define el concepto de «*datos de*

[370] Véase SANCHIS CRESPO, C., *La prueba por medios audiovisuales e instrumentos de archivo en la LEC 1/2000 (Doctrina, jurisprudencia y formularos)*, ed. Tirant lo Blanch, Valencia, 2002, pág. 96. Dicha autora sigue la descripción del sistema efectuado por GRAZIOSI, A., *Premesse ad uan teoria probatoria del documento informatico,* Rivista Trimestrale di Diritto e Procedura Civile, 2, 1998, págs. 507-509.

[371] Véase ILLÁN FERNÁNDEZ, J.M., *La prueba electrónica*…., ob. cit., pág. 274.

creación de firma» (art. 24.1 LFE) como los datos únicos que el firmante utiliza para crear la firma electrónica, por ejemplo códigos o claves criptográficas privadas, está haciendo referencia a los que anteriormente definíamos como «*clave privada»*. Y cuanto define como «*datos de verificación de firma»* los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica (art. 25.1 LFE), ello coincide con la definición de «*clave pública»*. Tanto la aplicación de los datos de creación de firma como la aplicación de los datos de verificación de firma se realiza a través de un dispositivo, es decir, un programa o sistema informático, que se denominan respectivamente «*dispositivos de creación o verificación de firma» (art. 24.2 y 25.2 LFE)*. Un «*dispositivo seguro de creación de firma»* es un dispositivo de creación de firma que cumple los requisitos establecidos en el art. 24.3 LFE, al que el legislador hace merecedor de un alto grado de fiabilidad[372]. Advertir, no obstante, que el legislador ha generado confusión, puesto que no todos los requisitos del art. 24.3 LFE se refieren a los dispositivos utilizados para aplicar los datos de creación de firma o clave privada, sino también a los dispositivos para generar esta clave (por ej. las letras a y b).

Por otro lado, puede definirse el «*certificado electrónico»* como aquel documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un signatario y confirma su identidad (art. 6.1. LFE). Pueden ser firmantes personas físicas o jurídicas (art. 7 LFE) a quienes la ley grava con una serie de obligaciones (art. 17, 18 y 19 LFE). Y el «c*ertificado reconocido»* es un tipo cualificado de certificado que se caracteriza por contener la información descrita en el apartado segundo del art. 11 LFE y ser expedido por un prestador de servicios de certificación que cumple, además de los especificados en los art. 18 y 19, los requisitos u obligaciones enumeradas en los artículos 12, 13 y 20 LFE, lo que le proporciona especiales garantías de seguridad, y también será relevante a efectos probatorios[373].

---

[372] El artículo 24.3 LFE establece como requisitos: que los datos utilizados para la generación de la firma pueden producirse sólo una vez y se asegure razonablemente su secreto; que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma, y que la firma está protegida contra la falsificación mediante la tecnología existente en cada momento; que los datos de creación de firma puedan ser protegidas de forma fiable por el firmante contra su utilización por terceros.

[373] La información a que hace referencia el precepto cuando alude al art. 11.2 LFE es la siguiente: La indicación de que se expidan con aquella cualidad (de certificados reconocidos); el código identificativos único del certificado; la identificación del prestador de servicios de certificación que expide el certificado y su domicilio; la firma electrónica avanzada del prestador de servicios de certificación que expide el certificado; la identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de Documento Nacional de Identidad o a través de un pseudónimo que conste como tal de manera inequívoca y en el supuesto de

La certificación de estos dispositivos seguros de creación de firma se prevé en el artículo 27 LFE. En la certificación se utilizarán las normas técnicas cuyos números de referencia hayan sido publicados y excepcionalmente los aprobados por el Ministerio de Ciencia y Tecnología, que se publicarán en el directorio de Internet de este Ministerio (art. 27.3 LFE). Este sello de calidad podría influir en el valor probatorio que otorguen los jueces. En todo caso, la certificación ya no sirve, como sucedía con la acreditación del Decreto-Ley 14/1999, para otorgar clase alguna de presunción de autenticidad.

9.3.1.3 Documento electrónico público y documento electrónico privado

El documento electrónico puede haber tenido acceso al proceso como «*documento privado*» o mediante «*documento público*», se trataría en este último caso, por ejemplo, de un acta de protocolización o de presencia notarial para dar fe del contenido de una página web, o de la remisión de un mail. En este sentido, la Ley 59/2003 de Firma Electrónica, de 19 de diciembre, distingue dentro del concepto de documento electrónico en su artículo 3.6 entre: Los «*documentos públicos*», entendiendo por tales los firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley encada caso; los «*documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas*», conforme a su legislación específica; y finalmente los «*documentos privados*».

La consideración de los anteriores documentos como públicos o privados supone que *«tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable»* (art. 7.3 LFE). Por lo tanto, en su calidad de documentos públicos o privados les será de aplicación lo dispuesto en los artículos 267 y 268 LEC. Dicho Cuerpo

---

personas jurídicas, por su denominación o razón social y su Código de Identificación Fiscal; los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante; el comienzo y el fin del período de validez del certificado; los límites del uso del certificado, si se establecen; y los límites del valor de las transacciones para las cuales puede utilizarse el certificado, si se establecen.

Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en el caso que sea significativo de acuerdo con la finalidad propia del certificado y siempre que aquél lo solicite. Si los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la cual represente y, en caso de ser obligatoria la inscripción, de los datos registrales, de conformidad con el apartado segundo del artículo 13.

legal permite, además, la presentación de los documentos mediante copias correspondiendo a la contraparte la impugnación, en su caso, de la autenticidad.

El documento privado escrito podrá haber sido presentado en el juicio por original o copia autentificada por fedatario público, pudiendo, a instancia de los interesados, dejar testimonio (art. 268.1 LEC). *Estos documentos podrán ser también presentados mediante imágenes digitalizadas, incorporadas a anexos firmados electrónicamente (*en este caso no se exige una firma electrónica reconocida, porque ésta sólo es obligatoria en los documentos públicos tal y como requiere la normativa correspondiente). También podrá haber sido presentado mediante copia simple (art. 268.2 LEC), pues si se permite la aceptación de los documentos públicos por copia simple, *a fortiori* debe permitirse y está permitida la copia simple de los documentos privados. En el caso de que el original del documento privado se encuentre en un expediente, protocolo, archivo o registro público, se presentará copia auténtica o se designará el archivo, protocolo o registro, según lo dispuesto en el apartado 2 del artículo 265.

La LEC regula en su artículo 326.3 LEC la impugnación del documento electrónico privado señalando que «*cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica*». La remisión a la Ley de Firma Electrónica debe entenderse referida al apartado 8 del artículo 3, que regula la impugnación de la autenticidad de la firma electrónica «reconocida»[374]. Para acreditar la autenticidad basta la certificación oficial por el prestador del servicio de certificación acreditativa de los extremos del documento que contiene la firma electrónica reconocida. Es decir, si se

[374] Textualmente el artículo 3.8 de la LFE dispone: «*El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.// La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros.//Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil».*

impugna la autenticidad de la firma electrónica reconocida, «*la autentificación consistirá en comprobar que por el prestador de servicios de certificación que ha expedido los certificados electrónicos se cumplen los requisitos establecidos por la ley, en particular la garantía de confidencialidad del proceso y la autenticidad, conservación e integridad de la información y la identidad de los firmantes*» (SAP Cádiz de 25 de febrero de 2008[375]). La expresión «se procederá» no supone que deba iniciarse una investigación por el juez ante la alegación de falta de autenticidad sino que el aportante del documento electrónicamente firmado habrá de levantar la carga de proponer pruebas que demuestren la fiabilidad de los servicios del certificador. El carácter de «reconocida» de una firma no debe presuponerse, ni debe corresponder al adversario la carga procesal de acreditar que la firma merece tal calificativo.

De modo distinto, si se impugnare la autenticidad de la firma electrónica «avanzada» la LFE remite al artículo 326.2 LEC, aun cuando dicho artículo no está previsto para probar la autenticidad del documento electrónico. Es decir, en este supuesto se puede practicar «*cualquier medio de prueba que resulte útil y pertinente, pudiendo practicarse prueba pericial que acredite que el medio de prueba no ha sido manipulado, prueba testifical con el autor del documento aportado, etc*.» (SAP Cádiz, de 25 de febrero de 2008[376]). La prueba pericial puede resultar compleja y onerosa y si los litigantes se ven frecuentemente precisados de acudir a ella es probable que la utilización de la firma en el tráfico jurídico se resienta considerablemente. En todo caso, la necesidad de hacer uso de dicho medio de prueba dependerá de la confianza que se genere hacia la certificación de prestadores de servicios de certificación y de dispositivos de creación de firma que en la actualidad no disponen de ningún sistema de reconocimiento oficial.

El derogado Decreto-Ley de 1999 en su artículo 3.1.II dotaba a la firma electrónica que ahora la LFE denomina «reconocida» de una enérgica presunción de autenticidad, por supuesto desvirtuable, cuando el certificado reconocido en que se basaba hubiese sido expedido por un prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma con el que ésta se hubiese producido estuviese certificado.

Lo anterior potenciaba notablemente su valor probatorio, evitando una onerosa prueba pericial. El requisito que había que añadirse al hecho de tratarse de una firma electrónica de las que la actual LFE denomina «reconocida» era que el prestador de servicios de certificación y el dispositivo de firma hubieren sido

[375] SAP Cádiz, secc. 2ª, de 25 de febrero de 2008, fto.jco.4º (JUR\2008\23551).

[376] SAP Cádiz, secc. 2ª, de 25 de febrero de 2008, fto. jco.4º (JUR\2008\23551).

certificados, es decir, se hubieran sometido con éxito a cierto proceso dirigido a obtener un especial reconocimiento de fiabilidad, seguridad o solvencia técnica. Sin llegar a crear una verdadera presunción de autenticidad, se presumía que la firma electrónica reunía las condiciones para ser calificada de avanzada, que el certificado en que se basaba cumplía los requisitos para tener la condición de reconocido, y por lo tanto resultaba especialmente fiable o seguro; y que el dispositivo de creación de firma mediante el cual había sido producida reunía las condiciones para ser tenido como seguro. Quien pretendía cuestionar la autenticidad de la firma debía soportar la carga de desvirtuar los hechos presumidos por el antiguo 3.1.II LFE (que la firma tiene la condición de avanzada, etc.). En la actualidad no existe ningún precepto similar.

A diferencia de España, Alemania ha traspuesto a su ordenamiento la directiva europea sobre firma electrónica. Las consecuencias o efectos probatorios de la firma electrónica se han llevado a la norma procesal general, es decir, a la Zivilprozessordnung (ZPO), concretamente su SS 371.a), dispone que: «*La apariencia de autenticidad que una declaración en forma electrónica genere como consecuencia de su verificación según lo dispuesto en la Ley de Firma Electrónica sólo podrá ser arrumbada mediante hechos que permitan suscitar serias dudas de que dicha declaración haya sido realmente emitida por el titular de la clave de firma*». La verificación aludida en el precepto se refiere a la acreditación voluntaria de prestadores de servicios de certificación, prevista en el ss. 15.1 de la Ley alemana de Firma Electrónica (Signaturgesestz (SigG). Dicha acreditación corre a cargo de cierta autoridad pública y confiere una suerte de reconocimiento, marca o distintivo de calidad de carácter oficial, que certifica un alto grado de seguridad técnica y administrativa en relación a los certificados reconocidos emitido por el prestador de servicios.

En España, como hemos dicho anteriormente, no existe en la actualidad un reconocimiento oficial de ningún procedimiento de certificación, pudiendo, además, prestar dichos servicios tanto entidades públicas como privadas, aunque el prestador de servicios puede haber superado un procedimiento de certificación que pese a no estar reconocido puede ejercitar notable influencia en el juzgador. El valor judicial que finalmente se otorgue a las certificaciones expedidas por las entidades de certificación, públicas o privadas, dependerá de su seriedad y alto grado de solvencia técnica, e integración social, y de no producirse la creencia y confianza en las mismas deberá acudirse necesariamente a la costosa prueba pericial cada vez que el adversario cuestione la autenticidad de las mismas. En primero de dichos supuestos evidentemente llevará a una mayor confianza del público a la hora de autenticar las transacciones para las que han venido utilizándose celulosa y firma tradicional.

Tanto o más valor que la acreditación voluntaria de los prestadores de servicios de certificación tiene la certificación de que los productos de firma electrónica se ajusten a ciertas normas técnicas. En este sentido el artículo 28 LFE establece una novedad importante, al desprenderse del mismo que, si los productos de firma electrónica utilizados por los prestadores de servicios de certificación y los dispositivos seguros de creación de firma se ajustan a las normas técnicas correspondientes cuyos números de referencia hayan sido publicados en el «Diario Oficial de la Unión Europea», se presumirá: en primer lugar que el prestador de servicios de certificación que expide certificados reconocidos utiliza sistemas y productos fiables que están protegidos contra toda alteración y que garantizan la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte (art. 20.1.d LFE); en segundo lugar que el dispositivo de creación de firma ofrece garantía de que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto; en tercer lugar que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento; en cuarto lugar que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros; y finalmente que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.

Así, quien acredita la conformidad o ajuste de los productos de firma empleados con las normas técnicas correspondientes cuyos números de referencia hayan sido publicados en el Diario Oficial de la Unión Europea tiene fundados motivos para confiar en que su firma será considerada como auténtica por el Juez. Dicha declaración de ajuste o conformidad la deben llevar a cabo, si se trata de dispositivos de creación de firma, entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo a lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria, y en sus disposiciones de desarrollo (art. 27.2 LFE). Si se trata de otros «productos» de firma electrónica (dispositivos de verificación de firma, por ejemplo), la LFE no especifica quien deba o pueda llevar a cabo dicha verificación. Recuérdese que los productos de firma electrónica sobre los que recae la presunción no son los dispositivos de creación de firma, a los que se refiere el art. 24.3 ahora transcrito, sino cualesquiera otros, aludidos en el artículo 20.1d LFE. Tal acreditación, realizada por la entidad correspondiente, habría de introducirse en el proceso por la vía de la prueba pericial. Es el único modo en que el adversario procesal podrá aportar, asimismo, su dictamen o solicitar del Juez la designación de perito, solicitar la comparecencia del perito al objeto de formularle preguntas y pedirle las aclaraciones que crea precisas.

Como señalábamos anteriormente el documento electrónico puede tener acceso al proceso también como *documento público* entendiendo por tal el firmado electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso (art. 3.6 LFE). Tratándose de un documento público notarial el art. 17 bis de la Ley del Notariado, introducido por la Ley 24/2001, de 27 de diciembre, de medidas fiscales, administrativas y del orden social equipara el documento público electrónico notarial a cualquier otro documento público intervenido por notario. De este modo dispone que: «E*n todo caso, la autorización o intervención notarial del documento público electrónico ha de estar sujeta a las mismas garantías y requisitos que todo documento público notarial y producirá los mismos efectos. En consecuencia: a) Con independencia del soporte electrónico, informático o digital en que se contenga el documento notarial, el notario deberá dar fe de la identidad de los otorgantes, de que a su juicio tienen capacidad y legitimación, de que el consentimiento ha sido libremente prestado y de que el otorgamiento se adecua a la legalidad y a la voluntad debidamente informada de los otorgantes e interviniente»*. Dicho artículo extiende la dación de fe más allá de unos hechos sensorialmente perceptibles –como sucede con el art. 319 LEC, que se limita a la existencia del hecho, la fecha y la intervención de los sujetos-, para extender dicha dación de fe a lo que, en puridad, son juicios o apreciaciones del notario –sobre la capacidad y legitimación de los otorgantes, la libre prestación del consentimiento, el carácter debidamente informado de la voluntad y, en fin, la adecuación del otorgamiento a la realidad[377].

El documento público escrito podrá presentarse por copia simple (art. 267 LEC), sin necesidad de aportar su original, entendiéndose por copia simple la simple fotocopia, ya sea en soporte papel o, en su caso, en soporte electrónico a través de imagen digitalizada incorporada como anexo que habrá de ir firmado mediante firma electrónica reconocida**.** Y si se impugnare la autenticidad del documento público, «*podrá aportarse a los autos original, copia o certificación del documento con los requisitos necesarios para que surta efectos probatorios*» (art. 267 *in fine* LEC).

Los documentos públicos harán prueba plena si se aportaren al proceso en original o por copia o certificación fehaciente, ya sean presentadas éstos en soporte papel o mediante documento electrónico, o si, habiendo sido aportado por copia simple, en soporte papel o imagen digitalizada, conforme a lo previsto en el artículo 267, no se hubiere impugnado su autenticidad (art. 318

[377] Véase ORTELLS RAMOS, M., Objeto, *eficacia jurídica e impugnación del documento notarial. Reflexiones sobre el art. 17 bis, apartado 2, de la Ley del Notariado*, en Revista Crítica de Derecho Inmobiliario, núm. 684, julio-agosto, 2004, pág.2

LEC)[378]. El documento público goza de presunción de autenticidad, de modo que su poseedor no tiene la carga de demostrarla. Existe una previsión específica con respecto a los documentos electrónicos «notariales». El artículo 17 bis de la Ley Notariado dispone: «*los documentos públicos autorizados por Notario en soporte electrónico, al igual que los autorizados sobre papel, gozan de fe pública y su contenido se presume veraz e íntegro de acuerdo con lo dispuesto en esta u otras leyes*». Ello significa que los documentos electrónicos notariales gozan, al igual que los escritos, de la presunción de veracidad e integridad de su contenido, y que los documentos electrónicos notariales se sujetan a los mismos requisitos de impugnación de los documentos en soporte papel.

El documento público suele acceder al proceso mediante copia, certificación o testimonio y no mediante original, siendo la parte adversa quien tiene la carga de demostrar su eventual falta de exactitud, no correspondiendo a la parte aportante la carga de acreditar su exactitud. El mecanismo para comprobar la autenticidad del documento público consiste en el cotejo de las copias, certificaciones o testimonios con los originales y se practica por el secretario judicial (art. 320. 2 LEC). Lo anterior plantea una doble problemática: el artículo 320.2 LEC está pensado para el cotejo de documentos en soporte papel y no en soporte digital y el secretario judicial, encargado de comprobar la concordancia

[378] A tenor de los dispuesto en el artículo 319 relativo a la fuerza probatoria de los documentos públicos: «1. *Con los requisitos y en los casos de los artículos siguientes, los documentos públicos comprendidos en los números 1 a 6 del artículo 317 harán prueba plena del hecho, acto o estado de cosas que documenten, de la fecha en que se produce esa documentación y de la identidad de los fedatarios y demás personas que, en su caso, intervengan en ella. 2. La fuerza probatoria de los documentos administrativos no comprendidos en los números 5 y 6 del artículo 317 a los que las leyes otorguen el carácter de públicos, será la que establezcan las leyes que les reconozca tal carácter. En defecto de disposición expresa en tales leyes, los hechos, actos o estados de cosas que consten en los referidos documentos se tendrán por ciertos, a los efectos de la sentencia que se dicte, salvo que otros medios de prueba desvirtúen la certeza de lo documentado.3. En materia de usura, los tribunales resolverán en cada caso formando libremente su convicción sin vinculación a lo establecido en el apartado primero de este artículo*».

En resumen, tendrán el valor de prueba plena: Documentos públicos, en original, copia certificada o copias simples no impugnadas (art. 318 y 319 LEC); documentos públicos impugnados, que después del cotejo con la matriz resultan auténticos (art. 320 LEC); documentos públicos no susceptibles de cotejo, salvo prueba en contrario (art.322 LEC); documento privado no impugnado (art. 326.1 LEC). SAP Barcelona de 28.3.2007 (AC 2007\730); documento privado impugnado, que después de pruebas practicadas resulta auténtico (art. 326.2 LEC a contrario); instrumento de archivo de documento electrónico con firma electrónica avanzada o reconocida no impugnado (art. 3.8 LFE a contrario y art. 318, 319, 320, si es documento público y 326.1 y 326.2 LEC si es documento privado); instrumento de archivo con «documento electrónico» con firma electrónica avanzada o reconocida impugnado, que después de las pruebas practicadas resulta auténtico (art. 3.8 LFE y art. 326.2 LEC). RAMOS ROMEU, F. y CAÑABATE PÉREZ, J. *Los datos digitales en el proceso civil: prevención, producción y autenticación*, Revista Jurídica de Catalunya. Núm.1-2011, pág. 93.

de la copia, certificación o testimonio con el original carecerá, por lo general, de la formación técnica para efectuar dicha comprobación. Para obviar tal dificultad y que pueda efectuarse una comprobación será necesario que el secretario judicial cuente con el auxilio de un perito informático.

Finalmente señalar que en el supuesto de impugnación de autenticidad del documento electrónico, ya sea público o privado, si resulta la autenticidad del medio de prueba, los gastos de verificación corresponden al impugnante. Así RAMOS ROMEU y CAÑABATE PÉREZ efectúan algunas recomendaciones para que dicho principio no quede en papel mojado, en particular recomiendan en primer lugar, si ello es posible, en el momento de proponer el medio de prueba de la autenticidad, indicar a efectos informativos que la verificación resulta necesaria exclusivamente debido a la impugnación efectuada. Esto puede contribuir a evitar la discusión *a posteriori* sobre si el medio de prueba se refería también al principal o sólo a la autenticidad. Por ejemplo, puede discutirse si, propuesto un dictamen pericial para probar la autenticidad, no hubiera sido suficiente un requerimiento a un tercero con un coste significativamente inferior. Dado que normalmente estará presente la otra parte después no deberá darse pie a entender que el coste es excesivo. En segundo lugar, también será fundamental discutir sobre la necesidad de acudir a dicho medio de prueba o la existencia de medios alternativos más baratos, lo cual deberá efectuarse también en el momento de la proposición del medio de prueba de la autenticidad. En tercer lugar, realizar la petición expresa de que se impongan los gastos de dichos medios de prueba en sentencia. Dicha petición podrá efectuarse en el momento de las conclusiones, o en cualquier otro momento que corresponda. Téngase en cuenta que la decisión de imponer los gastos de impugnación debe resolverla el juez en la sentencia o resolución que pone fin al pleito, pronunciándose específicamente sobre los mismos. Y finalmente en caso de no existir resolución expresa, puede ser necesario pedir la aclaración o complemento de la sentencia (art. 214 y 215 LEC). Puede darse el caso de que la condena en costas no sea suficiente o incluso puede que no los cubra, o puede que no coincida el beneficiario de la condena en costas derivadas de la autenticidad del medio de prueba, y en caso de que coincidan la precisión no estaría de más[379].

