DERECHOS DE LOS CIUDADANOS: SEGURIDAD Y GARANTÍAS EN LA UTILIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES - D. Valentín Carrascosa López
Director del C.A. de la UNED en Mérida

Señoras y Señores:

Gracias en primer lugar por haberme invitado a intervenir en algo tan importante como las VI Jornadas sobre Tecnologías de la Información para la Modernización de las Administraciones Públicas, TECNIMAP´2000.

En estas Jornadas han participado y van a participar figuras señeras con las que, por evidentes razones, no me es dado competir. Permítaseme, por lo tanto, dar a mi intervención un tono cuasi coloquial y que en esta breve exposición tan sólo pretenda dejar esbozadas algunas de las ideas que el nuevo fenómeno sugiere desde la perspectiva jurídica.

Los derechos tienen como razón de ser la satisfacción de las necesidades básicas de las personas, aquellas que las hacen ser propiamente seres humanos. Así como su ejercicio en el seno de una comunidad de respeto mutuo, de convivencia pacífica.

Es preciso considerar que estos derechos se esgrimen o ejercen por unas personas respecto de otras, que son igualmente titulares de los mismos o de otros derechos, por lo que hace falta deslindarlos cuando entran en conflicto y ponderar hasta donde llega el de cada uno.

Por otra parte, no se puede desconocer el dinamismo que caracteriza a las nuevas tecnologías. En efecto, en cuanto manifestación jurídica y política de la realidad social, los derechos de las nuevas tecnologías han de reflejar, por fuerza, los cambios que se producen en las ideas y convicciones, sobre las que la sociedad fundamenta la convivencia.Y esas ideas evolucionan al tiempo que cambia la realidad, buscan respuesta a los nuevos retos, pero las nuevas tecnologías se adelantan al más acabado de los ordenamientos jurídicos y por eso, cada vez surgen ante nosotros, preocupados por el principio de inseguridad jurídica en que se vive, reivindicaciones de nuevos derechos, con los que proteger bienes jurídicos que la sociedad considera valiosos como por ejemplo la vida, la libertad, la salud, la seguridad, el patrimonio .....

En el tiempo transcurrido desde la aparición de las primeras normas sobre las nuevas tecnologías hasta nuestros días se han abierto camino con dificultades, sin embargo, a pesar de los obstáculos que ha encontrado a su paso, la convicción de que las

personas poseen ciertos derechos, y que son merecedores del máximo reconocimiento y respeto, se ha convertido en uno de los rasgos distintivos de nuestra cultura y de nuestra civilización.

La introducción de las Tecnologías de la Información en casi todas las actividades de la sociedad ha generado nuevos problemas que el derecho debe contemplar, o presentado bajo otra óptica, vertientes novedosas de viejos problemas que plantean al jurista desafíos impensados ante los nuevos interrogantes que genera el impacto tecnológico.

Nuestra ley de leyes, es decir nuestra Constitución, intenta dar pautas para solucionar algunos de estos problemas y no hay más que acudir a su texto para encontrar preceptos, incluso dentro del título primero dedicado a los derechos y deberes fundamentales, como su artículo l0.1 que nos deja claro la necesidad de este nuevo derecho cuando dice "La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social".

Sin ningún genero de duda podemos decir que la seguridad y garantías en la utilización de las Tecnologías de la Información y de las Comunicaciones, han dado lugar a una serie de derechos de los ciudadanos. La amplitud de estos no es compatible con la brevedad del tiempo que se me ha concedido, por lo que trataré únicamente de los derechos que se pueden considerar más ilustrativos y ello para ofrecer al auditorio puntos de debate y reflexión.

