X CONFERENCIA ANUAL EBEN (JUNIO 2002)

COMUNICACION

TITULO: **LA SEGURIDAD JURIDICA EN EL ENTORNO DE LAS TECNOLOGIAS DE LAS TELECOMUNICACIONES Y LA INFORMACION. NUEVOS INSTRUMENTOS JURIDICOS EMERGENTES.**

AUTOR:

- **FRANCISCO DE QUINTO ZUMARRAGA**
- **ABOGADO Y ECONOMISTA**
- **SOCIO DEL BUFETE PIQUE ABOGADOS ASOCIADOS**
- **DOCTORANDO EN LA FACULTAD CC. ECONOMICAS (UNIVERSITAT DE BARCELONA) y en la UNIVERSITAT OBERTA DE CATALUNYA (Programa de Doctorado de la Sociedad de la Información y el Conocimiento).**
- **Miembro del EBEN ESPAÑA.**

FECHA: **28 de mayo de 2.002.**

1. **EL ENTORNO DE LAS NUEVAS TECNOLOGIAS.**

   1.1. **LA DIGITALIZACION Y SUS EFECTOS.**

   1.2. **UN NUEVO PARADIGMA Y SU INCIDENCIA SOBRE EL DERECHO.**

2. **LOS COMPONENTES DE LA SEGURIDAD EN UN ENTORNO TIC'S.**

   2.1. **APROXIMACION AL CONCEPTO SEGURIDAD.**

   2.2. **LOS COMPONENTES DE LA SEGURIDAD EN EL ENTORNO TIC'S.**

   2.3. **LOS CONFLICTOS ENTRE DERECHOS FUNDAMENTALES; SEGURIDAD, PRIVACIDAD Y LIBERTAD.**

3. **LOS NUEVOS INSTRUMENTOS JURIDICOS.**

   3.1. **LA AUDITORIA ETICA.**

   3.2. **LOS CODIGOS TIPO (ó ETICOS).**

   3.3. **EL ARBITRAJE.**

   3.4. **LA AUDITORIA JURIDICA Y EL INFORME DE "DUE DILIGENCE".**

   3.5. **LOS PROCEDIMIENTOS OBLIGATORIOS EN ENTORNOS CONCRETOS (obligaciones entre partes contratantes).**

   3.6. **LA PRUEBA PERICIAL EN EL ENTORNO TIC'S (COMPUTER FORENSICS).**

1. EL ENTORNO DE LAS NUEVAS TECNOLOGIAS.

1.1. LA DIGITALIZACION Y SUS EFECTOS.

Cabe incorporar una técnica que podría definirse como inamovible y omnipresente en el fenómeno de convergencia tecnológica que nos ocupa; me refiero a la DIGITALIZACION. La digitalización se puede sintetizar como la técnica que permite la sustitución de átomos por bits, la substitución de lo real por lo virtual. Ella aporta elementos fundamentales para el éxito del modelo, sea éste cual sea; rapidez, economía y fidelidad al modelo. Los dos primeros elementos son de naturaleza cuantitativa y por lo tanto medibles. Por el contrario el tercero de ellos es cualitativo y en síntesis consiste en la perfecta replicación de los contenidos originales (ya sean imagen, sonido o audiovisuales) de modo que resulta imposible la distinción entre las copias y su original.

Vamos a intentar una aproximación comprensible sobre las repercusiones que la digitalización proyecta sobre el ámbito de la seguridad en el entorno T.I.C..

Las dos primeras consecuencias/efectos de la digitalización provocan la doble "desubicuación" espacial y temporal configurando un nuevo plano relacional que ha dado en denominarse "realidad virtual". Este término no es más que un oximorón y como tal no hace más que aportar confusión e inseguridad en el ámbito de las nuevas relaciones; económicas, sociales, jurídicas, políticas, educativas, etc. ¿Cómo incide este nuevo plano relacional es en la correcta aceptación e implantación social de las TIC'S? Indudablemente aporta más preguntas que respuestas, más ruido que música. En definitiva genera inseguridad. Esta nueva percepción genera una exigencia a la regulación jurídica de las nuevas tecnologías (quizás cabría hablar de un Nuevo Derecho, como se habla de las nuevas tecnologías y hasta de la nueva economía), al tiempo que define las circunstancias que dificultan enormemente la concienciación de respuestas eficaces a las nuevas exigencias. En este orden de consideraciones y tan sólo a modo de ejemplo podríamos señalar:

a) ¿Cómo es posible compatibilizar un entorno territorial como la U.E. con una rígida regulación sobre la intimidad y privacidad de los ciudadanos europeos, con la posición U.S.A. al respecto a partir de una absoluta desregulación legal? La respuesta la encontraremos en el acuerdo EU/USA sobre Protección de Datos Personales conocido como "Safe Harbour".

b) ¿Cómo adaptar los convenios internacionales sobre Propiedad Intelectual (Comercio de Berna de 1.886 y sus sucesivas actualizaciones) y la Directiva Europea 01/29/CE de la C.E. y el Consejo sobre el particular a una realidad caracterizada por la desubicación especial?

c) Generalizando la anterior dificultad en relación con la protección de la propiedad intelectual, también cabría preguntarse cómo definir las jurisdicciones civiles y penales y su legitimación para entender en conflictos reales generados en un espacio virtual.

A modo de ejemplo citamos el acuerdo alcanzado por una treintena de países, entre ellos los pertenecientes a la U.E., U.S.A., Canadá, Japón y Sudáfrica, el pasado 23 de noviembre de 2.001 en Budapest. Se trata de; *"el primer acuerdo internacional contra los delitos en el ciberespacio. El acuerdo alcanzado incluye 48 artículos que han sido objeto de múltiples retoques y debates políticos durante los cuatro años de trabajo que se han invertido en el proyecto. El acuerdo es un referente histórico innegable ya que se trata del primer consenso internacional sobre el tema, aunque no faltan aspectos polémicos. Uno de ellos son los capítulos que atañen a la privacidad de los usuarios. El segundo, es la aplicación real que harán los respectivos gobiernos, ya que países como Estados Unidos, tras los ataques terroristas del 11 de septiembre, han anunciado medidas especiales de vigilancia y control sobre Internet"*.

El primer acuerdo internacional contra el crimen en Internet se conoce como CONVENCION SOBRE EL CIBERESPACIO y se basa en tres grandes principios:

a) Definir de un mismo modo las prácticas delictivas en Internet. Esta unidad de criterio es aceptada por todos los países firmantes de la convención.

b) Aceptar, por parte de todos, reglas comunes para los procesos penales que entiendan de este tipo de delitos.

c) Establecimiento de la suficiente cooperación internacional que funcionará de modo permanente a través de equipos de control comunes en cada país.

"El consenso alcanzado entre los países no ha sido total. Europa se ha opuesto a la idea norteamericana de crear una policía sin fronteras para la red. Y las peticiones de Alemania y Francia para que se prohibiesen todos los contenidos xenófobos y racistas en Internet han sido aplazadas por Estados Unidos, que ha argumentado el gran valor que su Constitución da a la defensa de la libertad de expresión. El caso se ha incluido en un protocolo anexo y se debatirá de nuevo el próximo año".

El tercero y último efecto de la digitalización antes apuntado el relativo a la fidelidad, por no decir exactitud, de la copia respecto al original lo que a su vez provoca una necesidad absoluta de replantear los grandes principios jurídicos en que se basa la regulación de la Propiedad Intelectual.

Retomando una perspectiva más elevada podemos detectar la incidencia de la digitalización en nuestro entorno. En opinión de Manuel Castells Sociólogo de la Universidad de Columbia, el proceso de digitalización de la tecnología en el ámbito de Internet se caracteriza por:

a) Ha generado una arquitectura abierta y gratuita configurada a partir de redes y nudos.

b) La esencia de Internet es la interacción entre productores y usuarios. Valga como ejemplo la realidad del e-mail.

c) Internet segmenta y discrimina los hábitos y la cultura con mayor fuerza que la cultura en general. De ahí que se comience a definir la llamada "quiebra generacional".

d) Variación en los flujos financieros y en los métodos de valoración a partir de la capacidad para generar aceptación en los mercados.

e) Internet acelera la crisis de las organizaciones tradicionales y la aparición de nuevas organizaciones a partir de intereses comunes. Aparecen nuevos movimientos en torno a "valores comunes".

f) Surge la dialéctica entre las Redes Globales (utilizadas por el poder y recientemente por el anti-poder del terrorismo) y las Redes Locales que son aquellas utilizadas por la gente normal.

g) A nivel político, los partidos y las organizaciones utilizan Internet, pero a diferencia de los demás sectores, lo hacen unidireccionalmente, como si de un mero "tablón de anuncios" se tratara.

h) Privacidad: Se deben separar dos planos distintos desde esta perspectiva:

- INTERNET
  - GOBIERNO ——— CIUDADANOS
  - CIUDADANOS —— CIUDADANOS

Según Castells se puede concluir que Internet es la Nueva Sociedad, a la que incorpora la novedad de su estructura en "Sociedad Red".

