LAS TIC EN LA NUEVA OFICINA JUDICIAL.

Universidad de Burgos

Autor del proyecto: *María Asunción Fidalgo Barrios*
Tutor del proyecto: Prof. Miguel Ángel Davara Rodríguez
Directores del Magíster:
Dr. Emilio S. Corchado Rodríguez
Dr. Álvaro Herrero Cosio

MAGÍSTER EN ASESORÍA Y CONSULTORÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
(MAC-TIC)

UNIVERSIDAD DE BURGOS
II Edición. Burgos, Julio 2010.

Magíster financiado por la Fundación Centro de Supercomputación de Castilla y León

INDICE DE CONTENIDOS.

1.- INTRODUCCIÓN.

1.1.- PREFACIO.

La implantación de una nueva Oficina Judicial, capaz de promover una Justicia que actúe con rapidez, eficacia y calidad, con métodos más modernos y procedimientos menos complicados, cumpliendo satisfactoriamente el mandato constitucional de garantizar en tiempo razonable los derechos de los ciudadanos y de proporcionar seguridad jurídica, al actuar con pautas de comportamiento y decisión previsibles, constituye un objetivo esencial del Ministerio de Justicia, así como de las CCAA con competencias transferidas en materia de Justicia.

Entramos en una nueva etapa que muchos han dado en llamar la Era de la Información, marcada por el papel central que juegan las Tecnologías de la Información y las Comunicaciones en los ámbitos político social y económico. El uso de estas tecnologías permite conectar en tiempo real y a nivel planetario a los individuos, pero se cuestiona la

capacidad de los poderes públicos de adaptarse al cambio y ofrecer soluciones a los desafíos que se plantean. Las Instituciones Públicas no pueden dejar creer entre la ciudadanía la creencia de contar con un Estado obsoleto e incapaz de actuar. El Ministerio de Justicia puede presentar proyectos que demuestran que esa percepción carece de fundamento.

Un ejemplo de ello es el Plan Estratégico de Modernización de la Justicia 2010-2012. Con este Plan el Ministerio deja de ser un mero espectador de la transformación de la sociedad por las Tecnologías de la Información y las Comunicaciones para convertirse en un agente del cambio capaz de liderar la aplicación de estas tecnologías a las relaciones entre los ciudadanos y de éstos con la Administración de Justicia. Justicia y tecnología pasan a ser conceptos que se complementan entre si.

Toda la actividad que se desarrolla en el ámbito de la Justicia se centra en procesos que implican notificaciones, tratamiento de información, envío, almacenamiento, clasificación y búsqueda de esa información… y la gestión de todo esto es uno de los puntos fuertes de las tecnologías de la información.

Es esencial que el Ministerio de Justicia asuma el liderazgo en este cambio de transformación de la Justicia a partir de las Nuevas Tecnologías.

Desde el Ministerio se parte de una evaluación rigurosa de la situación actual para realizar un programa de modernización que convertirá a la Administración de Justicia en un servicio público de calidad, tecnológicamente avanzado y siempre atento a las trasformaciones de la sociedad.

El objetivo de la Administración de Justicia siempre será la tutela efectiva de los derechos de los ciudadanos aún en un contexto complejo como el actual donde la dimensión internacional subyace en la mayoría de las actividades sociales. Esta transformación provoca el uso frecuente de conceptos como "sociedad-red" "estado-red" "empresa-red" que exige la aplicación de determinados desarrollos tecnológicos en el ámbito de la Justicia. Esta actividad ya se está emprendiendo con éxito y ejemplo de ello es el papel participativo y protagonista del Ministerio de Justicia en el desarrollo de lo que podríamos denominar una Justicia-red. Me refiero al programa E-Justice [1]que trata de garantizar la tutela judicial efectiva de los ciudadanos mediante la interconexión y coordinación de los sistemas judiciales europeos.

El desarrollo de una Justicia tecnológicamente avanzada es un requisito para la conexión entre los sistemas jurídicos nacionales, algo que resulta necesario para la mejora constante de la legislación mediante el intercambio de buenas prácticas y para una tutela judicial efectiva a nivel internacional. Además sería un elemento esencial para la defensa de los intereses individuales en la sociedad-red.

En definitiva un Estado moderno requiere una Justicia tecnológicamente avanzada; a la hora de afrontar los desafíos de la globalización y de la era de la información, la Justicia no debe ser parte del problema sino una solución.

La Justicia del siglo XXI será la que sepa adaptarse a las transformaciones sociales; desde esta perspectiva el Plan de Modernización de la Justicia convierte al Ministerio de Justicia en una fuerza transformadora, accesible a los ciudadanos y protectora de sus derechos e impulsora de la Justicia del siglo XXI.

En una Justicia valorada en los últimos años de forma negativa por los ciudadanos, que no están de acuerdo con lo que tardan los pleitos, con el trato que reciben, con las suspensiones y faltas de planificación de los órganos judiciales, con la inefectividad de las sentencias, la Oficina Judicial contagiada por los mismos problemas

[1] En el seno de la UE ofrece soluciones innovadoras a través de la integración de las TIC y la biometría en los procesos jurídicos en territorio comunitario. También ofrece soluciones para los procedimientos transfronterizos.

generales que afectan al ejercicio del poder judicial, reclama cuanto antes un funcionamiento más racional y moderno.

La contradicción entre la idea de "poder judicial" y la noción de servicio público, el enfoque de la Justicia como un instrumento para conseguir determinados objetivos sociales y no como un fin en sí misma, han puesto en crisis la creencia de que el sistema judicial debía mantener una situación por encima de cualquier análisis funcional o evaluación de resultados.

La consideración de la Justicia como servicio público lleva aparejada como consecuencia la necesaria evaluación de su funcionamiento, del grado de eficacia y de eficiencia de su gestión. Entendemos por eficacia la adecuación de los resultados a los objetivos perseguidos y esperados por los ciudadanos y requeridos por el derecho positivo y por eficiencia la proporcionalidad entre los recursos de toda índole que el sistema judicial consume y los resultados que produce, tanto en términos sociales como económicos.

La consecución de este objetivo exigirá necesariamente el consenso de todos los actores de la Admon de Justicia, entre los que juegan un papel esencial el cuerpo de secretarios judiciales y los cuerpos de funcionarios al servicio de la misma, ya que su aportación al cumplimiento de ese proyecto constituye un presupuesto determinante para conducirle a buen fin.

Es necesario que se garanticen los principios de igualdad, mérito, capacidad y publicidad, predicados por el artículo 103 de la Constitución española, para que estos funcionarios se reconozcan en el proceso de reformas, asegurando, asimismo, un impulso definitivo en la modernización y mejora del servicio público de la Admon de Justicia, porque la garantía del éxito del proyecto reclama necesariamente que los ciudadanos, destinatarios últimos del servicio, se reconozcan también en el mismo, lo que sólo sucederá cuando comprueben efectivamente que la Justicia constituye una solución real para sus problemas.

Será también presupuesto del éxito de las reformas en curso, que los profesionales, que intervienen interna y externamente en el proceso y los propios justiciables tengan un conocimiento cabal de su contenido, así como de las consecuencias de las mismas, ya que la experiencia demuestra sistemáticamente que una gran parte de las resistencias a los procesos de cambio tiene relación con el desconocimiento de los objetivos perseguidos, así como de los valores añadidos que supondrán en la mejora del servicio.

1.2.-ANTECEDENTES HISTÓRICOS.

Para gestionar bien la Oficina actual y para poder implantar el cambio, es imprescindible conocer algo de los antecedentes de la Oficina Judicial, porque su configuración histórica, precisamente y ya desde los años posteriores a la Constitución ha sido, sin duda, causa de muchas de las disfunciones que se pretenden corregir.

En la estructura procesal del derecho castellano clásico, quien realmente era el técnico en derecho era el Secretario Judicial y no el Juez, que era lego. Era el Juez quien decidía pero lo hacía de palabra y el Secretario era quien le daba forma jurídica.

A lo largo del siglo XIX, momento en el que se consolida la base procesal y organizativa actual de nuestro ordenamiento, el juez cada vez se profesionaliza más y el Secretario va perdiendo competencias reales en la estructura organizativa de los sistemas judiciales. De todas formas ese proceso no concluye definitivamente hasta que en el año 1988, por la Ley de Presupuestos Generales del Estado[2], se acuerda la desaparición de las tasas judiciales y los Secretarios pierden definitivamente toda capacidad de cobrar directamente de los particulares.

La capacidad técnica de los Secretarios Judiciales implicaba que, al igual que sucede con los Notarios o los Registradores, ellos subvencionaban las propias Oficinas Judiciales. Es decir, el Secretario era el propietario de su escribanía; él elegía y pagaba a sus empleados a través de los aranceles y tasas judiciales. La Admon pública pagaba, solo y poco, al Juez, quien de forma más o menos regular, solía recibir algún tipo de estipendio también del Secretario. Los aranceles judiciales, al igual que los de las notarías, se facturaban, además de por la naturaleza de las acciones ejercitadas, por el número de folios.

Así pues los conflictos permanentes a los que la Oficina Judicial se enfrenta a lo largo de las tres últimas décadas, tienen mucho que ver con esa configuración histórica que hacía que aún en los primeros años ochenta en muchas poblaciones los Secretarios Judiciales cobraran más que los Jueces y que resultara muy interesante, económicamente hablando, escribir mucho y "dictar" para un mismo trámite y asunto muchas resoluciones aunque realmente no fueran necesarias. Estas malas costumbres procesales las hemos heredado, y son las que hacen engordar indebidamente los asuntos, añadiendo papeles inútiles.

[2] Ley 37/1988, de 28 de diciembre de Presupuestos Generales del Estado para 1989.

La desaparición en 1988 de todo tipo de estipendios privados, regulares e irregulares en la Admon de Justicia determinó inicialmente una paralización de la Justicia que fue el origen de la primera reforma real de las Oficinas judiciales: la creación de los Servicios Comunes.

1.3.- LA LEY ORGÁNICA DEL PODER JUDICIAL DE 1985.

El proceso de democratización de la sociedad española que provocó la proclamación de la Constitución del 78, precipitó en 1985 la aprobación de una nueva Ley Orgánica del Poder Judicial. Probablemente la convicción de los responsables políticos de aquellos años de que era preciso democratizar la Justicia española instaurando un poder judicial independiente hizo que, a pesar de ser la LOPJ[3], sobre todo, una ley organizativa, se focalizara en diseñar garantías de esa independencia y descuidara diseñar una estructura organizativa moderna para las Oficinas Judiciales.

De todas formas, y aunque sin duda la LO de 1985 reprodujo la organización tradicional de las Oficinas Judiciales, sí se apuntaron algunas líneas, expresadas en determinados artículos de la ley, que tuvieron un índice de cumplimiento desigual. Así como todos los esfuerzos que la ley hizo para dar más competencias a los Secretarios Judiciales- propuestas de autos, de providencias y las diligencias de notificación, constancia y ejecución- quedaron en nada, casi sin querer y de hecho, un solo artículo de la ley determinó la reforma más importante, en mucho tiempo, en las estructuras de las Oficinas Judiciales.

Esta fue la creación de los Servicios Comunes. La LO los pensó exclusivamente como un soporte efectivo de las Salas de Notificación de los Procuradores, que ya existían en las poblaciones grandes, pero por razones no explicadas, el Art. 280 de la LOPJ permitió que en torno al final de los años ochenta, y ante la paralización que supuso la supresión de los cobros irregulares por salidas, se crearan los primeros Servicios Comunes de notificaciones y embargos. Desde entonces y con las modificaciones que sufrió la propia LO en el año 94, los Servicios Comunes de notificaciones y embargos se generalizaron en todo el Estado, con el apoyo también de las CCAA que fueron recibiendo los traspasos de competencias en materia de Admon de Justicia, de forma que en la actualidad han tomado carta de naturaleza en la organización judicial y nos hemos habituado a ellos.

[3] Ley Orgánica 6/1985, de 1 de Julio del Poder Judicial.

Aunque inicialmente contaron con importantes detractores entre diferentes sectores de abogados, funcionarios, jueces, procuradores y secretarios, hoy día está aceptado de forma generalizada que su resultado- siempre que se gestionen bien- es bueno. Esta aceptación del modelo de grandes Servicios Comunes ha inspirado, sin perjuicio de lo que luego diremos, el nuevo modelo de Oficina Judicial que contiene la modificación de la LO aprobada en diciembre del 2003.

2.-GESTIÓN DE LAS OFICINAS JUDICIALES

En el CGPJ[4] que ejerció sus funciones entre 1996 y 2001 se acordó hacer un diagnóstico sobre la situación de la Justicia del que se deberían derivar algunas propuestas para resolver sus evidentes graves problemas. Aquellos debates se convirtieron finalmente en lo que se conoce como el Libro Blanco de la Justicia[5]. Se consiguió que, por primera vez, se incorporara el término de gestión judicial a las necesidades de reforma de la Justicia. Allí no solamente se decía que era necesario un nuevo modelo de Oficina Judicial sino que se precisaba que, para que ese o cualquier otro modelo pudiera verdaderamente funcionar, era imprescindible que todos fuéramos conscientes de que había que saber cómo se gestionan las organizaciones judiciales, y que para eso había que aprovechar todos los conocimientos que en ese terreno pudiera haber.

Cuando el Libro Blanco de la Justicia apostó por primera vez sobre la implantación de nuevos sistemas de gestión en las organizaciones judiciales, era consciente de que, sin perjuicio de recomendar determinadas reformas en la propia estructura de la organización, estas no tendrían ninguna virtualidad si no iban acompañadas de una buena y eficaz gestión. Pero la gestión es un instrumento tan eficaz que es necesario recalcar que, hoy en día, con los modelos, sin duda trasnochados, que tenemos de Oficina Judicial y con las dificultades en medios y personal que son aún frecuentes, unas oficinas judiciales logran, a pesar de todo, un buen funcionamiento y otras no. Lo que diferencia unas organizaciones de otras no es el que la carga de trabajo sea mayor en unas que en otras, ni que en unas haya habido más funcionarios de baja que en otra, o que los interinos que se hayan enviado desde las bolsas tuvieran menos o más experiencia: la diferencia radica en que en esa oficina que funciona bien hay alguien que la dirige y la gestiona bien.