Uno de los problemas claves de los derechos de los ciudadanos gira en torno a la seguridad en la utilización de las tecnologías de la información, pero la seguridad de la información se puede considerar desde los siguientes puntos de vistas:

a. La seguridad física, cuya finalidad es la de proteger con ellas a los Centros de Procesos de Datos y a su entorno de posibles amenazas físicas tanto procedentes de la naturaleza de los propios medios, como del hombre: inundaciones, fuego, corte de fluido eléctrico, interferencias, atentado, robo, hurtos, etc, etc.
b. La seguridad lógica, tiene por finalidad proteger las aplicaciones informáticas y el contenido de las bases de datos y de los ficheros.
   Esta protección se puede realizar a través de contraseñas, firmas digitales y fundamentalmente por la utilización de métodos criptográficos.
c. La seguridad organizativo-administrativa pretende cubrir el hueco dejado por las dos anteriores y viene, en cierto modo, a completarlas, pues difícilmente se puede lograr de forma eficaz la seguridad de la información sino existen claramente definidas: la política de seguridad, de personal, de contratación, de análisis de riesgos y planes de contingencia.
d. La seguridad jurídica pretende, a través de la aprobación de normas legales, fijar el marco jurídico necesario para proteger los bienes informáticos, fijar los derechos de los ciudadanos y como no determinar jurídicamente cuales deban ser las medidas de seguridad y garantías en la utilización de las Tecnologías de la Información y de las Comunicaciones.

La seguridad jurídica es un derecho de todos los españoles, conforme al art. 9 de la Constitución, pero no siempre se comprende su significado y valor.

La noción de seguridad jurídica tiene un doble aspecto:

En un sentido objetivo, la seguridad jurídica supone la existencia de leyes, claras y suficientes, sin lagunas, y su aplicación efectiva por los Tribunales.

En sentido subjetivo, la seguridad jurídica consiste, de una parte, en la posibilidad de todo ciudadano de conocer la Ley, su significado y alcance y de otra, en la libertad de con arreglo a aquella confiando en la eficacia de lo actuado.

En este sentido la seguridad jurídica es un saber a que atenerse, pues los ciudadanos saben de antemano cuales van a ser las consecuencias y que efectos van a derivarse.

Los profesionales del Derecho decimos con frecuencia que la vida va por delante de las leyes de manera que éstas se dictan para regular las nuevas situaciones y necesidades que la realidad social plantea a los ciudadanos.

Pues bien, no cabe duda de que el fenómeno de la utilización de las Tecnologías de la Información y de las Comunicaciones es hoy un caso claro de ello, una realidad nueva que suscita la cuestión fundamental de su regulación. Hay que proporcionar un marco legal a este fenómeno imparable.

Pero, a pesar de la regulación de ámbito estatal, las características de las Tecnologías de la Información y de las Comunicaciones impide proceder con los métodos tradicionales porque no se trata simplemente de regular una situación nueva, que esté enmarcada dentro del territorio de un Estado soberano, sino de regular algo que tiene un fundamento "mundial" sin estar asentado físicamente en un territorio determinado sino en "La Red".

En este punto, como europeos, observamos que, de una parte, la Unión Europea está haciendo un gran esfuerzo para marcar las directrices de esta regulación, de este nuevo marco legal. Los trabajos se han plasmado en diversos proyectos o propuestas o Directivas sobre firma electrónica, comercio electrónico, o protección de datos personales.

Estas Directivas han sido traspuestas a nuestro ordenamiento jurídico interno.

En estas medidas jurídicas internas es en las que vamos a centrar nuestra intervención y si bien son muchas las normas que se han dictado, nosotros nos limitaremos a: La Ley Orgánica 10/1995, de 23 de noviembre de 1995, aprobando el Nuevo Código Penal Español; La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal; el Real Decreto-Ley 14/1999, sobre Firma Electrónica; la Ley Orgánica 1/2000, de 7 de enero, de Enjuiciamiento Civil, por considerarlas piezas clave de nuestro ordenamiento jurídico, y en el anteproyecto de Ley de Comercio Electrónico.

Tras este planteamiento general podríamos hacer una pequeña reseña de las principales normas reguladoras del ordenamiento jurídico español que ofrecen seguridad y garantía en la utilización de las Tecnologías de la Información y que esquematizamos en los siguientes bloques:

A).- EN EL CÓDIGO PENAL

El ciberespacio es un mundo virtual en el que los defectos, miserias y malos hábitos del ser humano se reproducen con la misma fidelidad que las virtudes, y por ello podemos decir que:

No puede ser ilegal en la red lo que es legal fuera de ella.

No se puede permitir en la red lo que está prohibido en la calle.

El derecho penal asume la misión de proteger bienes jurídicos reconocidos por la comunidad frente a la eventualidad de ser lesionados, violados, o ante la posibilidad de ponerlos en peligro. Todo esto con la finalidad de poder convivir con los demás dentro de la comunidad confiando en que se respete la propia libertad de manera que se respete la de los demás y por tanto los derechos de los ciudadanos.