La LEC prevé sanciones –multas de contenido económico- para los supuestos de impugnaciones temerarias cuando recaigan sobre documentos públicos o privados (arts. 320 y 326.2 LEC), y de igual modo, establece sancione la LFE respecto a los supuestos de impugnación de documentos electrónicos firmados por una firma electrónica reconocida (art. 3.8 LFE).

[379] Véase RAMOS ROMEU, F. y CAÑABATE PÉREZ, J. *Los datos digitales en el proceso civil: prevención, producción y autenticación*, Revista Jurídica de Catalunya. Núm.1-2011, pág. 92.

9.3.1.4. Problemas en cuando a la validez del documento original y la copia.

El original y la copia de un documento no tienen igual valor jurídico. Las peculiaridades propias del hecho electrónico hacen que no sea fácil distinguir en este ámbito un documento electrónico original de una copia. La discusión oscila entre quienes consideran que documento original sólo lo es el conservado en la memoria del soporte informático que lo crea y toda otra representación es copia, hasta quienes consideran que por la propia naturaleza del documento electrónico no puede diferenciarse entre original y copia. En rigor sólo podría ser original el creado en la memoria RAM del ordenador que por ser volátil termina volcándose en el disco duro, sin embargo, por ser poco operativo termina grabándose en cualquier tipo de soporte. De ahí que parte de la doctrina entienda que en el documento electrónico carece de sentido hablar de original y copia siempre que este tenga la virtud de asegurar autoría e integridad[380].

La legislación no prevé de forma expresa criterios específicos que nos permitan efectuar de forma clara tal distinción, aunque tanto a nivel internacional como nacional encontramos regulación sobre la copia. Así por ejemplo la Ley sobre Comercio Electrónico aprobada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) por resolución 51/162, de 16 de diciembre de 1996 hace referencia a ciertos criterios necesarios para poder considerar la información electrónica como original. Dicha norma dispone en su artículo 8.1 que cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos «*si existe alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos no en alguna otra forma*» y de requerirse que la información sea presentada si dicha información puede ser mostrada a la persona a que se deba presentar. En el primer caso ello será aplicable tanto sin el requisito en él previsto está expresado en forma de obligación, como si la ley simplemente prevé consecuencias en el caso de que la información no sea conservada o presentada en su forma original. Establece también dicha norma que la integridad de la información será evaluada conforme el criterio de que haya permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación. Y finalmente señala que el grado de

[380] En este sentido CANELO, C., ARRIETA, R., MOYA, R., ROMO R., *Documento electrónico, aspectos procesales*. Revista Chilena de Derecho Informático. págs. 88-89, puede consultarse en la dirección electrónica http://goo.gl/drTQD

fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso.

En España la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP), reconoció el derecho de los ciudadanos a relacionarse electrónicamente con las Administraciones, recogiendo un expreso mandato a las mismas de imponer las relaciones electrónicas con los ciudadanos (artículo 42.3). En consecuencia y para poder llevar a cabo dicho mandato el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica estableció en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas. Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se están desarrollando y perfeccionando a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica. Dentro de este conjunto de Normas Técnicas de Interoperabilidad, encontramos las normas relativas al documento electrónico, al expediente electrónico, a la digitalización de documentos en soporte papel, a los procedimientos de copiado auténtico y conversión y a la política de gestión de documentos electrónicos que responden a lo previsto en el citado Real Decreto 4/2010, de 8 de enero, sobre interoperabilidad, recuperación y conservación del documento electrónico, a la luz de la necesidad de garantizar todos estos aspectos para el documento electrónico a lo largo del tiempo.

En particular y a los efectos del tema que aquí tratamos la Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de «*Procedimientos de copiado auténtico y conversión entre documentos electrónicos*» establece las reglas para la generación y expedición de copias electrónicas auténticas, copias papel auténticas de documentos públicos administrativos electrónicos y para la conversión de formato de documentos electrónicos por parte de las

Administraciones públicas[381]. En su apartado IIII dicha norma regula las «características generales» de las copias electrónicas auténticas estableciendo que: *«…1) Las copias electrónicas generadas que, por ser idénticas al documento electrónico original no comportan cambio de formato ni de contenido, tendrán la eficacia jurídica de documento electrónico original; 2) las copias auténticas se expedirán a partir de documentos con calidad de original o copia auténtica; 3) las copias electrónicas auténticas serán nuevos documentos electrónicos que incluirán total o parcialmente el contenido del documento sobre el que se expiden y que cumplirán con lo establecido en la Norma Técnica de Interoperabilidad de Documento electrónico; 4) el valor de cada uno de los metadatos mínimos obligatorios del documento electrónico copia será asignado en función de las características propias de cada metadato y de las propiedades específicas del documento bajo la responsabilidad del órgano u Organismo que lo expide; 5) la relación entre la copia electrónica auténtica y el documento origen se reflejará en los metadatos del documento electrónico copia a través del metadato «Identificador del documento origen» que tomará el valor del identificador de aquél; y 6) las copias electrónicas auténticas serán firmadas mediante alguno de los sistemas de firma previstos en los artículos 18 ó 19 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos».*

En el ámbito del proceso judicial las partes podrán presentar determinados documentos mediante copia y por otro lado deberán aportar también copias de los documentos aportados como medio de prueba para las demás partes intervinientes en el proceso a fin de garantizar el principio de contradicción, aún cuando no existe alusión específica en la LEC, ya que el art. 273 alude tan sólo a escrito y documento. Tal exigencia puede deducirse, con carácter general, de los principios de defensa y contradicción que informan el proceso civil.

La Ley 18/2011 de 5 de julio reguladora del uso de las tecnologías de la información y la Comunicación en la administración de justicia al regular en el capítulo II del Título IV el «expediente judicial electrónico» regula en su art. 28 qué debe entenderse por «copia auténtica» al señalar «*1. Las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el propio interesado o por las oficinas judiciales, manteniéndose o no el formato original, tendrán inmediatamente la consideración de copias auténticas con la eficacia prevista en las leyes procesales, siempre que el documento electrónico original se encuentre en poder de la oficina judicial donde haya sido originado o incorporado y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan comprobar la coincidencia con dicho documento. Si se alterase el formato original, deberá incluirse en los metadatos la condición de copia.*

[381] Para los aspectos relativos a la gestión de los documentos resultantes del proceso de copiado auténtico o conversión se remite a la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

Tendrán, asimismo, la consideración de copias auténticas «*…2. Las copias realizadas por las oficinas judiciales, utilizando medios electrónicos, de documentos emitidos originalmente por ellas en soporte papel»*. Por otro lado, también prevé en su apartado tercero que las *oficinas judiciales puedan «… obtener imágenes electrónicas de los documentos privados aportados por los ciudadanos, con su misma validez y eficacia, a través de procesos de digitalización que garanticen su autenticidad, integridad y la conservación del documento imagen, de lo que se dejará constancia. Esta obtención podrá hacerse de forma automatizada, mediante el correspondiente sello electrónico». «…4. A los documentos emitidos originalmente en soporte papel de los que se hayan efectuado copias electrónicas de acuerdo con lo dispuesto en este artículo, se les dará el destino previsto en la normativa vigente en materia de archivos judiciales.* Y finalmente establece que *«…5. Las copias realizadas en soporte papel de documentos judiciales electrónicos y firmados electrónicamente por el secretario judicial tendrán la consideración de copias auténticas, siempre que incluyan la impresión de un código seguro de verificación que permita contrastar su autenticidad mediante el acceso a los archivos electrónicos de la oficina judicial emisora».*

Por su parte, la Ley del Notariado, en su artículo 17 bis, efectúa una aclaración de qué debe entenderse por «copia» indicando que «*los instrumentos públicos a que se refiere el artículo 17 de esta Ley, no perderán dicho carácter por el sólo hecho de estar redactados en soporte electrónico con la firma electrónica avanzada del Notario y, en su caso, de los otorgantes o intervinientes, obtenida la de aquel de conformidad con la ley reguladora del uso de la firma electrónica por parte de los notarios y demás normas complementarias*». Las copias autorizadas de las matrices podrán expedirse y remitirse electrónicamente, con firma electrónica avanzada, por el Notario autorizante de la matriz o por quien le sustituya legalmente. Dichas copias sólo podrán expedirse para su remisión a otro notario o a un registrador o a cualquier órgano de las administraciones públicas u órgano jurisdiccional, siempre en el ámbito de su respectiva competencia y por razón de su oficio. Las copias simples electrónicas podrán remitirse a cualquier interesado cuando su identidad e interés legítimo le consten fehacientemente al notario. Si las copias autorizadas, expedidas electrónicamente, se trasladan a papel, para que conserven su autenticidad y garantía notarial, dicho traslado deberá hacerlo el notario al que se le hubiere remitido. Las copias electrónicas se entenderán siempre expedidas por el notario autorizante del documento matriz y no perderán su carácter, valor y efectos por el hecho de que su traslado a papel lo realice el notario al que se le hubiere enviado, el cual signará, firmará y rubricará el documento haciendo constar su carácter y procedencia.

Los Registradores de la Propiedad y Mercantiles, así como los órganos de las Administraciones públicas y jurisdiccionales, también podrán trasladar a soporte papel las copias autorizadas electrónicas que hubiesen recibido, a los únicos y exclusivos efectos de incorporarlas a los expedientes y archivos que correspondan por razón de su oficio en el ámbito de su respectiva competencia. Las copias electrónicas sólo serán válidas para la concreta finalidad para la que fueran solicitadas, lo que deberá hacerse constar expresamente en cada copia indicando dicha finalidad. En lo no previsto en esta norma la expedición de copia electrónica queda sujeta a lo previsto para las copias autorizadas en la Ley notarial y su Reglamento.

9.3.1.5 Juicio de admisión de la prueba documental.

Una vez propuesta la prueba el Juez dictará resolución admitiendo o inadmitiendo la misma. El juez estará sujeto a los criterios de admisión de cualquier prueba, pertinencia, utilidad y legalidad (art. 283 LEC). La prueba debe ser pertinente, es decir, debe tener relación con el *thema decidendi*, y debe proponerse en tiempo y forma (arts. 284, 414.1, 429.1, 435.1, 444.4 y 460.2 LEC). Debe ser útil, es decir, debe inadmitirse aquella prueba que según reglas y criterios razonables y seguros, en ningún caso pueda contribuir a esclarecer los hechos controvertidos (art. 283.2 LEC). En el supuesto que el juez decida inadmitir una prueba debe razonar la inadmisión sin que dicha resolución pueda incurrir en incongruencia, irrazonabilidad o arbitrariedad (STC de 14 de enero de 2004)[382].

El régimen de recursos frente a la admisión o inadmisión de la prueba documental electrónica es el común al resto de los medios de prueba. En el juicio ordinario, frente la admisión o inadmisión de las pruebas documentales electrónicas cabrá un recurso de reposición de interposición, substanciación y resolución oral (art. 285.1 LEC) y si fuere desestimado, la parte perjudicada podrá formular protesta a los efectos de hacer valer sus derechos en la segunda instancia (art. 285.2 LEC). En el juicio verbal, frente a la inadmisión de una prueba documental electrónica o la admisión de una prueba electrónica de las que se denunciara como obtenidas con violación de derechos fundamentales, las partes podrán formular protesta a los efectos de hacer valer sus derechos en segunda instancia (art. 446 LEC). En el juicio verbal, pues, no cabe protesta contra la admisión de una prueba documental electrónica que la parte considera impertinente, inútil o que infringe la legalidad del procedimiento.

[382] STC 14 enero 2004, fto. jco.2º, (EDJ 2004/389).

La impugnación del juicio de admisión de la prueba documental electrónica dependerá fundamentalmente de los criterios de temporalidad (momento de acceso al proceso) y legalidad (requisitos legales de acceso al proceso) a que hemos hecho referencia. Partiendo de dichos requisitos legales, y supliendo por vía analógica las lagunas legales, señalar que la admisión de la prueba documental electrónica deberá analizarse en cada caso concreto, siquiera con carácter general puede afirmarse, en primer lugar, que los «medios e instrumentos» fundamentales, serán en principio siempre admitidos, salvo escasas excepciones, principalmente formales. Por otro lado, los «medios e instrumentos» complementarios podrán inadmitirse por no reunir tal carácter, sino el de fundamentales (art. 265.1.2º LEC). Los «medios e instrumentos» aportados en un documento no inicial, esto es, en los supuestos del artículo 270 LEC, podrán impugnarse por ser de fecha anterior a la demanda y contestación o haberse podido confeccionar con anterioridad (art. 270.1 LEC), por no justificarse el desconocimiento del medio o instrumento (art. 270.2 LEC), o por no acreditarse la falta de disponibilidad inicial del «medio o instrumento» (art. 270.3 LEC). Los «medios e instrumentos» aportados por vía de diligencias finales podrán impugnarse por no referirse a hechos nuevos o de nueva noticia o no ser anteriores al momento de formular conclusiones, o no ser decisivos en términos del fallo (art. 271.2 LEC). Y finalmente, los «medios e instrumentos» requeridos de exhibición se podrán impugnar: por falta de los requisitos previstos para la exhibición entre parte (328 LEC) –como puede ser por ejemplo la falta de disponibilidad del medio o instrumento-; por falta de requisitos para la exhibición por terceros (art. 329 LEC) – como puede ser por ejemplo que el medio o instrumento no tienen el carácter de trascendente para dictar sentencia-; o por falta de requisitos para la exhibición por las entidades oficiales (art. 333 LEC) –como puede ser, por ejemplo, que se trate de medios o instrumentos de carácter reservado-[383].

9.3.2 Interrogatorio de las partes y los testigos

Los medios de prueba más eficaces a la hora de probar el hecho electrónico son la prueba documental y la prueba pericial. La primera referida a la manifestación del hecho electrónico y la segunda relativa al hecho electrónico desde un punto de vista técnico. No obstante, la manifestación del hecho electrónico puede probarse en juicio a través de otros medios de prueba como las pruebas personales, es decir, el interrogatorio de parte o el interrogatorio de testigos. En

[383] Véase ABEL LLUCH, X. *La prueba electrónica*, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.4, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, págs.180 a 182.

juicios de poca cuantía los interrogatorios de partes y testigos son por lo general las únicas pruebas propuestas o se complementan junto a la prueba documental. La prueba pericial suele resultar demasiado costosa económicamente y en pleitos de poca cuantía puede incluso rebasar el propio importe del pleito por lo que la parte opta la mayor parte de las veces por no proponerla.

9.3.2.1 Interrogatorio de las partes

La prueba de interrogatorio de las partes es una declaración oral de conocimiento sobre hechos controvertidos prestada, durante el proceso, por una parte –o por terceros en los supuestos previstos en la ley- a instancia de la adversa o colitigante[384].

El interrogatorio de las partes se compone de elementos subjetivos, objetivos y formales. Son elementos subjetivos las partes (actor/es y demandados) y otros terceros cualificados el titular de la relación controvertida (art. 301.2 LEC), el tercero con conocimiento personal de los hechos (art. 308 LEC) y la persona que tuvo intervención personal en los hechos en nombre de la persona jurídica (art. 309 LEC). El interrogatorio es un acto personalísimo, sin posibilidad de delegación o apoderamiento, a salvo los supuestos de declaración de tercero. Partiendo de un punto de vista objetivo la declaración que presta la parte deberá versar sobre hechos conocidos por la parte declarante («*de los que tenga noticia*») y sobre hechos controvertidos («*que guarden relación con el objeto del juicio*»). El interrogatorio podrá versar sobre hechos personales y sobre hechos no personales del interrogado (arts. 301 y 308 LEC). Y finalmente, entre los requisitos formales se hallan la exigencia de que la declaración de la parte se preste oralmente en el curso de un proceso y a instancia de la parte adversa o, en algunos supuestos a instancia del colitigante. La declaración durante un proceso presidido por la inmediación y la concentración en la práctica de las pruebas comporta la oralidad, siquiera aún persiste la forma de respuestas escritas para la práctica del interrogatorio de Administraciones y Organismos Públicos (art. 315 LEC)[385].

[384] Así la define ABEL LLUCH, X. en *El interrogatorio de partes en la Ley 1/2000, de Enjuiciamiento Civil*, ed. Bosch, 2008, pág. 30.

[385] Véase ABEL LLUCH, X. *El interrogatorio de partes en la Ley 1/2000, de Enjuiciamiento Civil*, ed. Bosch, 2008, pág. 29-30.

Especial referencia debemos efectuar respecto a la capacidad para ser interrogado en el juicio. El menor de edad no podrá exigir ni someterse a interrogatorio de parte ya que carece de capacidad procesal (art. 7.1 LEC), debiendo solicitar y rendir interrogatorio su representante legal. La única excepción será el menor emancipado a quien se reconoce capacidad para comparecer en juicio y por ende capacidad procesal (art. 323.II Cc). De igual modo el incapaz tiene limitada su capacidad de obrar por lo que su capacidad procesal deberá suplirse por su representante legal, en el caso que haya recaído sentencia de incapacitación deberá estarse a la extensión y límites de la misma.

El juez, al igual que en los demás medios de prueba, declarará la pertinencia de la prueba de interrogatorio de las partes si concurren los presupuestos de admisibilidad, necesidad, pertinencia, utilidad y licitud. La vigente LEC no exige la formulación del interrogatorio con preguntas escritas salvo casos concretos como el interrogatorio domiciliario, del interrogatorio por vía de auxilio judicial e interrogatorios de organismos públicos (art. 290 LEC). El interrogatorio se caracteriza por la oralidad y la inmediación del juez.

La prueba de interrogatorio de las partes se practicará en primer lugar en el juicio, aunque el Juez puede acordar otro orden en la práctica de las pruebas de oficio o a instancia de parte (art. 300.1 LEC). En primer lugar, formulará las preguntas el letrado proponente y con posterioridad los letrados de las demás partes y por último el letrado de aquélla que declare. También podrá formular preguntas el tribunal para obtener aclaraciones y adiciones (art. 306.1 LEC). En el supuesto de que no intervengan abogados por no ser preceptivo las partes, con la venia del tribunal, podrán hacerse recíprocamente preguntas y afirmaciones (art. 306.2 LEC). Las preguntas deben ser formuladas en sentido afirmativo, con la debida claridad y precisión, sin incluir valoraciones ni calificaciones y referidas a los hechos litigiosos (art. 302 LEC). Por su parte, el interrogado responderá por sí mismo sin valerse de ningún borrador de respuestas, pero se le permitirá consultar documentos y notas o apuntes como auxilio a su memoria (art. 305.1 LEC). Las respuestas serán afirmativas o negativas, y de no ser posible se exige que sean precisas y concretas, pudiendo agregar aquellas explicaciones que estime convenientes y que guarden relación con las cuestiones planteadas (art. 305.2 LEC).

Salvo que exista la obligación de guardar secreto, la ley prevé para el supuesto que la parte se negare a declarar que puedan considerarse reconocidos como ciertos los hechos a que se refieren las preguntas, ello siempre y cuando se tratare de hechos personales del declarante y que le fuesen perjudiciales en todo o en parte (art. 307.1 LEC). El reconocimiento de los hechos (art. 301 LEC) supondrá, si no contradice el resultado de las demás pruebas, la certeza de los hechos expuestos por el confeso, siempre que éste haya intervenido

personalmente en los mismos, y su fijación como ciertos le sean enteramente perjudiciales (art. 316 LEC). En otro caso, se valorará la declaración por parte del juez según las reglas de la sana crítica. Respecto a la obligación de guardar secreto se aplicará analógicamente lo previsto en el artículo 371 LEC en sede de prueba testifical ya lo sea por razón de estado o profesión (art. 371.1 LEC), ya lo sea por tratarse de materia declarada reservada o secreta (art. 371.2 LEC)

9.3.2.2 Interrogatorio de testigos

El interrogatorio de testigos es un medio de prueba personal en virtud del cual una persona ajena al juicio presta declaración sobre los hechos presenciados (vistos u oídos) por ella o que ha sabido de referencia.

Es tercero a efectos de la prueba testifical quien no forma parte del órgano jurisdiccional ni es parte directa o indirecta, excluyendo a cualquier litigante, aunque por razones de lugar, de tiempo o de forma no hayan comparecido en el en el proceso, y a aquellos sujetos que representan o dirigen actividades de las partes, como son sus procuradores o abogados[386]. Respecto a los representantes legales puede ser de aplicación lo previsto en los artículos 308 y 309 LEC.

Los testigos pueden ser personas físicas o jurídicas. En cuanto a las personas físicas, podrán ser testigos todas las personas, salvo las que se hallen permanentemente privadas de razón o del uso de sentidos respecto de hechos sobre los que únicamente quepa tener conocimiento por dichos sentidos. Los menores de catorce años podrán declarar como testigos si, a juicio del tribunal, poseen el discernimiento necesario para conocer y para declarar verazmente (art. 361 LEC). Salvo que haya recaído una declaración judicial de incapacidad prohibiendo la declaración en juicio de una persona, puede resultar idónea una persona presuntamente incapaz como testigo, siempre que posea razón suficiente en el momento de la percepción y declaración, dado que los motivos de incapacidad siempre han de interpretarse restrictivamente (ej. Sujeto presuntamente incapaz por trastornos mentales transitorios con intervalos lúcidos). E inversamente, puede resultar idónea una persona, aún no incapacitada, si carece de razón suficiente (ej. un sujeto sin declaración judicial de incapacitación y con un trastorno mental permanente). Puede admitirse la declaración del testigo en intervalo lúcido si se dio tanto en el momento de la

[386] Véase GUASP DELGADO, J. Derecho *Procesal Civil,* Madrid, 3ª ed., 1968 (1ª reimp., 1973), T. 1, pág. 368.

percepción como en el momento de la declaración[387]. Las personas jurídicas o entidades públicas también pueden ser propuestas como testigos (art. 381 LEC). De naturaleza discutida, se trata en realidad de una prueba de informes sujeta a un posterior trámite de aclaraciones o de contradicción. Trámite de aclaraciones singular en cuanto no se circunscribe al autor del informe, permitiéndose incluso que sea una persona desvinculada con la persona jurídica o entidad pública informante. La ley regula detalladamente en procedimiento probatorio (art. 381 LEC).