Vamos a pensar, que cada Oficina Judicial es como un pequeño campo de futbol.; unos ganan y otros pierden, y a veces hasta los que tienen menos opción de ganar, rompiendo las expectativas van y ganan.

Con esto no queremos decir que no deseemos que se produzcan modificaciones legales que puedan ayudar a mejorar la gestión de la Oficina Judicial, pero, como hablaremos un poco más adelante, también las nuevas leyes hay que gestionarlas y

[4] Consejo General del Poder Judicial.
[5] Abordaba de una manera sistemática los crónicos problemas de organización y funcionamiento de la Administración judicial española.

desgraciadamente estamos hartos de ver nuevas normas que quizás teóricamente puedan parecer acertadas y que sin embargo, en la práctica y por razones de diferente índole, acaban arrinconadas en la más total inoperatividad.

2.1.- ¿QUÉ QUIERE DECIR GESTIONAR BIEN UNA OFICINA JUDICIAL?

La necesidad de las empresas privadas de conseguir más eficacia y eficiencia en sus producciones llevó a estudiar el funcionamiento de los métodos de producción, primero y luego, lo que ahora nos importa, a elaborar una verdadera teoría de las organizaciones, de las que un aspecto importante es el saber como conducirlas.

Las organizaciones tienen su propio comportamiento. Podemos decir que éstas son la suma de la interactividad de los seres humanos que la componen, de la estructura organizativa y de los medios con los que cuenta. Sin embargo, el comportamiento de las mismas no es el resultado matemático de la adición de organización, capital humano y medios materiales, ya que las organizaciones tienen su propia manera de reaccionar y sus propias dinámicas interiores que multiplican o disminuyen los resultados.

La gestión sería, de una forma más precisa, la ciencia que estudia el movimiento de la organización. La organización como cualquier organismo vivo es, sobre todo movimiento y no tiene sentido el que solamente la estudiemos como algo estático y parado. Digamos que es algo parecido a lo que ocurre si nos empeñamos en estudiar y analizar con todo detalle el cuerpo humano en reposo absoluto. Podemos estudiar sus órganos con detalle, pero si no le vemos mover no sabremos exactamente cómo es el movimiento que se produce, ni por qué se produce ni por qué se produce un movimiento y no otro.

La gestión de las Oficinas Judiciales pretende conocer el movimiento de las organizaciones judiciales y esto tiene poco que ver con su organización.

El modelo organizativo y los medios de que se dote a una Oficina Judicial, por muy acertado que sea aquel y generoso el presupuesto que se le asigne, no garantiza el buen funcionamiento de la Oficina Judicial en cuestión.

2.2.-NUEVAS TÉCNICAS DE GESTIÓN EN LA ADMINISTRACIÓN PÚBLICA.

El término inglés "Management[6]" ha revolucionado las técnicas de gestión de todo tipo de empresas y organizaciones humanas. Surgió en el mundo de la empresa privada, como consecuencia de su natural necesidad de ser competitiva, pero otras organizaciones sin ánimo de lucro fueron conscientes de que para conseguir un resultado eficaz y eficiente en sus propósitos precisaban revisar sus sistemas de gestión. Esto mismo sucedió con las Administraciones Públicas que durante los años 80 comenzaron a interesarse seriamente en aplicar esas técnicas de organización.

Debemos señalar que la técnica más versátil y adecuada para mejorar las organizaciones públicas ha sido lo que ha venido a llamarse "gestión por objetivos" y los "procesos de mejora continua"

- **La gestión por objetivos:**

Parte de la idea de que cada organización pública, y en ella cada unidad administrativa debe tener un propósito y unos objetivos a conseguir.

- *método para establecer los objetivos:* la delimitación de los objetivos a conseguir es, principalmente, una decisión política (entendida como la capacidad de tomar decisiones que conduzcan a una organización pública en una u otra dirección). Sin embargo es necesario hacer un análisis del comportamiento de una organización antes de establecer los objetivos de la misma. Las organizaciones tienen que analizarse a sí mismas para diseñar cómo pueden actuar para conseguir los objetivos que se han propuesto. Por ejemplo, en el caso de las Oficinas Judiciales, si el objetivo es conseguir que no se suspenda más de un 1% de los juicios señalados, es imprescindible analizar la forma en la que en esa Oficina Judicial, en concreto, se realizan los señalamientos de los juicios.

- *análisis de las áreas concretas de la organización, en las que pretendemos establecer los objetivos*: en primer lugar hay que estudiar con detalle el funcionamiento de la Oficina Judicial que pretendemos mejorar. . Las leyes procesales definen los actos procesales que se deben observar para la consecución de los procesos judiciales, pero la

[6] Conjunto de conocimientos que tienen que ver con la economía, la sociología y la psicología.

manera de llevarlos a cabo en concreto debería formar parte de un libro de instrucciones generales para el funcionamiento de la Oficina Judicial.

En la Admon de Justicia no se suelen utilizar este tipo de herramientas de funcionamiento pero gran parte de lo que denominamos Diligencias de Ordenación [7]son un conjunto de instrucciones de funcionamiento concreto que tendrían que formar parte de simples normas de carácter general, de las que no debería quedar ningún tipo de reflejo en la documentación de los propios procesos judiciales.

Los programas informáticos utilizados hoy en día permiten integrar los libros de funcionamiento en la propia estructura de la programación genérica.

Un sistema útil para analizar el funcionamiento, en la práctica, de la Oficina Judicial es dibujar Diagramas de Funcionamiento. En primer lugar se deben reunir todas las personas afectadas por el análisis del área en concreto de mejora. Cada una de ellas explicará, con detalle, los actos concretos que realiza para el cumplimiento de los trámites procesales que la ley impone en cada momento.

Los funcionarios que llevan el señalamiento de los juicios desempeñan el mismo trabajo pero cada uno tiene unos determinados números lo que les obliga a cruzarse y a repetir gestiones constantemente. El análisis de este funcionamiento evidencia además la necesidad de preparar la disponibilidad de los "actores del proceso" con anterioridad al señalamiento de la fecha.

Resolver o prever adecuadamente las causas que ocasionan las suspensiones de los juicios constituirán los diferentes proyectos de mejora que deberán establecerse para conseguir el objetivo global de disminución de la suspensión de juicios.

- **Proyectos de mejora:**

Son los elementos que nos van a permitir cumplir los objetivos que hemos establecido. Pensemos por ejemplo en una de las causas de suspensión de juicios, cómo es la de la falta de control de la situación de libertad provisional de los acusados. El cambio que pudiera ocasionar el que se controlaran de una forma eficaz las presentaciones a las que están obligadas las personas que deben comparecer como acusados al acto del juicio oral, podría ser determinante para mejorar el índice de suspensiones de juicios. Un proyecto de mejora podría ser, en este caso, el establecer un

[7] Son resoluciones de tramitación que se insertan en la función jurisdiccional como función de impulso, equiparadas a las providencias de mera tramitación, que sólo pueden versar sobre el impulso del proceso en la dirección única y precisa que resulta de la aplicación automática de una norma legal.

departamento de control de la libertad provisional de las personas que se encuentran sometidas a estas presentaciones, de forma, que sin necesidad de esperar al día en el que se ha de celebrar el juicio oral, se sepa con antelación si el acusado está cumpliendo o no sus obligaciones, y si, por tanto, es previsible que se presente al señalamiento del juicio.

El que la Oficina Judicial conozca todo lo necesario respecto al comportamiento de los acusados, permite que, si es necesario, se tomen las medidas concretas precisas para asegurar la presencia del acusado en el juicio oral, con anterioridad a efectuar el señalamiento o la convocatoria del propio juicio oral.

Evaluación de los proyectos de mejora y análisis de la consecución o no de los objetivos establecidos:

La evaluación de la actividad pública es un elemento de control democrático esencial. El ánimo de lucro o el propósito de beneficio crean una evaluación natural en las organizaciones privadas. Cuando no logran los beneficios que pretenden, las empresas saben que van por mal camino, y sus ejecutivos también saben que están en cuestión sus puestos de trabajo.

Desgraciadamente en la Admon Pública, son muy poco frecuentes los procesos objetivos de evaluación, por lo que lo público se sigue identificando con la ineficiencia y el despilfarro de recursos. La evaluación en lo público es un instrumento verdaderamente esencial.

Para que haya evaluación y ésta sea una ayuda eficaz para la gestión pública, los objetivos establecidos deben tener un plazo y este plazo no debe ser demasiado largo. Si cualquier organización pública se propone mejorar un área de su actuación sin concretar el plazo en el que se ha de producir esa mejoría, se desactiva el instrumento de control que significa la evaluación. Por esto conviene que los objetivos se establezcan en plazos concretos y que transcurridos esos plazos se lleve a cabo, sin lugar a ninguna duda, la evaluación. La existencia y formación de una estadística correcta es un instrumento imprescindible para analizar los procesos de mejora en las organizaciones públicas.

Una vez transcurrido el plazo fijado para el cumplimiento de los objetivos, es imprescindible que la propia organización evalúe si ha conseguido alcanzar los logros que se propuso. Si efectivamente se han conseguido, la organización decidirá el paso siguiente hacia el proceso de mejora continua. Si, por el contrario, no se han alcanzado, será necesario evaluar de nuevo los trámites que se realizaron para analizar cuáles pudieron ser los obstáculos que impidieron conseguir esta mejora.

2.3.-INERCIAS Y RUTINAS EN LA GESTIÓN DE NUESTRAS OFICINAS JUDICIALES

El proceso directivo de la Oficina Judicial tradicional es un proceso jerárquico y basado en normas. El derecho orgánico administrativo que rige las organizaciones públicas está basado, esencialmente, en leyes y reglamentos que se ordenan desde los superiores jerárquicos a los inferiores, todo ello en base a escalas administrativas estrictamente concebidas.

Hoy en día se cuestiona la gestión jerárquica basada exclusivamente en la promulgación de leyes administrativas. Existen doctrinas que evidencian que la nueva manera de concebir la administración permite perfectamente la convivencia de las normas administrativas con las nuevas pautas de gestión, siempre que no se regule el funcionamiento de los órganos administrativos de forma agobiante por reglamentos, es decir si se separan con claridad las normas trascendentales para las garantías para los administrados de las normas de gestión.

Existe una ausencia absoluta de dirección exterior de las Oficinas Judiciales. Estas acaban convirtiéndose en pequeños reinos. La CE[8] al establecer la necesaria división de poderes, optó por un camino complejo para la gestión de las Oficinas Judiciales. Aunque el CGPJ[9] sólo tiene competencias respecto a los jueces, mantiene un sistema de inspección de las Oficinas Judiciales respecto las que, paradójicamente, no tiene ninguna capacidad de decisión, puesto que ni los Secretarios Judiciales, ni los funcionarios judiciales, ni la provisión de los medios materiales dependen del CGPJ. Los Secretarios Judiciales dependen del Ministerio de Justicia, la provisión de los medios materiales y la regulación de los funcionarios judiciales ha sido transferida, prácticamente en su totalidad a las CCAA, por lo que podemos decir que en cada una de las Oficinas Judiciales existe un entramado complejo de responsables jerárquicos.

Queda claro que la dirección de la Oficina Judicial es muy compleja, ya que por un lado está en manos de los Secretarios Judiciales, pero la dirección de los procesos judiciales corresponde a los Jueces y Magistrados.

No existe ningún método que consiga que las organizaciones judiciales funcionen de forma homogénea y coordinada. Cada microorganismo judicial funciona según sean los elementos humanos que lo conforman. Además es muy frecuente ver que dentro de

[8] Constitución Española.
[9] Consejo General del Poder Judicial.

cada organización judicial hay a su vez funcionarios que tramitan un determinado número de asuntos según sus propios criterios y sin someterse a ninguna planificación general.

Es también muy frecuente que los funcionarios se repartan el trabajo exclusivamente por el número de orden del asunto o diligencias. Se trata de darle a todos los asuntos una numeración única, para después hacer una distribución de los distintos asuntos, exclusivamente, por números. Hay veces que un funcionario de forma particular ha diseñado y hasta inventado métodos de tramitar los asuntos a él atribuidos tan inteligentes que deberían ser conocidos valorados y generalizados por toda la organización.

Hay que tener en cuenta que los funcionarios llegan a las Oficinas judiciales después de haber superado una oposición, con desconocimiento de lo que significan los trámites judiciales. Cuando llegan por primera vez a sus destinos, copian las resoluciones judiciales que utilizan otros compañeros y elijen las que aquellos les dicen de entre las que ofrecen los programas informáticos instalados en sus correspondientes ordenadores. Así, en la mayoría de los casos los funcionarios teclean resoluciones sin saber si verdaderamente valen para algo, simplemente es lo que siempre se hizo, y lo que paradójicamente los sistemas informáticos han consagrado.

2.4.-LOS CONTENIDOS DE LA GESTIÓN.

Las leyes procesales son el conjunto de normas que establece el comportamiento que deben observar en los procesos, tanto los interesados o partes procesales, como los abogados y demás profesionales intervinientes, y de forma especial los Secretarios Judiciales y los Jueces; en resumen la propia organización judicial.

Las normas procesales son por definición la garantía para los ciudadanos de que sus reclamaciones van a tramitarse y resolverse con unos métodos predeterminados, de forma objetiva e igualitaria para todos los que acudan a la Administración de Justicia en busca de la tutela judicial efectiva que garantiza la CE[10].

Las leyes procesales describen cuáles deben ser los comportamientos que han de observar todos los intervinientes en los procesos. Pero además de estas disposiciones específicas existen los principios generales que regulan los procesos y que forman un conjunto de normas genéricas que derivan de la propia CE, de la Declaración de los

[10] Constitución Española.