Debe reconocerse, la existencia de una realidad criminal, surgida al socaire de las altas tecnologías de la información, que interesa a parcelas bien diversas del Derecho Penal (desde delitos contra la intimidad a las falsedades documentales, desde los delitos económicos hasta otros tan distantes como los delitos contra la seguridad interior y exterior del estado, por citar algunos ejemplos), realidad criminal frente a la cual las legislaciones tradicionales no estaban preparadas, dadas las características propias de estos nuevos delitos.

Las características del delito informático, podríamos resumirlas en:

- La acumulación de la información en grandes bases de datos posibilita considerablemente el acceso a cualquier tipo de información, una vez que se han violado las medidas de seguridad o control de acceso.
- Inexistencia de Registros Visibles, pues la información grabada se registra en impulsos eléctricos sobre soportes magnéticos que son ilegibles para el ojo humano.
- Falta de Evidencias en la Alteración de Datos y Programas. La alteración de programas y datos pregrabados en soportes magnéticos pueden hacerse sin dejar rastro alguno.
- Eliminación de las pruebas.- Sumamente fácil y atribuido a error fortuito.
- Especialidad del Entorno Técnico.- Con gran complejidad.
- Dificultad para Proteger Ficheros o Archivos.- La protección es muy compleja.
- Concentración de Funciones.- Especialmente en los centros de dimensiones mediana y pequeña en los que predominan los conceptos de funcionalidad y versatilidad del personal sobre la seguridad.
- Falta de Controles Internos de Seguridad.
- Carencia de Controles del Personal Técnico.
- Dispersión Territorial de los Puntos de Entrada al Sistema.
- Interdependencia de Redes de Transmisión.

Las anteriores características nos llevarían a una clasificación de nuevos delitos y así nos encontraríamos, entre otros, con los siguientes:

- Manipulación desde un Ordenador a un Sistema de Procesamiento de datos.
- Espiar y robar software.
- Sabotaje informático.
- Robo de servicios.
- Acceso no autorizado a Sistemas de Procesamiento de Datos.
- Defraudación en los negocios asistidos por un ordenador

Si acudimos a nuestro Código Penal vemos que en él hay una serie de preceptos que sancionando determinados comportamientos pretenden garantizar los derechos de los ciudadanos y entre ellos podemos citar:

La captación no autorizada de datos, incluidos los mensajes del correo electrónico está castigada con la pena de prisión de uno a cuatro años y multa de 12 a 14 meses (artículo 197).

El que sin estar autorizado, se apodere, utilice o modifique, en perjuicio de terceros, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, o en cualquier otro tipo de archivo o registro público o privado, conforme al art.197.2 primer párrafo, podrá ser condenado a pena de prisión de 1 a 4 años y multa de 12 a 14 meses.

El artículo l97 del Código Penal, en los párrafos a que hemos hecho referencia así como en el resto del articulado establece una serie de sanciones, como hemos visto incluso con penas de cárcel, para todos aquellos ilícitos informáticos del Código Penal en relación con la intimidad, pues garantiza, bajo pena, los mensajes del correo electrónico, los datos reservados de carácter personal o familiar, la difusión o descubrimiento, o cesión de datos personales, hechos o las imágenes captadas sin estar autorizado para ello, aun sin haber tomado parte en el descubrimiento de tales datos, hechos o imágenes.

De la lectura global del texto del Código Penal se infiere:

a. Que para el legislador no existe un delito informático, sino una realidad criminal compleja, vinculada a las nuevas tecnologías de la información, imposible de reconducir a un único tipo legal.
b. Que, no obstante, tres han sido las parcelas más directamente afectadas con el intento de aprehender esa realidad criminal: los atentados contra la intimidad; los atentados contra intereses de contenido económico (particularmente a través de los artículos 239, 248.2, 256, 264.2, 278 y 623.4); y las falsedades documentales, remozadas por mor del nuevo concepto de documento que suministra el art. 26 del nuevo Código Penal, comprensivo también del documento electrónico.