1.2. UN NUEVO PARADIGMA Y SU INCIDENCIA SOBRE EL DERECHO.

Desde la mitad de los años sesenta, un nuevo sistema tecnológico viene desplazando gradual y progresivamente el anterior que surgió a finales del S. XIX. Entendiendo por paradigma científico (según la definición de T.S. KUHN[1]) como; "las realizaciones científicas universalmente aceptadas que, durante cierto tiempo, proporcionan modelos de problemas y soluciones a una comunidad científica". La adquisición de un nuevo paradigma así como del tipo más avanzado y esotérico de investigación que dicho paradigma permite, es un signo de madurez en el desarrollo de un campo científico concreto.

En nuestro caso el paradigma superado que apareció a caballo entre los dos siglos anteriores estaba basado en las siguientes tecnologías: acero, cemento, aleaciones y plásticos. Sus realizaciones genéricas fueron: la electricidad, el motor de explosión, equipamientos, sistemas y productos relacionados con aquellos materiales y las nuevas fuentes de energía. Por contra, ahora, el paradigma emergente se basa en cuatro grupos de tecnologías genéricas; microelectrónica, biotecnología, nuevos materiales y electróptica. Su acierto es que, gracias a la incorporación del enfoque de las ciencias de la complejidad, ha sabido adoptar el enfoque capaz de permitirle

[1] Thomas S. Kuhn: "La estructura de las revoluciones científicas. "Fondo de Cultura Económica 1.962. University of Chicago Press y 2.000 Madrid decimonovena reimpresión.

realizaciones a partir de plantear cambios de escala, ritmos y alianzas. De este modo aparecen como efecto la Nanotecnología (por cambio de escalas al definir problemas y soluciones) y las TIC'S al plantear nuevas alianzas y convergencias.

La cuestión radica en definir si estamos ante un "Nuevo Paradigma Científico" con vocación interdisciplinar y todo apunta en la dirección de una respuesta afirmativa. La amplitud del campo científico afectado por la "Revolución Digital" abarca al menos las siguientes disciplinas; Física, Biología, Economía y Derecho.

El núcleo duro del cambio consiste en que se ha evolucionado en la relación entre los individuos y los grupos con el entorno desde una Estructura Jerarquizada (vertical), pasando por una Estructura Matricial (horizontal), hasta una Estructura en Red que, tras una primera definición bidimensional en el plano, ha cobrado volumen y se ha concretado en la famosa GLOBALIZACION (organización a partir de redes sobre esferas).

En opinión de Lluis Mª Pugés; Director General de Esade); "*Cada nuevo paradigma tecnológico comporta una nueva forma de organizar la producción y el trabajo, conceptos estratégicos nuevos y una más compleja internacionalización de las actividades. El resultado operativo es el siguiente; integración de operaciones internas y externas de la empresa, descentralización, flexibilidad y rapidez. En el ámbito de la función se detecta un desplazamiento desde las tareas de poca calificación y repetitivas, hacia aquellas que exigen polivalencia y flexibilidad. Se premia la capacidad de dirigir personas y equipos y de trabajar con diferentes culturas. El cambio tecnológico exige la formación permanente y se pasa de la "Sociedad de la producción" a la "Sociedad del Conocimiento"*".

Por su parte Barry Wellman, Profesor de Sociología de la Universidad de Toronto[1] ha dedicado su esfuerzo investigador en determinar como las TIC'S (fundamentalmente Internet) han influido en el reforzamiento, supresión o innovación de los modelos standars de relación entre los individuos y los grupos y entre diferentes grupos. A grandes rasgos su conclusión no puede ser más tajante; realmente estamos ante un nuevo paradigma en el ámbito de la Sociología. Es importante recordar que ello supone que los sociólogos disponen de un nuevo abanico de realizaciones que les permite plantear nuevas preguntas y nuevas respuestas. A nivel de detalle con cierta perspectiva, sus conclusiones se pueden concretar como sigue:

a) Los trabajadores tienen más intimidad para realizar su trabajo. Las relaciones entre compañeros y con los superiores se estructuran de forma global. La gestión de esta estructura en red, sustituye las tradiciones en árbol jerárquico o matriciales.

b) Las empresas y corporaciones están menos preparadas para afrontar estrategias en términos de autarquía. Las unidades económicas y organizativas se entremezclan en complejas redes de alianzas e intercambios entre ellos, por encima de consideraciones sobre la competencia. Algunos tipos de relaciones

[1] Wellman, Barry; "Living Networked in a Wired World. The Persistence and Transformation of Community. "Report to the law Commission of Canada" 30 octubre 2.001.

entre los componentes de una empresa o sector comienzan a resolverse en el plano virtual, vía videoconferencia.

c) La política de bloques en el comercio y en el Sistema Mundial ha perdido su carácter monolítico, superando así la dinámica resultante del final de la política de bloques generada al principio de los años noventa. Las redes resultantes han propiciado un incremento de las relaciones entre naciones y zonas comerciales.

Todo ello se ha visto fuertemente alterado, en más o en menos, por la situación surgida tras los atentados del 11 de septiembre de 2.001.

A nivel esquemático, Barry Wellman nos propone la siguiente alteración de patrones relacionales y modelos de estructuras:

SOCIEDADES BASADAS EN GRUPOS JERARQUICOS Y MATRICIALES	SOCIEDADES BASADAS EN RELACIONES (SOCIEDAD RED)
- Unidad familiar	- Matrimonios seriados y custodia alternativa de los hijos.
- Vecindad	- Redes dispersas en el espacio real y virtual.
- Organizaciones Voluntarias (Voluntariado)	- Tiempo libre.
- Cara a cara	- Comunicación pública a través de computadoras.
- Espacios abiertos	- Espacios Privados.
- Unidades de trabajo centralizadas	- Organizaciones en red.
- Trabajo en equipo	- Progresar en la profesión.
- Autarquia	- Outsourcing.
- Fábrica, oficina	- Avión, Internet, teléfono, móvil.
- Adscripción a un grupo	- Realización personal.
- Conglomerados	- Alianzas.
- Enfrentamiento de bloques	- Alianzas fluidas y transitorias.

A la vista del anterior resumen, no cabe duda de que algo profundo está cambiando. A pesar de que en unas sociedades el cambio esté más adelantado que en otras, no cabe sino concluir que el futuro, si no el propio presente, es diferente.

2. LOS COMPONENTES DE LA SEGURIDAD EN UN ENTORNO TIC'S.

2.1. APROXIMACION AL CONCEPTO SEGURIDAD.

Es evidente que el término "seguridad" es un vocablo de amplio espectro en el sentido que podemos llegar a definirlo desde diversas aproximaciones del modo más científico y objetivo posible. Pero además cada uno de nosotros tiene una personal interiorización del concepto seguridad.

Cualquier concepto integrante del saber humano, por muy complejo que resulte se puede definir a través de dos caminos diferentes. Uno de ellos consiste en compararlo con conceptos y términos próximos pero distintos, tanto por su complementariedad como por su competitividad. Entendemos por conceptos complementarios aquellos que pueden crecer o decrecer en su gradación de forma paralela. Por contra los competitivos son aquellos que a medida que uno aumenta el otro disminuye y viceversa. En esta línea definitiva podemos señalar que en principio "Seguridad" parece un concepto competitivo de "libertad" en el sentido antes descrito, pero nada más lejos de la realidad porque se llega a un punto de inflexión en la evolución de ambas variables de modo que por debajo de un umbral mínimo de "libertad" la "Seguridad" no solo deja de aumentar sino que también inicia un proceso decreciente pudiendo llegar a niveles bajo mínimos. Siguiendo con el discurso encadenado, si aceptamos que en niveles normales "Seguridad" e "Intimidad" son conceptos complementarios porque se retroalimentan en su evolución ya sea creciente o decreciente y aceptando como cierto el silogismo que vincula "Seguridad" con "Libertad", en los términos antes descritos, podemos llegar a la siguiente paradoja:

1) A más libertad, más Intimidad.

2) A más Intimidad, más Seguridad.

3) En consecuencia a más Libertad más Seguridad lo cual es una contradicción con la vinculación que hemos establecido entre ambas variables en condiciones normales.

Esta paradoja del raciocinio se produce porque los tres conceptos que venimos analizando no son unidimensionales (con permiso de Umberto Eco) sino por al contrario son poliedros de irmumerables caras. Las relaciones causa/efecto son ciertas a medias y en determinadas circunstancias. Sobre el particular Wittgenstein tendría mucho que decir pero intuyo, simplemente intuyo, que su conclusión no se distanciaría mucho de la nuestra.

1. La SEGURIDAD como concepto está profundamente eraizado con el instinto de conservación tanto a nivel de individuo como a nivel de especie y como tal concepto atávico tiene, necesariamente, una descomposición en factores conceptuales integradores. Más adelante habrá ocasión de entrar en dicho desglose.

2. La INTIMIDAD, uno de los integrantes sin duda de la "seguridad", también es un concepto complejo que permite una aproximación multidisciplinar. Siguiendo al Dr. Josep Monserrat Catedrático de la Universitat Ramón Llull cabria una relación directa entre "propiedad" e "intimidad" y así parece confirmarlo el origen histórico de ambos conceptos y sus respectivos derechos vinculados y ahondando un poco más, encontraremos un concepto más profundo e individualista, eco la idea de que; "en la intimidad encuentra refugio aquello que nos define" (sic) en alusión a la persona, espiritual e irreductible al yo diferenciable, etc. ..