Derechos Humanos en la que ésta se inspira, y de las decisiones, interpretando estos principios, del TS[11] y del TC.[12]

Es claro, por tanto, que todos los funcionarios de la Admon de Justicia, cuando tramitan los procesos judiciales, deben cumplir las normas expresadas tanto en las propias leyes procesales como en los principios que las inspiran. Sin embargo el cumplimiento de las normas procesales ha de ser gestionado de una manera eficaz. No es así, cuando en lugar de establecer pautas de gestión de los procesos judiciales, se deja que cada funcionario las interprete a su forma.

Debemos distinguir claramente lo que son las normas procesales y lo que son las pautas de tramitación de esas normas procesales. Podemos definir las normas de gestión de la tramitación como normas instrumentales, que hacen posible cumplir las disposiciones legales procesales. Muchas veces por una inadecuada gestión de las normas procesales se producen vulneraciones de los principios procesales y de las garantías de los ciudadanos, por ejemplo cuando se producen dilaciones indebidas en la tramitación de los procedimientos.

El CGPJ [13]ha formulado estudios en los que se evidencia que la duración legal de los procesos poco tiene que ver con la duración real. La gestión procesal, ha de ser un instrumento imprescindible para que las Oficinas Judiciales puedan llevar a cabo en plazo el cumplimiento de los trámites procesales, ya que es un principio constitucional el principio de celeridad (Art. 24 CE). También es necesario contemplar el principio de eficacia establecido en el Art.103 de la CE. Cuando infringimos el principio de celeridad procesal y dilatamos indebidamente los procedimientos, o resolvemos con trámites innecesarios, encarecemos los procesos y convertimos a la Administración de Justicia en ineficaz e ineficiente.

Las normas de gestión de los procedimientos deben cumplir escrupulosamente las normas procesales establecidas en las correspondientes Leyes de Enjuiciamiento, interpretadas por los principios constitucionales, y ser además eficaces y eficientes, tal y como exige también la propia CE.

El cumplimiento de las normas procesales no quiere decir sin embargo la utilización burocrática y rutinaria de las mismas. La mayor parte de las leyes procesales adolecen de pautas claras en los actos más sencillos del desarrollo de los procesos.

[11] Tribunal Supremo.
[12] Tribunal Constitucional.
[13] Consejo General del Poder Judicial.

La LEC[14] no contiene una descripción clara y sencilla sobre como deben ejecutarse estos actos esenciales para dar satisfacción a los ciudadanos que han acudido a los juzgados no para obtener una sentencia, sino para que esa sentencia, produzca los efectos de restablecimiento de los derechos que han sido lesionados. Es ahí donde adquieren una trascendental importancia las normas de gestión. El que los funcionarios que tramitan los procedimientos reciban instrucciones claras de sus superiores es un elemento trascendental en su forma de tramitar que ha de fundamentarse en la simplificación y la celeridad.

La gestión de los medios materiales:

La implantación de las nuevas tecnologías está muy atrasada, con carácter general, en la Administración de Justicia. Desde mediados de los 90, las CCAA que fueron adquiriendo esta competencia, iniciaron esfuerzos modernizadores que se han traducido en diversos sistemas informáticos con diferentes grados de desarrollo.

El territorio correspondiente al Ministerio de Justicia se halla en una fase menos avanzada, debido a su insistencia en apoyarse en un sistema "Libra"[15] que presento en su momento dificultades de adaptación. Cada vez que se hablaba de la problemática de la Oficina Judicial, se decía que la implantación en todos los juzgados de la informática resolvería los graves problemas existentes. La Consejería de Justicia del Gobierno Vasco dio los primeros pasos informáticos en los Juzgados del País Vasco. Se emplearon técnicas avanzadas pero desgraciadamente no se informatizaron protocolos de gestión de los procesos, sino simplemente se convirtieron en documentos electrónicos, modelos de resoluciones procesales, sin guías de gestión procesal, que solamente consiguieron informatizar la burocracia existente. En general los sistemas procesales informáticos que se utilizan en los juzgados y tribunales funcionan como una simple colección de documentos judiciales y no hay protocolos de actuación que puedan indicar a los funcionarios cómo deben comportarse con los ciudadanos precisamente en el desarrollo de los procesos.

La utilización de la informática en todas sus vertientes (gestión del proceso, gestión de los órganos judiciales, agenda judicial, comunicaciones internas y externas, acceso desde la red, gestión de personal y del sistema en su conjunto, obtención de la

[14] Ley de Enjuiciamiento Civil.
[15] Programa informático utilizado en la Oficina Judicial. En la actualidad se prepara su sustitución por el programa "Minerva".

estadística judicial, supervisión de los órganos judiciales, utilización para la gestión de recursos de los datos del sistema, acceso a colecciones de jurisprudencia, etc.), se plantea como una necesidad urgente.

Los sistemas informáticos concebidos inicialmente como asistentes de la gestión procesal, se han revelado en su desarrollo como una herramienta de gran utilidad para otras tareas: controlar la marcha del órgano judicial, realizar los alardes y la estadística, facilita la supervisión, proporcionar información muy valiosa sobre el funcionamiento del sistema judicial y del sistema jurídico, permitiendo evaluar los efectos de modificaciones legales procesales y sustantivas, etc. A ello se añade todo lo referente a la tecnología de las comunicaciones, tanto entre órganos judiciales (con el consiguiente ahorro de trámites y tiempo), como con abogados y procuradores, formalización de agendas de señalamientos, publicidad de resoluciones (subastas y otras ejecuciones, edictos, etc.).

El proceso de informatización iniciado, como cualquier proceso de cambio, precisa tiempo para incorporar a la Admón. de Justicia el cambio de cultura que significa, lo que únicamente será posible mediante la formación continuada de los usuarios y el apoyo eficaz a los puestos de trabajo, de forma que cualquier pequeño inconveniente no se convierta en un obstáculo insalvable.

Características de un buen sistema informático:

La incorporación de las nuevas tecnologías de la información a los sistemas judiciales se ha revelado en todo el mundo como una cuestión crucial, y de su aprovechamiento depende el éxito o fracaso de la política judicial y de otras políticas públicas. Uno de los problemas que se plantea tras la implantación de los sistemas informáticos de gestión procesal consiste en la escasa utilización que parece hacerse de ellos.

Un primer obstáculo proviene de las dificultades que siempre conlleva el cambio, y de ahí que resulte tan importante la gestión del mismo. Otro inconveniente proviene de la dificultad o la complejidad de su uso juegue contra la innovación. El tercero se traduce en graves defectos en la cumplimentación de un gran número de campos que los usuarios de la aplicación consideran sin interés para su trabajo, por más que sean de importancia central para otros usuarios del sistema judicial. El cuarto consiste en el desconocimiento, y por ello la falta de uso, de la información que generan las aplicaciones informáticas, a pesar de su gran valor.

Se pone de relieve la necesidad de mantener un esfuerzo inversor en nuevas tecnologías para dotar a los órganos judiciales de medios idóneos que faciliten el impulso procesal y la utilización en la Justicia de los sistemas informáticos para la gestión, tanto de los procesos como de los órganos judiciales.

La informática judicial debe servir para:

- la gestión de los procedimientos judiciales, lo que supone definir las aplicaciones procesales y su desarrollo en cada orden jurisdiccional, de forma que permitan la tramitación ágil de los procedimientos, manteniendo la plena seguridad de sus contenidos, y llevando a cabo de forma automática la incorporación y actualización de los datos procesados a una base de datos general.

- el mantenimiento, mediante la creación de una red integrada, de un flujo fluido de información de un órgano judicial a otro, y, además de ello, la posibilidad de obtención de información sobre el funcionamiento del sistema judicial, analizándolo bajo diferentes requerimientos, para gestionarlo de forma eficaz.

- constituir una red integrada y compatible de comunicaciones que permita, no sólo el diálogo horizontal y vertical entre los distintos juzgados y tribunales, sino, también, la posibilidad de extender estas comunicaciones a los profesionales relacionados con la Admon de Justicia e, incluso a las futuras redes judiciales implantadas o a implantar en España y Europa.

- disponer de un buen banco de datos jurídicos, accediendo a sus recursos y nutriéndolo con las resoluciones judiciales que se produzcan.

La inversión en nuevas tecnologías puede proporcionar progresos en la gestión de los procesos pero no podría justificarse si lo principal fuese instalar ordenadores en los juzgados para el procesamiento de textos. Los resultados deben corresponderse con la inversión, que no se debe hacer únicamente para el mejor trabajo de Jueces, Magistrados, Fiscales y personal al servicio de la Admón. de Justicia, sino, de forma prioritaria, para que la tutela solicitada por los ciudadanos ante los juzgados y tribunales se obtenga de forma eficaz y rápida. Las inversiones y actuaciones en Justicia no tienen otro horizonte que el de mejorar la prestación de este servicio público fundamental en nuestro Estado de

Derecho. Y como todo servicio público, necesitamos poder evaluar la calidad de esta prestación y si, verdaderamente, estamos cubriendo los objetivos que a toda inversión pública hay que exigirle.

Un órgano judicial ha de estar inmerso en procesos de mejora, lo que supone una evaluación permanente de su funcionamiento y requiere información, y saber cómo aprovecharla. En este campo, la informática alcanza un alto grado de eficacia, pues puede proporcionar una información completa y esencial sobre cuestiones de gran importancia para la mejora del sistema judicial y jurídico, tales como, cantidad de litigios, duración, usuarios, materias etc.

La informática judicial debe hacer posible:

- conocer qué procedimientos hay y cuántos de cada clase en cada orden jurisdiccional.
- saber la duración, en conjunto, de la tramitación, de cada una de sus fases y de la ejecución.
- saber quienes son los usuarios de la Justicia y por qué acuden a ella.
- establecer sobre qué materias, cuantías y tipo de actividad se requieren pronunciamientos de la Justicia.
- evaluar qué efectos tienen sobre los órganos judiciales las medidas de apoyo, la actividad de los servicios comunes, los incrementos de plantilla, la movilidad de jueces, secretarios o funcionarios, etc.
- valorar cual es la incidencia de las modificaciones legales.

La posibilidad de obtención de esta información depende no sólo de las características del sistema informático, sino también del grado en que los usuarios hayan hecho un uso adecuado del mismo. En este sentido, se presenta como una necesidad optimizar el aprovechamiento de todas las posibilidades que ofrecen los sistemas informáticos, y dotar de una adecuada formación a sus usuarios.

La informatización integral de los órganos judiciales debe suponer:

- Dotación de equipamientos: parque instalado, reprografía, audiovisuales…etc.
- Comunicaciones: recursos de comunicaciones, intranet, servicios de Internet.
- Aplicaciones: Sistemas de Gestión Procesal (sistema, base de datos, plataforma de desarrollo), Sistemas Documentales (jurisprudencia y legislación, bases propias y de

terceros), estadística y gestión del órgano judicial, estadística e información agregada del sistema judicial y sus partes.

- Protección de datos: Ficheros con datos de carácter personal; Medidas de Seguridad (accesos, firma electrónica, encriptación de documentos).
- Recursos dedicados: Personal de Soporte (a usuarios, a sistemas, desarrollos…); Acciones de Formación y Adiestramiento; Inversiones (equipamientos, desarrollo y soporte e implantación).

La gestión de los medios personales.

Jueces y funcionarios. Los elementos humanos de la justicia española:

El concepto "medios personales" es el que habitualmente se utiliza al referirse a las personas que trabajan en las Oficinas Judiciales cuando se habla de su organización. Cualquier organización, sea pública o privada, depende fundamentalmente de las personas que trabajan en ella. En nuestro país, en virtud de lo que establece la CE en su Art.103.3, los funcionarios de la Admon Pública deben ser elegidos por los sistemas de mérito y capacidad. En España la selección de todos los funcionarios es a través de oposiciones esencialmente memorísticas. Sabemos que no es el sistema más indicado, pero con él tenemos que conseguir gestionar mejor el personal que trabaja en las Oficinas Judiciales.

En las oficinas de los Juzgados y Tribunales, además de los Jueces, Magistrados y Secretarios Judiciales, trabajan otros funcionarios con las categorías de Oficiales, Auxiliares y Agentes Judiciales. La nueva Ley Orgánica[16] ha dado nuevas denominaciones[17] para estos cuerpos de funcionarios judiciales, diseñando nuevos catálogos de tareas en las Oficinas Judiciales.

También tenemos que mencionar a los funcionarios interinos judiciales, que son aquellas personas que, sin haber superado ningún tipo de oposición y con las simples titulaciones académicas exigidas para los titulares, una vez admitidos en la correspondiente "Bolsa de interinos", gestionada por la Admon competente en cada caso, son destinados a los juzgados para cubrir las vacantes por marca a otro destino de los

[16] LO 19/2003, de 23 de diciembre, de modificación de la LOPJ 6/1985.
[17] Oficiales, Auxiliares y Agentes Judiciales, con la LO 19/2003, pasan a llamarse Cuerpo de Gestión Procesal y Administrativa, Cuerpo de Tramitación Procesal y Administrativa y Cuerpo de Auxilio Judicial.

funcionarios titulares o para sustituir a aquellos, que por alguna razón se encuentran de baja

En el sistema judicial español nos encontramos con las siguientes figuras de empleados:

- ✓ Jueces y Magistrados.
- ✓ Fiscales.
- ✓ Secretarios.
- ✓ Jueces de Paz
- ✓ Personal Administrativo: Oficiales, Auxiliares, Agentes y Médicos Forenses.

El cometido fundamental del sistema judicial es resolver plenamente los conflictos que se le plantean mediante sentencias, autos u otras formas de terminar los procedimientos, actos todos ellos que, para ser eficaces, deben trascender de la mera declaración de derechos y tener consecuencias ejecutivas, adecuadas a las pretensiones expuestas por los ciudadanos.