El nuevo Código Penal contempla específicamente delitos que pueden ser cometidos a través de las nuevas tecnologías, entre otros, los siguientes:

- La estafa informática (artículo 248.2).
- La utilización de tarjetas electromagnéticas a los efectos del delito de robo con fuerza (artículo 239).
- El intrusismo informático-defraudaciones (artículo 256).
- El espionaje informático (artículo 278 y ss.).
- La intimidad (artículo197 y ss.)
- La propiedad intelectual (artículo 270 y ss).
- Daños informáticos (artículo 264.2).
- Difusión y exhibición de material pornográfico a menores (art.186)
- Pornografía infantil (artículo 189).
- Difusión de Mensajes injuriosos o calumniosos (artículo 211).
- Publicidad engañosa (artículo 282).

- Revelación de secretos (artículo 278).
- Falsedad documental (artículo 390).

Podríamos seguir concretando otros delitos, como la piratería de programas, etc, pero concluiremos este recorrido con el artículo 238, precepto de nuevo cuño, que castiga la manipulación en aparatos automáticos en perjuicio de los consumidores.

De lo anterior se deduce que estos y otros preceptos del vigente Código Penal establecen una serie de derechos a los ciudadanos para dar una mayor seguridad y garantía en la utilización de las Tecnologías de la Información

B) PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

Hoy día los grandes almacenes, las empresas gestoras de tarjetas de crédito, los hospitales, la propia Administración disponen de tal cantidad de datos de nosotros que fácilmente pueden lograr un perfil muy completo de nuestra persona.

Este perfil, en algunos casos, puede ser determinante a la hora de solicitar un trabajo o al tratar de contratar un seguro, por ello su protección es cada día más importante.

La Constitución incluye en el art. l8.4 un mandato al legislador para que limite el uso de la informática al objeto de garantizar "el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Como es bien sabido, el fundamento de este mandato es el peligro real y efectivo que la acumulación informática de datos sobre las personas puede representar sobre la libertad y derechos de los ciudadanos y, en especial, sobre su vida privada.

España, con cierto retraso respecto a sus obligaciones derivadas de acuerdos internacionales, desarrolló este mandato constitucional mediante la LO 5/92, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, vulgarmente conocida como LORTAD, derogada y sustituida por la actual Ley Orgánica 15/1999, de l3 de diciembre, de Protección de Datos de Carácter Personal. (a partir de ahora LOPD).

En ella se regula el mantenimiento por particulares o instituciones públicas de ficheros de datos que admitan su tratamiento automatizado, aunque se exceptúan del ámbito de la Ley algunos ficheros públicos sometidos a regulaciones específicas (los ficheros de datos electorales, el del Registro Civil, el del Registro Central de Penados y Rebeldes y algunos otros) y algunos particulares que no plantean problemas (los de uso personal, y algunos otros).

La Ley somete a los ficheros a una serie de requisitos y garantías para las personas afectadas. Los ficheros sólo pueden emplearse para la finalidad que los justifica y están sometidos a la obligación de veracidad, actualización y rectificación de sus datos. Los afectados han de tener conocimiento del destino de los datos y han de dar su consentimiento para el tratamiento automatizado de los mismos cuando se les solicitan. Por otra parte se prohiben los ficheros creados con la exclusiva finalidad de almacenar datos de carácter personal que revelen la ideología, religión, creencias, origen racial o vida sexual, y se someten a garantías específicas aquéllos en los que se almacenen datos de esa naturaleza. Las personas ostentan en todo caso el derecho de información sobre la existencia y caracteres de los ficheros; tienen, asimismo, derecho de acceso a los ficheros y de rectificación y cancelación de datos inexactos o ya superados, con algunas excepciones por razones de seguridad pública, defensa del Estado, derechos y libertades de terceros o necesidad de investigaciones criminales en

curso.

En función de los principios enumerados vemos como emergen una serie de derechos para las personas, que pueden igualmente colisionar con otros derechos igualmente legítimos. (la intimidad puede colisionar con el derecho a la información; el secreto de las operaciones financieras claramente entra en colisión con el derecho a la seguridad del tráfico mercantil que precisa de la publicidad de determinadas operaciones; el interés público del Estado puede colisionar con el derecho a la intimidad individual....)