3. No podemos hacer abstracción de que estamos intentando proyectar conceptos tradicionales en el plano real sobre un nuevo entorno definido por las TIC'S. Aquí vendría de nuevo al caso todas las reflexiones sobre el posible cambio de paradigma que se han vertido en el epígrafe anterior y cuando menos deberíamos hacer una pregunta: ¿Los integrantes del concepto "Seguridad" en el plano real, son los mismos que ayudan a definir el mismo concepto en el plano virtual? Como primera aproximación ala respuesta vamos a establecer algunos de los componentes que integran el CONCEPTO SEGURIDAD en el PLANO REAL. y con esta finalidad obtenemos, sin ánimo de ser exhaustivos:

   a) DISTANCIA: lejos/cerca.
   b) TIEMPO: inmediato/remoto.
   c) SIMETRIA/ AS IMETRIA: relación indirecta Seguridad/Riesgo.
   d) EQUILIBRIO y ESTABILIDAD: miedo al cambio.
   e) INFORMACION y CONOCIMIENTO: miedo a lo desconocido.

A la vista del anterior despiece y proyectando el contenido del Epígrafe n° 1 anterior sobre el entorno virtual nos vemos obligados a concluir que: "LA SEGURIDAD VIRTUAL ES UN CONCEPTO SUSTANCIALMENTE DIFERENTE DEL TRADICIONAL CONCEPTO DE SEGURIDAD REAL".

- El entorno TIC'S se caracteriza por una desubicación espacio/temporal, en clara incidencia sobre los apartados a), b) y c) anteriores.

- El entorno TIC'S se caracteriza por una creciente aceleración del cambio.

Parece ser que una vez aceptado el NUEVO PARADIGMA no tenemos más remedio que re-definir algunos conceptos profundos y fundamentales, uno de ellos es necesariamente la SEGURIDAD y, en consecuencia, procedemos a su re-definición como antesala necesaria para la definición de nuevas relaciones y nuevas estrategias del individuo y de la Sociedad en el nuevo entorno.

2.2. LOS COMPONENTES DE LA SEGURIDAD EN EL ENTORNO TIC'S.

Abundamos una vez más en nuestra obsesiva fijación consistente en que en el entorno virtual la "Seguridad" debe abordarse necesariamente al menos desde la doble perspectiva técnica y jurídica. Los expertos en Seguridad Tecnológica (recordar a nuestros efectos la tesis de L. Lessig) que son los que trabajan desde hace décadas en la cadena: necesidad —— diagnóstico —— solución, se han puesto de acuerdo tradicionalmente en que la

SEGURIDAD en el nuevo entorno TIC'S viene definida por los siguientes elementos:

COMPONENTES DE LA SEGURIDAD EN UN ENTORNO VIRTUAL DEFINIDO POR LAS TIC'S.

A. CONFIDENCIALIDAD.
B. INTEGRIDAD.
C. DISPONIBILIDAD.
D. AUTENTICIDAD/ AUTENTICACION .
E. NOREPUDIO =A+B+D.

A continuación procedemos a llenar de contenido cada una de las ideas-flashes que acabamos de exponer.

A. CONFIDENCIALIDAD. Es la expresión más próxima a la Tecnología de la Información que presenta el mismo significado que los vocablos INTIMIDAD o PRIVACIDAD que presentan un perfil más coloquial y jurídico.

   Podemos entender por CONFIDENCIALIDAD la cualidad que reviste la información protegida frente a terceros no autorizados. En el ámbito de la información tecnológica estamos en el terreno del secreto de empresa o secreto científico, con ramificaciones excepcionales hacia el "secreto de Estado" y también hacia el "secreto militar". Su homólogo en el ámbito de la información con contenido personalizado lo encontramos en el término INTIMIDAD, entendido como Derecho a preservar la esfera interna, íntima y próxima del individuo frente a su proyección pública. Una de las mejores síntesis en relación con la dialéctica clásica íntimo "versus" público la ha conseguido el ya citado Dr. J. Montserrat, en los siguientes términos: "Nuestra vida parece oscilar entre dos polos de una extraña línea: en un extremo se halla la publicidad absoluta (vida pública) y en el otro, la absoluta soledad (vida privada, intimidad). Se trata de una tensión fabricada, pero no por ello menos tangible. Nuestra época, por múltiples normativas, relacionadas con la tecnología y su complementación en el mundo de las comunicaciones, parece ser una de aquellas en que lo público se filtra en todos los ámbitos de la vida".

B. INTEGRIDAD y D. AUTENTICIDAD (o autenticación).

   Se entiende por INTEGRIDAD la cualidad de un mensaje por lo que resulta imposible su manipulación por persona distinta de su autor. La integridad como concepto persigue que el mensaje no sea alterado en el proceso de transmisión entre emisor y el receptor ya sea de forma intencionada o por error del propio proceso.

   La AUTENTICIDAD o AUTENTICACION, puesto que de las dos formas se define, consiste en la cualidad por lo que en un proceso de comunicación, los sujetos intervinientes; emisor/es y receptor/es, son realmente quienes dicen ser, sin que resulte posible el equívoco de identidades ni la suplantación por parte de terceros.

Abordamos ambos términos de forma conjunta por dos razones:

a) Son conceptos complementarios para blindar un proceso de comunicación en su objeto (contenidos) y en sus sujetos (las partes que intervienen).

b) Los mecanismos conceptuales y tecnológicos desarrollados para su protección tienen un tronco común y se basan en la codificación y encriptación de los mensajes.

Retomando esta última idea podemos decir que el origen y desarrollo de ambas técnicas en el mundo moderno: codificación y encriptación se encuentran en los ámbitos diplomáticos y militar. Posteriormente el centro de interés invade el terreno del "secreto industrial" y no es hasta fecha reciente, cuando se instala plácidamente orientado hacia la protección de los Derechos Humanos llamados de tercera generación, como conceptos capaces de preservar la confidencialidad, intimidad y privacidad de los mensajes y de las personas que los intercambian, dentro del esquema para preservar el cierre o cobertura de las Categorías de Información de O. Gandy.

C. DISPONIBILIDAD. Se trata de la característica por la cual una información está de modo permanente a disposición de los sujetos legitimados para acceder a ella. Estamos en el ámbito de los vulgarmente conocidos como virus y antivirus que por extensión incluyen a figuras como los "troyanos" y los llamados "gusanos".

¿Qué es un virus informático? El término agrupa uno o varios programas de ordenador que actúan de modo coordinado. Se introducen en los sistemas de información por diversas vías de acceso, según la configuración de aquellos y una vez dentro se activan de modo automático con el fin de producir diversos tipos de daños en el sistema. La característica principal de los virus informáticos es su capacidad para propagarse a partir de la auto-replicación.

Las agresiones a la disponibilidad también presentan una doble vertiente ya comentada desde la perspectiva de agresiones/defensas. La tecnología es la reina en este terreno y, lógicamente, también se encuentra sometida a la omnipresente "Ley de Moore". Estamos de nuevo en una alocada carrera armamentista en donde tan importante como los sistemas de ataque se manifiestan los sistemas de defensa; "misiles y antimisiles". Los daños y perjuicios provocados por estas agresiones a la disponibilidad que representan los virus son enormes. Jurídicamente su ámbito se inscribe en el Derecho Penal y su aplicación tiene una doble dificultad:

a) Por un lado la tecnología, consecuencia de lo que podríamos llamar la huida hacia adelante.

b) Por otro lado la jurídica, tanto en la materialización de la prueba como en la persecución y castigo de los culpables en un entorno desubicado especialmente y de difícil asignación de jurisdicción competente. Al lado de los tradicionales "Paraísos Fiscales" comienzan a desarrollarse los balbucientes "Paraísos Tecnológicos" en entornos al margen de cualquier tipo de legislación.

D. NO REPUDIO. Desde una perspectiva legal y jurídica es lógico concluir que cualquier información que goce de los atributos descritos anteriormente en A, B y C se califica como "no repudiable" y su consecuencia más transcendental es que necesariamente debe ser admitida como PRUEBA EN JUICIO. En este sentido y con este propósito se elaboró el Real Decreto Ley 14/1999 de 17 de septiembre sobre la Firma Electrónica, como consecuencia de la transposición obligada de la Directiva de la Unión y del Consejo Europeo de xxx. En su preámbulo, a modo de exposición de motivos, se dice textualmente:

En el Art. 2 se introduce, a nivel jurídico, as definiciones de los instrumentos que hemos visto antes al tratar de la "integridad" y "autenticación" de la información, en los siguientes términos:

"Artículo 2. *Definiciones.*

A los efectos de este Real Decreto-ley, se establecen las siguientes definiciones:

a) «Firma electrónica»: Es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.

b) «Firma electrónica avanzada»: Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo ya los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos."

El espíritu del "no repudio" que es el eje vertebrador del R.D. Ley que nos ocupa se concreta en el Art. 3:

"Artículo 3. Efectos jurídicos de la firma electrónica.

1. *La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales.*

Se presumirá que la firma electrónica avanzada reúne las condiciones necesarias para producir los efectos indicados en este apartado, cuando el certificado reconocido en que se base haya sido expedido Por un Prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma con el que esta se produzca se encuentre certificado, con arreglo a lo establecido en el artículo 2 1.