En cada una de las crisis que experimenta el sistema judicial se pone en cuestión su eficacia, debido a la tardanza de las resoluciones judiciales.

Se han multiplicado y modernizado los medios materiales y se han incrementado los recursos humanos en una importante cuantía, que no produce resultados proporcionales.

Los recursos económicos del sistema judicial proceden de dos fuentes: el Ministerio de Justicia y las CCAA. Después del traspaso efectivo de funciones y servicios que se ha llevado a cabo, hemos llegado a una situación en la que ya es mayor el gasto en Justicia que efectúan las CCAA que el del Ministerio de Justicia. Sin embargo hay un grave déficit de autonomía en cuanto a la elección por éstas de compromisos de gasto.

A las Administraciones responsables de la Justicia les debe interesar comprobar si los recursos que aplican al sistema (dotaciones presupuestarias) tienen correspondencia con la actividad (producción) del mismo. No sería síntoma de un buen sistema judicial disponer de más medios y además, tener menos carga de trabajo, y sin embargo disminuir la producción y aumentar la duración de los asuntos.

Se han ido introduciendo fuertes modificaciones en el gasto en Justicia. Nos encontramos hoy con un gasto en Justicia multiplicado, en parte por dotación de nuevos edificios y la informatización en distintos grados y con fuertes desequilibrios territoriales. En cierto modo en la Justicia se proclaman necesidades urgentes que demandan gastos urgentes.

La ejecución de sentencias ha sido históricamente la pata de la que ha cojeado el sistema judicial, y sigue siéndolo a pesar de las mejoras que se han introducido en la LEC[18]. Hay que arbitrar sistemas de organización que faciliten la ejecución de las sentencias, lo que también debería afrontarse desde el momento de plantear la acción por el demandante, y de resolver el conflicto por el juez.

Nuestro sistema judicial ha pasado, en un plazo relativamente breve, de recibir alrededor de dos millones de asuntos, a tener que resolver alrededor de ocho millones. Parece evidente, que no es capaz ya de aumentar su rendimiento.

Por ello, y aunque es necesario seguir incrementando el gasto, especialmente en nuevas tecnologías, lo verdaderamente imprescindible es cambiar la organización del trabajo. Sin este cambio, será imposible conseguir la eficacia y eficiencia que ha de tener el gasto público.

¿Hace la Oficina Judicial todo lo que puede? No, podría desarrollar mucho más trabajo, y no lo hace por dos razones: porque no hay una incentivación del personal relacionada con los resultados, ni una adecuada evaluación de los mismos, y porque los únicos resultados que se tienen en cuenta son los que dependen exclusivamente del trabajo del juez (fundamentalmente las sentencias dictadas), que está saturado.

La consecuencia inmediata de lo anterior es que, para mejorar la eficiencia del sistema, es necesario, no tanto crear nuevos juzgados, sino dotar al sistema de más jueces, que puedan resolver todo lo que la Oficina Judicial es capaz de tramitar.

Cualquier propuesta sobre la mejora de la eficacia de la Oficina Judicial pasa por un replanteamiento en profundidad de las funciones del Secretario Judicial.

La eterna coartada de la fe pública judicial es algo que decae por el propio impulso de las aplicaciones informáticas y la nueva forma de acreditar y certificar contenidos, tiempos, firmas, personaciones, que hacen irrelevante la dación de la fe pública.

El Secretario Judicial ha de centrar sus funciones en la ordenación e impulso del procedimiento, en la ejecución del mismo, en los procedimientos de jurisdicción voluntaria.

La Oficina Judicial ha de adaptar su estructura a las tareas reales definidas por las leyes procedimentales, eliminando trámites y añadidos que nada mejoran las garantías ni los contenidos de los procesos. Del mismo modo, deben incorporarse con urgencia al

[18] Ley de Enjuiciamiento Civil.

diseño organizativo los sistemas informatizados de gestión, que aún no se utilizan con carácter general y de los que no se explotan todas las potencialidades.

Saber que ocurre en cada órgano judicial, evitar tareas tediosas de identificación en los procesos, tener actualizado y en agenda cada uno de los trámites, introducir en el sistema información que posibilite mejorar el acceso a la Justicia, y también la eficiencia en la oferta y en la demanda de Justicia, compatibilizar todos los sistemas, tener redes de conexión que permitan la comunicación fácil y segura entre los órganos judiciales son tareas básicas de la informática.

El destinatario de las prestaciones del servicio público de Justicia es el ciudadano. Es el ciudadano quien tiene derecho a una Justicia sin dilaciones indebidas, a la información, al conocimiento sobre el estado de tramitación de sus asuntos, etc. Y a esa finalidad se ordena la actuación de los poderes públicos.

Desde esta perspectiva, debe abordarse la creación de un servicio de información al ciudadano, que atienda a todas las posibles demandas de información general y específica, reclamaciones sobre la justicia y la administración de justicia, quejas, sugerencias, demandas de servicios y atención específica etc.

Pensamos en un servicio que atienda a los siguientes frentes:

- Información logística: dónde están los órganos y servicios judiciales.
- Información de contenidos: dónde debe dirigirse para resolver asuntos de distinta índole: civiles, penales, etc. Qué debe hacer para resolver determinados problemas: certificados penales, asistencia a subastas, actos relacionados con el Registro Civil, etc.
- Información sobre el estado de tramitación de cada asunto, sobre el tiempo previsible para su resolución.
- Información sobre la asistencia jurídica gratuita.
- Información sobre derechos individuales: víctimas, denunciantes, etc.
- Consultas, reclamaciones y quejas sobre servicios administrativos.
- Consultas, reclamaciones y quejas sobre infraestructuras de la Administración de Justicia y sobre su personal.
- Consultas, reclamaciones y quejas sobre tramitación de asuntos en el ámbito judicial.
- Consultas, reclamaciones y quejas sobre los contenidos de las resoluciones judiciales.

- Cumplimentación de formularios para la Administración, los órganos de gobierno de los Juzgados (Decanato, Junta de jueces) y el CGPJ.
- Contestación a los ciudadanos.
- Correo electrónico. Pág. Web.
- Etc., etc.

La nueva LOPJ ofrece la posibilidad a las administraciones gestoras de los recursos de instalar unidades de gestión que, sin formar parte de la Oficina Judicial, lleven adelante las tareas que están en la base organizativa de ésta: personal medios materiales, informática, transportes y comunicaciones, mantenimiento del edificio, sistemas de seguridad, etc. La existencia de estas unidades de gestión releva al Secretario de multitud de tareas tediosas, y le permitiría dedicarse íntegramente al impulso y trámite procesal.

3.- EL FUTURO: NUEVO MODELO DE OFICINA JUDICIAL.

3.1.- LA LEY ORGÁNICA 19/2003.

El modelo de configuración de la Oficina Judicial vigente ya analizado, construido en torno a "Juzgado" o "Tribunal", con Secretarios Judiciales responsables de la jefatura de personal, bajo la dirección del Juez o Presidente del Tribunal, cambia radicalmente en las previsiones y regulación de la LO 19/2003, de 23 de diciembre, de modificación de la LOPJ 6/1985, en vigor desde el 15 de enero del 2004.

Se logra mediante una nueva regulación estructural desarrollada en tan solo cuatro preceptos (Art. 435 a 438, ambos inclusive) del Libro V denominado "De los secretarios judiciales y de la Oficina Judicial". Regulación tan escueta que provoca, inevitablemente, lagunas. Pero, pese a incertidumbres y lagunas resulta incuestionable que se trata de la primera y gran oportunidad de poner fin al anquilosado aparato burocrático judicial.

La regulación legal establece, con carácter imperativo, para la nueva estructura básica de la Oficina Judicial, un principio general de homogeneidad en el territorio nacional, a compatibilizar con una idea de flexibilidad. También principios estructurales: jerarquía, división de funciones, y coordinación, a la vez que criterios de actuación: agilidad, eficacia, eficiencia, racionalización del trabajo, responsabilidad por la gestión.

El Art.435.1 define la Oficina Judicial como "la organización de carácter instrumental, que sirve de soporte y apoyo a la actividad jurisdiccional de Jueces y Magistrados", lo que evidencia una concepción en la que, al fin, se deslinda:

a) Actividad jurisdiccional desempeñada por Jueces y Magistrados, depositarios de la potestad jurisdiccional, en función, constitucionalmente prevista, de juzgar y hacer ejecutar lo juzgado.
b) Actividad procedimental y administrativa que permita y haga eficaz la anterior, mediante las infraestructuras humanas y técnicas que se precisen.

La nueva LO convierte la figura del Secretario Judicial en una de las claves de la reforma. Al margen de redefinir su función de fe pública, o de una mayor y más precisa definición de sus funciones, su posición de directores del personal integrante de la Oficina Judicial en su aspecto técnico-procesal, ordenando su actividad y dirigiendo, con exclusividad, la totalidad de las tareas de carácter procesal y toda la actividad de cada Unidad de la nueva estructura supone potenciar de modo efectivo sus capacidades

profesionales, a la par que les convierte en exclusivos responsables de los resultados que cada unidad obtenga, poniendo así fin a las disfunciones derivadas del solapamiento actual de responsabilidad de Juez y Secretario de cada juzgado.

La vigente LOPJ delimita de manera minuciosa las funciones del personal al servicio de la Admon. de Justicia

Los actuales cuerpos de funcionarios (Oficiales, Auxiliares y Agentes de la Administración de Justicia) desaparecen, pasando a crearse nuevos cuerpos de:

a) Cuerpo de Gestión Procesal y Administrativa. Ocuparán las jefaturas de funcionarios en Unidades de la Oficina Judicial, Secretarías de la Oficina Judicial en Juzgados de Paz o de Agrupaciones de Secretarios de Juzgados de Paz.
b) Cuerpo de Tramitación Procesal y Administrativa. Les corresponde la realización de cuantas actividades tengan carácter de apoyo a la gestión procesal, según nivel de especialización de cada puesto, bajo el principio de jerarquía y según las funciones concretas asignadas a cada puesto de trabajo.
c) Cuerpo de Auxilio Judicial. Les corresponde la realización de cuantas tareas tengan carácter de auxilio a la actividad de los órganos judiciales, de acuerdo con lo establecido para cada puesto de trabajo.

3.2.-LA GESTIÓN DEL CAMBIO. FASES Y TÉCNICAS PARA IMPLANTAR EL NUEVO MODELO.

La implantación de una reforma tan importante y trascendente provoca una compleja problemática. El proceso para acabar con una estructura tan tradicional, enraizada y atomizada y sustituirla por otra más moderna y racional, supone todo un reto. A los cambios estructurales deberán, necesariamente, añadirse, profundos cambios en lo que a gestión y pautas de actuación se refiere, como único modo de alcanzar el objetivo: que la Administración de Justicia preste un servicio de calidad a sus destinatarios.

Analizar:

El éxito de un proceso de reestructuración exige atender, analizar y valorar los aspectos afectados por el cambio y que deberán tenerse en cuenta para la puesta en marcha del proyecto.

Preparar. Información y participación en el proceso

Es imprescindible que el proceso se realice contando con los protagonistas del cambio: el personal integrante de la Administración de Justicia, en todos sus niveles. Los procesos de cambio no pueden imponerse contra la voluntad de sus protagonistas. Hay que favorecer divulgaciones de todos los proyectos a todos los estamentos para que todos comprendan y asuman el papel que corresponde a cada uno. Hay que añadir además una detallada información del proyecto y de sus características. Es necesario un Plan de Información, distinto e independiente del Plan de Formación.

Formación:

La idea de Oficina Judicial para el futuro ofrece la siguiente conclusión: se coloca al Secretario Judicial en posición de exclusivo director del funcionamiento de la organización, figura imprescindible al frente de cada una de la totalidad de Unidades que la conforman. El éxito o fracaso del cambio depende de su actuación. La actual formación teórica y práctica de los Secretarios Judiciales es manifiestamente insuficiente y poco o nada idónea para la nueva función que se le adjudica. Los Secretarios Judiciales, además de técnicos procesales, ejercerán funciones de dirección de la actividad de equipos humanos, por tanto es necesario que su formación incluya el conocimiento de técnicas de dirección, de elaboración de programas de actuación y estrategias adecuadas, además de las propias de la labor de organizar, dirigir y evaluar resultados.

Experiencias piloto:

El paso de lo viejo a lo nuevo debe hacerse prestando servicios de forma ininterrumpida. Resulta prudente considerar que la puesta en marcha del proceso de reestructuración en pequeña escala, con carácter experimental, eligiendo lugares de implantación idóneos por sus características, volumen de trabajo, necesidades de especialización, etc., permitiría conocer los resultados de esas experiencias comprobar los desajustes evaluar riesgos y resultados, imponer ajustes convenientes, etc., experiencia previa que permitiría dotar al posterior inicio real del proceso de mayor control y seguridad, garantizando, además de evitar el caos, una continuidad en la prestación del servicio.

Racionalizar el cambio

La fase preparatoria incluye adecuar estructuras, reasignar efectivos, planificar la implantación, etc. Pero, además, debe incluir los trabajos precisos para preparar otra gestión del proceso y de las actividades de los miembros de la organización. Secretarios Judiciales y funcionarios van a desarrollar funciones en ámbitos muy limitados de la actividad procesal, por lo que la especialización habrá de resultar inevitable.

De este modo, el aprovechamiento de los conocimientos y capacidades ya adquiridos por los integrantes de la organización, la formación de equipos, y su dedicación a actividades especializadas, serán principios de actuación y bases de partida en la implantación.

Protocolos y Manuales de Gestión

Probablemente ahora se nos presenta la oportunidad óptima para tramitar de un solo modo. Del modo que se haya considerado ajustado a la legalidad, más razonable, eficaz y práctico para el fin que se pretende. Y más rentable y al menor coste posible, puesto que consumimos recursos públicos.