No están obligados a declarar como testigos aquellos que estén obligados a guardar secreto o cuando su declaración verse sobre materias legalmente reservadas o clasificadas (art. 371 LEC).

La LEC regula en el artículo 370.4 la figura del testigo-perito como testigo cualificado, es decir, se trata de aquel testigo con conocimientos científicos, técnicos, artísticos o prácticos sobre la materia a que se refieran los hechos del interrogatorio. Lo que permitirá al juzgador no solo aceptar el interrogatorio sino también juicios por aplicación de dichos conocimientos, pero solo en cuanto a los hechos percibidos.

El interrogatorio de los testigos se practicará en segundo lugar en el juicio, aunque el Juez puede acordar otro orden en la práctica de las pruebas de oficio o a instancia de parte (art. 300.1 LEC). Antes del inicio del interrogatorio de preguntas al testigo, la ley exige que éste preste juramento o promesa de decir verdad con la conminación de las penas establecidas para el delito de falso testimonio en causa civil (art. 458.1 y 460 CP), de las que le instruirá el tribunal si manifestara ignorarlas (365.1 LEC). Cuando se trate de testigos menores de edad penal, no se le exigirá juramento ni promesa de decir verdad (art. 365.2 LEC). Una vez contestadas la preguntas generales reguladas en el art. 367 LEC (nombre, relación con las partes etc.) el testigo será examinado por la parte que lo hubiera propuesto, y si hubiera sido propuesto por ambas partes, se comenzará por las preguntas que formule en demandante (art. 370.1 LEC).

Los hechos sobre los que es interrogada deben ser hechos controvertidos relativos a lo que sea objeto de juicio (art. 360 LEC), es decir, deben tener relevancia procesal. Deberán versar sobre conocimientos propios del mismo (art. 368.3 LEC). Las preguntas deben formularse oralmente, con la debida claridad y precisión, y prescindiendo de calificaciones y valoraciones (art. 368.1

[387] Véase ABEL LLUCH, X., El *interrogatorio de testigos*, en la obra en la obra colectiva del mismo título, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.4, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, 2008, pág. 41.

LEC)[388]. Y las respuestas del testigo deberán serlo de palabra, sin valerse de ningún borrador de respuestas (art. 370.2 LEC) y expresando la razón de la ciencia de lo que diga (art. 370.3 LEC) la razón de la ciencia se identifica con la fuente o motivo del conocimiento y «*supone una justificación de la declaración, es decir, la expresión del cómo, cuándo, y donde se percibió lo que se declara*» (SAP Santa Cruz de Tenerife 19 de junio de 2006[389]).

En el ámbito de las tecnologías de la información y comunicación y en concreto en el ámbito informático si bien toda testifical tiene por objeto prestar declaración sobre unos hechos presenciados (vistos u oídos) por el testigo o que ha sabido de referencia, podemos distinguir aquellos supuestos en que la testifical tiene por objeto solo y exclusivamente manifestar un hecho presenciado u oído, que implica el uso de tecnologías de la información y comunicación y que se ha producido de una forma por lo general espontánea, de aquellos otros en que la prueba testifical además de poner en conocimiento del juez los hechos presenciados tiene una finalidad garantista. Es decir, pretende más allá de transmitir el conocimiento de un hecho que supone el empleo de medios o dispositivos electrónicos, garantizar que una determinada actividad se ha efectuado conforme a la ley sin menoscabar los derechos protegidos constitucionalmente, o por ejemplo, garantizar la identificación de una prueba obtenida por un tercero. En estos últimos supuestos existe un requerimiento previo al sujeto para que presencie una actividad, y el testigo no lo puede ser por referencia, por cuanto la finalidad de garantía perseguida perdería su objeto.

Veamos algunos ejemplos. Nos hallaríamos en el caso del testigo que presta declaración de un hecho visto u oído sin otra finalidad de que el juez pueda valorar la certeza del mismo, por ejemplo, cuando una persona declara en juicio que ha visto como el sujeto X ha escrito en un ordenador un correo electrónico con el destinatario Y ha pulsado a través del ratón con el cursor que ve en el monitor del ordenador a enviar; o ha oído a la persona X comentar que había enviado un correo electrónico con determinado contenido a la persona Y. Otros supuestos serían aquellos en que el testigo tiene conocimiento del hecho por referencia de terceras personas, es decir, la persona X le comentó que Y había enviado un correo electrónico a Z.

[388] La exigencia del sentido afirmativo de la pregunta en el interrogatorio de los testigos ha sido suprimida del artículo 368.1 LEC por la Ley 13/2009, de 3 de noviembre, de reforma de la legislación procesal para la implantación de la Oficina Judicial.

[389] SAP Santa Cruz de Tenerife, secc. 1ª, de 19 de junio de 2006, fdo. Jco. 2º (EDJ 2006/280524).

Distintos de los anteriores son aquellos casos en los que además la prueba testifical cumple con una función garantista. A modo de ejemplo, son supuestos en que habitualmente se requiere la presencia de testigos: a) El registro de dispositivos electrónicos en el ámbito corporativo o empresarial en casos de mal uso de los mismos por los trabajadores; b) o los supuestos en que se efectúan copias de un archivo desde un disco rígido a un soporte externo (por ej. un disquete) por parte de expertos en informática-forense. Es estos casos el testigo podrá afirmar que el archivo del disco precedía al del disquete evitando que se afirme que la situación ha sido la inversa. Recordemos que por la naturaleza específica de la prueba electrónica, ésta no se somete al clásico y reconocido principio lógico de identidad, en los archivos digitales dos archivos iguales bit a bit no son similares sino idénticos y es imposible determinar cual es copia de cual, sin recurrir a otros medios secundarios para establecer la precedencia[390].

El testigo que además de prestar declaración sobre los hechos vistos u oídos tiene conocimientos técnicos, científicos o prácticos sobre la materia objeto de interrogatorio declarará en juicio en calidad de testigo perito (art. 370.3 LEC). Esta figura es de especial utilidad en la prueba de hechos electrónicos, en cuanto no sólo se valorará el conocimiento personal de los hechos por parte del mismo, sino también se admitirán por parte del juez manifestaciones efectuadas por aquél sobre conocimientos técnicos o prácticos siempre referidos a los hechos percibidos. Se trata en este supuesto de una pericial especializada en cuanto se trata de un testigo cualificado que posee conocimientos técnicos. En este caso el testigo se diferencia del perito en cuanto el testigo tiene un conocimiento histórico de los hechos enjuiciados, mientras que el perito es requerido expresamente para estudiar un hecho con trascendencia para un eventual proceso sin previo conocimiento (SAP Coruña, de 31 de mayo de 2006[391]). Un ejemplo de testigo perito lo sería el informático que es llamado a declarar en juicio sobre el hecho de haber observado determinados archivos en un ordenador que se le dejó en su día para reparar.

El interrogatorio de los testigos podrá emplearse como medio de prueba, sujeta de igual modo a las reglas de la sana crítica, y siempre tomando en consideración la razón de ciencia que hubieren dado, las circunstancias que concurrieren en los testigos, y en su caso, las tachas formuladas y los resultados de la prueba que sobre éstas se hubieran practicado (art. 376 LEC).

---

[390] DARAHUGE, M.E Y ARELLANO GONZALEZ, L.E. *Manual de Informática Forense (Prueba Indiciaria Informático Forense)*, Ed. Errepar, 2012, pág.25.

[391] SAP Coruña, de 31 de mayo de 2006, fdo. Jco. 2º (EDJ 2006/94811).

9.3.2.3 Careo

La vigente LEC recoge el careo de testigos atribuyendo al titular del órgano jurisdiccional la facultad de acordar a instancia de parte o de oficio, que se celebre careo entre las partes y alguno o algunos testigos (art. 373.2 LEC) o de estos entre sí. En este último caso, la ley exige expresamente que hayan de incurrir en graves contradicciones (art. 373.1 LEC). Lo cual parece exigirse también en el supuesto de que entre las declaraciones de las partes y alguno o algunos testigos existan divergencias que sean consideradas de gravedad por el juzgador.

El legislador, siguiendo una jurisprudencia consolidada y recaída en el proceso penal, conceptúa el careo como una diligencia complementaria de prueba, con carácter instrumental, excepcional y subsidiario. Es una diligencia instrumental por cuanto sirve de cauce para la confrontación de otros medios de prueba, cuales son las declaraciones prestadas a través del interrogatorio de testigos o de partes, o en otras palabras es un instrumento de verificación y contraste de la fiabilidad de otras pruebas (STS 18 de marzo de 1997). Es excepcional porque su adopción se restringe no a la apreciación de cualquier discrepancia sino de «graves contradicciones» (art. 373.1 LEC); es subsidiaria (STC 55/1984, de 7 de mayo) porque únicamente se deberá recurrir a ella cuando los hechos probados no puedan deducirse a través de otros medios probatorios[392].

La Ley de Enjuiciamiento Civil no regula cómo debe practicarse el careo. Únicamente precisa que habrá de solicitarse al término del interrogatorio, en cuyo caso se advertirá al testigo que no se ausente para que dichas actuaciones puedan practicarse a continuación (art. 373.3 LEC). Un modo correcto de practicar el careo es observando el siguiente orden: a) Lectura o, preferiblemente la reproducción de la grabación de las previas declaraciones testificales (o en su caso, de parte), pues el acta del Secretario Judicial no suele recoger con todo extensión y detalle las declaraciones de los testigos o las partes, ni tampoco ello constituye una exigencia legal en aquellas actuaciones que, por imperativo legal, deban registrarse en soporte apto para la grabación o reproducción (Art. 146.2 LEC); b) Las advertencias a los careados sobre el modo de llevar a cabo la diligencia, comprensivas de los deberes de guardar turno de palabra, no interrumpirse y respetar a la adversa, así como del recordatorio que la declaración se efectúa bajo juramento o promesa de decir verdad (art. 365.1 LEC) y la sanción por el delito de falso testimonio (art. 458 LEC); c) La

[392] Véase ABEL LLUCH, X., *El interrogatorio de testigos*, en la obra en la obra colectiva del mismo título, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.4, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, pág. 94.

delimitación de la contradicción, esto es, de los extremos objeto de careo, a fin de evitar una reiteración de las previas declaraciones testificales; y finalmente d) La discusión o careo propiamente dicho, mediante una declaración oral y cruzada de los testigos (o en su caso, entre el testigo y la parte) dirigida por el juez, a cuyo efecto puede ser útil interesar de cada uno de los careados, y respecto de cada extremo, si se ratifican en su previa declaración o tienen algo que rectificar indagando, en su caso, sobre los motivos de la rectificación[393].

El careo solo resultará efectivo si se los declarantes están incomunicados, y se practica en unidad y concentración del acto de todos los declarantes[394].

9.3.3 Reconocimiento Judicial

El reconocimiento judicial es un medio de prueba en virtud del cual el Juez examina directamente, a través de cualquiera de los sentidos, un lugar, un objeto o una persona y de los cuales extrae percepciones y apreciaciones relevantes para el proceso[395].

La prueba de reconocimiento judicial en procesos en que intervengan tecnologías de la información y comunicación puede tener por objeto lugares u objetos no virtuales pero relacionados con medios o dispositivos electrónicos-supuestos de reconocimiento del espacio en que se hallan medios o dispositivos electrónicos, éstos por sí mismos, o sus conexiones a otros etc., o puede tener lugar a través de espacios virtuales. En este segundo caso, el reconocimiento judicial permitirá al juez tener, a través de navegación por la red o cibernavegación, una percepción directa de espacios u objetos virtuales. No obstante, debemos tener en cuenta que la visualización por parte del juez de una página web o un dato que se halle en la misma, o la visualización de la cuenta de correo de una persona donde se encuentra un e-mail, no garantiza más que la visualización del espacio virtual que ve y que puede haber sido

[393] Véase ABEL LLUCH, X.*, El interrogatorio de testigos*, en la obra en la obra colectiva del mismo título, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.4, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, pág. 97-98.

[394] Véase FERNÁNDEZ SEIJÓ, J.M, *Comentario al artículo 373*, en el "Proceso Civil", Vol. III, ed. Tirant Lo Blanch, Valencia, 2004, pág. 2663.

[395] Véase ABEL LLUCH, X., *El reconocimiento judicial*, en la obra colectiva obra La prueba de reconocimiento judicial, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.6, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, pág.32.

creado ficticiamente, alterado o sustituido. Es por ello que carece de utilidad proponer una prueba de reconocimiento judicial cuando exista impugnación de la inexactitud o autenticidad de un documento, como la impresión en papel de un correo electrónico o de una página web (art. 326.2 LEC), por cuanto la única prueba capaz de determinar la inexactitud o autenticidad de tales documentos es la prueba pericial. Tengamos en cuenta que incluso tratándose de documento público el mecanismo para comprobar su autenticidad consiste en el cotejo de las copias, certificaciones o testimonios con los originales, y se practica por el secretario judicial (art. 320. 2 LEC). Lo anterior plantea una doble problemática: Por un lado el artículo 320.2 LEC está pensado para el cotejo de documentos en soporte papel y no en soporte digital; y por el otro el secretario judicial, encargado de comprobar la concordancia de la copia, certificación o testimonio con el original carecerá, por lo general, de la formación técnica para efectuar dicha comprobación. Para obviar tal dificultad y que pueda efectuarse una comprobación será necesario que el secretario judicial cuente con el auxilio de un perito informático forense.

En cuanto a los requisitos temporales de proposición de dicho medio de prueba se efectuará en el juicio ordinario en fase de audiencia previa y en el juicio verbal durante la vista. La parte proponente deberá precisar: a) los extremos principales objeto del reconocimiento (art. 353.1 LEC); b) si desea concurrir a la prueba del reconocimiento con alguna persona técnica o práctica en la materia (art. 353.1 LEC) - No es necesario identificar la persona en la audiencia previa o juicio-; y c) si el reconocimiento judicial se llevará cabo en la sede del tribunal, aportando (o no) los medios técnicos para su práctica, o, por el contrario, el juez deberá desplazarse al lugar donde se encuentra el ordenador. A la vista de la proposición del reconocimiento efectuada por la parte proponente, las demás partes personadas podrán proponer la ampliación del reconocimiento judicial a otros extremos distintos e indicar, igualmente, si proponen una persona técnica o práctica (art. 353.2 LEC). En la misma audiencia previa o en la vista del juicio verbal, el juez admitirá (o, en su caso, denegará) el reconocimiento propuesto, precisando los extremos del mismo, si se admite la presencia del técnico o práctico propuesto y el lugar en que debe practicarse. La ley atiende para su admisión a los criterios de «necesidad» y «conveniencia» favoreciendo la práctica de dicha prueba y abandonando el carácter de necesaria entendido como imposibilidad de acudir a otro medio de prueba, que se derivaba de la LEC 81. Sin embargo, los costes temporales hacen reacios a los jueces a su admisión, lo cual es contrario al derecho de prueba de las partes reconocido constitucionalmente y que debe prevalecer.

Una vez acordada la práctica de dicha prueba el Secretario señalará con cinco días de antelación, por lo menos, el día y la hora en que haya de practicarse el mismo (art. 353.3 LEC). Al acto de reconocimiento judicial además del juez y el

secretario judicial pueden concurrir con carácter facultativo las partes, sus abogados y procuradores (art. 354.2 LEC). Las partes también podrán concurrir a dicho acto auxiliándose de personas técnicas o prácticas en la materia si así lo hubiesen solicitado y se hubiese admitido. Respecto a la naturaleza de las personas «técnicas» o «prácticas» se las ha asimilado: a los peritos, pero no emiten dictamen ni pueden ser objeto de recusación o tacha; a los testigos, pero no se les formulan preguntas ni repreguntas, ni declaran sobre hechos del proceso; como testigos-peritos, pero no declara sobre hechos históricos y es fungible; y como asistentes de las partes. Aunque la posición más acertada es la que considera que se trata de sujetos auxiliares del reconocimiento judicial, que pueden ser interrogados sobre las peculiaridades de la cosa pero no sobre los restantes hechos del proceso[396].

El reconocimiento judicial, cuando no deba llevarse a cabo fuera de la sede del tribunal, se practica el día del juicio o vista, y como regla general, siguiendo el orden en la práctica de los medios de prueba, después del interrogatorio de las partes, de testigos y de la contradicción de los peritos, a salvo que el juez, de oficio o a instancia de parte, aprecie la concurrencia de circunstancias que permitan alterar dicho orden (art. 300 LEC). También podrá practicarse como prueba anticipada (art. 294 LEC) y como diligencia final (art. 435 LEC)[397]. La práctica de reconocimiento judicial como prueba anticipada exige se lleve a cabo mediante contradicción (art. 295 LEC), no siendo en este sentido efectiva por cuanto existe la posibilidad de que los hechos electrónicos puedan falsificarse, alterarse o intentar borrarse. Es por ello, que la única vía de que se dispone en la práctica para preservar la prueba es la medida de aseguramiento (art.298 LEC), en la que si bien como regla general se exige la audiencia de la contraparte antes de ser acordada (art. 298.4 LEC), está prevista la posibilidad de acordar la medida sin audiencia cuando exista el riesgo de que se destruyan pruebas o se imposibilite su práctica (art. 298.5 LEC) [398].

---

[396] Véase ABEL LLUCH, X., *El reconocimiento judicial*, en la obra colectiva obra La prueba de reconocimiento judicial, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.6, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, págs. 85-86.

[397] También se regula en la LEC la práctica de reconocimiento judicial en la adopción de medidas cautelares (art. 734 LEC).

[398] La medida de aseguramiento se hace necesaria para preservar la evidencia electrónica. «….Si no se concede la medida, el demandado puede eliminar la prueba ante la notificación de la demanda. Suponer que no lo hará es tan posible y probable como suponer que se allanará (que en caso de certeza, hace innecesaria la demanda)». «…*La recuperación de los archivos borrados, como casi todo en Criminalística en general y en Informática forense en particular, depende de la inexperiencia del actor que realiza la acción de borrado. Existen mecanismos de borrado seguro establecidos y normados por instituciones de nivel de credibilidad del FBI y el IEEE de los EE.UU.) que aseguran la irrecuperabilidad absoluta de los datos eliminados. Aún en el mejor de los casos,*

El reconocimiento se practica en presencia del juez, asistido por el secretario, y con la intervención de letrados, procuradores, técnicos o prácticos. Estos pueden hacer al tribunal de palabra las observaciones que estimen oportunas, que junto a las efectuadas por el juez, serán consignadas en la correspondiente acta (art. 358 LEC). Eventualmente el reconocimiento judicial puede practicarse, de oficio o a instancia de parte, con la prueba pericial (art. 356 LEC) y puede practicarse también, aun cuando solo a instancia de parte, con el interrogatorio de las partes y/o de testigos (art. 357 LEC).

9.3.3.1 Práctica conjunta de reconocimiento judicial y prueba pericial

La LEC prevé la posibilidad de concurrencia de la prueba pericial junto a la prueba de reconocimiento judicial (art. 356 LEC). La práctica conjunta de ambas pruebas podrá ser acordada de oficio por el propio tribunal bajo el criterio de «conveniencia» (art. 356.1 LEC), o en su caso, a instancia de parte, cuando el juez así lo estime «procedente» (art. 356.2 LEC). En el supuesto que las partes no hayan propuesto prueba pericial el juez no podrá acordar el reconocimiento judicial junto a la prueba pericial, tal y como se desprende del tenor literal de la ley, quedando solo la posibilidad de que el juez señale la conveniencia de dicha prueba en la audiencia previa -o en el propio juicio tratándose de juicio verbal- y las partes completen o modifiquen sus proposiciones a la vista de lo manifestado por el tribunal (art. 429.1 LEC).

La práctica de la prueba de reconocimiento judicial y de prueba pericial se efectuará en un solo acto, tal y como señala de forma expresa el artículo 356.1 LEC. La mayor parte de la doctrina entiende que cuando se da el reconocimiento judicial con prueba pericial se produce una «concentración de trámites» en la prueba pericial. De modo que el reconocimiento, la emisión y contradicción se producen en un solo acto[399]. En contra: quienes sostienen que la práctica conjunta se refiere solo al reconocimiento judicial pues en todo lo

---

la recuperación de los archivos borrador siempre será parcial y los modificará, ya que el acto de recuperar impone su fecha sobre los datos recuperados, siendo muy difícil establecer con certeza la fecha original de los archivos modificados (conjuntamente con su carácter original y copia) y, por lo tanto se perderá una de las características principales de este tipo de prueba: la determinación de su contemporaneidad (precedencia y sucedencia relativas) con los hechos que se intenten probar, en aras de brindar soporte a la argumentación que pretende hacer convincente la pretensión expresada, al juzgado interventor». DARAHUGE, M.E Y ARELLANO GONZALEZ, L.E. *Manual de Informática Forense (Prueba Indiciaria Informático Forense),* ed. Errepar, 2012, pág. 26.

[399] RIFA SOLER, J.M., *Comentario al art. 356,* en "Comentarios a la nueva Ley de Enjuiciamiento Civil", T. II, págs. 1660-1661.

demás se seguirán los trámites de la pericial con emisión posterior de dictamen; y quienes sostienen que lo que se solicita del perito no es la emisión de un dictamen o informe sino que se lleve a cabo un reconocimiento aportando conocimientos técnicos cuyo resultado se recogerá en el acta única que se levante. Entendemos que tanto puede practicarse en unidad de acto - cuando se trate de supuestos poco complejos-, como practicarse en primer lugar el reconocimiento efectuándose las observaciones necesarias, y que con posterioridad el perito emita dictamen escrito. Esto último será recomendable en supuestos más complejos en que exista mayor dificultad en plasmar en el acta por parte del Secretario términos técnicos, aportando a su vez mayor claridad y celeridad al acto de reconocimiento.