2. *A la firma electrónica que no reúna, todos los requisitos previstos en el apartado anterior, no se le negarán efectos jurídicos ni será excluida como prueba en JUICIO, por el mero hecho de presentarse en forma electrónica.*

La transcendencia de esta disposición para la pacífica intersección entre el mundo del Derecho y de las Nuevas Tecnologías es fundamental. Se trata del principio de convergencia y yo diría que hasta de reconciliación entre ambos planos de suyo tan distantes y distintos.

2.3. LOS CONFLICTOS ENTRE DERECHOS FUNDAMENTALES; SEGURIDAD, PRIVACIDAD Y LIBERTAD.

Los problemas conceptuales derivados de los temas que hemos analizado en el Apartado 2.1. "Aproximación al concepto de Seguridad" tienen una directa y potenciada repercusión en el plano jurídico de los Derechos Fundamentales de las personas. La controversia tiene su origen en la Ciencia Política con unas raíces en el Derecho Romano, un tronco en la configuración de la Teoría del Estado Liberal (S. XVIII, Hobbes, Rouseau, Hume, etc.) y unas ramas que son los que nos perturban actualmente en un mundo que tiende ala globalización apalancándose en las potencialidades de las TIC'S.

A partir de 1.995 venía alimentándose una polémica entre los partidarios de la libertad y los de la seguridad en Internet. ¿Prima en Internet o debería primar el componente del entorno de libertad? Quizás sería oportuno traer a colación la idea antes comentada de que sin e-confianza no hay e-negocio. La contradicción está magistralmente descrita en palabras de Reg Whitakers ([*]): "El ciberspacio será un tesoro escondido para aquellos que ya posean un tesoro para gastarse. Para el resto de los mortales, puede consistir en un sobrecargado, desordenado, anárquico y desorganizado revoltijo de inforbasura, tan poco valioso que incluso se ha descartado su inclusión en los arcenes de las autopistas de la información" y remata su profecía con la siguiente sentencia; "Incluso Internet, tal y como conocemos actualmente, puede ser reemplazado, y sin duda lo será, por intranets privadas".

En palabras de la Dra. Montserrat Nebrera, Catedrática de Derecho Constitucional de la Universidad Internacional de Catalunya:

"La seguridad es efectivamente un derecho fundamental de los ciudadanos en el sistema constitucional español, y al tiempo un principio fundamental de vertebración del Estado de derecho, es decir, de un tipo de Estado en el

[*] Whitaker, Reg: "El fin de la privacidad". Ed. Paidos Comunicación (1.999) Barcelona.

que se llega a la seguridad personal, entre otras vías, a través de la seguridad jurídica. Pero para conseguir esa seguridad que los ciudadanos reclaman, el Estado impone una contra prestación necesaria: el recorte de ciertos ámbitos de intimidad costosamente ganados en la consolidación de ese Estado de derecho. Por eso es necesario abordar el estudio complementario, a menudo contrario e incluso en ocasiones interesadamente contradictorio de ambas realidades.

La pregunta de obligada formulación en este tema puede resumirse a mi juicio en la cuantificación de las razones que la seguridad puede dar para intentar limitar la intimidad. En los umbrales del nuevo siglo ha quedado claro que no se pueden evitar las intromisiones en la salud personal. Queda también claro que en ocasiones la intimidad puede verse limitada por otros derechos, incluso de menor envergadura, como es el caso de la libertad de empresa o la propiedad privada. Tal es la situación que provocan ciertas medidas de seguridad que puedan implantarse en algunas empresas, o el mero hecho de que se pueda velar por el buen uso de los recursos económicos de la empresa.

Los campos en los que intimidad y seguridad se enfrentan son múltiples. En algunos casos el primado de aquélla está tan claro que se han configurado incluso delitos respecto de su lesión. Otros, en cambio, no lo están tanto, ya por la trascendencia pública del sujeto (y su importancia para la formación de la opinión pública libre), ya por su vinculación al tráfico económico, ya por la intervención del Estado en el ámbito de que se trate.

De todas formas de seguridad, sin duda la seguridad informática es la única que redunda en un reforzamiento de la intimidad de las personas, porque justamente pretende garantizar que no se producirá un tráfico indiscriminado de sus datos, sean éstos los que sean.

La relación entre intimidad y seguridad es, por tanto, plurimorfe, su objetivo ha de ser el respeto de todos hacia todos, es decir, hacia nosotros mismos. Porque el primer presupuesto en la protección de la intimidad es tenerla (es decir, no venderla) y, en la consecución de la seguridad, quererla."

Al inicio del año 2.002 resulta imposible abordar este tema, sin realizar una aproximación desde la perspectiva de la situación internacional surgido tras los atentados del 11 de septiembre de 2.001 en N.Y. y Whasington.

La historia de la globalización no hace referencia tan sólo a sus vertientes tecnológicas y económicas en términos de expansión de mercados. Para entender el fenómeno hay que hacer también una lectura en términos de Derecho y Justicia en su devenir progresivamente internacional:

- La desregularización neoliberal.
- El Sistema de Naciones Unidas (ONU).
- La Unión Europea (VE).
- Cambios en el Derecho de Guerra.
- Normativa internacional sobre medio ambiente (¿Kioto?).

- Constitución reciente del Tribunal Penal Internacional.

Está evolución nos cuenta otra versión de la misma historia, un relato que persigue afianzar la ley, los derechos y las responsabilidades. E. Kant escribía ya en el S.XV111; "una violenta abrogación de la Ley y la Justicia en un lugar determinado tiene consecuencias en otros muchos y se puede experimentar en todas partes". Quizás estaba iniciando el concepto de globalización legal.

También es cierto que un fenómeno nuevo se venía detectando, aún antes del 11-S, en lo relativo al deterioro de la democracia, de los Derechos Humanos y de las libertades. Desde mediados de la década de los setenta se vivió un lento pero constante progreso en el sentido de más democracia, más derechos y más libertad. El fenómeno comenzó en el Sur del Mediterráneo (Portugal, Grecia y España) y pasando por el Este de Europa y Rusia, recaló en América del Sur y su famoso Cono. Por contra, a finales de los noventa se aprecia un punto de inflexión en el proceso, basado en la aparición de lideres populistas en determinados países: Menem (Argentina), Hugo Chavez (Venezuela) y Putin (Rusia) por citar algunos ejemplos y el cambio de todo en políticos democráticos "pura cepa" como Blair, Schroeder, Aznar y más recientemente George Bush. En la reciente cumbre celebrada en Madrid bajo el pomposo título "Conferencia sobre Transición y Consolidación Democráticas" se presentó un estudio de Ronald Inglehart de la Universidad de Michigan sobre el particular. Las conclusiones del Informe Inglehart son sorprendentes:

a) La tentación del autoritarismo es anterior al 11-S y está alimentada por una crisis general de liderazgo político y la derivada sensación de vulnerabilidad, a modo de "Complejo de Edipo" mal resuelto.

b) Amplios sectores de la población están dispuestos a considerar "soluciones autoritarias".

c) La única respuesta a los que atacan a la democracia tan sólo puede ser más democracia.

Lo que resulta incontrovertible es que tras el 11-S el referido punto de inflexión se convierte en punto de ruptura (discontinuidad) y de nuevo podemos hablar de cambio de paradigma en el ámbito de los Derechos y la Justicia. En este sentido es necesario citar la reciente ley aprobada por el Congreso USA a propuesta del Presidente conocida como ATA (Against Terrorism Act).

Además, en el ámbito de las TIC'S no cabe duda de que "pintan bastos". Los SISTEMAS GLOBALES DE VIGILANCIA están a estas horas echando chispas, los conocidos (Carnívoro y Echelon) y los desconocidos por nuevos. Sin duda el futuro inmediato nos traerá sorpresas al respecto. El "código" en la acepción que le atribuye L. Lessig cambiará necesariamente para facilitar el control de la información. Todo ello en detrimento de la libertad de información y de la intimidad de las personas.

Otro ámbito de actividad en la esfera internacional se verá también afectado por un cambio de regulación: el mercado internacional de capitales y de flujos

internacionales financieros, que serán, de hecho lo están siendo ya, regulados de forma muy estricta para impedir la financiación de las actividades terroristas y romper sus vínculos reales con el narcotráfico.

Comienzan a alzarse las sempiternas voces de los pacifistas en el sentido de que la violencia tan sólo engendra violencia, cosa cierta en términos relativos pero nunca en términos absolutos. La doctrina jurídica occidental viene respaldando desde siempre que la LIBERTAD y la SEGURIDAD están por encima de la PAZ. Curiosamente en este análisis libertad y seguridad han dejado de ser términos contrapuestos y se han convertido en complementarios.