El sistema está inventado. Falta asumirlo, extenderlo y aplicarlo. En la medida que afecta a la calidad y costes del servicio público, la discrecionalidad en su utilización parece inaceptable. En la Oficina Judicial se desarrollan muchas actividades no expresamente previstas en las leyes procesales, o previstas pero sin indicar el modo de hacerlo en casos en los que puede materializarse el acto de muchos modos, el manual, protocolo, o libro de instrucciones, será más útil en la medida que incluya la mayor parte posible de la totalidad de la actuación de quienes conforman el equipo. Se confeccionan los modelos correspondientes al nuevo esquema. Se redactan instrucciones generales de cómo actuar en cada situación previsible.

Y así queda redactado y listo el Manual de Gestión: ordenación de tareas, modo de practicarlas, y enumeración de modelos aplicables a cada situación, con redacción clara destinada a los tramitadores, dejando claro quien es el responsable de la realización de cada tarea. Tras un periodo de rodaje, vigilando y evaluando su implantación y utilizando los errores apreciados y sugerencias para mejorar y perfeccionar, se ajustan los extremos precisos. El resultado es racionalizar, simplificar y abaratar la tramitación. Pero sobre todo fijar y establecer un modo de tramitar cada tipo de procedimiento. Solo falta ponerlo en conocimiento de todos los que han de intervenir en ese tipo de tramitación e imponer su uso.

Definición de objetivos e indicadores:

Para una transición ordenada, las fases y calendario de implantación deben corresponderse con un listado de "objetivos" concretos que se pretenden alcanzar paulatinamente.

Conocemos con el nombre de indicadores los instrumentos o herramientas útiles para controlar y medir el grado de cumplimiento de los objetivos previamente establecidos.

La mejora constante en las Oficinas Judiciales

Destacados secretarios judiciales mantienen que la adopción de este principio de mejora continua por la Oficina Judicial supone la aplicación de metodologías e instrumentos internos que le permitan adaptarse a los diversos cambios y que hagan factible el establecimiento de objetivos cada vez más ambiciosos. Para conseguir que la Oficina Judicial se encuentre en todo momento actualizada, modernizada y capacitada para dar respuesta al ciudadano y demás clientes hay dos vías:

- la mejora día a día, a base de cambios constantes y graduales. Es la mejora continua, también llamada Kaizen,[19] que proporciona una mejora ilimitada.
- la mejora extraordinaria, que puede originarse en un cambio brusco de leyes, en la organización, a través de reingeniería de procesos o una revolución tecnológica, por ejemplo. Se denomina también Kairu [20]y puede proporcionar una mejora cualitativa importante.

La integración de ambos métodos (Kairu-Kaizen), es además de factible, deseable.

La nueva regulación supone toda una ruptura con el modelo conocido en aspectos esenciales de la organización. Sin duda, un gran cambio. El único modo de ir adaptando la actuación a las necesidades reales que se presentan será analizar las deficiencias, identificar sus causas, pensar alternativas, seleccionar y adoptar las medidas oportunas para modificar lo preciso, estudiar sus efectos, comprobar la

[19] Es una sistema para la mejora contínua del trabajo que implica mejoras graduales incrementales. Es la estrategia perfecta para desarrollar el hábito de la mejora en todo el personal, y la toma de conciencia del valor económico de las cosas.

[20] Es el sistema que busca la mejora a través de cambios radicales, innovaciones importantes, donde es fundamental el trabajo con especialistas, donde se busca modificar los grandes temas, donde la información es cerrada a unos grupos y se busca replantearse la organización desde cero.

desaparición de la deficiencia. Es decir, lo ya conocido: planificar, ejecutar, comprobar y ajustar. O, analizar, planificar, controlar y medir resultados. Y corregir.

"*La buena Justicia ha de ser tan competente como imparcial, o tan eficaz como independiente, sin que un posible alto nivel en cualquiera de tales cinco dimensiones pueda compensar o "sanear" una situación deficiente en cualquiera de las otras. Porque ¿cómo podría ser considerada buena una Justicia que fuera independiente pero lenta, o rápida pero incompetente, o competente pero parcial*?"[21]

Una Administración efectiva de la Justicia es una de las condiciones fundamentales para el establecimiento del Estado de Derecho.

Un sistema jurídico que tiene en cuenta los derechos del individuo será inútil si no funciona de manera eficaz.

Desde el Consejo de Europa se reiteran recomendaciones (nº 817, 845, 8612) para promover y lograr un sistema judicial efectivo, en coherencia con la exigencia formulada por el Convenio Europeo de Derechos Humanos (Art.6) de juzgar cada caso en tiempo razonable.

[21] Juan José Toharia; "La buena Justicia".

4.-LAS TIC COMO HERRAMIENTAS AL SERVICIO DE LA JUSTICIA.

La Justicia es uno de los valores superiores del Estado y un servicio público esencial. Su buen funcionamiento afianza el sistema democrático y el Estado del Bienestar, ofreciendo seguridad a los ciudadanos y a las empresas.

El sistema judicial español sufre desde hace tiempo de una situación de congestión. La llamada "crisis de la Justicia en España" tiene que ver con la carencia de medios materiales, a veces de medios personales y la falta de organización pero la solución de problemas no siempre consiste en aumentar el gasto. Por ello voy a tratar de identificar los principales retos a los que se enfrenta la Justicia en la actualidad.

Las Tecnologías de la Información y las Comunicaciones son un buen instrumento para reconducir la gran mayoría de los cambios que debemos afrontar, cambios que no serían posibles de no ser adoptadas masivamente las nuevas tecnologías.

Sería bueno que afrontásemos los desafíos a los que se enfrenta la Justicia como oportunidades de transformación y mejora y no como amenazas. Las TIC no podrán resolver todos los retos pero pueden ser el cauce adecuado por el que discurra el cambio. Las TIC son las aliadas perfectas para la Justicia en este momento.

Seguidamente voy a enumerar las áreas en las que las TIC pueden aportar un valor fundamental y por tanto canalizar la transformación tan demandada por la sociedad y los profesionales de la Justicia:

Organización del trabajo y de los órganos judiciales. Se trata de uno de los principales retos a los que se enfrenta la Justicia. Con la preparación de la implantación del nuevo modelo de Oficina Judicial, las TIC se perfilan como la herramienta ideal para mejorar la productividad, configurar y hacer efectiva la propia organización. Hay que saber utilizar todo su potencial y mejorar los procesos de manera que:

- se posibilite la separación del trabajo jurisdiccional del organizativo. Se trata de desvincular la función de juzgar de la dirección de la Oficina Judicial y el impulso procesal. Aplicar en la organización, técnicas de gestión pública y privada y utilizar para ello las nuevas tecnologías.
- contribuyan a mejorar la gestión de las cargas de trabajo. Las Oficinas Judiciales sufren las circunstancias imprevistas que afectan al personal que las integra dando lugar a

situaciones de saturación y excesiva carga de trabajo. Las TIC podrían contribuir a repartir las tareas de trabajo de manera más racional.

- se delimiten las funciones encomendadas al personal que integra la Oficina Judicial mediante la utilización de sistemas y aplicaciones. Los sistemas de gestión procesal incorporan esquemas de tramitación claros que establecen la función de cada perfil integrante de la Oficina Judicial (juez, secretario, funcionarios).
- se favorezca la especialización de los órganos judiciales, de sus titulares y del personal; habría que establecer un nuevo mapa judicial que determine el número, tipo y distribución territorial de los órganos jurisdiccionales teniendo en cuenta la carga de trabajo que puede soportar cada uno.
- se incentive la deslocalización y la desintermediación. El acceso a la información debería ser posible desde cualquier lugar y en cualquier momento; esto aumentaría la fluidez y disminuiría las perdidas de tiempo, además de optimizar recursos, tanto humanos como técnicos y materiales.

Los profesionales de la Justicia. Serían los primeros interesados en que se materialice un cambio que agilice los procesos y aumente su productividad y eficacia. Han llegado a la convicción de que con las TIC sería factible, pues:

- las TIC redefinirían los procesos provocando una reducción de tiempo, costes económicos y esfuerzos de personal; a esto contribuirá la utilización del expediente judicial digital.
- la coordinación y comunicación entre los distintos agentes experimentaría una mejora; además se contribuiría al intercambio de datos entre las distintas instituciones.
- facilitarían el control de la actividad jurisdiccional a través de un sistema de indicadores de valoración de actividad que fomentaría las buenas prácticas en el desempeño de la actividad llevada a cabo por los profesionales de la Justicia.
- se fortalecerían los mecanismos de seguridad de acceso a la información; las TIC facilitarían la trazabilidad, la auditoría de acceso a la información y el seguimiento de dicha información en tiempo real; con esto se mejora el seguimiento del cumplimiento de objetivos y los mecanismos de seguridad por lo que se contribuye a un sistema más robusto e inmune a errores.
- se favorecería la formación continua específica de todos los agentes al servicio de la Justicia. Las TIC ofrecen herramientas de apoyo a la labor judicial (consulta de legislación, jurisprudencia, bibliografía, etc.).

Escasez de recursos. Superar la falta de medios humanos, físicos y tecnológicos es el gran reto al que se enfrenta la Justicia. Las TIC también serían muy útiles a la hora de afrontar este desafío:

- es crucial que se resuelva el problema de la falta de espacio de los edificios y lugares de trabajo en los que se desarrolla la actividad jurisdiccional. Se habla de una "Justicia sin papel" como el sistema que acabaría con este problema. El uso del expediente judicial electrónico y de la firma digital son determinantes en este propósito.
- se incrementaría la productividad, realizando más trabajo con menos recursos.
- las TIC facilitarían el acceso a la información (tarea esencial en el ámbito de la Justicia), así como el almacenamiento y recuperación de dicha información en cualquier momento y desde cualquier lugar, con lo que se produce un gran ahorro de tiempo.

Interoperabilidad. Es otro de los grandes retos de la Justicia. Es esencial que los órganos judiciales dispongan de manera rápida de toda la información necesaria para el desempeño eficiente y eficaz de su actividad. Se trata de que se puedan compartir datos e intercambiar información y conocimientos en dos áreas diferentes:

- entre Juzgados y Tribunales; estaríamos hablando de interoperabilidad interna. El expediente judicial electrónico y los registros electrónicos de la Administración de Justicia juegan un papel fundamental.
- entre los órganos jurisdiccionales y otras Administraciones o instituciones, así como con los profesionales jurídicos; se trataría de una interoperabilidad externa. Sistemas como el Punto Neutro Judicial [22]y Lexnet[23] son herramientas que ya favorecen esa comunicación.

Nos encontramos con una marcada descentralización en lo que se refiere a la gestión de los planes de modernización; en la actualidad existen múltiples sistemas de gestión procesal, así como servicios electrónicos no homogéneos ni basados en un plan coordinado por lo que se hace necesaria esta interoperabilidad.

[22] Red de comunicaciones privada y segura cuyo punto central está en el Consejo General del Poder Judicial, que permite la conexión del Consejo con todos los órganos judiciales, la interconexión de estos entre si y con distintos registros, administraciones e instituciones.

[23] Sistema informático desarrollado por el Ministerio de Justicia que permite que los órganos judiciales y los distintos agentes que se relacionan con ellos (procuradores, fiscales, graduados sociales, etc.) puedan intercambiar información en formato electrónico, de forma segura y fiable.

Podemos hablar de tres niveles de interoperabilidad: organizativo, semántico y tecnológico. La interoperabilidad organizativa se centraría en los procesos de trabajo, la semántica se ocuparía de llegar a un acuerdo sobre lo que realmente significan los datos y la tecnológica permitirá que sistemas distintos puedan cooperar entre si.

Frecuentemente se dan situaciones en que existe una tecnología disponible pero la demora en la firma de acuerdos impide su aplicación. Por eso es tan importante la agilidad en la asunción de compromisos entre las distintas Administraciones Públicas.

En ocasiones también existen trabas considerables como la compatibilidad entre sistemas, estructuras de las bases de datos o la estandarización de procesos. Existe además cierta reticencia a la hora de compartir determinados datos, algunos de ellos muy sensibles como ocurre en el ámbito de la Justicia, debido a las imposiciones de la LOPD.

Como vemos, el desafío consiste en llegar a disponer de sistemas que permitan un intercambio de información entre las Administraciones Públicas y conseguir una base tecnológica lo suficientemente sólida como para poder implantar trámites en línea.

Tanto el Plan de Modernización de la Justicia[24] del CGPJ como el Plan Estratégico de Modernización del Sistema de Justicia[25] del Ministerio de Justicia establecen como principios básicos de actuación fijar los mecanismos adecuados para garantizar la interoperabilidad en la Administración de Justicia. Todas estas actuaciones han dado sus frutos y de esta manera se ha suscrito el Convenio del Esquema Judicial de Interoperabilidad y Seguridad (EJIS[26]), firmado por el CGPJ, el Ministerio de Justicia y la Fiscalía General del Estado el 30 de Septiembre del 2009. Este Convenio pretende incorporar un sistema de servicios tecnológicos en el que la interoperabilidad y la seguridad en la prestación de servicios sean los ejes fundamentales.

Los Ciudadanos. La sociedad actual demanda una Justicia más accesible, próxima y transparente; pide más servicios, más eficientes y con menos costes; espera que se establezcan nuevos canales de acceso a la información.

Por otro lado, en los últimos años estamos experimentando un aumento considerable de la litigiosidad pues los ciudadanos toman conciencia de sus derechos y se dirigen más habitualmente a la Justicia. Las TIC ayudarán a mejorar este panorama:

[24] Aprobado por el Pleno del Consejo General del Poder Judicial el 12 de noviembre del 2008.
[25] Prevé realizar una gran inversión en nuevos sistemas de comunicación y servicios electrónicos que estarán a disposición tanto de los profesionales de la Justicia como del resto de ciudadanos con lo que se obtendrá una Admon de Justicia tecnológicamente avanzada.
[26] Garantizará, entre otras cosas, la interoperatividad de los sistemas informáticos del Estado y las CCAA, permitiendo a todos los Juzgados y Tribunales operar entre sí y con el Ministerio Público.