La LEC remite en cuanto al procedimiento a las normas contenidas en dicha sección, aunque no regula el procedimiento de forma detallada. Entendemos que en dicho acto el juez examinará el objeto de reconocimiento por sí y el perito contestará a las preguntas que efectúen tanto el juez como los letrados, efectuando las aclaraciones pertinentes sobre sus conclusiones, de todo lo cual se dejará constancia en la correspondiente acta levantada por el Secretario Judicial (art. 358 LEC). La ley regula también el empleo de medios técnicos de constancia, como la grabación de imagen y sonido u otros instrumentos semejantes, aunque sin omitir el acta (art. 359 LEC).

La práctica de dichas pruebas conjuntamente podrá efectuarse tanto si el perito de designa de parte ha aportado el dictamen pericial con anterioridad al acto de reconocimiento, acompañado a la demanda o contestación (art. 265.1.4º y 336.1 LEC) o en los cinco días anteriores al juicio o vista tratándose de un dictamen emitido por perito de designa judicial (art. 339.2 LEC), como si lo aporta con posterioridad, con el correspondiente traslado a las parte para que puedan efectuar las correspondientes observaciones. No obstante, parte de la doctrina, como FONT SERRA, LÓPEZ YAGÜES, MONTERO AROCA o DÍAZ FUENTES entienden que sólo se refiere al dictamen de designación judicial, ya que el reconocimiento del perito de parte sobre el objeto reconocido ya ha tenido lugar[400].

Como señala ABEL LLUCH el sometimiento a la normativa de la sección del reconocimiento judicial implicará cuando menos: 1º Que las partes serán citadas a la práctica de las operaciones del reconocimiento pericial, en todo caso, y salvo que concurran razones para que sea secreto (art. 355.1 LEC), a diferencia

[400] ABEL LLUCH, X. *El reconocimiento judicial* en la obra en la obra colectiva "La prueba de reconocimiento judicial", ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.4, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, 2012, págs. 88 y 89.

de lo previsto en el artículo 345 LEC; 2º Que el perito deberá rendir su dictamen o sus apreciaciones en el propio acto (art. 358 LEC), salvo que, por razón de la dificultad o complejidad de la materia, el perito solicite y el juez admita la emisión diferida del dictamen[401]. Serán igualmente de aplicación las normas que regulan la pericial en cuanto designación, aceptación, nombramiento y solicitud de provisión de fondos por el perito.

La valoración del dictamen pericial se efectuará conforme a las reglas de la sana crítica. Ello aportará mayor eficacia a la prueba de reconocimiento judicial puesto que las percepciones judiciales irán acompañadas de comentarios de técnicos en la materia.

9.3.3.2 Práctica conjunta de reconocimiento judicial con el interrogatorio de partes y testigos

El legislador ha previsto la práctica conjunta del reconocimiento judicial con el interrogatorio de testigos (art. 357.1 LEC) o el interrogatorio de partes (art. 357.2 LEC).

En este supuesto la concurrencia de prueba de reconocimiento judicial e interrogatorio de testigos y de partes se practica a instancia de parte y a su costa, a diferencia de la práctica conjunta del reconocimiento judicial y el dictamen pericial, que podrá ser acordado conjuntamente de oficio o a instancia de parte (art. 356.1 LEC). Sin perjuicio de ello, no debería existir obstáculo para que el juez pudiera acordar su práctica conjunta, por facilitarlo las circunstancias del lugar, cuando ambas pruebas han sido solicitadas por ambas partes (SAP Zamora 21 de septiembre de 2004). En tal caso no se infringe el principio de aportación de parte, sino que el juez acuerda una acumulación de pruebas ya propuestas por las partes, por estimar que ello favorece su práctica más adecuada[402] .

La decisión de practicar conjuntamente dichas pruebas es potestativa del juez como se desprende del tenor literal del artículo, que podrá acordarlo cuando

[401] Véase ABEL LLUCH, X., *La prueba pericial,* ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.3, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, pág. 131

[402] Véase ABEL LLUCH, X., *El interrogatorio de testigos*, en la obra en la obra colectiva del mismo título, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.4, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, pág. 90.

considere oportuna la práctica de dicha prueba al tener relación las preguntas de los testigos o de las partes con el objeto de reconocimiento, pudiendo la vista del lugar o de las cosas contribuir a la claridad de su testimonio.

La ley prevé que la práctica de dichas pruebas lo sea de forma sucesiva, primero el reconocimiento y a continuación el interrogatorio (art. 357.1 LEC), aun cuando se practican en igual lugar y momento. Ello la distingue también de la prueba conjunta de reconocimiento judicial y prueba pericial que se practican simultáneamente (art. 356.1 LEC).

Previa a su práctica las partes habrán propuesto los extremos del reconocimiento (art. 353 LEC) y se habrá señalado día y hora para su práctica con cinco días de antelación (art. 353.3 LEC), de igual modo las partes habrán propuesto los testigos cuyo examen interesan en el lugar de reconocimiento (art. 357.1 LEC). Se practicará el reconocimiento y una vez finalizado, los letrados podrán formular las preguntas a los testigos, empezando por el proponente. El Secretario redactará la correspondiente acta donde constarán las preguntas efectuadas por cada uno de los letrados, las respuestas, protestas e impugnaciones.

* * *

CAPÍTULO X.- LA VALORACIÓN DE LA PRUEBA SOBRE EL HECHO ELECTRÓNICO

10.1 Introducción

El hecho electrónico como resultado de una actividad podrá ser objeto de prueba a través de cualquiera de los medios previstos por la Ley de Enjuiciamiento Civil (art. 299 LEC). Aunque ello no es óbice para que como actividad en sí misma –prueba electrónica- probablemente solo pueda acceder al proceso a través de la prueba pericial. En cualquier caso, el juez una vez fijado el resultado de los medios de prueba practicados en juicio procederá a valorarla[403].

El sistema de valoración de la prueba previsto por nuestro legislador es un sistema de libre valoración, lo cual no significa discrecionalidad por parte del juez. La libre valoración presupone la ausencia de las reglas que predeterminan el valor de la prueba e implica que la eficacia de cada prueba para la determinación del hecho sea establecida caso a caso, siguiendo criterios no predeterminados, discrecionales y flexibles, basados esencialmente en presupuestos de la razón[404].

Nuestra Ley de Enjuiciamiento Civil alude a las «reglas de la sana crítica» al igual que la antecedente, expresión introducida, por primera vez, en la LEC 1885 (art. 317) y recogida también en el Reglamento del Consejo Real (arts. 147 y 148). La sana crítica constituye un sistema de valoración de la prueba que permite ajustarse a las circunstancias «cambiantes locales y temporales y a las particulares del caso concreto; es un sistema de libre valoración motivada; supone un enfoque de la valoración de la prueba desde la perspectiva de los medios y no del fin»[405].

---

[403] La distinción entre los conceptos de «interpretar» y «valorar» fue elaborada por CALAMANDREI, P., *La génesis lógica de la sentencia*, que puede consultarse en Sentís Melendo, S. en "Estudios sobre el proceso civil", Buenos Aires, 1945, págs.379 y ss. y recientemente ha sido abordada por MONTERO AROCA, J., *La valoración de la prueba como garantía en el proceso civil*, en III Congreso Panameño de Derecho Procesal, Instituto Colombo Panameño de Derecho Procesal, 2006, págs.421-424.

[404] Véase TARUFFO, M., *La prueba de los hechos* (traducción Jordi Ferrer Beltrán), ed. Trotta, Madrid, 2002, pág.387.

[405] Véase ABEL LLUCH, X., *Valoración de los medios de prueba en el proceso civil*, págs. 4-5. Dicho artículo puede descargarse en PDF desde itemsweb.esade.edu (http://goo.gl/dlyimq).

No obstante, nuestro legislador ha establecido en cuanto a la valoración de la prueba por parte del juez algunas reglas en las que establece un efecto determinado a una prueba, así en el interrogatorio de partes, cuando no siendo contradicho por otros medios de prueba, la parte interrogada admita como ciertos hechos enteramente perjudiciales y en los que intervino personalmente (art. 316.1 LEC), respecto a la fuerza probatoria de los documentos públicos (arts. 319 LEC y 1218 Cc) y en cuanto a la fuerza probatoria de los documentos privados (arts. 326 LEC y 1225 Cc –). Dicha prueba ha sido a nuestro modo de ver llamada inadecuadamente «prueba tasada», ya que tal regulación establece únicamente una serie de efectos que la ley reconoce a dicha prueba pero ello no obsta a que dicha prueba al igual que toda la demás quede finalmente sometida a la valoración razonada del juez en sentencia. La valoración por parte del juez del resultado de la prueba con arreglo a la sana crítica como norma general no es óbice para que también existan reglas tasadas de valoración de la prueba. Ahora bien se trata de una excepción, que en realidad lo que pretende es cierta normalidad probatoria, es decir, una serie de normas que dotan *a priori* de una determinada eficacia a la prueba pero que en realidad no dejarán de poder ser impugnadas, en su caso, y siempre valoradas finalmente por la sana crítica judicial. Un documento público en el que interviene un notario alcanza a lo que el notario ve, oye o percibe por los sentidos, la fecha etc. pero en realidad ello es cosa distinta de la veracidad intrínseca. En realidad no existen pruebas tasadas propiamente dichas sino que todas las pruebas se someterán a la sana crítica judicial.

10.2 Valoración de la prueba pericial electrónica

La valoración de la prueba pericial puede estar sujeta a un sistema de prueba tasada, en el cual el juez quedaría vinculado al dictamen de los peritos, o bien a un sistema de prueba libre, que le faculta para efectuar una crítica del modo en que se han empleado los conocimientos técnicos por parte del perito. En cualquier caso el dictamen pericial deberá ponerse en relación con los demás medios de prueba practicados (SAP la Coruña, 27 de septiembre de 2006).

En cuanto al sistema acogido en nuestro ordenamiento jurídico la Ley de Enjuiciamiento Civil de 1881 en su artículo 632 indicaba de forma expresa que el tribunal no estaba obligado a sujetarse al dictamen de peritos, acogiendo el sistema de prueba libre en la valoración de la prueba pericial. No obstante, la vigente Ley de Enjuiciamiento Civil modificó tal redacción indicando en su artículo 348 que la prueba pericial «*se valorará según las reglas de la sana crítica*». Es difícil definir qué debe entenderse por «sana crítica». GUASP definía las reglas de la sana crítica como aquellos «criterios normativos («reglas» pero

no jurídicas) que sirven al hombre normal en una actitud prudente y objetiva («sana») para emitir juicios de valor»[406]. Según ABEL LLUCH «*en definición sintética podemos afirmar que son las reglas derivadas de la lógica, la experiencia y la ciencia. Más ampliamente, que son las reglas no jurídicas derivadas de la lógica, la experiencia y la ciencia que sirven para fundar una valoración razonada de la prueba y permiten su control posterior por otro órgano superior*»[407].

Dichas reglas evolucionan con el paso del tiempo y permiten la adaptación a las circunstancias y situación del caso en concreto. Es decir, parece tratarse de aquellas reglas que guían un correcto razonamiento por parte del Juez[408]. En definitiva, ello supone que el juez no puede someterse sin valoración crítica y razonamiento alguno a un dictamen pericial emitido como prueba en juicio, aun cuando se trate de supuestos de especial complejidad técnica o científica, ya que en ese caso nos hallaríamos ante prueba tasada. Por ello hubiera sido más acertada la regulación expresa en la norma de la motivación judicial y el hecho que la falta de motivación en la prueba pericial fuera de modo expreso motivo de casación[409].

La función crítica por parte del juez en sentencia del dictamen del perito pasa por una crítica razonada del dictamen pericial. Sin desmerecer ni ignorar el carácter orientador de criterios jurisprudenciales tales como la cualificación del

---

[406] Véase GUASP, J., *Comentarios a la Ley de Enjuiciamiento Civil, T*. II, Vol. 1º, 2ª parte, M. Aguilar, editor, Madrid, 1947, pág. 647.

[407] Véase ABEL LLUCH, X., *Configuración de las reglas de la sana crítica en la Ley 1/2000, de Enjuiciamiento Civil*, Revista Vasca de Derecho Procesal y Arbitraje, 2013, 2.

[408] Como señala Font Serra «*la sana crítica constituye el sistema de prueba libre en contraposición al sistema de prueba tasada. No constituye frente a lo sostenido por Couture un sistema intermedio entre ambos, ya que el juez debe atenerse a la lógica siempre. Las reglas de la sana crítica no modifican el prudente arbitrio del juzgador en la apreciación de la prueba pericial, y no vienen determinadas por precepto legal ni por la jurisprudencia. Couture distinguía entre el sistema de prueba legal, en que el legislador le dice al juez que debe apreciar la prueba según los criterios reglados; el de libre convicción, según el cual le dice tu aprecias la prueba como te parezca oportuno, ateniéndote a la prueba, sin atenerte o aún en contra; y el de la sana crítica, luego de haberle dado facultades para completar el material probatorio suministrado por las partes, le dice: tu aprecias la prueba como tu inteligencia te lo indique, razonando de acuerdo a la experiencia y la ciencia que puedan darte los peritos*». FONT SERRA, E. *La prueba de peritos en el proceso civil español.* Ed. Biblioteca hispano europea de ciencias sociales, 1974, págs. 209-212. Cita a COUTURE, *Fundamentos de Derecho Procesal Civil*, 3ª Ed. (póstuma), Buenos Aires, 1958, págs. 270 y ss.

[409] En este sentido se pronuncian SERRA DOMÍNGUEZ y PICÓ I JUNOY entre otros. SERRA DOMINGUEZ, M., *La prueba pericial, en "*Instituciones del nuevo proceso civil. Comentarios sistemáticos a la Ley 1/2000", Vol. II, Alonso-Cuevilles Sayrol, J (coord.) edit. Difusa, Barcelona 2000, págs. 321 y 324.

perito, la solvencia competencia profesional, especialización, currículo profesional etc.), la solvencia o prestigio de la institución que lo emite de tratarse de pericial corporativa, o el criterio mayoritario de los dictámenes que concurren (SAP Sevilla núm. 238/2007 de 21 de mayo de 2007) el juez no puede fundamentar su decisión exclusivamente en los mismos[410], sino que debe efectuar una valoración crítica que, como señala RICHARD debe «… *evitar la tentación de dar por resueltos los asuntos con base en pericias con conclusiones absolutamente científicas, pero que siempre deberemos someter a lo que llamaba Kant el uso crítico de la razón. Razón que en nuestro oficio jurídico se llama sana crítica*»[411]. Es decir, en prueba científica existe, siguiendo a C. Champod, la necesidad de abandonar el «*paradigma de la individualización»* y sustituirlo por el que ROYALL denomina «*paradigma de la verosimilitud»,* propuesto como solución desde que HACKING lo enunciara en 1965 como «ley de verosimilitud»[412].

El paradigma de la individualización, hoy dominante en el ámbito de las pruebas científicas, las considera como pruebas irrefutables por estar basadas en leyes que se consideran universales y que son aplicadas dentro de la metodología científica, por lo que si la prueba se ha realizado bien proporciona resultados

[410] MARTÍNEZ DE CARVAJAL, perito informático, cita, en un supuesto de concurrencia de dictámenes contradictorios, el extracto de una sentencia que indica lo siguiente: «…*Por tanto, para dirimir la controversia que se suscite entre periciales contradictorias parece claro que los tribunales, por la propia índole y naturaleza de esta clase de pruebas, no deben entrar a revisar los criterios científicos, artísticos, técnicos o prácticos propios de la pericia y que hubieren dado lugar a la discrepancia surgida entre los peritos, sino que, para fundamentar su opción por aquél que les hubiese parecido más convincente, deberán acudir a otra clase de criterios, externos al conocimiento especializado de que se trate, como en su caso, la distinta cualificación profesional de los peritos; grado de inmediación en la práctica de la pericia respecto de lo que sea su objeto; objetividad e imparcialidad de los peritos; claridad expositiva; fuerza lógica en la argumentación empleada y mayor o menor expresión de las razones científicas o técnicas que sirvan de fundamento a las conclusiones alcanzadas; exhaustividad en el análisis del objeto de la pericia; etc.».* Añade el autor «*Mencionar por cierto que uno de los peritos de parte perjudicó a su propio cliente cuando se supo que su supuesta titulación de «Diplomado» se correspondía en realidad a un diploma que le dieron tras realizar un cursillo en informática*». MARTÍNEZ DE CARVAJAL HEDRICH, Ernesto. *Informática Forense, 44 casos reales.* Julio 2012, ed. Ernesto Martínez de Carvajal Hedrich, pág. 137, caso 34.

[411] Así se pronuncia RICHARD, M., en el artículo *Reflexiones sobre la práctica y valor de la prueba científica en el proceso penal (a propósito del asunto de los niños desaparecidos en Córdoba)*, en diario La Ley, año XXXIII, núm. 7930, de fecha 25 de septiembre de 2012. Puede consultarse en la dirección electrónica www.diariolaley.es.

[412] Véase CHAMPOD, C., *Interpretation of evidence and reporting in the light the 2009 NRC report*. Keynote Speech of the Interpretation and Evaluation Session of the V Conference of the European Academy of Sciences held in Glasgow (Scotland), University of Strathclyde, 8-11 septiembre de 2009.

concluyentes. Como señala GASCÓN ABELLÁN la convicción anterior no sólo propicia la creencia de que las decisiones probatorias apoyadas en pruebas científicas son difícilmente contestables sino que además, de paso, descarga al juez de hacer un esfuerzo argumentativo por fundar racionalmente la decisión: basta con alegar que hubo prueba científica y que esta apuntaba justamente en la dirección de la decisión probatoria final. La idea de que las pruebas científicas son infalibles y permiten realizar identificaciones categóricas (del tipo «el vestigio v pertenece al imputado») debe ser rechazada. Y no sólo porque la propia realización de las pruebas puede debilitar la calidad espistémica de sus resultados (piénsese, por ejemplo, en el impacto que sobre los resultados de una prueba puede tener una ejecución técnicamente deficiente de la misma o una contaminación de los vestigios analizados), sino también porque para muchas de estas pruebas son posibles varios métodos de análisis con distinto grado de aceptación en la comunidad científica; o porque la mayoría de las leyes sobre las que descansan son de naturaleza estadística y por consiguiente arrojan resultados estructurados según patrones de verosimilitud[413].

El paradigma de la verosimilitud se asienta, como indica dicho autor, en esencia sobre la necesidad de distinguir entre las siguientes cuestiones que cabe plantear una vez el perito ha realizado los análisis pertinentes y se han alcanzado unos resultados: ¿Qué debemos creer?, ¿Qué debemos hacer?, y ¿Qué nos dicen esos datos como evidencia?. Según el paradigma de la verosimilitud es el juez quien debe responder a las dos primeras preguntas y es el perito quien debe responder a la tercera, es decir, el juez evalúa la veracidad de las hipótesis en conflicto a partir de los datos y de las demás pruebas e informaciones existentes, y decide que debe hacer –toma una decisión con base a lo que debe creerse, decisión que será distinta en el marco de un proceso civil que en marco de un proceso penal-[414]. De modo opuesto en el paradigma de la

[413] Véase GASCÓN ABELLÁN, Marina; LUCENA MOLINA, José Juan y GONZÁLEZ RODRÍGUEZ, Joaquín. *Razones científico-jurídicas para valorar la prueba científica: una argumentación multidisciplinar.* Diario La Ley, Nº 7481, Sección Doctrina, 4 oct. 2010, Año XXXI, Ref. D-292, Ed. La Ley.

[414] Lo que debe hacerse depende obviamente de lo que hay que creer –cuestión valorativa de la prueba, racionalidad epistémica-, pero también del contexto normativo en el que se encuadra la decisión a adoptar –la toma de decisiones en presencia de una probabilidad remite a estándares de prueba que en cuestión de policy, es decir dependientes de lo tolerante que sea el sistema con cada uno de los dos errores que pueden cometerse al adoptar una decisión: declarar probado lo falso y declarar no probado lo verdadero- . Por eso, ante una misma creencia no es lo mismo tomar una decisión en el marco de un proceso civil que en el marco de un proceso penal. Y aun en este último supuesto, no es lo mismo que la decisión se adopte en el marco de una instrucción que en el del juicio oral. El estándar de prueba en el proceso civil es mucho más bajo que en el penal (es decir mientras en el primero podríamos aceptar que la prueba de un hecho descanse sobre una probabilidad preponderante, en el segundo sólo estamos dispuestos a condenar con una probabilidad muy cualificada) y ello por la simple razón de que somos

individualización es el perito quien responde a la primera de las preguntas. En paradigma de la verosimilitud el juicio sobre los hechos es de tipo inductivo y no deductivo, por consiguiente sus resultados han de evaluarse en términos de probabilidad, por más alta que esta pueda ser[415].

La dificultad radica en los criterios que puedan tenerse en cuenta para efectuar tal valoración, en concreto cuales son aquellos criterios que servirán al juez para la validación de la prueba científica en cuanto a la metodología y herramientas empleadas por el perito. Un criterio útil a este fin puede ser la conocida sentencia dictada en el caso DAUBERT VS. MERRELL DOW PHARMACEUTICALS, Inc., en 1993 por el Tribunal Supremo de los Estados Unidos. En este caso la Corte Suprema de Estados Unidos de América establecía que los jueces debían revisar el razonamiento y la metodología seguida en las periciales científicas, y señaló los criterios que debían exigirse a una prueba pericial científica para poder ser admitida en un procedimiento judicial determinado. Dichos criterios son los siguientes: a) Si la técnica ha sido comprobada o refutada; b) si ha sido objeto de examen y publicación en el ámbito científico que procede; c) la tasa de error conocida o potencial de la técnica empleada; d) la existencia y mantenimiento de normas y controles en cuanto a su práctica; y e) el grado de aceptación de la técnica en el marco de la comunidad científica[416]. Cabe señalar que los criterios expuestos se ubican en el derecho procesal de los Estados Unidos en sede de admisión de la prueba pericial, teniendo en cuenta el hecho de que un jurado va a ser el destinatario del informe pericial. Ahora bien, estos criterios se pueden aplicar en sentido amplio para establecer el criterio previo de validez del informe pericial en un sistema, como el nuestro, en el que es el juez profesional el que valora la prueba.