3. LOS NUEVOS INSTRUMENTOS JURIDICOS.

Ya hemos dicho que el Derecho siempre va a remolque de la realidad y otra forma de decir lo mismo es que el Derecho siempre acaba por adaptarse a la nueva realidad, con mayor o menor premura. Esta segunda lectura también resulta válida en el entorno TIC'S y es la causa de que en pocos años el mundo del Derecho haya visto cómo cobran nuevo brío instrumentos jurídicos conocidos de siempre pero relativamente poco aplicados, al tiempo que otros han sabido reconvertirse al nuevo entorno y por último, también estamos asistiendo a la definición y aplicación en fase de prueba de nuevos instrumentos jurídicos porque los nuevos problemas exigen nuevas soluciones. Estos pueden venir de la mano de nuevos conceptos e instrumentos o bien mediante la utilización de los clásicos pero aplicados con nuevos criterios. Ambos caminos son los que va recorriendo el Derecho lentamente, o al menos no tan deprisa como nos gustaría, con el fin de aportar soluciones a los problemas que surgen en el nuevo entorno. En este epígrafe procedemos a detallar una exposición de las mismas, de su naturaleza y aplicaciones.

3.1. LA AUDITORIA ETICA.

Todos los lectores conocen sobradamente los conceptos y los procedimientos de los diferentes tipos de "Auditoría" que con mayor o menor perspectiva temporal, se han convertido en habituales no tan solo en los entornos profesionales o de empresa, sino también en los planos social e individual. Nos referimos a los siguientes tipos de auditoría:

- Auditoría Financiera (contable).
- Auditoría Informática (tecnológica).
- Auditoría Medio Ambiental (ecológica).
- Auditoría de Calidad.

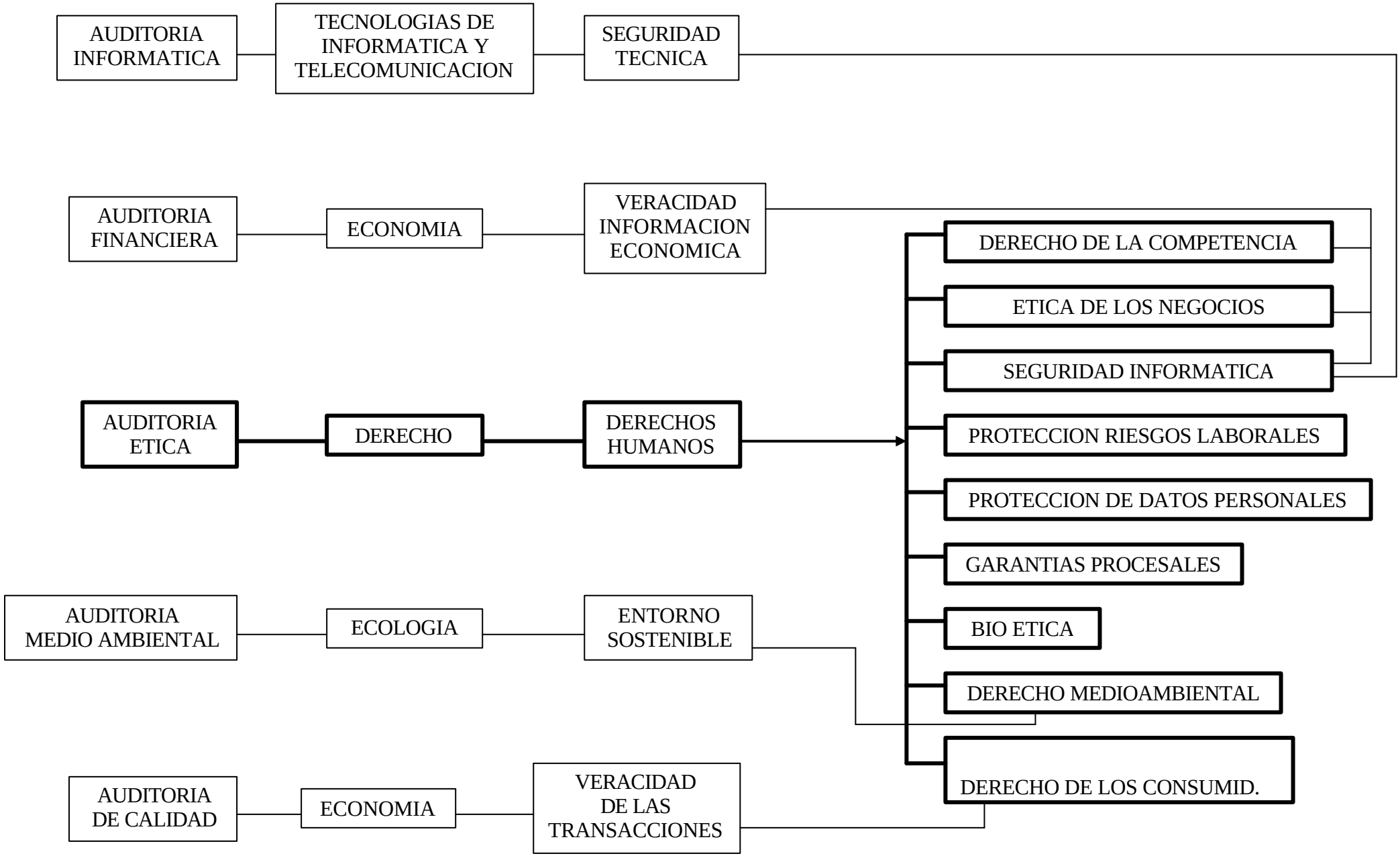
Aprovechando este notorio nivel de conocimiento presentamos el gráfico adjunto en el que se incardina de manera multirrelacional el nuevo concepto que incorporamos: LA AUDITORIA ETICA.

La Auditoría Etica se desarrolla en el ámbito del Derecho y su objetivo consiste en que los ciudadanos del "primer mundo" podamos disfrutar de forma plena y pacífica de todos los Derechos Fundamentales, incluidos los de segunda, tercera y los de la hoy en día incipiente cuarta generación. Para huir de esoterismos aclararemos que por esta incipiente "cuarta generación" de Derechos Humanos se entiende los relativos a la propiedad y uso del propio código genético, la clonación

de individuos, la eutanasia, el derecho al ante/diagnóstico, etc. En resumen aquellos Derechos que vinculan a la persona con las opciones y riesgos de la Bioética.

Se trata pues de un concepto instrumental y material fundamentalmente jurídico y como no podía ser de otra forma, está fuertemente relacionado con los otros tipos tradicionales de auditoría, como se aprecia visualmente en el cuadro adjunto.

La Auditoría Etica actúa como telón de fondo sobre el que se proyectaría entre otros, la Auditoría Jurídica de las Nuevas Tecnologías, de acuerdo con la estructura que hemos expuesto anteriormente. A su vez la proyección, de dicho telón de fondo sobre la realidad económico/empresarial, nos define el concepto y aplicaciones del Informe de "due diligence" que no es más que la traducción práctica del concepto teórico que nos ocupa y que hoy por hoy viene a ser un instrumento de aplicación generalizada en supuestos de fusiones y adquisiciones de empresas donde se ha demostrado muy útil a la hora de evaluar riesgos y contingencias más o menos ocultas. Más adelante tendremos ocasión de volver en detalle sobre este instrumento (ver epígrafe 3.4).


AUDITORIA INFORMATICA
TECNOLOGIAS DE INFORMATICA Y TELECOMUNICACION
SEGURIDAD TECNICA
AUDITORIA FINANCIERA
ECONOMIA
VERACIDAD INFORMACION ECONOMICA
AUDITORIA ETICA
DERECHO
DERECHOS HUMANOS
AUDITORIA MEDIO AMBIENTAL
ECOLOGIA
ENTORNO SOSTENIBLE
AUDITORIA DE CALIDAD
ECONOMIA
VERACIDAD DE LAS TRANSACCIONES
DERECHO DE LA COMPETENCIA
ETICA DE LOS NEGOCIOS
SEGURIDAD INFORMATICA
PROTECCION RIESGOS LABORALES
PROTECCION DE DATOS PERSONALES
GARANTIAS PROCESALES
BIO ETICA
DERECHO MEDIOAMBIENTAL
DERECHO DE LOS CONSUMID.

3.2. LOS CODIGOS TIPO (ó ETICOS).

Se trata de instrumentos que tienen el carácter de códigos deontológicos o de buena práctica profesional que definen y aplican una voluntad de autorregulación en un área específica de la regulabilidad jurídica dentro del ámbito de un colectivo homogéneo; sectorial, geográfico, etc.

Este instrumento jurídico aparece en nuestro ordenamiento jurídico de la mano de la primigenia LORTAD (1.992) en el ámbito de la protección de datos personales y a partir de ahí casi la totalidad de las normas legales que regulan diferentes aspectos de las Nuevas Tecnologías incorporan de modo sistemático el desarrollo de los "códigos tipo" en sus respectivos ámbitos de actuaciones. A modo de ejemplo cabe citar el RDL que regula la Firma Electrónica o la actualmente en proyecto Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI). Pero fraseando el refrán podríamos decir que "algo tendrá el agua para que la bendigan" y además a cada paso.

A modo de ejemplo exponemos la aplicación práctica de este instrumento en el ámbito de la Protección de Datos Personales en España por tratarse de la parcela que ha propiciado un mayor desarrollo normativo y práctico desde su incorporación legal en el ámbito de la hoy derogada LORTAD DE 1.992.