- contribuyendo a garantizar la tutela judicial efectiva a los ciudadanos como derecho fundamental reconocido por la Constitución.
- configurando un sistema judicial más robusto frente a potenciales errores. Es evidente que las TIC aportarían el rigor necesario para ello.
- modernizando las relaciones de los ciudadanos con la Administración de Justicia a través de medios electrónicos.
- fortaleciendo los derechos de protección de datos de carácter personal. Las TIC imponen mecanismos muy estrictos en este campo.
- mejorando la proximidad y trasparencia del servicio que se ofrece al ciudadano. Los ciudadanos deben ser informados sobre el estado en el que se encuentran sus asuntos de una manera inteligible.
- mejorando la formación de la sociedad en materia jurídica. Es un buen punto de partida para conseguir una Justicia más adaptada a las necesidades de los ciudadanos.
- mejorando los servicios de atención al ciudadano, facilitando el acceso a estos servicios, haciéndolos más rápidos y funcionales etc.

4.1.-INTRODUCCIÓN DE LAS TIC EN LA JUSTICIA. LA JUSTICIA EN RED.

La propuesta para introducir las TIC en la Justicia tiene que tener en cuenta aspectos técnicos, organizativos y culturales.

Desde el punto de vista técnico. Vislumbramos la idea de un futuro con una Justicia sin papel gracias a la implantación del expediente judicial electrónico o digital. Deberá ser una Justicia accesible e interoperable, es decir, una Justicia en Red. Deben darse una serie de características técnicas:

- digitalización de la información disponible, de manera que se ofrezca un fácil acceso allí donde se necesite.
- expediente judicial electrónico o digital que recoja la información judicial necesaria para permitir interoperar, a través de la red a los distintos actores que participan en este ámbito. Relacionado con esto tengo que mencionar la importancia que tiene en este campo la firma electrónica en las notificaciones y comunicaciones.
- automatización de la gestión procesal que facilite la gestión y supervisión y ofrezca mayor transparencia a los ciudadanos, además de garantizar las medidas de seguridad y control necesarias.

- implantación de mecanismos de integración de sistemas que hagan posible la compatibilidad entre los sistemas y aplicaciones existentes.
- impulso de la videoconferencia en la declaración de testigos y peritos y grabación de juicios como herramienta impulsora de los procesos.

La Justicia en Red garantizará la interconexión telemática de la Administración de Justicia con el resto de Administraciones Públicas, con los profesionales del derecho así como el acceso telemático de los ciudadanos a las sentencias y resoluciones judiciales siempre que estas sean públicas.

La provisión de los servicios en red podría realizarse por empresas especializadas que garanticen la operación y el mantenimiento, asegurando la evolución tecnológica del sistema.

Este es un buen momento para implantar las nuevas tecnologías en el ámbito de la Justicia y para asegurar su sostenibilidad a lo largo del tiempo.

Desde el punto de vista organizativo. Es necesario que se consiga un acuerdo entre todos los agentes jurídicos sobre un plan estratégico de aplicación de las nuevas tecnologías a la Justicia. Es preciso que se consiga un espacio tecnológico común mediante la figura jurídica que se considere más conveniente (convenios de colaboración, consorcios…etc.).

Desde el punto de vista cultural. Es crucial diseñar y llevar a la práctica un plan de gestión del cambio de todos los profesionales al servicio de la Justicia. Dentro de dicho plan debe incluirse un epígrafe dedicado a la formación en nuevas tecnologías. Al fin de cuentas, la Justicia es el conjunto de las personas que la integran y la hacen posible.

4.2.-IMPLANTACIÓN DE LAS TIC EN LA JUSTICIA ESPAÑOLA

La tecnología sería una gran ayuda para mejorar la Administración de Justicia en España. Su introducción se encara como un objetivo, un desafío. La modernización y reforma de la Justicia depende en gran medida de las nuevas tecnologías.

No obstante debemos tener en cuenta una serie de cuestiones que hay que superar o corregir si queremos implantar con éxito las TIC en la Administración de Justicia. Entre ellas figuran las siguientes:

• **la Justicia española adolece de una falta de liderazgo** definido a la hora de implantar las soluciones. El sistema judicial español tiene una estructura fuertemente descentralizada, nada jerarquizada, compleja y con fuerte atomización de competencias. Podemos decir que en el panorama actual de la Justicia española existen tres administradores de medios tecnológicos: las CCAA con competencias transferidas, el Ministerio de Justicia y el CGPJ (como prestador de servicios a jueces y magistrados y además como garante de la compatibilidad de los sistemas.). Desde estas tres instituciones se están impulsando importantes progresos, pero es evidente la necesidad de una figura rectora que imponga la utilización o adopción de ciertas aplicaciones o soluciones tecnológicas.

Además se da la circunstancia de que la Justicia española es muy casuística, la manera de trabajar de cada órgano judicial es muy diferente, por lo que se plantea una enorme dificultad a la hora de implantar una aplicación útil para todos.

• **es necesario tomar conciencia de que la Nueva Oficina Judicial es la gran oportunidad para introducir las TIC en la Justicia.** En la actualidad nos encontramos con un modelo de Oficina Judicial todavía no desarrollado, pero si definido; es el momento idóneo para introducir la tecnología mientras que se acometen las reformas necesarias mediante el modelo de Nueva Oficina Judicial.

La nueva Oficina Judicial se compone de Unidades de Apoyo Jurisdiccional,[27] de Servicios Comunes Procesales[28] y no Procesales y de Unidades Administrativas.[29] Las Unidades de Apoyo y los Servicios Comunes Procesales se encargan de la tramitación y ejecución de tareas reguladas por leyes procesales. Las Unidades Administrativas se ocupan de la gestión de los medios materiales y humanos y también podrán desarrollar actividades no regidas por leyes procesales siempre que sirvan de apoyo a la actividad de los jueces. Estas Unidades Administrativas estarán ligadas orgánica y funcionalmente a los órganos del Ministerio de Justicia y de las CCAA con competencias asumidas quienes establecerán su estructura y objetivos de actuación, controlando el ejercicio de su

[27] La Orden JUS/3244/2005 de 18 de octubre determina la dotación básica de las Unidades Procesales de Apoyo Directo a los órganos judiciales.

[28] Son Unidades de la Oficina Judicial que asumen labores centralizadas de gestión y apoyo en actuaciones procesales, prestan servicio a todos o alguno de los órganos judiciales de su ámbito territorial cualquiera que sea el orden jurisdiccional al que pertenezcan. Cada Servicio Común estará dirigido por un Secretario Judicial.

[29] Son unidades descentralizadas dependientes de la Dirección General de Justicia y ubicadas en las sedes de los órganos judiciales. Desde ellas se realizan las gestiones y tramitación de los medios humanos, materiales y tecnológicos.

actividad. Sería una buena idea comenzar por estas Unidades que no se rigen por las leyes procesales, en lo que se refiere a la introducción de las nuevas tecnologías ya que no supondría una tarea de modificación de normas y por lo tanto se perfila como una buena vía para impulsar los cambios.

Por otro lado debo mencionar el Servicio Común Procesal para la Ordenación del Procedimiento[30] como el elemento problemático en el proceso de implantación de la Nueva Oficina Judicial. Se requieren muchos esfuerzos para afrontar su reforma, ya que supone un gran cambio de cultura de la organización de la Administración de Justicia, pero si se realiza de manera adecuada supondría un paso de gigante para la configuración de la nueva Oficina Judicial. Se conseguirían racionalizar los recursos disponibles considerablemente. El uso de la tecnología (especialmente el uso del expediente electrónico o digital y el modelo de Justicia en Red) ayudarían a dar ese salto.

Si las actividades de impulso procesal, hasta ahora desarrolladas por los secretarios judiciales se pudieran redireccionar a servicios centralizados encargados de dar apoyo a los órganos judiciales, se produciría una auténtica transformación. En esta empresa también jugaría un papel importantísimo la introducción de las nuevas tecnologías.

• **sería conveniente acometer cambios normativos que favorecieran la evolución tecnológica de la Justicia.** La reforma de normas procesales facilitaría la puesta en marcha de la nueva Oficina Judicial. El punto clave es el fortalecimiento de las competencias del Secretario Judicial pues esto facilitaría el funcionamiento de los Servicios Comunes Procesales dirigidos por ellos; esto precisará la ayuda de la tecnología que deberá tener, por supuesto, una regulación legal. La modificación de determinadas leyes procesales tiene que impulsar el uso de la tecnología en un futuro para que se generalice su implantación, imponiendo su aplicación.

La Administración de Justicia quedó excluida del ámbito de aplicación de la Ley 11/2007[31], con lo que se perdió una excelente oportunidad de lograr ese avance tecnológico tan necesario.

• **es preciso un cambio de mentalidad entre los profesionales de la Administración de Justicia.** Son muchos los profesionales de la Justicia los que ofrecen resistencia a la

[30] Entre otras funciones, se encarga del examen de los requisitos formales del procedimiento.
[31] Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

introducción de nuevos métodos y herramientas de trabajo, aun conociendo las ventajas que supondría en el desarrollo de su actividad. Es evidente que la tecnología puede ayudar a transformar y mejorar la manera de hacer las cosas. Es cierto que existe un alto grado de desconocimiento de las TIC, por lo que hay que dedicar un gran esfuerzo a la formación. Es previsible que esta formación y reciclaje se vea afectada por el alto grado de interinidad que caracteriza a la Justicia española. Estamos, por tanto, ante un problema de *modernización de mentalidad*. Hay que implantar la idea de que la asunción de las nuevas tecnologías no es un problema de aptitud sino de actitud o predisposición al cambio.

- **es preciso contar con todos los agentes para proponer soluciones tecnológicas válidas**. Es fundamental contar con todos los agentes que componen e integran la Administración de Justicia; es necesario que todos aporten su grano de arena, de la misma manera que deben tenerse en cuenta sus opiniones a la hora de instaurar el uso generalizado de las tecnologías. De esto derivarán grandes beneficios para toda la sociedad.

5.-SEDE ELECTRÓNICA DEL MINISTERIO DE JUSTICIA

5.1.-LA ORDEN JUS/485/2010 DE 25 DE FEBRERO.

El artículo 1 de la Orden JUS/485/2010 establece que el objetivo de esta Orden es crear la Sede Electrónica para el Ministerio de Justicia, dando cumplimiento, de esta manera, al artículo 3 del RD 1671/2009 que desarrolla parcialmente la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

La Ley 11/2007, de 22 de Junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos crea el concepto de "sede electrónica". El artículo 10.1 de la Ley define la sede electrónica como "dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias"; en el apartado 3 del artículo 10 se establece, además, que "cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas".

Está claro que existe una necesidad de definir claramente la "sede" administrativa electrónica con la que se establecen las relaciones, promoviendo un régimen de identificación, autenticación, contenido mínimo, protección jurídica, accesibilidad, disponibilidad y responsabilidad.

Por otro lado, el RD 1671/2009, de 6 de Noviembre, por el que se desarrolla parcialmente la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, además de regular esta figura en sus artículos 3 al 9, determina en su artículo 3.2 que "las sedes electrónicas se crearán mediante Orden del Ministro correspondiente o Resolución del Titular del Organismo Público que deberá publicarse en el BOE" determinando el contenido mínimo de esta norma aprobatoria. Con esto se ofrecen a los ciudadanos garantías de plena certeza y seguridad que sólo alcanzaban parcialmente las oficinas virtuales que hasta el momento venían canalizando las relaciones electrónicas con los ciudadanos.

La Disposición Final cuarta del RD 1671/2009 de 6 de Noviembre establece que "los puntos de acceso electrónico pertenecientes a la Administración General del Estado o sus organismos públicos dependientes o vinculados en los que se desarrollan actualmente comunicaciones con terceros, propias de sede electrónica, deberán adaptarse, en el plazo de cuatro meses a partir de la entrada en vigor de este RD, a lo dispuesto en el

mismo para las sedes o, en su caso, subsedes, electrónicas, sin perjuicio de lo previsto en las disposiciones transitorias primera y segunda de este RD y en la disposición final tercera de la Ley 11/2007".

Con la implantación de la sede se pretende, por un lado, reducir al máximo la dispersión actual de los servicios que ofrece el departamento, lo que facilitaría el acceso a los mismos, y por otro lado crear un espacio en el que la Administración y el ciudadano se relacionen en el marco de la gestión administrativa con las garantías necesarias, distinguiendo, de esta manera, el concepto de portal de comunicación del de sede electrónica. El primero tiene un componente institucional, de información general sobre el Ministerio de Justicia, mientras que el segundo ofrece un marco de comunicación e interacción con el ciudadano en relación con los servicios provistos por el Ministerio de Justicia.

La sede electrónica del Ministerio de Justicia responderá a los criterios relativos al ámbito de la administración electrónica establecidos en el RD 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y en el RD 4/2010 de 8 de enero por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, derivados de la ley 11/2007 y del RD 1671/2009.

5.2.-CONTENIDOS Y SERVICIOS DE LA SEDE ELECTRÓNICA DEL MINISTERIO DE JUSTICIA.

El artículo 6 de la Orden JUS 485 establece que a través de esta sede se realizarán todas las actuaciones, procedimientos y servicios que requieran mecanismos de autenticación de los ciudadanos o del Ministerio de Justicia en sus relaciones con estos por medios electrónicos así como otros respecto a los cuales se decida su inclusión en la sede por razones de eficacia y calidad en la prestación de servicios a los ciudadanos.

La SEMJ[32] dispondrá del siguiente **contenido mínimo**:

- Identificación de la sede, así como del órgano u órganos titulares y de los responsables de la gestión y de los servicios puestos a disposición en la misma y, en su caso, de las subsedes de ella derivadas.