---

menos tolerantes con el error consistente en condenar a un inocente que con el consistente en absolver a un culpable. GASCÓN ABELLÁN, Marina; LUCENA MOLINA, José Juan y GONZÁLEZ RODRÍGUEZ, Joaquín. Razones científico-jurídicas para valorar la prueba científica: una argumentación multidisciplinar. Diario La Ley, Nº 7481, Sección Doctrina, 4 oct. 2010, Año XXXI, Ref. D-292, Ed. La Ley, pág. 7-11.

[415] Véase GASCÓN ABELLÁN, Marina; LUCENA MOLINA, José Juan y GONZÁLEZ RODRÍGUEZ, Joaquín. *Razones científico-jurídicas para valorar la prueba científica: una argumentación multidisciplinar*. Diario La Ley, Nº 7481, Sección Doctrina, 4 oct. 2010, Año XXXI, Ref. D-292, Ed. La Ley.

[416] Véase Improving judicial gatekeeping: Technical advisors and scientific evidence. Full Text Available Harvard Law Review. Feb 97, Vol. 110 Issue 4, pág. 945-946; Hess, Robert L., Judges cooperating with scientists: A proposal for more effective limits on the federal trial judge's inherent power to appoint technical advisors, V. II. Vanderbilt Law Review 54. 2 (Mar 2001), pág. 564; H.T. Greely y A.D. Wagner, Reference Manual on Scientific Evidence, Third Edition, federal Judicial Center, National Academic Press, Washington D.C. 2011, págs. 772 y ss.

Todos los anteriores criterios deberían tenerse en cuenta por parte del juez a la hora de valorar la prueba pericial, de ahí la importancia de que el dictamen sea completo y contenga los apartados que señalábamos en el § 8.2.1. Puesto que cada uno de ellos, -datos identificativos y profesionales del perito, método, herramientas, cadena de custodia, criterios que los validan científica o técnicamente y conclusiones- serán elementos que ayuden a valorar de una forma crítica el dictamen pericial y a formar la convicción del juez[417].

En relación a los pasos que debe seguir el juez en su razonamiento crítico de la prueba pericial recientemente se ha propuesto la «*reformulación del paradigma de la sana crítica*», como reacción frente a la apreciación acrítica del dictamen único del perito de designación judicial, atendiendo a una serie de factores. En primer lugar, refieren «*el control del método utilizado por el perito*» de modo que el juez actúa como «gatekeeper» o controlador del método tecnológico o científico, admitiendo solo aquella prueba pericial que resulte metodológicamente segura. Entendemos que no podemos hablar de métodos «seguros» puesto que la ciencia y la tecnología evolucionan con el tiempo y no son infalibles. Es por ello que en este supuesto debiera hablarse de aquellos métodos más validados por la comunidad científica. En segundo lugar, sería necesario «*el análisis de la pericia misma conforme a criterios lógico-deductivos*», reforzando aspectos, ya tenidos en cuenta, de lógica racional, de valoración probatoria, de argumentación y de análisis técnico-jurídicos. Y finalmente, es necesaria «*la plasmación clara en la resolución judicial del control del método y de su valoración racional*», lo que comprende, entre otros extremos, la identificación de los extremos de la pericia y la justificación de la convicción judicial, la selección de la información relevante, la aplicación de técnicas de detección de errores o lagunas, el uso adecuado de la terminología, la coherencia y conclusividad del razonamiento[418].

---

[417] La importancia para el valor de la prueba del procedimiento y de una correcta cadena de custodia a la hora de realizar la prueba pericial son puestos de relieve por MARTÍNEZ DE CARVAJAL, perito informático, quien comenta a raíz de una Sentencia dictada por el Juzgado de Instrucción núm. 28 de Barcelona, en el Procedimiento Abreviado 289/05 dimanante de las Diligencias Previas núm. 3163/03 «*…Obsérvese que la argumentación de la Juez contiene errores técnicos pero la parte demandante no recurrió la sentencia toda vez que, al margen de las cuestiones técnicas que comenta la magistrada, relacionadas con la IP, la realidad es que la principal prueba de cargo carecía de valor probatorio al no haber existido cadena de custodia y, por otro lado, el procedimiento seguido por el perito judicial, ciertamente arbitrario, había invalidado todo su informe*». MARTÍNEZ DE CARVAJAL HEDRICH, Ernesto. *Informática Forense, 44 casos reales*, ed. Ernesto Martínez de Carvajal Hendrich, julio 2012.

[418] Véase PEREDA GAMEZ, F.J., *La prueba pericial en los litigios derivados de la Ley de la edificación*, en "La prueba pericial en el proceso civil", Ledesma Ibáñez, P y Zubiri de Salinas, F (dirs), Cuadernos de Derecho Judicial, núm. XII/2006, CGPJ, Madrid, 2006, págs.116-122. En línea similar, y sobre la necesidad de someter la valoración de la prueba pericial a métodos científicos, Zubiri De Salinas, F., *Valoración de la prueba pericial*, en "La prueba pericial en el proceso civil".

La función encomendada a los jueces de valoración crítica de la prueba pudiera plantear dificultades especialmente en el ámbito de la prueba pericial en materia de ciencia o tecnología. Efectivamente, la valoración de la prueba para la determinación de los hechos y del derecho aplicable en la sentencia, puede resultar especialmente difícil en las materias señaladas, en tanto que pueden ser precisos conocimientos técnicos o científicos que puede que el juez no posea[419].No obstante, resulta claro que los Jueces no pueden excusarse de dictar sentencia aduciendo oscuridad o ausencia de criterio técnico. Es por ello que resulta clara la necesidad de mejorar la formación de los juzgadores, no sólo inicialmente sino también en toda su carrera en materias de ciencia y técnica. Incluso debe mejorarse la formación de los Jueces en epistemología y en metodología científica. Ahora bien, lo que no cabe postular es una suerte de Juez que por sí mismo o auxiliado de otros se convierta en una suerte de superhombre con conocimientos avanzados superiores a los del hombre medio[420]. Precisamente, la ley sirve al hombre, al medio y al que no lo es. De modo que tanto la ley, como el sistema de impartición de justicia deben ser comprensibles por los ciudadanos. Mucho más las sentencias deben contener la decisión del juez en un lenguaje entendible por el hombre medio al que van destinadas. Imagínense una sentencia plagada de fórmulas matemáticas y técnicas que no pudieran entender sus destinatarios. Sin ninguna duda ello supondría el fracaso seguro del sistema de justicia que se convertiría en un sistema de justicia sacerdotal. En cualquier caso, como ya aduje (§ 8.1.1), es aconsejable que en caso de insuficiencia o contradicción de la prueba el Juez pueda acordar un dictamen dirimente como diligencia final a fin de poder aclarar las dudas que pudiera tener con relación a la pericia practicada.

Otro de los aspectos que ha sido objeto de discusión en el ámbito de la valoración de la prueba pericial es el valor que se atribuye por parte del juez a la prueba pericial emitida por un perito designado judicialmente o un perito designado por la parte. No existe ninguna norma positiva que obligue o faculte

---

[419] Véase MIRANDA VAZQUEZ propone la reformulación del brocardo «iudex est peritus peritorum» (el juez es el perito de los peritos) sustituyéndola por el brocardo «iudex est custos peritorum». Los jueces deben adoptar una postura activa, de vigilancia, control o fiscalización del hacer pericial. MIRANDA VAZQUEZ, C., *¿Es realmente el Juez el "peritus peritorum"? (Propuesta de reformulación del brocardo y análisis del alcance efectivo de la valoración judicial de la prueba pericial)* en "Derecho Probatorio Contemporáneo. Prueba científica y técnicas forenses", Bustamante, M.M. (coord), Universidad de Medellín, 2012.

[420] DARAHUGE y ARELLANO señalan que en el momento de revisar la integridad material y formal de la cadena de custodia el profesional debe considerarla desde tres puntos de vista complementarios: validez técnica informática, validación técnica criminalística y validación técnica legal. DARAHUGE, M.E Y ARELLANO GONZALEZ, L.E. *Manual de Informática Forense (Prueba Indiciaria Informático Forense)*. Ed. Errepar, 2012, págs. 66-67.

al juez a otorgar mayor valor probatorio al dictamen de un perito designado judicialmente que al de elección directa de parte, sino que ambos dictámenes se sitúan en pie de igualdad en orden a su eficacia probatoria. El legislador del 2000 ha optado por otorgar naturaleza de medio de prueba al dictamen extrajudicial, y reconoce la facultad de las partes de aportar dictámenes por peritos por ellos designados con los escritos de alegaciones (arts. 265.1.4º y 336 LEC). Ello frente a la LEC de 1881 en la que si bien se admitía la incorporación de dictámenes extrajudiciales se les negaba la consideración de medio de prueba, aun cuando se les reconocía cierto valor probatorio.

No obstante, la vigente regulación y partiendo de la identidad de eficacia probatoria en la doctrina y jurisprudencia se advierten dos sectores que matizan la previsión legal. Un primer sector otorga mayor credibilidad al dictamen de designación judicial por cuanto en el mismo coincide una presunción de mayor objetividad (STS de 31 de marzo de 1997). Superior credibilidad al haber sido designado imparcialmente, sin haber sido elegido por una sola parte y mayor posibilidad de contradicción[421]. Un segundo sector parte de la identidad de valoración centrándose en la mayor o menor fundamentación del perito. Partiendo de que la LEC ha articulado una serie de previsiones legales que preservan la objetividad del dictamen, tales como la tacha del perito de parte (at. 343 LEC); la facultad de intervención de las partes en las operaciones de reconocimiento (art. 345 LEC); la facultad de solicitar la ampliación del dictamen de parte (art. 427.2 LEC) y la facultad de solicitar la comparecencia del perito a los efectos de la contradicción del dictamen pericial (art. 337, 338, 346 y 347 LEC)[422].

En otro orden de cosas, señalar finalmente que el dictamen de parte o designación judicial impugnado en la audiencia previa y no sometido en el acto del juicio o la vista a contradicción deberá ser valorado en el momento de dictar sentencia y conforme a las reglas de la sana crítica, sin necesidad que sea confirmado por otros medios de prueba, y sin necesidad que sea sometido a contradicción en el acto del juicio o de la vista. Ahora bien, en la motivación del juicio de hecho y en el examen personal del dictamen pericial por el juez deberá

[421] STS, Sala 1ª, de 31 de marzo de 1997, Fdo. Jco. 4º (EDJ 1997/2111). Véase también SERRA DOMÍNGUEZ, M. *La prueba pericial,* ob. cit., pág. 310.

[422] Véase FONT SERRA, E., *El dictamen de peritos y el reconocimiento judicial en el proceso civil,* edit. La Ley, Madrid, 2000, pág. 66, 126-127; RIFA SOLER, J.M., *Comentarios a la nueva Ley de Enjuiciamiento Civil,* M.A. Fernández-Ballesteros, J.Mª. Rifa Soler y J.F. Valls Gombau (coords.), edit. Atelier, Barcelona, 2000, págs.43-44.

atender a los motivos de la impugnación, como un factor de ponderación más integrado del juicio de la sana crítica[423].

10.3 Cuestiones sobre la valoración de la prueba documental del hecho electrónico

La valoración de la prueba documental implica necesariamente efectuar dos operaciones diferentes sucesivas en el tiempo, cual es, en primer lugar la verificación documental, esto es la prueba de la autenticidad del documento, y acto seguido, una vez verificada la autenticidad la atribución de su eficacia probatoria. Distinguiendo la eficacia probatoria a todo documento, la eficacia probatoria privilegiada del documento público y la eficacia del documento privado no impugnado[424].

La verificación documental se inicia después del posicionamiento de las partes ante los documentos aportados de contrario (art. 427.1 LEC), fase a la que anteriormente hemos hecho referencia en el § 9.3.1.2. La expresión «eficacia probatoria» se utiliza frente a la autenticidad del documento –concordancia de autor aparente y autor real- cuando nos referimos al valor que cabe atribuir al contenido de un documento (que no haya sido declarado carente de autenticidad «*condictio sine qua non*» para la idoneidad valorativa)[425]. Siguiendo a SERRA DOMINGUEZ existe una eficacia común a todo documento, que comprende el hecho mismo de su existencia, bien sea documento público, bien sea documento privado y que no puede ser ignorada por el juez. A partir de esta eficacia común, el documento público goza de una eficacia privilegiada, teniendo el valor de prueba legal en los extremos relativos al hecho de su otorgamiento, de su fecha y de los intervinientes (art. 319.1LEC), debiéndose extender también el ámbito de la prueba tasada al lugar en que se produjo esa documentación, salvo que se demuestre la falsedad material del documento. Reiterada y constante jurisprudencia ha sostenido que el ámbito cubierto por la fe pública no se extiende a la «veracidad intrínseca» de las afirmaciones

---

[423] Véase ABEL LLUCH, X., *La valoración del dictamen pericial* en "*La prueba pericial*", ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.3, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, págs. 455-461.

[424] Véase SERRA DOMÍNGUEZ, M., *La prueba documental*, en "Instituciones del Nuevo Proceso Civil. Comentarios sistemáticos a la Ley 1/2000", Alonso-Cuevillas Sayrol, J. (coord.), ed. dijusa, Barcelona, 2000, págs. 256-261 y 262-268.

[425] SSTS, Sala 1ª, de 25 de noviembre de 2002 (RJ 2002\10275) y de 14 de diciembre de 2005 (RJ 2005\10168).

contenidas en el documento público, las cuales deberán ser valoradas libremente por el juez en una apreciación conjunta con el resultado de las demás pruebas[426].

La eficacia del documento privado no impugnado o cuya autenticidad haya resultado acreditada se equipara, por disposición legal, a la del documento público (art. 326.1 LEC). No obstante, tal equiparación solo se produce en los extremos relativos al hecho de su otorgamiento y la identidad de los intervinientes, en la medida que la fecha del documento privado solo tendrá valor de prueba legal respecto de terceros cuando se acredite fehacientemente por alguna de las formas previstas en el art. 1227 CC o por otros medios de prueba. La eficacia de un documento privado impugnado, y cuya autenticidad no se ha podido acreditar o sobre la que no se ha propuesto prueba alguna, queda remitida a las reglas de la sana crítica (art. 326.2, II LEC).

La manifestación o resultado que produce el hecho electrónico podrá acceder al proceso a través de prueba documental, es decir, a través del documento electrónico. Es por ello que se le aplican al mismo las normas específicamente previstas para la prueba documental en cuanto a su eficacia probatoria. En otro caso, de no aplicarse al documento electrónico criterios de prueba tasada se llegaría como señala SANCHÍS CRESPO «*al absurdo de penalizar con la prueba libre la utilización de los avances informáticos, premiando con la prueba legal, el mantenimiento de las formas tradicionales*»[427]. Sin embargo, la vigente Ley de Enjuiciamiento Civil en contra de dicho criterio regula los medios de prueba audiovisuales (arts. 382 y 383 LEC) y los instrumentos informáticos (art. 384 LEC) independientemente de la prueba documental como otro medio de prueba más

---

[426] Véase SSTS, de 6 de mayo de 1993, fto. jco. 1º (RJ 1993, 3445) y de 26 de enero de 2001, fto. jco. 5º (RJ 2001/528). Así la STS de 7 de julio de 1989, fto. jco. 6º (RJ 1989/5414) mantiene que «*el documento público no tiene prevalencia sobre otras pruebas y por sí solo no basta para enervar una valoración probatoria conjunta, vinculando al Juez sólo respecto del hecho de su otorgamiento y de la fecha de éste, dado que el resto de su contenido puede ser sometido a apreciación con otras pruebas*». Y más recientemente la STS, de 31 de mayo de 2006, fto. jco. 3º (RJ 2006/3176) recuerda que el valor tasado del documento público no se extiende a su contenido, de modo que «*la veracidad intrínseca del documento público puede ser desvirtuada mediante prueba en contrario, sin que tal medio probatorio tenga prevalencia sobre los demás, vinculando tan sólo al órgano judicial su otorgamiento y fecha*». Cfr. tb. ORMÁZABAL SÁNCHEZ, G., *La prueba documental y los medios e instrumentos idóneos para reproducir imágenes o sonidos o archivar y conocer datos*, ed. La Ley, Madrid, 2000, págs. 66-67. Véase también ABEL LLUCH, X., *Valoración de los medios de prueba en el proceso civil*, disponible en http://goo.gl/dlyimq, págs. 8-10.

[427] Véase SANCHÍS CRESPO, C y CHAVELI DONET., *La prueba medios audiovisuales*…, ob. cit., pág.124.

y señala que ambos se valoran conforme a las reglas de la sana crítica. Según el tenor literal del artículo 384.3 LEC, «*la sana crítica según su naturaleza*»[428].

Este último inciso ha dado lugar a distintas interpretaciones doctrinales[429]. Un primer sector doctrinal entiende que la apostilla «según su naturaleza» no aporta nada, dado que las reglas de la sana crítica, por definición, se refieren siempre a las circunstancias del caso concreto y se trata de una simple redundancia, en la medida que la libre valoración supone tener en cuenta la naturaleza propia del medio que se aplica, llegándose a afirmar que se podría incluso haber prescindido de esta previsión legal[430]. Para un segundo sector doctrinal la expresión «según su naturaleza» permitiría distinguir entre: a) Aquellos instrumentos informáticos que son semejantes a los audiovisuales, a los que se aplicarán las mismas reglas de valoración, y que por disposición del artículo 382.3 LEC son las reglas de la sana crítica; b) Aquellos otros medios, que por su naturaleza se aproximan o equiparan a los documentos, en cuyo caso habrá que tener en cuenta las distintas reglas de valoración de documentos, según sean públicos, privados o electrónicos[431]. Y finalmente para un tercer sector la valoración de la prueba electrónica se halla sujeta a una «sana crítica especialísima». Desde esta perspectiva se han enumerado unos criterios valorativos específicos y que pueden resumirse como: a) atender a la naturaleza del documento; b) comprobar si viene firmado electrónicamente o no; c) el control del uso del conocimiento privado del juez; d) el recurso a la pericial informática, con carácter general; e) el examen del binomio hardware-software; f) las características del tipo de documento que se trate[432].

---

[428] Dispone el artículo 384.3 LEC: "*El tribunal valorará los instrumentos a que se refiere el apartado primero de este artículo conforme a las reglas de la sana crítica aplicables a aquellos según su naturaleza*".

[429] Véase ABEL LLUCH, X. *La prueba electrónica,* ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.4, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, págs. 169-172.

[430] Véase ORMÁZABAL SÁNCHEZ, G., *La prueba documental y los medios e instrumentos idóneos para reproducir imágenes o sonidos o archivar o conocer datos*, ed. La Ley, Madrid, 2000, pág. 202.; SACRISTÁN REPRESA, G., *Comentario al art. 384 LEC*, en "Comentarios a la nueva Ley de Enjuiciamiento Civil", t.II, Fernández-Ballesteros; Rifá-Soler; Valls Gombau (coords.), ed. Atelier, Barcelona, 2000, pág. 1773; SAMANES ARA, C., *Comentario al art. 384 LEC*, en "Comentarios a la Ley de Enjuiciamiento Civil", vol. I, Cordón-Moreno; Armenta-Deu; Muerza-Esparza; Tapia-Fernández (coords.), ed. Aranzadi, Navarra, 2001, pág.1286.

[431] Véase ARAGONESES MARTÍNEZ, S., HINOJOSA SEGOVIA, R. y otros, Cien cuestiones controvertidas sobre la prueba en el proceso civil, ed. Colex, Madrid, 2004, pág.185.

[432] DE URBANO CASTRILLO, E., *La valoración de la prueba electrónica*, ob. cit., págs. 51 y ss. y 121; GARCÍA PAREDES, A., *La prueba en juicio: ¿y si es electrónica?*, en Rev. Contratación Electrónica, núm. 62, julio 2005., pág. 9.

Las deficiencias que presenta la regulación contenida en la LEC intentan corregirse a través de otras leyes especiales posteriores. Leyes posteriores a la LEC, que como a continuación veremos, se pronuncian sobre eficacia del documento electrónico, otorgándole un tratamiento similar a la prueba documental también en cuanto a su eficacia, frente a la regulación y criterio seguido por la LEC que remite a las reglas de la sana crítica (art. 382.3 y 384.3). En este sentido en el artículo 17 bis Ley Notariado, añadido por Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social) y en el RD 45/2007, de 19 de enero, por el que se modifica el Reglamento de la organización y régimen del Notariado, el legislador equipara, en cuanto a su eficacia probatoria, el documento público notarial y el documento público electrónico y admite que éste último pueda recogerse en cualquier soporte, esto es, en soporte informático, electrónico o digital.

Por otro lado, el apartado 1 del artículo 24 de la Ley 34/2002, de 11 de julio, de Servicios de Sociedad de la Información y comercio electrónico sujeta la prueba de un contrato electrónico a las normas generales del ordenamiento jurídico, entre las que, por supuesto, se encuentra la LEC y efectúa una remisión directa a la LFE. El apartado 2 del artículo 24 LSSI otorga la consideración de prueba documental al soporte electrónico que recoge el contrato electrónico. Según ABEL LLUCH ello significa que, por una parte, los contratos electrónicos accederán al proceso por el cauce de la prueba documental y, por otra parte, que su eficacia probatoria será la propia de la prueba documental, esto es, que podrán tener eficacia de prueba tasada –en cuanto al hecho, estado de cosas o acto documentado, fecha de la documentación e identidad del fedatario y demás intervinientes- cuando accedan al proceso a través de un documento público (art. 319.1 LEC) y también cuando accedan a través de un documento privado y éste no resulte impugnado (art. 326.1 LEC). La admisibilidad en juicio del contrato electrónico por la vía de la prueba documental significa otorgarle la eficacia probatoria tasada de la prueba documental, con derogación de la regla de la libre valoración del apartado 3º de los artículos 382 y 384 LEC[433] .