La forma en que el ordenamiento español de protección de datos incorpora la figura del Código tipo se encuentra a medio camino entre la mentalidad europea y la americana sobre el particular. En efecto la postura europea, de larga tradición en los países anglosajones y nórdicos, es reglamentista y rígida por lo que ha conducido a desarrollar jurisdicciones especiales con gran carga de normas, inspecciones y sanciones.

Por el contrario en los E.E.U.U. impera la posición voluntarista de los códigos tipo (no sólo en el ámbito de la protección de datos, por ser práctica muy extendida en las relaciones sociales y mercantiles) basados en la autorregulación de las partes. Es el propio cuerpo del acuerdo libremente aceptado el que se autodepura y si el incumplimiento es grave, se recurre a los tribunales ordinarios para proceder a la sanción del infractor del código.

En España aparece la figura del "Código Tipo" en la derogada L.O.R.T.A.D. y se mantiene en la vigente L.O.P.D.. Tal como está regulado en nuestra norma, es un paso intermedio entre las dos posiciones antes descritas por cuanto no sustituye a lo dispuesto en las leyes, pero se sitúa como una opción voluntaria entre los particulares, organizados en un grupo de intereses y la norma, pero con total y plena sujeción a ésta. El Código Tipo en nuestro ordenamiento está reglado en la L.O.P.D. y controlado en su actividad por la Agencia de Protección de Datos.

3.3. EL ARBITRAJE.

La aparición y desarrollo de la Sociedad de la Información como sociedad en la que sus individuos se relacionan a través de las redes de comunicaciones con una desubicación espacio-temporal ha supuesto una modificación de los modelos de negocio dotándolos de una mayor proyección tanto a nivel estatal como internacional.

Los elementos de comunicación han revolucionado y con ellos los métodos de solución de conflictos. Aún así el arbitraje no es pese a lo que pudiera parecer una nueva vía de resolución extrajudicial de controversias ya que como veremos los Convenios Internacionales de arbitraje datan aproximadamente de mediados del siglo pasado.

El arbitraje en el estado español se halla regulado en la Ley 36/988, de 5 de diciembre, la cual analizaremos a continuación. En primer lugar conviene cuál es el concepto y las características del arbitraje. Podríamos definir al arbitraje como un medio alternativo de solución de controversias por el cual las partes someten a su disputa previo convenio, a un tercero, el árbitro, que será el que decidirá sobre dicha disputa mediante una resolución denominada laudo el cuál será de obligado cumplimiento. Sus características principales son:

- **Especialización**: el árbitro o árbitros designados son expertos en la materia concreta sobre la que se deba resolver. Pensemos la ventaja del arbitraje por ejemplo en el campo relativo al Derecho de las Nuevas Tecnologías o Derecho de la Sociedad de la Información, el cual no se imparte todavía como materia específica obligatoria dentro de la carrera universitaria, y mucho menos durante las oposiciones a judicatura.

- **Rapidez**: los arbitrajes poseen una duración siempre inferior a los procedimientos judiciales.

- **Confidencialidad**: las resoluciones que se deriven de los arbitrajes, al contrario que con la jurisdicción ordinaria, no están obligadas al requisito de la publicidad.

3.4. LA AUDITORIA JURIDICA Y EL INFORME DE "DUE DILIGENCE".

Es la proyección práctica del concepto antes definido de la Auditoría Etica y en síntesis su objetivo consiste en la CERTIFICACION DE PAGINAS WEB que en inglés se conoce como "web trust" enfocado tanto a los negocios entre empresas (B2B), ISP's y autoridades reguladoras, como a negocios entre empresas y consumidores (B2C).

"LAS AUDITORIAS DE SEGURIDAD".

En general el concepto técnico de auditoría extraído del marco jurídico en España relativo a la Auditoría contable y financiera, (ver Ley 8/988 Ley de Contabilidad y Auditoría de Cuentas) podría resumirse en los siguientes términos:

"El término auditoría se aplica al informe emitido por un experto independiente que tras haber aplicado normas técnicas de general aceptación, define una opinión profesional en relación con el ámbito (objeto) revisado, susceptible de provocar efectos frente a terceros en general, al margen de cualquier veleidad de legitimación".

Los términos encerrados en la definición anterior se resumen en:

- Revisión de un entorno determinado.

- Revisión realizada mediante la aplicación de normas técnicas (de procedimiento) generalmente homologados.

- Se concreta en la "opinión profesional" emitida por una "independiente".

- Esta opinión es susceptible de causar efectos frente a terceros en general.

En el ámbito jurídico que nos ocupa la única referencia al término "auditoría" es la recogida en el R.D. 994/99 de 11 de junio, por el que se desarrolla el Reglamento de Medidas de Seguridad de los ficheros que contengan datos de carácter personal. Concretamente en el contenido que define las medidas de seguridad de los ficheros denominados de "nivel medio" sobre los que resulta obligada, la realización de una "auditoría bianual" sobre protección de datos. Dicho esto el marco normativo guarda silencio y las preguntas que nos provocan zozobra por la falta de respuestas son las siguientes:

- ¿Cuál es el contenido y extensión de dicha "auditoría" de protección de datos? No hay respuesta.

- ¿Quién debe hacer dicha auditoría? En un punto de una de las normas sobre protección de datos se dice que podrá ser realizada la auditoría por medios externos o internos. ¿Dónde queda salvaguardada la independencia que se le supone al auditor?.

- En alguno de los R.D. de mediados de los años noventa que regulaban la ya derogada L.O.R.T.A.D., se menciona que la auditoría deberá ser realizada por un "experto en datos". De nuevo nos vemos obligados a cerrar el bucle; ¿qué es un experto en datos? Y de nuevo no tenemos respuesta estructurada en el ámbito legislativo.

Una vez hemos acotado lo que las normas establecen sobre el particular procedemos a desarrollar el contenido del técnico genérico AUDITORIA JURIDICA EN EL AMBITO DE LAS NUEVAS TECNOLOGIAS.

A. METODOLOGIA PARA DESARROLLAR UNA AUDITORIA JURIDICA EN EL AMBITO TIC'S: NECESARIA APROXIMACION INTERDISCIPLINAR: TECNICA Y JURIDICA.

1º Determinar objetivos.

2º Delimitar áreas de actuación.

3º Elaboración de la propuesta de trabajo que deberá explicar la metodología concreta a desarrollar, el programa de tiempos para su realización (calendario) y presupuesto económico.

4º Recabar información sobre el terreno. Para ello se debe desarrollar un trabajo de campo abierto pero estructurado en la medida de lo posible mediante cuestionarios (check-list) para facilitar la recogida de información de la forma más sistematizada posible, en función de las concretas circunstancias

de cada caso. Si el entorno a estudiar estuviera fuertemente estructurado, automatizado y controlado, gran parte de esta fase se podría desarrollar vía Internet, con la consiguiente reducción de costes. En este supuesto la visita sobre el terreno se limita a la inspección física de las medidas de seguridad y al cotejo de los documentos originales.

5º **Análisis de la información recogida**. Cruce de los antecedentes obtenidos en la fase anterior con los siguientes elementos:

a) Marco normativo vigente en cada área examinada.

b) Marco normativo de referencia: Tratados Internacionales, Directivas de la Unión Europea, Convenios de las organizaciones internacionales (OCDE, GATT, etc.) y Códigos Eticos Internacionales.

c) Control Interno; puntos fuentes y débiles.

d) Nivel de aplicación de los instrumentos y estructuras tecnológicas. Determinar el grado de incorporación de las últimas soluciones tecnológicas.

6º **Establecimiento de diagnóstico** en relación con las áreas de actuación y objetivos previamente definidos.

7º **Propuesta de medidas correctoras**, a modo de la carta de recomendaciones usual en el ámbito de la Auditoría Contable.

8º **Emisión de opinión** en el ámbito de lo que sería el espíritu de un informe de "due diligence".

Todo este proceso se debe ejecutar mediante la colaboración entre profesionales técnicos (ingenieros en telecomunicaciones, informáticos, etc.) jurídicos (abogados) y de organización (economistas, graduados sociales, auditores). En caso de no hacerse del modo aconsejado vamos a obtener como resultado final soluciones parciales y en consecuencia ineficaces. Como ejemplo de lo que no se debe hacer, es relativamente frecuente encontrar empresas que para mayor seguridad han aplicado esquemas de Protección de Datos Personales dobles; uno desde la perspectiva jurídica y otro desde la perspectiva técnica. Con ello la empresa cree estar doblemente protegida y la verdad es que tan sólo dispone de dos soluciones parciales que no necesariamente deben satisfacer el 100% de todas las necesidades, debido principalmente a que el trabajo se ha realizado con toda seguridad sin la debida colaboración entre ambos equipos profesionales. El resultado es que con un coste doble seguimos careciendo de la solución total. La situación se agrava lógicamente cuando sólo se aplican de inicio soluciones parciales ya sean éstas tecnológicas o jurídicas.

B. AMBITO DE ACTUACION DE LA AUDITORIA JURIDICA.

Potencialmente el ámbito de actuación está definido por los cinco elementos que hemos expuesto anteriormente como definidores del concepto SEGURIDAD. (ver Apartado 2 xx anterior pág. xx).