[32] Sede Electrónica del Ministerio de Justicia

- Información necesaria para la correcta utilización de la sede incluyendo el mapa de la sede electrónica o información equivalente, con especificación de la estructura de navegación y las distintas secciones disponibles, así como la relacionada con propiedad intelectual.
- Servicios de asesoramiento electrónico al usuario para la correcta utilización de la sede.
- Sistema de verificación de los certificados de la sede, que estará accesible de forma directa y gratuita.
- Relación de sistemas de firma electrónica que, conforme a lo previsto en este RD, sean admitidos o utilizados en la sede.
- Normas de creación del registro o registros electrónicos accesibles desde la sede.
- Información relacionada con la protección de datos de carácter personal, incluyendo un enlace con la sede electrónica de la AEPD.

La SEMJ, dispondrá también de los siguientes **servicios** a disposición de los ciudadanos:

- Relación de los servicios disponibles en la sede electrónica.
- Carta de servicios y carta de servicios electrónicos.
- Relación de los medios electrónicos a los que se refiere el artículo 27.4 de la Ley 11/2007, de 22 de Junio[33].
- Enlace para la formulación de sugerencias y quejas ante los órganos que en cada caso resulten competentes.
- Acceso al estado de tramitación del expediente.
- Publicación de los diarios o boletines.
- Publicación electrónica de actos y comunicaciones que deban publicarse en tablón de anuncios o edictos, indicando el carácter sustitutivo o complementario de la publicación electrónica.
- Verificación de los sellos electrónicos de los órganos u organismos públicos que abarque la sede.
- Comprobación de la autenticidad e integridad de los documentos emitidos por los órganos u organismos públicos que abarca la sede que hayan sido autenticados mediante código seguro de verificación.

[33]Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

- Indicación de la fecha y hora oficial a los efectos previstos en el artículo 26.1 de la Ley 11/2007.

Los órganos titulares responsables de la sede podrán además incluir en la misma otros servicios o contenidos, con sujeción a lo previsto en el artículo 10 de la Ley 11/2007 y en el RD 1671/2009.

Los contenidos publicados en la SEMJ responderán a los criterios de seguridad e interoperabilidad que se derivan de la Ley 11/2007 y de los Reales Decretos 1671/2009, RD 3/2010 de 8 de enero que regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y RD 4/2010 que regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

La SEMJ posibilitará paulatinamente el acceso a sus contenidos y servicios en las lenguas cooficiales en el Estado español.

5.3.-REQUISITOS DE RESPONSABILIDAD

El artículo 4.a) de la Orden JUS 485, atribuye la titularidad de la sede a la Subsecretaría del Departamento. El mismo artículo en su apartado d) establece que al titular de la SEMJ le compete la gestión de los contenidos comunes de la sede y la coordinación con los centros directivos del Departamento y los Organismos incorporados.

El apartado c) del mencionado artículo 4 determina que los titulares de los centros directivos del Departamento y en su caso de los Organismos que se incorporen a la sede serán responsables de la gestión, de los contenidos y de los servicios puestos a disposición de los ciudadanos en la sede.

El establecimiento de la SEMJ conlleva una serie de **responsabilidades** para el titular de la misma:

- respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda acceder a través de la misma (Artículo 10.2 de la Ley 11/2007 y artículo 7 del RD 1671/2009)
- respecto a la articulación de los medios necesarios para que el ciudadano sea capaz de identificar si la información o servicio al que tiene acceso corresponde a la propia sede o procede de un punto de acceso desprovisto del carácter de sede o de un tercero. (Artículo 7.1 del RD 1671/2009)

- respecto a la determinación de las condiciones e instrumentos de creación de la sede, con sujeción a los principios de publicidad oficial, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad.
- respecto de la identificación del titular de la sede, que debe quedar garantizada en todo caso. (Artículo 10.3 de la Ley 11/2007).
- respecto de los medios disponibles para la formulación de sugerencias y quejas (artículo 10.3 Ley 11/2007).

El artículo 7 de la Orden JUS 485 establece claramente que los medios disponibles para la **formulación de sugerencias y quejas** en relación con el contenido, gestión y servicios ofrecidos en la SEMJ son los siguientes:

1.-presentación presencial o por correo postal ante los registros generales y las oficinas de atención al público de los servicios centrales y las oficinas periféricas del Departamento dirigidas a los órganos u organismos responsables, de acuerdo con el establecimiento establecido en el artículo 15 del RD 951/2005 de 29 de Julio, por el que se establece el marco general para la mejora de la calidad en la Administración General del Estado.

2.-presentación telemática a través del Registro Electrónico sito en la SEMJ.

- respecto del establecimiento de sistemas que garanticen la seguridad en las comunicaciones (artículo 10.4 de la Ley 11/2007).
- respecto del cumplimiento de los principios de accesibilidad y "usabilidad" en la publicación de informaciones, servicios y transacciones en la sede (artículo 10.5 de la Ley 11/2007).

5.4.-IDENTIFICACIÓN Y AUTENTICACIÓN DE LA SEMJ.

El artículo 17 de la Ley 11/2007 establece que *"las sedes electrónicas utilizarán para identificarse y garantizar una comunicación segura con las mismas sistemas de firma electrónica basados en certificados de dispositivo seguro o medio equivalente"*.

El artículo 17.2 del RD 1671/2009 añade además que para facilitar su identificación, *"las sedes electrónicas seguirán las disposiciones generales que se establezcan para la imagen institucional de la Administración General del Estado y su dirección electrónica incluirá el nombre de dominio de tercer nivel -gob.es"*

El artículo 18 de la Ley 11/2007 establece que cada Administración Pública podrá utilizar para la identificación y autenticación los siguientes sistemas de firma electrónica:

1-**el sello electrónico** de Administración Pública, órgano o entidad de derecho público, basado en **certificado electrónico** que reúna los requisitos exigidos por la legislación de firma electrónica.

La creación de sellos electrónicos se realizará mediante resolución de la Subsecretaría del Ministerio o titular del organismo público y se publicará en la sede electrónica; según el artículo 19 del RD1671/2009 en él debe constar el órgano titular del sello responsable de su utilización, características técnicas generales del sistema de firma y certificado aplicable, servicio de validación para la verificación del certificado y las actuaciones y procedimientos en los que podrá ser utilizado.

Los certificados de sello electrónico deben incluir el número de identificación fiscal del suscriptor, descripción del tipo de certificado y la denominación correspondiente de "sello electrónico", pudiendo contener la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos.

La relación de sellos electrónicos, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos, y además, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.

2-un **código seguro de verificación** vinculado a la Administración Pública, órgano o entidad y a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Según el artículo 20 del RD 1671/2009 el sistema de código seguro debe garantizar, en todo caso:

a. el carácter único del código generado para cada documento.

b. su vinculación con el documento generado y con el firmante.

c. la posibilidad de verificar el documento por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento.

Quiero también mencionar los **Certificados de Sede electrónica** regulados en el artículo 18 del RD 1671/2009; según el mismo, el uso de estos certificados está limitado

a la identificación de la sede, quedando excluida su aplicación para la firma electrónica de documentos y trámites. Estos certificados electrónicos de sede electrónica tendrán, al menos, los siguientes contenidos:

a) descripción del tipo de certificado, con la denominación "sede electrónica".
b) nombre descriptivo de la sede electrónica.
c) denominación del nombre del dominio.
d) número de identificación fiscal de la entidad suscriptora.
e) unidad administrativa suscriptora del certificado.

La SEMJ podrá utilizar estos certificados por ejemplo, para la identificación de la titularidad de la sede, para garantizar la confidencialidad de las comunicaciones, para poner a disposición de los ciudadanos modelos o formularios electrónicos, para la publicación de diarios oficiales o tablón de anuncios, para la prestación de servicios electrónicos, para el acceso al registro electrónico o a la sede electrónica para gestionar notificaciones telemáticas.

El Esquema Nacional de Seguridad, ya mencionado, determinará las características y requisitos que cumplirán los sistemas de firma electrónica, los certificados y los medios equivalentes que se establezcan en las sedes electrónicas para la identificación y garantía de una comunicación segura (artículo 18.3 del RD1671/2009).

6.-REGISTROS, COMUNICACIONES Y NOTIFICACIONES ELECTRÓNICAS

6.1.-REGISTROS ELECTRÓNICOS.

Están regulados en la Sección 1ª del Capítulo III de la Ley 11/2007[34]. En el artículo 24 de dicha ley se establece que las Administraciones Públicas crearán registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones. Y que esos registros electrónicos podrán admitir:

1. Documentos electrónicos normalizados correspondientes a los servicios, procedimientos y trámites que se especifiquen conforme a lo dispuesto en la norma de creación del registro, cumplimentados de acuerdo con formatos preestablecidos.
2. Cualquier solicitud, escrito o comunicación distinta de los mencionados en el apartado anterior dirigido a cualquier órgano o entidad del ámbito de la administración titular del registro.

Continúa el precepto estableciendo que cada Administración Pública poseerá, al menos un sistema de registros electrónicos suficiente para recibir todo tipo de solicitudes, escritos y comunicaciones dirigidos a dicha Administración Pública. Las Administraciones Públicas, podrán, mediante convenios de colaboración, habilitar a sus respectivos registros para la recepción de las solicitudes, escritos y comunicaciones de la competencia de otra Administración que se determinen en el correspondiente convenio.

- En cuanto a la **creación y funcionamiento** de los Registros electrónicos, establece la Ley 11/2007, que:
  - Las disposiciones de creación de estos se publicarán en el Diario Oficial correspondiente y su texto íntegro deberá estar disponible para consulta en la sede electrónica de acceso al registro. Las disposiciones de creación de registros electrónicos especificarán el órgano o unidad responsable de su gestión, así como la fecha y hora oficial y los días declarados inhábiles.
  - En la sede electrónica de acceso al registro figurará la relación actualizada de las solicitudes, escritos y comunicaciones, a las que se refería el primer apartado del

[34] Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

artículo 24 que ya he mencionado, que pueden presentarse en el mismo así como la posibilidad de presentación de solicitudes, escritos y comunicaciones a los que se refería el apartado segundo del mismo artículo 24.

- Los registros electrónicos emitirán automáticamente un recibo consistente en una copia autenticada del escrito, solicitud o comunicación de que se trate, incluyendo la fecha y hora de presentación y el número de entrada de registro.
- Podrán aportarse documentos que acompañen a la correspondiente solicitud, escrito o comunicación, siempre que cumplan los estándares de formato y requisitos de seguridad que se determinen en los Esquemas Nacionales de Interoperabilidad y de Seguridad. Los registros electrónicos generarán recibos acreditativos de la entrega de estos documentos que garanticen la integridad y el no repudio de los documentos aportados.

- En cuanto al **sistema de cómputo de plazos** que debe seguir un registro electrónico la Ley 11/2007 establece las siguientes pautas:
  - Los registros electrónicos se regirán a efectos de cómputo de plazos por la fecha y hora oficial de la sede electrónica de acceso, que deberá contar con las medidas de seguridad necesarias para garantizar su integridad y figurar visible.
  - Los registros electrónicos permitirán la presentación de solicitudes, escritos y comunicaciones todos los días del año durante las veinticuatro horas.
  - A los efectos del cómputo de plazo fijado en días hábiles o naturales, y en lo que se refiere a cumplimiento de plazos por los interesados, la presentación en un día inhábil se entenderá realizada en la primera hora del primer día hábil siguiente, salvo que una norma permita expresamente la recepción en día inhábil.
  - El inicio del cómputo de los plazos que hayan de cumplir los órganos administrativos y entidades de derecho público vendrá determinado por la fecha y hora de presentación en el propio registro o, en el caso previsto en el apartado segundo del artículo 24, por la fecha y hora de entrada en el registro del destinatario. La fecha efectiva de inicio del cómputo de plazos deberá ser comunicada a quien presento el escrito, solicitud o comunicación.
  - Cada sede electrónica en la que esté disponible un registro electrónico determinará, atendiendo al ámbito territorial en el que se ejerce sus competencias el titular de aquella, los días que se considerarán inhábiles a los efectos de los apartados anteriores. No será de aplicación a los registros electrónicos lo

dispuesto en el artículo 48.5 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

6.1.1.-El Registro Electrónico del Ministerio de Justicia.

La Orden JUS 3000/2009 de 29 de Octubre crea y regula el Registro Electrónico del Ministerio de Justicia en aplicación de los artículos 24 y 25 de la Ley 11/2007. Esta Orden establece la obligatoriedad de la utilización del registro electrónico para la Administración en las relaciones electrónicas con los ciudadanos en las que, conforme a las normas generales, deba llevarse a cabo su anotación registral de acuerdo con lo establecido en el artículo 38 de la Ley 30/1992, de 26 de noviembre[35], y sus disposiciones de desarrollo, no pudiendo ser sustituida esta anotación por otras en registros no electrónicos o en los registros de las aplicaciones gestoras de los procedimientos.

- Esta Orden establece que las **funciones** del Registro electrónico del Ministerio de Justicia son las siguientes:
  - La recepción de solicitudes, escritos y comunicaciones de todo tipo y sus documentos adjuntos, relacionados con el ámbito de actuación y la competencia del Ministerio de Justicia.
  - La remisión de escritos, comunicaciones y documentos relativos a los procedimientos incluidos en el Anexo I a las personas, entidades y organismos interesados en los mismos.
  - La remisión de notificaciones relativas a los procedimientos para los que el interesado, de acuerdo con lo establecido en el artículo 28 de la Ley 11/2007, y siempre que el procedimiento específico así lo determine, haya consentido o señalado como medio de notificación preferente la vía electrónica.
  - La anotación de los asientos registrales de entrada o salida de las solicitudes, comunicaciones y notificaciones anteriormente enumeradas.

- El artículo 5 de la mencionada Orden JUS 3000/2009 establece que cada presentación de solicitudes, escritos y comunicaciones en el registro electrónico debe contener los siguientes datos:
  - un número o código de registro individualizado.

[35]Ley de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común.