Según el artículo 3.5 Ley 59/2003, de 19 de diciembre, de Firma Electrónica: «*Se considera documento electrónico la información de cualquier naturaleza en forma*

---

[433] ABEL LLUCH, X., *La prueba documental,* Serie estudios prácticos sobre los medios de prueba, núm.4, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, pág. 138.

En sentido distinto, GONZÁLEZ SÁNCHEZ, J.L., *Comentario al art. 24*, en "La nueva Ley de internet" (Comentarios a la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico), Cremades, J. y González Montes, J.L. (coords.), ed. La Ley, Madrid, 2003, pág. 390.

electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado. Sin perjuicio de lo dispuesto en el párrafo anterior, para que un documento electrónico tenga la naturaleza de documento público o de documento administrativo deberá cumplirse, respectivamente, con lo dispuesto en las letras a) o b) del apartado siguiente y, en su caso, en la normativa específica aplicable». Y el art. 3.7 establece que «*Los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad a la legislación que resulte aplicable*». Y la Ley 41/2007, de 7 de diciembre, de Reforma del Mercado Hipotecario que reforma artículo 318 LEC señala que *«Los documentos públicos tendrán la fuerza probatoria establecida en el artículo 319 si se aportaren al proceso en original o por copia o certificación fehaciente, ya sean presentados éstos en soporte papel o mediante documento electrónico, o si, habiendo sido aportado por copia simple, en soporte papel o imagen digitalizada, conforme a lo previsto en el artículo 267, no se hubiera impugnado su autenticidad»*.

La valoración del documento electrónico, sea de eficacia tasada o de eficacia libre, efectuada por el Juez de Primera Instancia puede ser revisada en su integridad por la Audiencia Provincial a través del recurso de apelación. Tal como se anticipa en la exposición de motivos de la LEC, se ha optado por el modelo de apelación limitada (*revisio prioris instantiae*), de modo que el tribunal de apelación goza de la misma libertad para valorar la prueba practicada en la instancia, pudiendo apreciar las mismas pruebas de modo distinto. Ahora bien, en aquellos supuestos en que la prueba del hecho electrónico no se haya aportado mediante su impresión en formato papel, sino a través de un instrumento informático (ej. pensemos en un CD o DVD unido a las actuaciones), dado que la práctica de la prueba exige la reproducción ante el tribunal, parece que lo razonable sería visionar la prueba ante los Magistrados de la Sala de Apelación.

* * *

CAPÍTULO XI.- LA IMPUGNACION DEL DICTÁMEN PERICIAL EN VÍA DE RECURSO

La Constitución Española garantiza en su artículo 24 la tutela judicial efectiva, lo que incluye el derecho a la defensa y a recurrir las resoluciones desfavorables o perjudiciales a la partes. Para ello el legislador pone a disposición de las mismas los recursos, que fundamentalmente se basan en tres motivos: quebrantamiento de la forma, infracción de la ley y error en la valoración de la prueba.

Los dos primeros presuponen la vulneración de normas sustantivas o procesales mientras el tercero implica al razonamiento judicial en la sentencia. En los dos primeros casos como señala RICHARD GONZÁLEZ se trata de un motivo de vocación pública que sirve a la corrección de la aplicación del derecho, pero que no atiende al elemento esencial del juicio que es la determinación de los hechos mediante la valoración de la prueba. El tercero se basa en la obligación judicial que los jueces tienen de motivar sus resoluciones haciendo constar sus razonamientos sin que puedan dictar resoluciones arbitrarias. Dicha motivación cumple con una doble finalidad: reforzar la seguridad jurídica expresando las razones del juzgador para adoptar la decisión y acreditando que no actúa de modo arbitrario; y una adecuada motivación de la sentencia permite que las partes puedan argumentar sus recursos, y proporciona al órgano jurisdiccional, que deba pronunciarse en vía de recurso, elementos que permitan valorar la legalidad y justicia de la sentencia sometida a recurso (STC 187/2000 de 10 de julio)[434].

La parte procesal que impugne la valoración efectuada por el juez del dictamen pericial discutirá las razones o elementos de juicio, que han fundado los criterios jurídicos base de la resolución. Es decir, la parte que interponga el recurso discutirá la explicación razonada del valor que le otorga a dicha prueba el juez. La valoración del dictamen pericial efectuada por el Juez de Primera Instancia en sentencia puede ser revisada por la Audiencia Provincial a través del recurso de apelación (recurso ordinario). En este caso el dictamen pericial se trasladará junto al resto de material recogido en la primera instancia a la segunda instancia de modo íntegro, pudiendo la Audiencia Provincial efectuar una nueva valoración de las pruebas practicadas en primera instancia (cognición plena). Las partes no podrán innovar en lo referente a los hechos ni a las pruebas, ya que en España rige el sistema de apelación limitada (atenuada), no se trata de un nuevo juicio sino de la revisión del efectuado en primera instancia. El tribunal de

[434] Véase RICHARD GONZÁLEZ, M., *La impugnación y revisión de la prueba mediante recursos ordinarios y extraordinarios en el proceso penal*, en "Estudios sobre Prueba Penal" Volumen III; ed. La Ley, 2013, págs. 425 y 427.

apelación puede valorar la prueba practicada en la instancia sin necesidad de su reiteración y puede incluso practicar nuevas pruebas, a instancia de parte en los supuestos del artículo 460 LEC (prueba indebidamente denegada en la instancia contra la que se formuló protesta; pruebas admitidas y no practicadas en primera instancia; pruebas sobre hechos ocurridos durante la primera instancia; y las pruebas del rebelde), sin olvidar que en los procesos no dispositivos el tribunal podrá decretar de oficio cuantas pruebas estime necesarias, tanto en la primera instancia como en la segunda instancia (art. 752.3 LEC) [435]. Tras la Ley 37/2011 de medidas de agilización procesal se establece una limitación a la apelación por razón de la cuantía, no siendo apelables las sentencias dictadas en juicios verbales cuya cuantía no supere los 3.000 euros (art. 456.1 LEC).

La impugnación posterior a la sentencia podrá efectuarse también vía recursos extraordinarios: recurso de casación, recurso extraordinario por infracción procesal y revisión. El dictamen pericial puede ser impugnado mediante recurso extraordinario por «infracción procesal», con fundamento en el artículo 469.3 LEC, alegando defectos procesales tales como la falta de citación de las partes a las operaciones periciales, si la hubieran solicitado, o la falta de citación a la emisión del dictamen pericial, o a la falta de cualquier aclaración al dictamen pericial, siempre y cuando la infracción procesal hubiera podido producir indefensión. La indefensión, como presupuesto para recurrir una sentencia o auto en casación, se tiene que haber producido «*como consecuencia de una infracción legal, que produzca un perjuicio real a la parte que lo invoca, que no haya sido provocada por ella misma, que sea real y no hipotética, siendo alegables solo por la parte que la sufre y que no haya sido subsanada la falta*»[436]. El recurso extraordinario por infracción procesal (art. 477 LEC) solo puede

[435] Véase PICÓ I JUNOY, J., *Valoración de la prueba y segunda instancia civil: hacia la búsqueda del necesario equilibrio*, en Revista Jurídica de Catalunya, núm. 3-2009, págs. 52-64. Puede consultarse en itemsweb.esade.edu. En dicho artículo el autor discute la indebida doctrina judicial de las Audiencias Provinciales en función de la cual el recurso de apelación no puede ser un instrumento para desvirtuar la valoración judicial de la prueba practicada en primera instancia al suponer vulnerar el principio de inmediación (salvo que la valoración sea absurda, ilógica o irracional, etc.). En lo relativo a la prueba pericial se deduce que no puede alegarse el principio de inmediación respecto a los medios de prueba no personales como es el caso de los dictámenes periciales, y tampoco cuando las actuaciones probatorias han sido grabadas audiovisualmente. Por otro lado las Audiencias Provinciales no pueden dejar de valorar el resultado de la prueba practicada en primera instancia por entender que no les corresponde esa función salvo que el razonamiento judicial de instancia sea ilógico, irracional, arbitrario, incongruente etc. por cuanto ello supone confundir el recurso de apelación –ordinario- con el de casación –extraordinario-. Por ello, en segunda instancia puede procederse libremente a «revalorar» los resultados de la prueba practicada, sin limitarse a corregir errores manifiestos o valoraciones ilógicas, absurdas o irracionales de los jueces de instancia.

[436] Véase BONET NAVARRO, A., *Los recursos en el proceso civil,* ed. La Ley, Madrid. 2000, pág.186.

interponerse contra sentencias dictadas en segunda instancia por la Audiencia Provincial.

La jurisprudencia más reciente de la Sala Primera del Tribunal Supremo viene sosteniendo que la disconformidad con la valoración de la prueba pericial efectuada por el Tribunal de Apelación debe impugnarse, cuando sea posible su presentación, por la vía del recurso extraordinario por infracción procesal y no por la vía del recurso de casación, habiéndose dictado ya, bajo tal argumento, numerosos autos de inadmisión del recurso de casación. Así se razona, entre otros muchos, en el Auto del Tribunal Supremo de 9 de octubre de 2007[437]. Jurisprudencia consolidada niega la revisión de la valoración del dictamen pericial en casación, salvo que contenga conclusiones absurdas o ilógicas, bajo el argumento que las reglas de la sana crítica no aparecen recogidas en precepto alguno y, por ello, no pueden fundar la casación en el error de derecho (art. 477.1º LEC). Frente a ello, algunos autores sostienen la posibilidad de revisar en casación la valoración del dictamen pericial por infracción de las máximas de la experiencia probatorias[438].

En el supuesto que el dictamen pericial se haya obtenido fraudulentamente cabe impugnarlo mediante la interposición del recurso extraordinario de «revisión». Constituye motivo de revisión que la sentencia recaída lo hubiera sido «*en virtud de prueba testifical o pericial, y los testigos o los peritos hubieren sido condenados por falso testimonio dado en las declaraciones que sirvieron de fundamento a la sentencia*» (art. 510.3º LEC). El TS exige: 1) Una sentencia penal que declare la existencia del delito de falso testimonio; 2) Que la declaración efectuada por el condenado haya sido decisiva para adoptar el fallo de la sentencia que se pretende rescindir o anular; 3) Que el carácter decisivo anterior haya sido reconocido o declarado en la sentencia dictada en el proceso penal[439].

* * *

[437] Auto del Tribunal Supremo, Sala 1ª, de 9 de octubre de 2007, Fdo. Jco. 4º.

[438] Véase SERRA DOMÍNGUEZ, M., *La prueba pericial, en Instituciones del nuevo proceso civil*. "Comentarios sistemáticos a la Ley 1/2000", vol. II, Alonso-Cuevilles Sayrol, J (coord.) edit. Difusa, Barcelona 2000, pág. 326 y del mismo autor *El recurso de casación en la LEC 1/2000,* en Revista jurídica de Catalunya, 2001, núm. 4, págs. 1149-1150. NIEVA FENOLL, J., *El recurso de casación civil,* ed. Ariel, Barcelona, 2003, págs. 176-178.

[439] STS, Sala 1ª, de 29 de marzo de 2004, fdo. Jco. 1º.

CONCLUSIONES

PRIMERA.- LA EVIDENCIA DEL CAMBIO HACIA UNA NUEVA ERA DE IMPLANTACIÓN GENERALIZADA DE LAS TECNOLOGIAS DE LA INFORMACIÓN.

El siglo XXI es el de la implantación general de las tecnologías de la información que son las que caracterizan esta nueva era de desarrollo tecnológico que se inicia en las últimas décadas del siglo pasado. El desarrollo de la informática y la computarización ha impulsado las redes de comunicación que se extienden por todos los ámbitos sociales desde la administración hasta las relaciones sociales y, especialmente, en el comercio electrónico. Las nuevas tecnologías se imponen en una sociedad caracterizada por la expansión de redes, servicios y aplicaciones digitales que determinan la competitividad de las empresas en un entorno cada vez más global. La administración pública y, concretamente, la de justicia no es ajena a los cambios en tanto que la realidad que va a ser objeto de protección y tutela jurídica tiene, cada vez más, su fuente y origen en relaciones y hechos de naturaleza electrónica.

SEGUNDA.- LA REGULACION JURIDICA DE LAS TIC.

La realidad tecnológica en la que vivimos conlleva una mayor presencia del hecho electrónico como objeto jurídico y de prueba en el proceso. El mundo tecnológico creado por las tecnologías de la información y comunicación (TIC) requiere de cobertura por parte del ordenamiento jurídico para que queden protegidos los derechos de los ciudadanos. El derecho necesita adaptarse para poder cumplir con la función social reguladora de la comunidad que le es propia. Ello implica la necesidad de regulaciones legales adecuadas a los retos que plantean las nuevas tecnologías en nuestra sociedad. También en el ámbito del derecho procesal debe atenderse al acceso del hecho electrónico al proceso y la fijación de su régimen jurídico. La regulación de la nueva realidad tecnológica debe atender especialmente al entorno global fomentándose la unificación normativa internacional con los instrumentos legales precisos de cooperación entre estados. Estos son requisitos fundamentales para garantizar la seguridad jurídica en nuestro nuevo entorno dentro y fuera de la red.

TERCERA.- LA NECESIDAD DE UNA POLITICA EMPRESARIAL DE PROTECCIÓN DE DATOS.

Una de las características del mundo globalizado es el interés y valor de los datos de cualquier clase y naturaleza que utilizan las empresas en su actividad comercial. La protección de los datos resulta, en razón de su importancia, una de las actividades esenciales en las empresas que deben adoptar una política empresarial de protección y de conservación de la información y datos personales y empresariales. De ese modo, se obtendrán mejores perspectivas de éxito respecto a eventuales litigios o infracciones que se puedan plantear en el futuro.

CUARTA.- LA NECESIDAD DE UNA POLITICA EMPRESARIAL DE PREVENCION JURIDICA FRENTE EVENTUALES RECLAMACIONES.

Las personas jurídicas deberían dotarse de efectivos sistemas hábiles para prevenir o detectar injustos penales y evitar ser declaradas responsables en un proceso penal conforme a lo previsto en el artículo 31 bis del Código Penal que castiga al representante legal o de hecho que omita la adopción de las medidas de vigilancia o control exigibles. Es por ello que resulta imprescindible la implantación de un modelo o sistema de prevención y detección de delitos que actuará como eximente de la responsabilidad penal si se ha llevado a cabo con anterioridad a la comisión del delito.

QUINTA.- LÍMITES DEL CONTROL EMPRESARIAL DE LOS INSTRUMENTOS Y DATOS INFORMATICOS.

La actividad de prevención y control empresarial incluye la práctica de controles de los instrumentos electrónicos facilitados a sus trabajadores, pudiendo efectuar registros informáticos y adoptar las medidas oportunas para vigilar el cumplimiento de las obligaciones laborales de sus empleados. Esta actividad de control no puede practicarse de modo arbitrario, sino respetando el marco de derechos relacionados con los trabajadores y su actividad laboral y observando los principios de idoneidad, necesidad y proporcionalidad, que, en su caso, serán valorados por los Tribunales. Y siempre, previa comunicación a los trabajadores de los sistemas de control y consecuencias disciplinarias en caso de mal uso de los mismos, en aras al principio de buena fe.

SEXTA.- DEFINICIÓN DEL HECHO ELECTRÓNICO.

El hecho electrónico se conforma y define desde tres aspectos: 1º Una dimensión técnica-científica. 2º Una dimensión social-empresarial. 3º Una dimensión jurídico-procesal. Desde el punto de vista científico-técnico el hecho electrónico se relaciona con los electrones que son una de las partículas que conforman la estructura atómica de la materia y al mismo tiempo con la electrónica entendida como el ámbito físico de actuación de electrones caracterizado principalmente por el movimiento. Para su manifestación y percepción por nuestros sentidos precisa de técnicas y dispositivos de captación, reproducción y/o traducción. En segundo lugar, desde una dimensión social el hecho electrónico se incardina en nuestra realidad y es lo que le convierte en objeto de interés para la contienda jurídica y la prueba en el proceso. Y en tercer y último lugar, el hecho electrónico actúa en el proceso jurisdiccional como tal hecho. En definitiva el adjetivo electrónico no modifica los requisitos y exigencias legales que debe cumplir cualquier hecho para ser introducido y valorado en el proceso como prueba.

SÉPTIMA.- LA PERSISTENCIA DEL HECHO ELECTRÓNICO.

El hecho electrónico al contrario de lo que suele predicarse se caracteriza por una mayor persistencia o perdurabilidad frente a otros hechos. Debemos matizar entre la persistencia del «hecho electrónico» y la volatilidad de la «expresión del hecho electrónico». Un registro electrónico es mucho más persistente que incluso una huella en un papel, por lo tanto el hecho electrónico se caracteriza por su persistencia y no por su volatilidad. Distinta del «hecho electrónico» en sí lo es «la expresión de ese hecho electrónico» como, por ejemplo, una muestra de datos en pantalla o un bit producido en un determinado momento, esa expresión del mismo sí se caracteriza por su volatilidad.

OCTAVA.- ACTIVIDAD Y ALMACENAMIENTO DE DATOS O DOCUMENTOS ELECTRÓNICOS.

El hecho electrónico puede almacenarse en soportes. Estos soportes suelen ser dispositivos de almacenamiento de datos, documentos o de registro de sucesos, que dan cuenta de la actividad electrónica producida en un determinado tiempo. Ello sin perjuicio de poder realizar una pericia técnica en tiempo real del comportamiento de un determinado sistema informático. En cualquier caso, debemos distinguir los dispositivos técnicos que realizan las actividades programadas para cada máquina, de los dispositivos terminales que ofrecen los

resultados en forma de imagen o de documento escrito. Desde este punto de vista, debemos tener clara la diferencia entre la actividad electrónica que se produce mediante fenómenos físicos de esa naturaleza y los resultados ofrecidos en los terminales de salida de datos que se ofrecen, por ejemplo, en una imagen.

NOVENA.- LÍMITES DE LA INVESTIGACIÓN DEL HECHO ELECTRÓNICO.

La investigación y pericia del hecho electrónico debe tener lugar con pleno respeto de los derechos fundamentales, puesto que en caso contrario los informes periciales pueden ser declarados nulos e ineficaces en razón de ser prueba ilícita. Este límite opera, especialmente, cuando la investigación del hecho electrónico afecta a las comunicaciones personales lo que puede implicar la necesidad de acceder a información que pertenece a la esfera privada del individuo y/o que se halla en poder de terceros. El único modo en que tales injerencias puedan considerarse lícitas es que estén reguladas por la ley y sean apreciadas por el Juez, en cuyo caso no existiría afectación de derechos procesales ni fundamentales protegidos por la Constitución Española. El problema se halla en la circunstancia de que la ley no regula esta cuestión mediante una regulación que permita a la parte solicitar al Juez civil autorización para poder acceder a datos o informaciones que puedan afectar al derecho a la intimidad o a las comunicaciones de los ciudadanos y/o se hallen en poder de terceros. La solución no puede hallarse, teniendo en cuenta la cuestión, en una interpretación de las normas de la LEC como las que regulan las diligencias preliminares.

DÉCIMA.- ACCESO AL PROCESO DEL HECHO ELECTRÓNICO.

El hecho electrónico accede al proceso, con carácter general, mediante una prueba pericial. Ahora bien, esto será así siempre que nos estemos refiriendo al hecho electrónico en su acepción más técnica, porque no cabe duda que la plasmación de hechos electrónicos en documentos o imágenes podrá acceder al proceso mediante una prueba documental. Más aún también cabe dar cuenta de la manifestación de un hecho electrónico por medio de la declaración de un testigo que puede dar cuenta de haber visto en una pantalla un determinado correo electrónico o, por ejemplo, una determinada medida o lectura en cualquier dispositivo electrónico. Ahora bien, la clave consiste en distinguir entre el hecho electrónico tal cual es en su auténtica naturaleza y su manifestación en forma de documento o imagen aprehensible para los seres humanos. En este segundo caso no podemos, *estricto sensu*, hablar de hecho electrónico, sino de documentos electrónicos.

DÉCIMO PRIMERA.- SOBRE EL CONCEPTO Y CARACTERISTICAS DE LA PRUEBA ELECTRÓNICA.

Lo que caracteriza a la prueba electrónica frente a los demás tipos de prueba es que su objeto es probar un hecho de naturaleza electrónica que tenga relación con la pretensión de la parte y que pueda ser valorada por el juez. Los hechos de naturaleza electrónica pertenecen a la realidad y no pueden enumerarse son ilimitados, evolucionan con las tecnologías y se amplían en número con el tiempo. Por ello el análisis de la prueba electrónica debe tener en cuenta una primera fase de generación del hecho electrónico y una segunda fase consistente en su documentación y aportación al proceso. La primera fase tiene una base y fundamento netamente técnicos; mientras que la segunda debe analizarse desde presupuestos básicamente jurídicos.

El hecho electrónico se manifiesta en su esencia en el mundo de la física o del lenguaje matemático en forma de impulsos electrónicos, códigos binarios, algoritmos o sistemas de encriptación. Se trata de hechos que contienen información no aprehensible directamente por el ser humano, pero que, sin embargo, puede ser almacenada, examinada, contrastada y valorada en documentos de distinta clase e informes periciales, aportada al proceso y valorada por el tribunal. El modo en el que se documente esta información basada en hechos electrónicos no se halla predefinida en nuestro sistema jurídico que parte de la base de la libertad de prueba. Siendo así, la parte puede dar cuenta del hecho electrónico mediante cualquier clase o medio de prueba. Efectivamente, los hechos de naturaleza electrónica pueden acceder al proceso mediante cualquier medio de prueba de los expresamente previstos por la ley, en cuanto los medios de prueba son tasados. Y si tales hechos de naturaleza electrónica pueden cumplir iguales funciones que otras instituciones jurídicas deben suponer iguales efectos. El artículo 299 apartado segundo de la LEC pretende por una parte englobar en determinados conceptos la realidad que supone el hecho electrónico sin tener en cuenta que dicha realidad es ilimitada y que dicha terminología es inadecuada para describir los conceptos que pretende; y en segundo lugar confunde además esos conceptos con medio de prueba.

DÉCIMO SEGUNDA.- FINALIDAD DE LA PRUEBA PERICIAL DEL HECHO ELECTRÓNICO.