- CONFIDENCIALIDAD
- INTEGRIDAD
- ACCESIBILIDAD
- AUTENTICIDAD/AUTENTICACION
- NO REPUDIO

Proyectando estos conceptos sobre el mundo del Derecho, del tradicional y del nuevo, obtendremos las siguientes áreas susceptibles de integrar el contenido de una AUDITORIA JURIDICA:

B.1. PROTECCION DE DATOS PERSONALES.

B.2. FIRMA ELECTRONICA.

B.3. MEDIOS DE PAGO.

B.4. CONTENIDOS.

B.5. CONDICIONES GENERALES DE CONTRATACION.

B.6. FISCALIDAD.

B.7. FRAUDES Y DELITOS.

LA AUDITORIA JURIDICA Y EL INFORME DUE DILIGENCE COMO INSTRUMENTOS DE EVALUACION DE UNA INVERSION.

Desde el punto de vista de concreción del riesgo de una inversión en una empresa concreta que consiste en el otro gran objetivo de la auditoría jurídica exponemos la siguiente metodología:

1. DEFINICION DE DUE DILIGENCE: Conjunto de versiones y análisis sobre las diferentes áreas significativas en aquellos aspectos que resulten de interés para un comprador o vendedor en el proceso de evaluación y valoración de una inversión en una empresa.

2. AREAS POTENCIALES DE INVESTIGACION: El alcance de la investigación varía de acuerdo con el tipo de comprador (inversor financiero vs inversor industrial) y la sociedad objetivo.

	Inversor	
	Financiero	Industrial
Auditoría	X	X
Análisis de la información financiera	X	X
Análisis de la información de gestión	X	
Aspectos fiscales	X	X

Aspectos legales mercantiles	X	X
Aspectos medioambientales	X	X
Aspectos organizativos	X	
Estudios de mercado	X	
Tecnología de la información y seguridad informática: - PROTECCION DE DATOS PERSONALES. - AUTENTICACION: firma digital y certificados electrónicos. - DEFENSA DE CONTENIDOS: Patentes y Marcas y Propiedad Intelectual. - REGISTRO DE NOMBRES DE DOMINIO. - REQUISITOS DE CONTRATACION "ON LINE" - FISCALIDAD EN INTERNET. - POLITICAS DE PREVENCION FRENTE AGRESIONES.	X	X
Consultoría de negocios y estratégica	X	
Recursos humanos y selección de directivos	X	
Expertos industriales	X	
Riesgos laborales	X	X

3. CONTENIDO DE UNA INVESTIGACION:

- Análisis financiero:

  - Análisis del performance histórico.

    - Historia y visión global.
    - Análisis de la información financiera.

  - Análisis del cash flow.

  - Evaluación de los sistemas de información y de la calidad de la información generada:

    - Procesos financieros básicos.
    - Evaluación de los criterios contables.
    - Revisión de estados financieros.

  - Proyecciones financieras.

- Análisis de negocio y de mercado:

  - Estrategia Corporativa y competencia.
  - Producción.
  - Productos/Servicios.
  - Clientes y mercados.
  - Proveedores y subcontratistas.
  - Organización de la empresa.
  - Estructura comercial y procedimientos de marketing.

- Otros aspectos.

- Análisis legal, laboral y fiscal:

  - Aspectos fiscales.
  - Aspectos laborales:

    - Aspectos generales.
    - Análisis de riesgos laborales.

  - Aspectos mercantiles y societarios.
  - Otras áreas del derecho.

- Aspectos medioambientales.
- Patentes y avances tecnológicos:

  - Patentes más importantes: fechas de finalización, posible impacto en caso de pérdida.
  - Posible infracción por uso de patentes pertenecientes a terceros.
  - Susceptibilidad a avances tecnológicos.

- Investigación y Desarrollo:

  - Areas actuales de concentración de I&D.
  - Desarrollos propios vs desarrollos de terceros.
  - Involucración de la Dirección.

4. ANALISIS LEGAL, DESARROLLO DEL AMBITO TIC'S.

- **Aspectos fiscales**: Análisis dirigido a verificar el normal cumplimiento por parte de la Sociedad Objetivo de sus obligaciones fiscales, así como a cuantificar las contingencias que por tales conceptos pudieran existir.

- **Aspectos laborales:**

  - **Aspectos generales:** Analizamos la situación laboral y de seguridad social de la Sociedad Objetivo con la finalidad de detectar cualquier aspecto y contingencia que pudiera tener relevancia para nuestro cliente a la hora de adoptar una decisión definitiva respecto de la conveniencia de realizar la adquisición, o las condiciones de la misma.

  - **Análisis de riesgos laborales:** El objetivo de nuestro trabajo es el de evaluar y cuantificar aquellas contingencias y riesgos laborales que se derivan de las actuaciones llevadas a cabo por la Sociedad Objetivo en esta materia.

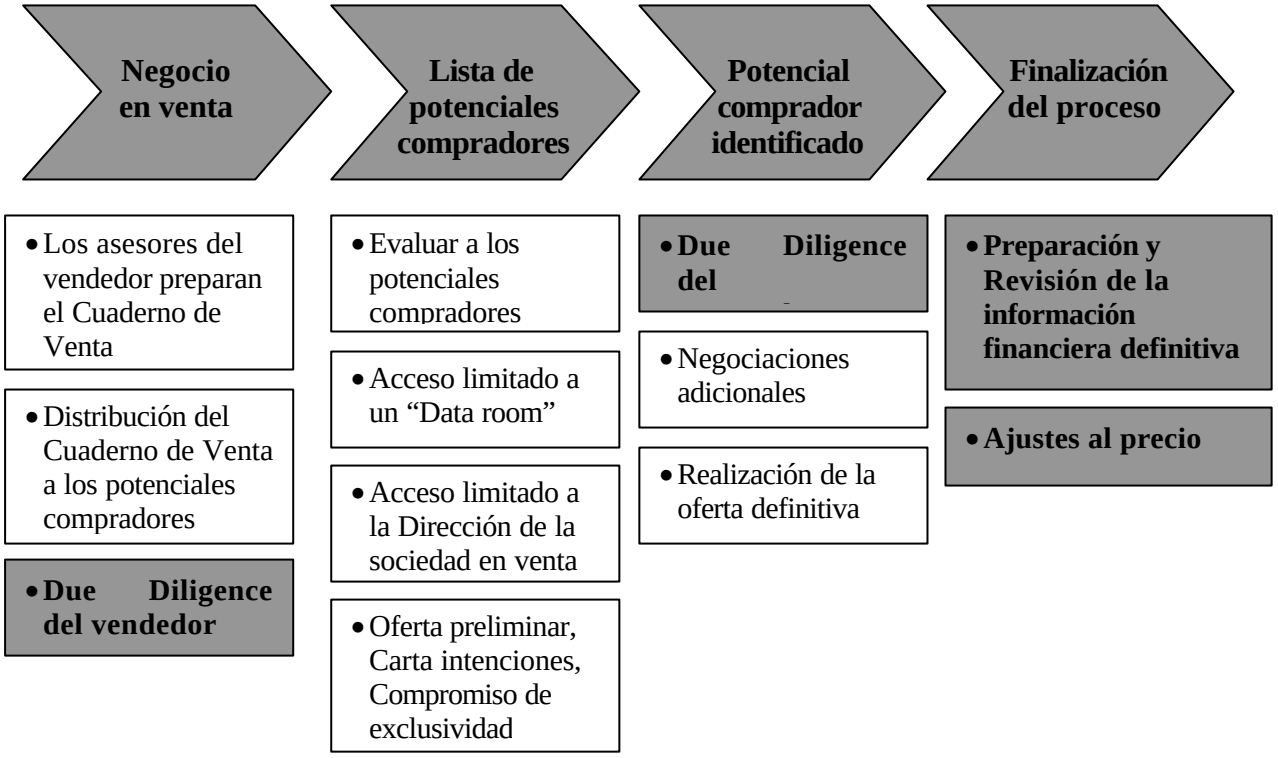
- **Aspectos mercantiles y societarios:** Revisamos los contratos mercantiles y otros aspectos societarios prestando especial atención a aquellos hechos que se pondrían de manifiesto ante un eventual cambio en el control de la Sociedad Objetivo.

- **Otras áreas del derecho:** Son objeto de análisis los aspectos jurídicos que, afectando a cualquier otro área del derecho, pudieran ser relevantes para la adopción de una decisión respecto de la conveniencia de llevar a cabo la operación o respecto de las condiciones de la misma.

- El objetivo de nuestro trabajo en esta área es el de determinar y cuantificar contingencias y riesgos actuales y/o potenciales de naturaleza medioambiental.