Podríamos resumir esos derechos de los ciudadanos reconocidos en la Ley de Protección de Datos Personales, en los siguientes:

- Impugnación de valoraciones.- El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezcan una definición de sus características o personalidad.
- Derecho de Consulta.- gratuita, al Registro General de Protección de Datos, sobre la existencia de ficheros de datos de carácter personal, sus finalidades y la identidad del responsable del fichero.
- Derecho de conocimiento.- Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, de las consecuencia de su contestación o negativa a facilitarlos.
- Derecho de acceso.- En intervalos no inferiores a doce meses, salvo interés legítimo. Este derecho junto a los de rectificación, cancelación y oposición son importantes pues en su conjunto delimitan lo que se puede entender como habeas data o habeas escriptum.
- El derecho de acceso a archivos y registros administrativos, configurado en el artículo 105,b) CE, recoge un auténtico derecho subjetivo alegable por las personas, tanto físicas como jurídicas, y que tienen por objeto material el conocimiento de datos en poder de la Administración cualquiera que sea el soporte que los contenga, derecho que conoce como límites, la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas, los cuales, además, que no deben ser interpretados de manera muy amplia, pues desvirtuarían en exceso el mencionado derecho de acceso.
- Derecho de rectificación y cancelación.- El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o
- Derecho de oposición.- Según el artículo 5.1.d) se debe informar al interesado de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. Y diversos artículos de la nueva Ley de Protección de Datos facultan a los interesados para oponerse a que sus datos personales puedan utilizarse, (ejemplo: con fines de publicidad o prospección comercial).
- Derecho de tutela.- El interesado podrá reclamar ante el Director de la Agencia de Protección de Datos. Contra la resolución del Director de la Agencia de Protección de Datos se podrá interponer recurso contencioso- administrativo.
- Derecho de indemnización.- Los interesados que sufran daños o lesiones en sus bienes o derechos, motivados por el incumplimiento por el responsable del fichero de lo dispuesto en esta Ley, tendrán derecho, según el artículo 19, a ser indemnizado. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones PúblicasEn el caso de ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

C).- LA FIRMA ELECTRÓNICA .

No resulta necesario destacar la importancia que en la actualidad, pero sobre todo en el futuro, tienen los medios de comunicación y la transmisión de datos e información a nivel mundial constituyen lo que se ha venido en denominar la Sociedad de la Información. Por ello, resulta necesario garantizar que los ciudadanos puedan acceder a esa información en las mejores condiciones posibles

Es por ello por lo que se ha realizado una apuesta decidida adoptando medidas reguladoras y medidas de promoción, tales como: Régimen especial de tarifas para acceso a Internet; comercio electrónico; ampliación del servicio universal de telecomunicaciones, pero fundamental, para el tema que estamos tratando: Seguridad en la Red, a través de la Firma Electrónica.

Con fecha 18 de septiembre de 1999 se publica el Real Decreto - Ley 14/1999, de 17 de septiembre, sobre firma electrónica.

El aspecto más importante de la norma es equiparar el valor jurídico de la firma manuscrita y de la firma electrónica, teniendo validez esta última como prueba en juicio, siempre que la firma electrónica se haya generado con las condiciones de seguridad necesarias.

El Real Decreto-Ley viene a llenar el vacío legal existente en la materia y dará mayor seguridad a las comunicaciones telemáticas y permitirá eliminar la principal barrera para el desarrollo del comercio electrónico a través de Internet, ofreciendo a los comerciantes y los usuarios las garantías necesarias para la realización de transacciones seguras a través de la red.

Es necesario que el envío de información a través de las redes de telecomunicaciones pueda ofrecer a los ciudadanos, consumidores y profesionales el mismo nivel de seguridad y confianza, al menos, que las informaciones o transacciones documentadas en papel.

De entre todos los instrumentos que se han experimentado para garantizar dicha confianza, la firma electrónica es la que mejor satisface las exigencias de seguridad y confianza que requieren las comunicaciones electrónicas.

Ello es así porque la firma electrónica cumple, en relación con los documentos electrónicos, las dos principales funciones que se atribuyen a la firma manuscrita sobre un documento en papel, a saber: permite identificar al autor del escrito (autenticación) y constatar que el mensaje no ha sido alterado después de su firma (integridad).

En realidad, la firma electrónica no identifica por si sola al autor de un escrito, sino mediante el complemento de un certificado electrónico, que constata que la clave pública del firmante pertenece a quien dice haberlo hecho.