El hecho electrónico, en la mayoría de los casos, suele ser en realidad «accesorio» al hecho fundamental que se pretende probar en el juicio. La prueba pericial electrónica persigue probar o acreditar hechos o una actividad de naturaleza electrónica que fundamenta o tiene relación con la tutela

pretendida en el proceso jurisdiccional. Sin embargo, nótese que si bien existen supuestos en que la finalidad es acreditar un hecho electrónico en sí mismo, la mayor parte de las veces la finalidad perseguida con la aportación de la prueba pericial al proceso es la de acreditar o valorar la certeza de una actividad humana de naturaleza electrónica.

DÉCIMO TERCERA.- PRINCIPIOS DE VALIDEZ Y EFICACIA DE LA PRUEBA ELECTRÓNICA E INFORMATICA.

La prueba electrónica o informática debe observar las normas legales sobre la prueba pericial y contener un análisis basado en procedimientos validados técnica y científicamente. Precisamente, la prueba pericial electrónica o informática puede adolecer de la debida transparencia y conocimiento público de los sistemas de análisis empleados para obtener las conclusiones, en tanto que los peritos suelen utilizar herramientas informáticas protegidas por derechos de propiedad. En ese caso se puede producir una deficiente información sobre la base científica y técnica del análisis que puede invalidar o hacer dudar de las conclusiones del dictamen a las que se habrá llegado por procedimientos no explicitados y por tanto que no son del pleno conocimiento de la comunidad científica.

DÉCIMO CUARTA.- EL PERITO ELECTRÓNICO O INFORMÁTICO

La electrónica y la informática forense son disciplinas que requiere no solo tener conocimientos técnicos y prácticos suficientes sino también conocimientos legales. Sin embargo, la profesión informática carece de regulación y de una titulación oficial unificada existiendo gran cantidad de titulaciones en informática. La falta de verdaderos expertos titulados universitarios oficiales en informática-forense y con experiencia acreditada puede permitir la actuación en juicio como peritos de personas no cualificadas debidamente con consecuencias sobre la eficacia y validez de la pericia informática. Esta posibilidad puede tener lugar, ya que el sistema de listas de peritos no garantiza la profesionalidad ni experiencia de quienes forman parte de las mismas, pudiendo formar parte de las listas para ejercer de peritos judiciales cualquier profesional (en los supuestos de profesiones de colegiación voluntaria) sin necesidad de acreditar requisito. Es por ello que sería aconsejable la unificación de las titulaciones oficiales en un único grado de ingeniería informática en todas las universidades y la existencia de especialización en «*informática forense*» cursando un master que daría lugar a un título oficial universitario. Este último título incluiría no sólo conocimientos técnicos sino también jurídicos. Siendo requisito indispensable

para poder ejercer como perito la necesidad de contar con una experiencia acreditada de entre dos y cinco años.

DÉCIMO QUINTA.- NECESIDAD DE UNA MAYOR PRESENCIA DE LA PERICIAL ELECTRÓNICA E INFORMATICA REALIZADA POR INSTITUCIONES.

En nuestros Tribunales no se hace apenas uso de la pericial corporativa en el ámbito de la evidencia electrónica. Probablemente ello es debido a la falta de Institutos o Instituciones informático-forenses de estudio e investigación de carácter público o privado y de cátedras específicas universitarias. Lo que va íntimamente ligado a la falta y a la inminente necesidad de regulación de estudios y titulaciones universitarias oficiales en informática forense. Y por otro lado, tampoco existen grupos de estudio e investigación dentro de los colegios oficiales, que pudieran emitir dichos dictámenes.

DÉCIMO SEXTA.- REQUISITOS Y CONTENIDO DEL INFORME PERICIAL SOBRE HECHOS ELECTRÓNICOS.

El dictamen pericial constituye un medio de prueba (art. 299 LEC) que será objeto de valoración por el juez a cuyo fin resulta fundamental que el informe se estructure de una forma clara y que contenga todos los elementos e información necesarios para que el juez pueda conocer y entender las operaciones y razonamientos llevados a cabo por el perito y a través de los cuales formula finalmente sus conclusiones. Lo anterior incluye tanto los exámenes, métodos, experimentos e investigaciones efectuadas por el perito como los fundamentos técnicos y científicos en que se basa. También será importante describir, en su caso, todas las operaciones de aprehensión y custodia de los datos y/o dispositivos con el fin de garantizar su integridad, conservación e inalterabilidad. Resulta especialmente importante que los peritos faciliten al tribunal las máximas de experiencia epistemológicas o netamente metodológicas relacionadas con el caso en concreto.

DÉCIMO SÉPTIMA.- VALORACIÓN POR EL JUEZ DEL INFORME PERICIAL SOBRE HECHOS ELECTRÓNICOS.

La valoración por parte del Tribunal del dictamen del perito se fundamenta en la libre y sana crítica razonada del dictamen pericial en el marco de los hechos debatidos en el proceso. A ese fin, el tribunal realiza un ejercicio complejo en el que tiene en cuenta las conclusiones contenidas en el informe con relación a los hechos objeto de enjuiciamiento en el marco amplio de la prueba practicada y

la carga de la prueba. El tribunal también valorará otros criterios como son la cualificación del perito (competencia profesional, especialización, curriculum profesional etc.), la solvencia o prestigio de la institución que lo emite de tratarse de pericial corporativa, o el criterio mayoritario de los dictámenes que concurren. En cualquier caso, el juez no puede dar valor concluyente a una prueba científica sin valoración crítica alguna, ya que la calificación como científica de una prueba no le otorga valor irrefutable o de prueba tasada. A ese fin, resulta necesario que los jueces se formen en materias tales como la epistemología y la metodología científica, con la finalidad de realizar mejor su función en una sociedad de creciente complejidad científica y técnica.

DÉCIMO OCTAVA.- SOBRE LA PRUEBA PERICIAL DE OFICIO COMO DILIGENCIA FINAL.

La importancia fundamental de la pericial como prueba determinante de la resolución de los litigios ha conducido a la coexistencia de una pericia que se denomina judicial junto a la pericia de parte. No obstante la pericia judicial no puede, en el momento presente, acordarse de oficio, sino a instancia de las partes, solución que comparto. No obstante, entiendo que una interpretación amplia de la regulación de las diligencias finales permite que el tribunal pueda acordar prueba pericial de oficio en los casos en los que el juez necesite conocimientos técnicos, científicos o prácticos en la materia y las partes no los hayan aportado o de aportarlos no fueran suficientes para poder adoptar una resolución.

DÉCIMO NOVENA.- SOBRE LOS CONSEJEROS TÉCNICOS DEL JUEZ O «*TECHNICAL ADVISOR*».

Una figura de especial interés en el marco del conocimiento y mejor resolución de los procedimientos en los que el conocimiento de la técnica y/o la ciencia son determinantes para la resolución de los litigios es la del Consejero técnico del Juez o «*technical advisor*». Se trata de un experto que no emite un dictamen pericial, sino que ilustra al juez de como es el conflicto desde el punto de vista técnico, permitiéndole conocer el problema y guiar el proceso con mayor idoneidad técnica. Dicho experto no aporta evidencia, no investiga fuera del caso, no ofrece su opinión sobre el mismo y se nombra con fundamento en el poder inherente del juez. El experto consejero del juez es considerado como empleado público y cobra por sus servicios. En Estados Unidos, como anteriormente hemos indicado, pese a la existencia de esta figura del consejero del juez o «*technical advisor*», durante mucho tiempo han existido reticencias por parte de los jueces americanos al nombramiento de estos asesores ya que

ello supone asumir un poder tradicionalmente reservado a las partes en dicho sistema. Desde mi punto de vista no cabe descartar su regulación en nuestro sistema, en tanto que es evidente la gran complejidad técnica de muchos asuntos. Desde ese punto de vista puede plantearse la posibilidad excepcional de que el tribunal pueda disponer de un experto de referencia imparcial. Es de hecho lo que sucede en el proceso penal con la pericial de laboratorios oficiales y con la asistencia de los médicos forenses en procesos penales y en los civiles no dispositivos. Ciertamente, en el proceso civil se ventilan derechos privados, pero también es cierto que en muchas ocasiones las resoluciones civiles tiene efectos sobre el conjunto de la sociedad.

* * *

BIBLIOGRAFIA

AAVV, *Directors and Corporate Advisor Guide to Digital Investigations and Evidence*, Information assurance advisory council (IAAC), Segunda Edición, Version, 2.1, www.iacc.org.uk, enero 2009.

AAVV, *Good Practice Guide for Computer-Based Electronic Evidence*, association of chief police officers (ACPO), publicado por 7safe, disponible en www.7safe.com/electronic_evidence/ , Reino Unido, 2009.

AAVV, *Guía práctica de la ley 11/1997, de acceso electrónico de los ciudadanos a los servicios públicos* (LAECSP), Comisión de Modernización y Calidad de la Federación Española de Provincias y Municipios (FEMP).

AAVV, *Informe Cloud Computing en España 2013,* Penteo. Disponible en la página web http://www. penteo.com

AAVV, *Informe de recomendaciones del Grupo de Expertos de Alto Nivel para la agenda digital para España*, Ministerio de Industria, Energía y Turismo, Gobierno de España. Puede consultarse este artículo en la dirección electrónica goo.gl/aCg9C.

AAVV, *Las Tecnologías de la Información en la empresa Española 2012*, Informe elaborado por ESADE – Penteo. Disponible en la dirección electrónica http://www. penteo.com.

AAVV, *Libro blanco de titulación de grado en ingeniería informática*, ed. Agencia Nacional de Evaluación de la Calidad y Acreditación, Madrid, marzo, 2005.

ABEL LLUCH, X.*, Derecho probatorio,* ed. Bosch, Barcelona, 2012.

El interrogatorio de partes en la Ley 1/2000, de Enjuiciamiento Civil, ed. Bosch, Barcelona, 2008

El interrogatorio de testigos, en la obra en la obra colectiva del mismo título, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.4, Colección de Formación Continua de la Facultad de Derecho ESADE, ed. J.M. Bosch, Barcelona, 2008

El reconocimiento judicial en la obra en la obra colectiva "La prueba de reconocimiento judicial", ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios

prácticos sobre los medios de prueba, núm.4, Colección de Formación Continua de la Facultad de Derecho ESADE, ed. J.M. Bosch, Barcelona, 2012.

Iniciativa probatoria de oficio en el proceso civil, ed. Bosch, Barcelona, 2005.

La configuración de las reglas de la sana crítica en la LEC, Revista Vasca de Derecho Procesal y Arbitraje, Vol. 2, Tomo XXV, 2013-2, 06/2013, págs. 135-166.

La prueba documental, en la obra colectiva del mismo título, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.4, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M., ed. Bosch, Barcelona, 2010.

La prueba electrónica, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.4, Colección de Formación Continua de la Facultad de Derecho ESADE, ed. J.M. Bosch, Barcelona, 2011.

La prueba pericial, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.3, Colección de Formación Continua de la Facultad de Derecho ESADE, ed. J.M. Bosch, Barcelona, 2009.

III. ¿Puede el juez al amparo del artículo 429.1.11 Ley de Enjuiciamiento Civil sugerir la práctica de una prueba pericial?, en "Jurisprudencia sobre derecho probatorio", Diario La Ley, Año XXXIV, Núm. 8187, 8 de noviembre de 2013, págs. 26-28, disponible en www.diariolaley.es.

Sobre la prueba y el derecho a la prueba en el proceso civil, en "*Objeto y carga de la prueba civil*", Picó i Junoy, J., y Abel Lluch, X., ed. J.M. Bosch Editor, Barcelona, 2007.

El dictamen médico-legal en supuestos de responsabilidad profesional médica: fuentes y contenido, ABEL LLUCH, X; ARIMANY-MANSO, J; GÓMEZ DURÁN, E.L., artículo inédito y facilitado por los autores.

ALMAGRO SERVET, Vicente. *La reforma de la prueba pericial en el proceso civil en la Ley 13/2009*, Revista de Jurisprudencia, núm. 4, 28 de julio de 2011. Puede consultarse en El Derecho.com/civil/.

ALONSO-CUEVILLES SAYROL, J. *La audiencia previa,* en "Instituciones del nuevo Proceso Civil. Comentarios sistemáticos a la Ley 1/2000", ed. Difusión Economist & Jurist, Barcelona, 2000.

ALVAREZ-CIENFUEGOS SUAREZ, J. M., *La libertad informática, un nuevo derecho fundamental en nuestra Constitución, Comentario a las sentencias del Tribunal Constitucional 290/2000 y 292/2000, de 30 de noviembre, sobre la Ley de Protección de Datos*, publicado en el diario La Ley de 22/01/01, sección doctrina.

ANZENHOFER, HEIM, SCHULTHEISS, WEBER, *Curso Moderno de electricidad*, Montesó Editor, Barcelona 1971.

ARAGONESES MARTÍNEZ, S., HINOJOSA SEGOVIA, R. y otros, *Cien cuestiones controvertidas en el proceso civil*, ed. Colex, Madrid, 2004.

ASENCIO MELLADO, J.M, *Proceso civil práctico,* Gimeno Sendra., V. (dir), t. IV, ed. La Ley, Madrid, 2005.

BANACLOCHE PALAO, J, *La pericia: claves para un planteamiento eficaz de la prueba,* en rev. Iuris, núm. 71, abril 2003.

Las diligencias prelimares, Thomson-Civitas, Madrid, 2003.

BARRIUSO RUIZ, C. *La contratación electrónica*, ed. Dykinson, Madrid, 1998.

BEVILACQUA, M., *¿Qué es el computer forensics?,* en e-newsletter Cybex, septiembre, 2008, núm. 41, págs. 21-24

BECKETT, Jason. Thesis: *Forensic Computing: A Deterministic Model for Validation and Verification through an Ontological Examination of Forensic Functions and Processes*. Adelaide South Australia, January 2010. School of Computer and Information Science. Division of Information Technology, Engineering, and the Environment. University of South Australia, disponible en http://www.tesisenred.net/.

BERNING PRIETO, A. D., *Derecho de la contratación electrónica*, Noticias Jurídicas, Artículos Doctrinales: Derecho Informático, Junio 2008. Puede consultarse este artículo en la dirección electrónica http://goo.gl/55KCX

BIA, A., *La preservación digital ¿un problema tecnológico u organizativo?,* en "El documento electrónico: aspectos jurídicos, tecnológicos y archivísticos", Universitat Jaume I, Castelló de la Plana, 2008.

BONET NAVARRO, A., *Los recursos en el proceso civil,* ed. La Ley, Madrid, 2000.

BORNARDELL LOZANO, R., *La firma electrónica. Especial consideración de sus efectos jurídicos*, Notariado y contratación electrónica, Consejo General del Notariado, Madrid, 2000.

BUENO DE LA MATA, F., *Prueba electrónica y proceso 2000, ed*. Tirant Lo Blanc, Valencia, 2014.

CABEZUDO RODRÍGUEZ, N., *Omisiones del legislador procesal ante los medios de prueba tecnológicos*, rev. La Ley, T.5, 2004.

CALVO GONZÁLEZ, S., *Compatibilidad entre la pericial de parte y la pericial judicial en la LEC 2000*, en Problemas actuales de la prueba civil, en la obra colectiva del mismo título, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), J.M. Bosch, Barcelona, 2005.

CANELO, C., ARRIETA, R., MOYA, R., ROMO R. *Documento electrónico, aspectos procesales*, Revista Chilena de Derecho Informático. Puede consultarse en la dirección electrónica http://goo.gl/PbqBH

CARNELUTTI, F., *La Prueba Civil*, ed. Arayu, Buenos Aires, 1955.

La Prueba Civil (Traducción Alcalá-Zamora y Castillo), 2ª ed., ed. Depalma, Buenos Aires, 1982.

Sistema de Derecho Procesal Civil, Trad. Alcalá Zamora y Sentís Melendo, t. II, Buenos Aires, 1944,

CARRERAS LLANSANA, J., *Facultades materiales de dirección*, Estudios de Derecho Procesal, Librería Bosch, Barcelona, 1962.

CHICO FERNÁNDEZ, T, *La facultad del juez de indicar la insuficiencia de la prueba propuesta y la preclusión probatoria. A propósito del art. 429.1.II y III LEC,* en "Aspectos Prácticos de la Prueba civil", Abel Lluch, X y Picó i Junoy, J (dirs), J.M. Bosch editor, Barcelona, 2006.

CHOZAS ALONSO, *La prueba del interrogatorio de testigos en el proceso civil*, ed. La Ley, Madrid, 2001.

CONNELLY, M., MUIR, J., *Special Masters, Court-Appointed Experts and Technical Advisors In Federal Court*. Full, Defense Counsel Journal. Jan2009, Vol. 76 Issue 1, págs. 77-90. 14p.

CORDÓN MORENO, *Entorno a los poderes de dirección el juez civil*, Revista de Derecho Privado, 1979, nº 9.

CORTÉS DOMINGUEZ, V. *Derecho Procesal Civil*, 4ª ed., ed. Colex, Madrid, 2001.

CRUZ RIVERO, D., *Eficacia formal y probatoria de la firma electrónica*, ed. Marcial Pons, Madrid, 2006.

CURTIN, C. Matthew. *Introduction to Forensic Computing*, ISACA Journal Online, 2006, disponible en www.isaca.org.

DARAHUGE, M.E Y ARELLANO GONZALEZ, L.E. *Manual de Informática Forense (Prueba Indiciaria Informático Forense)*. Ed. Errepar, Buenos Aires, 2012.

DE HOYOS SANCHO, M., *Hacia un proceso civil más eficiente: Comunicaciones telemáticas. El sistema "Lexnet"*, en "Oralidad y escritura en un proceso civil eficiente", Carpi, F., y Ortells Ramos, M.P, Vol. II, ed. Universitat de Valencia, 2008. Puede consultarse este artículo de De Hoyos Sancho en la dirección electrónica uv.es.

DE LA OLIVA, A y FERNÁNDEZ, M.A., *Derecho Procesal civil II, Objetos, Actos y Recursos del proceso civil. El proceso civil de declaración, e*d. Centro de Estudios Ramón Areces, Madrid, 1993.

DE LA RUA NAVARRO, J, *La facultad del art. 429.1, II y III LEC y la preclusión probatoria. ¿Puede el juez proponer medios de prueba cuyo momento procesal ha precluído (ej. Dictámenes y documentos)?,* en "Problemas actuales en la prueba civil", Abel Lluch, X y Picó i Junoy, J (coords), J.M. Bosch, Barcelona, 2005.

El "posicionamiento" ante documentos y dictámenes en la audiencia previa, en "Aspectos prácticos de la prueba civil". Abel Lluch, X., y Picó y Junoy. (dirs.), ed. J.M Bosch editor, Barcelona, 2006.

DE URBANO CASTRILLO, E., *La valoración de la prueba electrónica*, ed. Tirant lo Blanc, Valencia, 2009.

La prueba tecnológica en la Ley de Enjuiciamiento Civil, (con MAGRO SERVET, V.), ed. Thomson-Aranzadi, Cizur Menor, Marzo 2003.

DEVIS ECHANDÍA, H, *Teoría general de la prueba judicial,* t. II, 5ª ed, ed. Víctor P. de Zavalía, Buenos Aires, 1981.

DI IORIO, A. J., *Prueba anticipada,* ed. Abeledo-Perrot, Buenos Aires, 1970.

DÍAZ FUENTES, A., *La prueba en la nueva Ley de Enjuiciamiento Civil,* 2ª ed. Bosch, Barcelona, 2003.

DÍEZ PICAZO GIMENEZ I., (con DE LA OLIVA SANTOS), *Derecho Procesal Civil. El proceso de declaración*, ed. Universitaria Ramón Areces, Madrid, 2004.

DONOSO, Lorena. *Firma electrónica: análisis del estatuto jurídico en Chile*, en "Tópicos esenciales de Derecho Informático", Centro de Estudios en Derecho Informático, Facultad de Derecho, Universidad de Chile, 2003.

ELÍAS BATURONES, JJ. *La prueba de documentos electrónicos en los Tribunales de Justicia*, ed. Tirant Lo Blanch, Valencia, 2008.

EUGENIO DÍAZ, F., *La protección de la intimidad y el uso de Internet* en "*Informática y derecho",* Revista Iberoamericana de Derecho Informático*,* número 30-32, España, 1999.

EYNER ISAZA, H. *La prueba electrónica en Panamá y en el sistema interamericano,* ed. Universal Books, Panamá, 2013.

FAIREN GUILLÉN, V., *El Proyecto de la Ordenanza Procesal Civil Austríaca visto por Franz Klein*, Estudios de Derecho procesal, Revista de Derecho Privado, Madrid, 1955.

FERNÁNDEZ, I., *Comentarios a la ley de enjuiciamiento civil*, vol. I, ed. Aranzadi, Elcano (Navarra), 2001.

FERNANDEZ BLEDA, D., *Informática Forense*. *Teoría y Práctica*, Hackmeeting, Sevilla, 2004.

FERNÁNDEZ ESTEBAN, M. (con ARAGÓN REYES, M.), *Nuevas Tecnologías, Internet y Derechos Fundamentales,* ed. McGraw-Hill*,* Madrid ,1998.

FERNÁNDEZ LÓPEZ, M., *Las facultades probatorias del juez civil previstas en el art. 429.1.11 LEC,* artículo publicado en la revista jurídica Práctica de Tribunales, Revista de Derecho Procesal Civil y Mercantil, núm. 21, noviembre de 2005. Puede visualizarse en formato PDF en la página web rua.ua.es.

FERNÁNDEZ RODRÍGUEZ, J. J., *Secreto e intervención de las comunicaciones en Internet*, ed. Thomson Civitas, Madrid, 2004.

FERNÁNDEZ SEIJÓ, J.M, *Comentario al artículo 373*, en el "Proceso Civil", vol. III, ed. Tirant Lo Blanch, Valencia, 2004.

FLORES PRADA, I., *La prueba pericial de parte en el proceso civil,* ed. Tirant Lo Blanch, Valencia, 2005.

FONT SERRA, E., *El dictamen de peritos y el reconocimiento judicial en el proceso civil,* ed. La Ley, Madrid, 2000.