- **Análisis de la Tecnología y Seguridad Informática.**

5. PROCESO DE ANALISIS DE LA INVERSION.



3.5. LOS PROCEDIMIENTOS OBLIGATORIOS EN ENTORNOS CONCRETOS (obligaciones entre partes contratantes).

Una de las contradicciones de Internet es el carácter eficazmente estructurado de su red de ordenadores conectados mediante los protocolos TCP/IP que se enfrenta a un sistema vocacionalmente ácrata en su operativa. La eficacia de su funcionamiento ha provocado la necesidad de sustituir los números de código del referido protocolo, que son largos (entre 4 y 12 dígitos), por un nombre fácilmente identificable. De ahí nació el ICANN como respuesta capaz de satisfacer una real necesidad. Y de este modo nacieron las DNS (Domain Name System). Pero las contradicciones, aun las virtuales, siempre provocan disfunciones al proyectarse en la realidad y en nuestro caso la solución dada al problema, al trabajar en un entorno desregulado, ha provocado la aparición de un sinnúmero de agresiones al Derecho de Propiedad (en sentido tradicional) de multitud de marcas y denominaciones personales y societarias. La novedad de este problema derivado ha obligado a recurrir a nuevos mecanismos de resolución de conflictos. En primer lugar, se han activado algunos sistemas ya conocidos como el arbitraje, que tenían un papel más bien secundario en el mundo real de las disputas y discrepancias jurídicas. Posteriormente se ha recurrido a nuevas soluciones a partir de un viraje radical en la estrategia por parte del ICANN.

Como es sabido, existen dos formas para superar los problemas: evitarlos (posición ex-ante) o resolverlos (posición ex-post). Es la vieja polémica enmarcada por el binomio Seguridad "versus" Libertad, que desde la Filosofía invadió desde siempre la Ciencia Política, la Sociología, la Economía y también el ámbito del Derecho.

En el caso que nos ocupa, el ICANN decidió en agosto de 1999 variar su tradicional DNDP (Domain Name Dispute Policy) basado exclusivamente en el principio "first come, first served" por la que bautizó como Política uniforme de Solución de Controversias (PUSC), todo ello a partir de las presiones y recomendaciones de la OMPI. La PUSC se diferencia profundamente de la vieja DNDP y a modo de ejemplo podemos señalar que no exige identidad entre "dominio" y "marca" y que el dominio en litigio no se pone "on hold" y su primer titular puede continuar usándolo durante el procedimiento.

La esencia de la nueva PUSC es el PROCEDIMIENTO ADMINISTRATIVO OBLIGATORIO (PAO), que se estructura a partir de tres documentos:

a) La Política, que concreta el ámbito de su aplicación.

b) El Reglamento.

c) Los Reglamentos adicionales.

Éstos dos últimos contienen la regulación del procedimiento de técnicas generales (b) y en detalle (c).

Así la Política determina que para que pueda llevarse a cabo una PAO deben darse necesariamente tres circunstancias:

1º. Identidad o similitud capaz de confundir entre un nombre de dominio y una marca.

2º. Falta de interés legítimo (legitimación suficiente) por parte del demandado.

3º. Registro y su utilización de mala fe.

A destacar que los tres requisitos anteriores son acumulativos y que la carga de la prueba recae en el demandante.

Para una mejor comprensión de la novedad conceptual del PAO cabe señalar la que ha dado en llamarse la "Triple Negación"; no es judicial, **no es mediación y no es arbitraje**. A pesar de esta radical posición, casi bíblica, hay que advertir que las decisiones derivadas del PAO son plenamente jurídicas o de Derecho, como se deriva de los conceptos eminentemente técnico-jurídicos, que sustentan tanto al procedimiento como a sus conclusiones; marca, buena fe, derecho o interés legítimo, por no citar otros más y limitarnos a aquellos que están incorporados en los tres requisitos anteriores.

Ha llegado el momento de detallar y comentar las características más relevantes del PAO y para ello seguiremos como guia el excelente trabajo "Política uniforme para la resolución de conflictos en materia de nombres de dominio" del Profesor Ramón Casas Vallés, cuyo texto completo se localiza en:
http://campus.uoc.es/web/esp/uoc/ca-sas_imp.html.

1º. LA OBLIGATORIEDAD DE ACEPTAR EL PAO, en el marco de la PUSC a partir de la arquitectura contractual del sistema. En la práctica quiere decir que la

aceptación de la PUSC es requisito necesario para acceder al dominio. En ello radica la fuerza del sistema.

2º. LA COMPATIBILIDAD CON LA VÍA JUDICIAL. Ello supone una diferencia abismal con el arbitraje. Dice el Profesor Casas sobre el particular:

"El PAO no sustituye ni precede de forma obligada a la vía judicial. Quien considere que el registro de un nombre de dominio viola sus derechos -de propiedad intelectual o de otra naturaleza- puede acudir directamente a la jurisdicción competente, aunque ocurran las circunstancias que permiten aplicar la PUSC, y otro tanto podrá hacer el titular del dominio afectado. También cabe iniciar acciones judiciales mientras el PAO está en curso. Lo mismo vale para la vía arbitral *strictu sensu*."

"En ninguno de los casos, sin embargo, se producirá nada parecido a la litispendencia. Las acciones judiciales o arbitrales y el PAO discurrirán en paralelo, sin interferencias; sin perjuicio del valor de los tribunales y órganos de arbitraje quieran dar a las manifestaciones de las partes y a la apreciación de hechos efectuados en el curso del procedimiento".

Es importante destacar al respecto que una vez promulgada la conclusión del PAO, cualquiera de las partes, o las dos, pueden recurrir a la vía judicial sin que el procedimiento tenga que condicionar el devenir de esta nueva vía.

3º. LA EJECUTIVIDAD CONDICIONADA DE LA DECISIÓN. Es la continuación o segunda derivada del requisito antes descrito, en lo relativo a la situación del dominio respecto al titular, por cuanto la decisión del grupo de expertos vincula al registrado definitivo, protegido por la arquitectura técnica y contractual del sistema.

Las decisiones o conclusiones del PAO no son lógicamente "sentencias" y se conocen como Alternative Dispute Resolution (ADR), cuyas características procedemos a detallar con sus luces y sombras, de nuevo siguiendo el esquema del ya antes citado trabajo del Profesor Casas.

1. NEUTRALIDAD, INDEPENDENCIA E IMPARCIALIDAD.

2. ESPECIALIZACIÓN, TANTO EN LA ADMINISTRACIÓN COMO EN LA RESOLUCIÓN DE CONFLICTOS.

3. RAPIDEZ.

4.- COSTES REDUCIDOS.

5.- NO NECESIDAD DE ABOGADOS.

6.- ACTUACIÓN DE OFICIO Y ANTIFORMALISMO.

7.- CONFIDENCIALIDAD Y RESPONSABILIDAD.

A la vista de las características del PAO y de sus resoluciones (Alternative Dispute Resolutions) no cabe ninguna duda de que estamos ante un nuevo instrumento de resolución de conflictos que busca su posicionamiento entre el proceso judicial y el arbitraje y que se aprovecha de las especiales condiciones del entorno en el que opera; la arquitectura técnica de Internet.

3.6. LA PRUEBA PERICIAL EN EL ENTORNO TIC'S (COMPUTER FORENSICS).

Resulta evidente que una de las salidas jurídicas para la resolución de conflictos en el ámbito de las TIC'S pasa necesariamente por la PRUEBA PERICIAL como elemento que refleja la opinión de un experto independiente sobre el particular para su posterior interpretación por el juez o tribunal correspondiente. La complejidad técnica y organizativa de las Nuevas Tecnologías obligará sin duda alguna a que una parte importante de la información útil para la conformación de opinión sobre un litigio por parte del órgano judicial competente, pase necesariamente por una prueba de este tipo.

Uno de los problemas para su aplicación práctica consiste en la determinación de las circunstancias subjetivas y objetivas que la configuran. A modo de ejemplo citamos los siguientes puntos de necesaria concreción:

- ALCANCE TECNICO DE LA PRUEBA.
- MULTIDISCIPLINAS PARTICIPANTES.
- PROFESIONAL O EQUIPO DE PROFESIONALES ACTUANTE.

En los U.S.A y dentro de su especial conformación legal, procesal y judicial se viene desarrollando en los últimos años un modelo que integra tres vectores fundamentales: Seguridad, Derecho y Nuevas Tecnologías. Los americanos lo bautizan todo y a este nuevo modelo para plantear y resolver problemas lo denominan COMPUTER FORENSICS y en síntesis se trata de una estandarización para aplicar en la práctica con éxito, la convivencia positiva de los tres vectores antes citados.

Para sustentar nuestra exposición sobre este nuevo instrumento tecnológico/jurídico nos basamos en parte (no todo) del esquema desarrollado por IBM SERVICES bajo el nombre EMERGENCY RESPONSE SERVICES y no deja de sorprendernos la habilidad de los americanos para sintetizar conceptos en pocas palabras.

A modo de ejemplo podríamos citar la enorme problemática que presenta en la práctica la evacuación de una "Prueba Pericial" en el ámbito TIC'S, sea cual sea la instancia jurisdiccional en que se pretenda practicar. La dificultad principal se deriva de la naturaleza interdisciplinar y globalizadora de los entornos TIC'S; las interacciones son constantes, las repercusiones imprevisibles, la desubicación espacial, etc. etc. Todo ello dificulta "prima facie" las siguientes consideraciones jurídicas, entre otras:

- Foro aplicable.
- Ley aplicable.
- Instancia judicial; penal, civil, administrativa.

- Naturaleza jurídica del litigio.
- Naturaleza de la prueba pericial.

Si las diferentes instancias judiciales dispusieran de expertos, o de equipos de expertos, capaces de desenvolverse con soltura en un modelo metodológico como el descrito anteriormente, serían capaces de responder acertada y eficazmente a todos los interrogantes expuestos y a muchos otros omitidos.