Este certificado es emitido por un tercero digno de confianza, denominado "entidad de certificación".

El Real Decreto-Ley regula la prestación de los servicios de certificación, aportando, así, la necesaria seguridad jurídica para su generalización.

El marco jurídico establecido con la firma electrónica tiene por finalidad garantizar la seguridad y fiabilidad de las transacciones económicas, pues sin esta garantía jurídica unida a la seguridad técnica, las empresas y consumidores no confiarán en este canal de negociación.

La fiabilidad del dispositivo de firma electrónica es una materia de carácter técnico. El progreso de las técnicas de encriptación corre impulsado por el progreso en los instrumentos de desencriptación. Por ello no es posible asegurar que un dispositivo de firma electrónica sea infalsificable.

La Ley no puede garantizar que la firma electrónica no será falsificada, pero sí puede y debe establecer las consecuencias de tal supuesto. Por ello, el Real Decreto- Ley de Firma Electrónica establece que las entidades de certificación están obligadas a utilizar dispositivos que garanticen la seguridad en la prestación del servicio y consagra el principio de responsabilidad patrimonial por los daños y perjuicios que se hayan seguido al contratante como consecuencia de la negligencia de la entidad de certificación.

D) LA LEY DE ENJUICIAMIENTO CIVIL

El artículo 24.2 CE reconoce, a favor del justiciable, el derecho a utilizar los medios de prueba pertinentes para su defensa.

Por otro lado, el artículo 230 LOPJ establece que los Juzgados y Tribunales podrán utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y ejercicio de sus funciones.

Estos derechos carecían, prácticamente, de virtualidad, esperemos que la nueva Ley de Enjuiciamiento Civil, l/2000, cuya entrada en vigor esta prevista para el 7 de enero del 200l, haga realidad estos principios si se desea dar cumplimiento a los principios de celeridad, oralidad y eficacia que presidieron la reforma.

La entrada en vigor de la nueva Ley de Enjuiciamiento Civil, en la que se prevé la utilización de medios tecnológicos que permitan la grabación de la imagen y la reproducción de las actuaciones judiciales, exigirá, como premisa imprescindible, la implantación de programas informáticos modernos y la conveniente formación de los funcionarios judiciales.

La exposición de motivos de la nueva Ley, atenta al presente y previsora del futuro, abre la puerta a la presentación de escritos y documentos y a los actos de notificación por medios electrónicos, telemáticos y otros semejantes, pero sin imponer a los justiciables y a los ciudadanos que dispongan de esos medios y sin dejar de regular las exigencias de esta comunicación. Para que surtan plenos efectos, los actos realizados por esos medios será preciso que los instrumentos utilizados entrañen la garantía de que la comunicación y lo comunicado son con seguridad atribuibles a quien aparezca como autor de una y otros. Y ha de estar asimismo garantizada la recepción íntegra y las demás circunstancias legalmente relevantes.

Como vemos, la propia exposición de motivos de la Ley, apuesta como ha sido tradicional por la necesidad de la existencia de las seguridades y garantías necesarias en la comunicación.

De los cinco medios de prueba existentes en la actualidad la adaptación de la prueba

documental a los nuevos soportes es quizás la que más problemas puede plantear, no obstante los ciudadanos, haciendo uso de sus derechos podrán proponerla, al igual que la prueba pericial y el reconocimiento judicial, en los procesos en los que se utilicen las Tecnologías de la Información, y deberá ser admitida siempre que sea posible, lícita, pertinente, útil y se proponga de acuerdo con lo dispuesto en la Ley.

Podríamos seguir analizando otra serie de normas en las que se recogen mas derechos de los ciudadanos, tales como el Reglamento de Medidas de Seguridad; El Real Decreto por el que se regula la contratación telefónica o electrónica; la Directiva del Comercio Electrónico o el anteproyecto de ley de Comercio Electrónico, y como no la responsabilidad civil profesional de los teleinformáticos, que los usuarios podrán ejercitar directamente contra la institución, fabricante o suministrador del ordenador, e incluso contra los propios expertos, pero creo han quedado sobre la mesa suficientes puntos de reflexión y debate por lo que doy por concluida mi intervención, agradeciendo la atención prestada.