La prueba de peritos en el proceso civil español, ed. Biblioteca hispano europea de ciencias sociales, Barcelona, 1974.

FRÍAS MARTÍNEZ, E**.**, *El acceso a los datos de carácter personal por la Policía. Referencia a los datos de la Seguridad Social*, en artículos doctrinales sobre Derecho Informático, publicado en julio de 2012 en Noticias Jurídicas. Puede consultarse en la siguiente dirección electrónica http://goo.gl/B78QYd,

GARBERÍ LLOBREGAT, J. y BUITRON RAMIREZ, G, *La prueba civil,* ed. Tirant lo Blanch, Valencia, 2004.

GARCÍA GONZÁLEZ, C. *El nuevo régimen de peritos designados judicialmente*, en "La prueba pericial, el perito y la nueva Ley de Enjuiciamiento Civil", Jornada del Colegio de Abogados del Ilustre Señorío de Bizkaia, Bilbao, 2001.

GARCÍA PAREDES, A., *La prueba en juicio: ¿y si es electrónica?*, en revista Contratación Electrónica, núm. 62, julio 2005.

GARCIANDÍA GONZALEZ, P., *Del dictamen de peritos,* en *"Comentarios a la Ley de Enjuiciamiento Civil",* F. Cordón Moreno, T. Armenta Deu, J. Muerza Esparza y T. Tapia Fernández (coord.), edit. Aranzadi, Navarra, 2001.

GASCÓN ABELLÁN, M., LUCENA MOLINA, J. J. y GONZÁLEZ RODRÍGUEZ, J. *Razones científico-jurídicas para valorar la prueba científica: una argumentación multidisciplinar,* Diario La Ley, Nº 7481, Sección Doctrina, 4 oct. 2010, Año XXXI, Ref. D-292, ed. La Ley.

GÓMEZ DEL CASTILLO Y GÓMEZ, M. M., *Aproximación a los nuevos medios de prueba en el proceso civil*, en "*Derecho y Conocimiento"*, vol. 1, ed. Facultad de Derecho, Universidad de Huelva, 2001. Puede consultarse en formato pdf en uhu.es.

GÓMEZ ORBANEJA, E (con HERCE QUEMADA, V.), *Derecho Procesal Civil*, vol. 1, 8ª ed. Madrid, 1976.

GONZÁLEZ MONTES, Conceptos Básicos en Derecho Procesal Civil, ed. Tecnos. Madrid, 2010,

GONZÁLEZ SÁNCHEZ, J.L., *Comentario al art. 24*, en "La nueva Ley de Internet (Comentarios a la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico)", Cremades, J. y González Montes, J.L. (coords.), ed. La Ley, Madrid, 2003.

GOTZONE MUGICA ARRIEN, *Los contratos Informáticos*, Saberes, Revista de estudios jurídicos, económicos y sociales, vol. I, 2003, separata, Universidad Alfonso X El Sabio. Puede consultarse este artículo en la dirección electrónica goo.gl/2Z2yH o www.uax.es/publicaciones/archivos/SABDER03_029.pdf

GUASP, J., *Comentarios a la Ley de Enjuiciamiento Civil,* t.II, vol. 1º, 2ª parte, M. Aguilar, editor, Madrid, 1947.

Derecho Procesal Civil, (con ARAGONESES, J), t.I, 7ª ed, ed. Aranzadi, Navarra, 2005.

La prueba en el proceso civil español: principios fundamentales, en "Estudios Jurídicos", 1ª ed, ed. Civitas, Madrid, 1996.

GUZMAN FLUJA, V., en *El proceso civil,* v. III, Escribano Mora, F. (coords.), ed. Tirant Lo Blanch, Valencia, 2001.

HESS, ROBERT L., *Judges cooperating with scientists: A proposal for more effective limits on the federal trial judge's inherent power to appoint technical advisors*, v. II, Vanderbilt Law Review 54. 2 , Marzo 2001.

ILLÁN FERNÁNDEZ, J. Mª, *La prueba electrónica, eficacia y valoración en el proceso civil. Nueva oficina judicial, comunicaciones telemáticas (Lexnet) y el expediente judicial electrónico. Análisis comparado legislativo y jurisprudencial*, ed. Aranzadi, Navarra, 2009.

ILLESCAS RUS, V. *El dictamen de peritos, "La prueba en la nueva Ley de Enjuiciamiento Civil*", jornada monográfica A Coruña, 4 de mayo de 2001, organizada por Enfoque XXI y el Ilustre Colegio Provincial de la Coruña.

INSA, F., *Procedimiento de obtención y análisis forense de dispositivos electrónicos*, en "Jornadas sobre Prueba electrónica, obtención, admisibilidad y jurisprudencia" organizadas por la Sección de Derecho de las Tecnologías de Información y Comunicación del Colegio de Abogados de Barcelona en fecha 26 de enero de 2011.

Pruebas electrónicas ante los tribunales en la lucha contra la cibercriminalidad. Un proyecto europeo, (con LÁZARO HERRERO, C; GARCÍA GONZÁLEZ, N.), en Revista Venezolana de Información, Tecnología y Comunicación, año 5, mayo-agosto, 2008.

JAUME BENNASAR, A., *La validez del documento electrónico y su eficacia procesal*, ed. Lex Nova, Valladolid, 2010.

KÜSTER, I. y HERNÁNDEZ, A., *De la Web 2.0 a la Web 3.0: antecedentes y consecuencias de la actitud e intención del uso de las redes sociales en la web semántica*, Universia Business Review, primer trimestre 2013. Puede consultarse este artículo en la dirección electrónica http://goo.gl/05iV0

LASARTE, C., *Comunicaciones electrónicas peer-to-peer (P2P) versus Derechos de Autor*, Diario La Ley, num. 6951, 2008. Puede consultarse en www.fundacionblu.org.

LECOURS, A. P., *Usa Patriot Act. Efectos extraterritoriales de la Ley Patriota de los EEUU. Derechos de Privacidad de los ciudadanos norteamericanos*, La Crónica Jurídica, actualización octubre 2007, disponible en http//goo.gl/w24Xi o ponce.inter.edu

LESSIG L., *On the futures of IP Law,* Digital Law 1st world congress, ICAB, 29 de junio 2012. Puede consultarse este artículo en la dirección electrónica http://goo.gl/bbhTM.

LÓPEZ CUMPA, J., *La evolución de la Web,* Slideshare, 2012. Puede consultarse este artículo en la dirección electrónica http://goo.gl/pMylT o slideshare.net.

LÓPEZ-FRAGOSO ÁLVAREZ, T., *Las intervenciones telefónicas en el proceso penal*, ed. Colex, Madrid, 1991.

LOSADA, G., MARCO, C. Y ROMERO, C., *Destrucción de documentación confidencial,* Universidad Complutense de Madrid, no consta fecha. Puede consultarse en formato pdf en la página web gpd.sip.ucm.es.

MAGRO SERVET, V., *La reforma de la prueba pericial en el proceso civil en la Ley 13/2009*, Revista de Jurisprudencia, núm. 4, 28 de julio de 2011. El Derecho.com/civil/

La Prueba pericial civil en la LEC y en la Ley de Ordenación de la edificación, La Ley, Madrid, 2007.

MARTÍN LLORENTE, I., *Modelo orientado a procesos para la toma de decisiones sobre seguridad en tecnologías de la información dentro de una organización*, ponencia III, XX Seminario Duque de Ahumada., no consta fecha. Puede consultarse en formato pdf en la página web portal.uned.es.

MARTÍN MORALES, R., *El régimen constitucional del secreto de las comunicaciones*, ed. Civitas, Madrid, 1995.

MARTÍNEZ DE CARVAJAL HEDRICH, E., *Informática Forense, 44 casos reales*, ed. Ernesto Martínez de Carvajal Hedrich, Julio, 2012.

MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003, de firma electrónica*, 2ª ed., ed. Civitas, Madrid, 2009.

MENÉNDEZ FRAGUA, S., *Aplicación de técnicas heurísticas como salvaguarda de los derechos fundamentales en la búsqueda y filtrado de documentación en periciales informáticas,* artículo INCIDE, 2011.

MENÉNDEZ FRAGUA, S. y PASAMAR, A. *¿Cómo se pueden salvaguardar los derechos fundamentales al realizar investigaciones informáticas?,* en "Preguntas con respuesta: La prueba a consulta", Diario La Ley, 7 de noviembre de 2011. Puede consultarse en www.diariolaley.com.

MIRA ROS, C., *La prueba documental electrónica: algunas concesiones a la seguridad jurídico preventiva*, en "Oralidad y escritura en un proceso civil eficiente", vol. II, Carpi, F. y Ortells, M. (eds.), Universitat de Valencia, 2008.

MIRANDA VÁZQUEZ, C., *¿Es realmente el Juez el "peritus peritorum"? (Propuesta de reformulación del brocardo y análisis del alcance efectivo de la valoración judicial de la prueba pericial)* en "Derecho Probatorio Contemporáneo. Prueba científica y técnicas forenses", Bustamante, M.M. (coord), Universidad de Medellín, 2012.

MONTERO AROCA, J., *La prueba en el proceso civil*, 5ª ed., ed. Civitas, Madrid, 2007.

Presentación de documentos materiales con la demanda y contestación, en Revista Poder Judicial, núm. 17, Madrid, 1990.

MONTÓN REDONDO, A., *Medios de reproducción de la imagen y del sonido*, en "La prueba", Montero Aroca, J. (dir.), Cuadernos de Derecho Judicial, núm. VII/2000, CGPJ, Madrid, 2000.

MORALES PRATS, F., *La tutela penal de la intimidad: privacy e intimidad,* ed. Destino, Barcelona, 1984.

MUÑOZ SABATÉ, Ll., *¿Cómo afecta a la intimidad y al secreto de las comunicaciones la prueba electrónica en el ámbito laboral?* Preguntas con respuesta: La prueba a consulta. Diario La Ley, 7 de noviembre de 2011. Puede consultarse en www.diariolaley.com.

Curso sobre Probática Judicial, ed. La ley, Madrid, 2009

Fundamentos de la Prueba judicial civil LEC 1/2000, ed. J.M. Bosch Editor, Barcelona 2001.

Introducción a la probática. Serie Manuales y Monografías. núm. 1, Colección de Formación Continua de la Facultad de Derecho ESADE, ed. J.M. Bosch, Barcelona, 2007.

NIEVA FENOLL, J., *La prueba en documento multimedia*, en "Jurisdicción y proceso", ed. Marcial Pons, Madrid, 2009.

El recurso de casación civil, ed. Ariel, Barcelona, 2003.

NUÑEZ LAGOS, *Concepto y clases de documentos*, Revista de Derecho Notarial, núm. XVI, abril-junio de 1957.

ORELLANA CASTRO, R., *Lo que vale un perito,* publicado en Cuadernos de Probática, Diario La Ley 1260/2011, 8 de febrero de 2011, págs. 14-15.

ORMAZÁBAL SÁNCHEZ, G., *La prueba documental y los medios e instrumentos idóneos para reproducir imágenes o sonidos o archivar o conocer datos,* ed. La Ley, Madrid, 2000.

Informática y prueba judicial. Especial referencia a la firma electrónica en "*Empresa y prueba informática*", Colección de Formación continuada Facultad de Derecho de ESADE, ed. Bosch Educación, Barcelona 2006.

ORTELLS RAMOS, M., *Objeto, eficacia jurídica e impugnación del documento notarial. Reflexiones sobre el art. 17 bis, apartado 2, de la Ley del Notariado*, Revista Crítica de Derecho Inmobiliario, núm. 684, julio-agosto, 2004.

ORTUÑO NAVALÓN, MC, *La prueba electrónica ante los Tribunales,* ed, Tirant Lo Blanc, Valencia, 2014.

PASAMAR, A., *Empresa y prueba informática*, en el libro del mismo título "Empresa y prueba informática", Abel Luch, X. (dir.), Colección de Formación Continua de la Facultad de Derecho ESADE-URL, J.M. Bosch editor, Barcelona, 2006.

PEREDA GAMEZ, F.J. , *La prueba pericial en los litigios derivados de la Ley de la edificación,* en "*La prueba pericial en el proceso civil*", Ledesma Ibáñez, P y Zubiri de Salinas, F (dirs), Cuadernos de Derecho Judicial, núm. XII/2006, CGPJ, Madrid, 2006

PÉREZ GIL J., *Documento informático y firma electrónica: aspectos probatorios,* en "El comercio electrónico", Echebarría Sáenz J. A., (coord.), ed. Edisofer, Madrid, 2001.

PICÓ Y JUNOY, *Admisibilidad de la prueba pericial* en"La prueba pericial", ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.3, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, Barcelona, 2009.

Problemas actuales de la prueba civil, en la obra colectiva del mismo título, ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), J.M. Bosch, Barcelona, 2005.

El derecho a la prueba, J.M. Bosch, Barcelona, 1996.

La iniciativa probatoria del juez civil. A propósito de un caso, en "Los poderes del Juez Civil en materia Probatoria", ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), J.M. Bosch, Barcelona, 2003

La prueba ilícita en el Proceso Civil Español, artículo publicado en la revista electrónica Temas Actuais de Processo Civil, v.I, n. 5, Noviembre de 2011, puede consultarse en www.temasactuaisprocessocivil.com.br.

La prueba pericial en el proceso civil español, JM Bosch editor, Barcelona, 2001.

Valoración de la prueba y segunda instancia civil: hacia la búsqueda del necesario equilibrio, en Revista Jurídica de Catalunya, núm. 3-2009.

PRENAFETA RODRÍGUEZ, Javier. *Sobre el contrato de Escrow: Naturaleza jurídica y algunos problemas.*, Noticias jurídicas, artículos doctrinales, derecho informático. Marzo, 2002. Puede consultarse en la página http://goo.gl/pEyq6

PRIETO CASTRO y FERRANDIZ, L. *Derecho Pocesal Civil, 5ª* edit, ed. Tecnos, Madrid, 1989.

PUYOL, DANIEL. *La importancia de estar preparados para cualquier litigio.* Conferencia Online sobre software y soluciones TIC para que los documentos electrónicos e e-mail mantengan valor probatorio. Puede consultarse esta última en la página web Demosdesoftware www, it-latino.net. o goo.gl/dTnCn.

RAMOS MÉNDEZ, F. *Enjuiciamiento Civil,* t. I, ed. Atelier, Barcelona, 2008.

RAMOS ROMEU, F. y CAÑABATE PÉREZ, J. *Los datos digitales en el proceso civil: prevención, producción y autenticación*, Revista Jurídica de Catalunya, núm.1-2011. Pág. 57-98.

RICHARD GONZÁLEZ, M., *Admisibilidad, eficacia y valoración de las pruebas neurológicas en el proceso penal,* Revista Iuris, Probática, Coord. Instituto de Probática y Derecho del Proceso de la Facultad de Derecho ESADE-URL, 2ª enero de 2014, págs. 36- 41.

La cadena de custodia en el proceso penal español, Diario La Ley 8236/2013, Año XXXIV, Número 8187, Viernes, 8 de noviembre de 2013, pág. 3-4, www.diariolaley.es.

La impugnación y revisión de la prueba mediante recursos ordinarios y extraordinarios en el proceso penal, en "Estudios sobre Prueba Penal", volumen III, Richard González Manuel y Abel Lluch, Xavier (dirs.), ed. La Ley, Madrid, 2013.

Reflexiones sobre la práctica y valor de la prueba científica en el proceso penal (a propósito del asunto de los niños desaparecidos en Córdoba), en Diario La Ley, año XXXIII, núm. 7930, 25 de septiembre de 2012. Puede consultarse en la página web www.diariolaley.es.

RIFÀ POUS, Helena, SERRA RUIZ, Jordi y RIVAS LÓPEZ, José Luis, *Análisis Forense de Sistemas Informáticos,* Rifà Pous, Helena, y Serra Ruiz, Jordi (coords), septiembre de 2009, ed. UOC. Puede consultarse en la página web webs.uvigo.es.

RIFA SOLER, J.M., *Aspectos procesales referentes a la impugnación y valoración de la prueba pericial en el proceso civil*, Actualidad Civil, nº 17, 2010. Disponible en dialnet.unrioja.es.

Comentario al art. 356, en "Comentarios a la nueva Ley de Enjuiciamiento Civil", T. II, Fernández Ballesteros, M.A., Rifa Soler, J.M., y Valls Gombau, JF (coord.), ed. Atelier, Barcelona, 2000

Pericia de parte vs. Pericia judicial. La pericia dirimente. Ponencia presentada en el Congreso Europeo de Peritaje Judicial, celebrado en Barcelona, durante el mes de octubre de 2008.

RIVES SEVA, A. P., *La intervención de las Comunicaciones en la Jurisprudencia Penal*, ed. Aranzadi, Navarra, 2000.

RIZO GÓMEZ, B., *La anticipación de la prueba en el proceso civil*, ed. Tirant Lo Blanc, Valencia, 2010.

RODRÍGUEZ LAINZ, J.L, *El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones*, Diario La Ley, Nº 6859, Sección Doctrina, 11 Ene. 2008, Año XXIX, Ref. D-10, ed. LA LEY; diario La Ley, Nº 6860, Sección Doctrina, 14 Ene. 2008, Año XXIX, Ref. D-10, ed. LA LEY, La Ley 7062/2007, pág. 10.

RODRÍGUEZ RUIZ, B., *El secreto de las comunicaciones: tecnología e intimidad*, ed. Mc Graw Hill, Madrid, 1998.

ROWLINGSON, R., *A Ten Strep Process for Forensic Readines,* International Journal of Digital Evidence, v.2 I. 3, 2004. Disponible en www.ijde.org.

SACRISTÁN REPRESA, G., *Comentario al art. 384 LEC*, en "Comentarios a la nueva Ley de Enjuiciamiento Civil", t.II, Fernández-Ballesteros, Rifá-Soler, Valls Gombau (coords.), ed. Atelier, Barcelona, 2000.

Comentarios al art. 382 LEC, en "Comentarios a la nueva Ley de Enjuiciamiento Civil", Rifá-Soler J.Mª (coord.), ed. Iurgium, Barcelona, 2000.

*La prueba documental en la nueva ley de enjuiciamiento civi*l, Cuadernos de derecho judicial, en "La prueba", v. II., CGPJ, Madrid, 2000.

SALOM CLOTET, J., *Delito Informático y su Investigación,* Ponencia IV, en "Ponencias XX Seminario Duque de Ahumada. Seguridad y Nuevas Tecnologías". Puede consultarse en la página web portal.uned.es.

SAMANES ARA, C., *Comentario al art. 384 LEC,* en "Comentarios a la Ley de Enjuiciamiento Civil", vol.I, Cordón-Moreno, Armenta-Deu, Muerza-Esparza y Tapia-Fernández (coords.), ed. Aranzadi, Navarra, 2001.

SANCHIS CRESPO, C., *La prueba por medios audiovisuales e instrumentos de archivo en la LEC 1/2000 (Doctrina, jurisprudencia y formularos)*, ed. Tirant lo Blanch, Valencia, 2002.

SEGOVIA ARROYA, J. A, *¿Es el informe profesional del detective privado equivalente a un dictamen pericial*?, Derecho.com, 15 de febrero de 2003, puede consultarse en http://goo.gl/iSHW0q.

SENTÍS MELENDO, S, *La prueba*. Los grandes temas del derecho probatorio, EJEA, Buenos Aires, 1979.

SERRA DOMÍNGUEZ, M. *La prueba documental,* en "Instituciones del nuevo proceso civil. Comentarios Sistemático a la Ley 1/2000, de Enjuiciamiento Civil", vol. II, Alonso-Cuevilles Sayrol, J. (coord.), ed. Dijusa, Barcelona, 2000.

La prueba pericial, en "Instituciones del nuevo proceso civil. Comentarios sistemáticos a la Ley 1/2000", vol. II, Alonso-Cuevilles Sayrol, J (coord.) edit. Difusa, Barcelona 2000.

Liberalización y socialización del proceso civil, Revista de Derecho Procesal Iberoamericana, 1972, nº 2 y 3, págs. 520 y ss.

El recurso de casación en la LEC 1/2000, en Revista Jurídica de Catalunya, 2001, núm. 4.

SUÁREZ GONZÁLEZ, C., *Introducción al nuevo régimen jurídico del dictamen de peritos. Aportación al proceso, tacha, recusación y régimen económico*, en "La prueba pericial, el perito y la nueva Ley de Enjuiciamiento Civil", Jornada del Colegio de Abogados del Ilustre Señorío de Bizkaia, Bilbao, 2001, pág.5.

TARUFFO, M., *La prueba de los hechos* (traducción Jordi Ferrer Beltrán), ed. Trotta, Madrid, 2002.

VÁZQUEZ IRUZUBIETA, C., *Comentarios a la nueva ley de Enjuiciamiento Civil. Doctrina y jurisprudencia de la ley 1/2000, de 7 de enero*, ed. Dijusa, Madrid, 2000.

VAZQUEL VILLAR, A**.**, *Las medidas cautelares en el proceso penal por delitos ambientales. Fallos y doctrina de la Patagonia*, Alveroni Ediciones, revista trimestral, año II-núm. 2, marzo de 2007, pág. 13. Puede consultarse en la página web http://goo.gl/eL8o8.

VELÁZQUEZ VIOQUE, D., *Dictamen por perito designado a instancia de parte* en "La prueba pericial", ABEL LLUCH, X. y PICÓ i JUNOY, J. (dirs.), Serie estudios prácticos sobre los medios de prueba, núm.3, Colección de Formación Continua de la Facultad de Derecho ESADE, J.M. Bosch, Barcelona, 2009.

VIADA LOPEZ-PUIGCERVER, C., *Naturaleza jurídica de la pericia*, en "Anuario de Derecho Penal", Madrid, 1951, pág. 48.

YAÑEZ VELASCO, R, *El peritaje en el proceso civil,* ed. Grupo Difusión, Madrid 2005.

ZUCCARDI, G. y GUTIÉRREZ, J.D., *Informática Forense,* artículo publicado en ECURED, noviembre de 2006. Puede consultarse dicho artículo en la dirección electrónica http://goo.gl/j1XZu

* * *