- los datos de identificación del interesado: nombre, apellidos, DNI, NIF, NIE, pasaporte o equivalente. En el caso de personas jurídicas, CIF y denominación social.
- fecha y hora de presentación.
- identidad del órgano a quien se dirige el documento electrónico.
- procedimiento con el que se relaciona.
- contenido del formulario, que recogerá para personas físicas, la dirección postal o electrónica, y para personas jurídicas, el domicilio social y dirección electrónica.
- cualquier otra información que se considere necesaria en función del procedimiento telemático origen del asiento.

- En cuanto a los sistemas de identificación, autenticación y firma, el artículo 9 de la Orden establece que
  - se admitirán los sistemas de firma electrónica que sean conformes a la Ley 59/2003 de 19 de Diciembre de Firma Electrónica y que sean adecuados para garantizar la identificación de los interesados y en su caso la autenticidad e integridad de los documentos presentados.
  - los escritos, solicitudes y comunicaciones remitidos por medios electrónicos exigirán la identificación de los interesados remitentes y podrán firmarse mediante:
    a) los sistemas de identificación y firma electrónica incorporados al DNI de las personas físicas.
    b) los sistemas de firma electrónica avanzada y firma electrónica reconocida.
    c) las claves concertadas previo registro como usuario, la información conocida por ambas partes u otros sistemas no criptográficos en los términos que especifican las instrucciones de acceso y utilización del registro electrónico en cada procedimiento disponible en la sede electrónica del departamento.

La Orden encarga a la Subsecretaría de Justicia, a través de la División de Informática y Tecnologías de la Información [36]la gestión, disponibilidad y seguridad del Registro Electrónico creado y regulado por dicha Orden.

[36] La DITIC fue creada por el Acuerdo de Rectoría nº 379 con fecha 16 de enero del 2006 y está en operación desde el primero de febrero del 2006.

6.2.-COMUNICACIONES ELECTRÓNICAS.

El artículo 27 de la LO 11/2007 regula las comunicaciones electrónicas. En este artículo se establecen las siguientes disposiciones al respecto:

- Los ciudadanos podrán elegir en todo momento la manera de comunicarse con las Administraciones Públicas, sea o no por medios electrónicos, excepto en aquellos casos en los que de una norma con rango de ley se establezca o infiera la utilización de un medio no electrónico. La opción de comunicarse por unos u otros medios no vincula al ciudadano, que podrá, en cualquier momento, optar por un medio distinto del inicialmente elegido.
- Las Administraciones Públicas utilizarán medios electrónicos en sus comunicaciones con los ciudadanos siempre que así lo hayan solicitado o consentido expresamente. La solicitud y el consentimiento podrán, en todo caso, emitirse y recabarse por medios electrónicos.
- Las comunicaciones a través de medios electrónicos serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas, del contenido íntegro de las comunicaciones y se identifique fidedignamente al remitente y al destinatario de las mismas.
- Las Administraciones publicarán, en el correspondiente Diario Oficial y en la propia sede electrónica, aquellos medios electrónicos que los ciudadanos pueden utilizar en cada supuesto en el ejercicio de su derecho a comunicarse con ellas.
- Los requisitos de seguridad e integridad de las comunicaciones se establecerán en cada caso de forma apropiada al carácter de los datos objeto de aquellas, de acuerdo con criterios de proporcionalidad, conforme a lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal.
- Reglamentariamente, las Administraciones Públicas podrán establecer la obligatoriedad de comunicarse con ellas utilizando sólo medios electrónicos, cuando los interesados se correspondan con personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos.
- Las Administraciones Públicas utilizarán preferentemente medios electrónicos en sus comunicaciones con otras Administraciones Públicas. Las condiciones que

regirán estas comunicaciones se determinarán entre las Administraciones Públicas participantes.

6.3.-NOTIFICACIONES ELECTRÓNICAS.

El artículo 28 de la LO11/2007 se encarga de la regulación de la práctica de la notificación por medios electrónicos. En el se establecen las siguientes disposiciones:

- Para que la notificación se practique utilizando algún medio electrónico se requerirá que el interesado haya señalado dicho medio como preferente o haya consentido su utilización, sin perjuicio de lo dispuesto en el artículo 27.6. Tanto la indicación de la preferencia en el uso de medios electrónicos como el consentimiento citados anteriormente podrán emitirse y recabarse, en todo caso, por medios electrónicos.
- El sistema de notificación permitirá acreditar la fecha y hora en que se produzca la puesta a disposición del interesado del acto objeto de notificación, así como la de acceso a su contenido, momento a partir del cual la notificación se entenderá practicada a todos los efectos legales.
- Cuando, existiendo constancia de la puesta a disposición transcurrieran diez días naturales sin que se acceda a su contenido, se entenderá que la notificación ha sido rechazada con los efectos previstos en el artículo 59.4 de la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y normas concordantes, salvo que de oficio o a instancia del destinatario se compruebe la imposibilidad técnica o material del acceso.
- Durante la tramitación del procedimiento el interesado podrá requerir al órgano correspondiente que las notificaciones sucesivas no se practiquen por medios electrónicos, utilizándose los demás medios admitidos en el artículo 59 de la ya mencionada Ley 30/1992, excepto en los casos previstos en el artículo 27.6 de la presente ley.
- Producirá los efectos propios de la notificación por comparecencia el acceso electrónico por los interesados al contenido de las actuaciones administrativas correspondientes, siempre que quede constancia de dicho acceso.

7.-DOCUMENTO ELECTRÓNICO Y OFICINA JUDICIAL.

El artículo 29 de la Ley 11/2007 establece las siguientes disposiciones con respecto al documento administrativo electrónico:

- Las Administraciones Públicas podrán emitir válidamente por medios electrónicos los documentos administrativos a los que se refiere el artículo 46 de la Ley 30/1992 del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que incorporen una o varias firmas electrónicas conforme a lo establecido en la Sección 3ª del Capítulo II de la presente Ley.
- Los documentos administrativos incluirán referencia temporal, que se garantizará a través de medios electrónicos cuando la naturaleza del documento así lo requiera.
- La Administración General del Estado, en su relación de prestadores de servicios de certificación electrónica, especificará aquellos que con carácter general estén admitidos para prestar servicios de sellado de tiempo.

El artículo 45 de la mencionada ley 30/1992 establecía que *"las Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que a la utilización de estos medios establecen la Constitución y las leyes."*

En lo que respecta a la Administración de Justicia, el párrafo primero del artículo 230 de la LO 6/1985 del Poder Judicial, establecía 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, con las limitaciones que a la utilización de tales medios establece la LO 5/1992, de 29 de octubre, y demás leyes que resulten de aplicación"*. Hace mucho tiempo que la norma invocada en este precepto, la LORTAD[37], ha sido derogada por la actual ley protectora de datos de carácter personal, la LOPD.[38]

A causa de la obligada trasposición de Directivas europeas, el legislador español se ve impulsado a la introducción de nuevos métodos, procedimientos y herramientas en el trámite de los procesos administrativos; en estas circunstancias, ven la luz regulaciones

[37] LO 5/1992, de 29 de octubre de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, vigente hasta el 14 de enero del 2000.
[38] LO 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.

tales como la Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico, la Ley 59/2003 de Firma Electrónica, la Ley 11/2007 de Acceso Electrónico del Ciudadano a los Servicios Públicos etc., etc.

El artículo 3 de la Ley de Firma Electrónica define el documento electrónico como la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado. El mismo precepto distingue lo que debe entenderse también por documento público, documento expedido y firmado electrónicamente por funcionarios o empleados públicos y documento privado.

El documento electrónico debe poseer dos características fundamentales para poder incorporarse al flujo de un proceso administrativo:

- ✓ **autenticidad;** o certeza de que su autor es quien dice ser y además posee la autoridad o legitimidad para redactarlo
- ✓ **integridad**; o la certidumbre de que no ha sufrido alteración alguna.

Estos dos requisitos, junto con los de **confidencialidad** (la condición de un documento que permite que sólo sea visible para aquellos que estén autorizados) y el **no repudio en origen** (la imposibilidad de negar una acción hecha), constituyen los elementos imprescindibles para que el documento electrónico pueda desplegar los efectos que le atribuyen las leyes, alcanzados a través del uso de mecanismos de firma electrónica, entre los que cabe destacar la firma electrónica reconocida, que aplicada a un documento electrónico posee la eficacia jurídica equivalente a la de la firma manuscrita.

Los ciudadanos (a través del nuevo DNI-e [39]y las posibilidades que ofrecen otros Prestadores de Servicios de Certificación) y los operadores jurídicos (a través de los certificados digitales para jueces, abogados, procuradores y funcionarios) ya pueden disponer de las herramientas necesarias para firmar electrónicamente documentos electrónicos.

El documento-papel constituye el soporte habitual por el que las Administraciones Públicas desarrollan su actividad, pero en el ámbito de la Oficina Judicial, al constituir la base de las acciones procesales, ha experimentado tal crecimiento de volumen que se está convirtiendo en un auténtico problema o impedimento para el desarrollo de la Justicia. Pese a la implantación de modernos sistemas tecnológicos y el esfuerzo que se está

[39] DNI electrónico regulado por el RD 1553/2005, de 23 de diciembre.

exigiendo de todos los funcionarios, miles de papeles, de sentencias, de autos, de procedimientos, se apilan sin control por los juzgados.

No podemos evitar que gran parte de la información relevante que entra en un juzgado lo haga en forma de documento-papel. La implementación práctica de los mecanismos que hacen posible crear documentos en formato electrónico es todavía escasa. Por lo que es necesario adoptar medidas para que el documento-papel en la Oficina Judicial no suponga un obstáculo en el desarrollo de su actividad. Una de ellas podría ser la digitalización de documentos con plenas garantías legales; de esta manera el artículo 30 de la Ley 11/2007 de Acceso Electrónico del Ciudadano a los Servicios Públicos señala que "Las Administraciones Públicas podrán obtener imágenes electrónicas de los documentos privados aportados por los ciudadanos, con su misma validez y eficacia, a través de procesos de digitalización que garanticen su autenticidad, integridad y la conservación del documento imagen, de lo que se dejará constancia. Esta obtención podrá hacerse de forma automatizada, mediante el correspondiente sello electrónico".

Como vemos, es necesario conjugar la necesidad de informatizar el documento-papel, con la exigencia de mantener la cadena de la legalidad. Haciéndolo, nuestra Administración de Justicia obtendrá grandes beneficios:

- ✓ Aumentará la eficacia en el tratamiento de sus expedientes.
- ✓ Ahorrará recursos escasos (tiempo de tramitación y dinero).
- ✓ Mantendrá la debida confidencialidad de las informaciones contenidas en los documentos.
- ✓ Mejorará las condiciones de trabajo de los funcionarios, contribuyendo a respetar el medio ambiente.

7.1.-COPIAS ELECTRÓNICAS.

Los artículos 45 y 46 de la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común establecen la posibilidad de utilización de medios técnicos en todas las fases de los procedimientos administrativos, así como los principios básicos de validez y eficacia de los documentos y copias.

Siguiendo esta línea, la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, dedica el artículo 30 a regular el sistema de copias electrónicas, estableciendo lo siguiente al respecto:

- Las copias realizadas por medios electrónicos de documentos emitidos por el propio interesado o por las Administraciones Públicas, manteniéndose o no el formato original, tendrán inmediatamente la consideración de copias auténticas con la eficacia prevista en el artículo 46 de la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que el documento electrónico original se encuentre en poder de la Administración, y que la información de **firma electrónica** y, en su caso de **sellado de tiempo** permitan comprobar la coincidencia con dicho documento.
- Las copias realizadas por las Administraciones Públicas, utilizando medios electrónicos, de documentos emitidos originalmente por las Administraciones Públicas en soporte papel tendrán la consideración de copias auténticas siempre que se cumplan los requerimientos y actuaciones previstas en el artículo 46 de la ley 30/1992.
- Las Administraciones Públicas podrán obtener imágenes electrónicas de los documentos privados aportados por los ciudadanos, con su misma validez y eficacia, a través de procesos de digitalización que garanticen su autenticidad, integridad y la conservación del documento imagen, de lo que se dejará constancia. Esta obtención podrá hacerse de forma automatizada, mediante el correspondiente **sello electrónico**.
- En los supuestos de documentos emitidos originalmente en soporte papel de los que se hayan efectuado copias electrónicas de acuerdo con lo dispuesto en este artículo, podrá procederse a la destrucción de los originales en los términos y con las condiciones que por cada Administración Pública se establezcan.
- Las copias realizadas en soporte papel de documentos públicos administrativos emitidos por medios electrónicos y firmados electrónicamente tendrán la consideración de copias auténticas siempre que incluyan la impresión de un código generado electrónicamente u otros sistemas de verificación que permitan contrastar su autenticidad mediante el acceso a los archivos electrónicos de la Administración Pública, órgano o entidad emisora.

7.2.-EXPEDIENTE JUDICIAL ELECTRÓNICO

La Ley 11/2007 [40]define el expediente electrónico como "el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan".

Como medida para garantizar la integridad de este expediente electrónico, establece que el foliado de los expedientes electrónicos se llevará a cabo mediante un índice electrónico, firmado por la Administración, órgano o entidad actuante, según proceda. De esta manera, no sólo se garantiza la integridad del expediente electrónico, sino que también se permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

Prevé también, que la remisión de expedientes podrá ser sustituida a todos los efectos legales por la puesta a disposición del expediente electrónico, teniendo el interesado derecho a obtener copia del mismo.

El Expediente Judicial Electrónico, en el ámbito de la Administración de Justicia se define como el conjunto de información que se genera durante la tramitación de un expediente judicial, tanto la emitida desde la propia Oficina Judicial como la aportada por las partes durante el desarrollo del proceso o la que se deriva de los informes o aportaciones de peritos y profesionales.

De esta definición se deriva la necesidad de que se den en la práctica dos circunstancias importantes:

- Los sistemas de información implementados en las Oficinas Judiciales, permitirán que toda la información que se genera ya esté en formato electrónico y se integre de forma natural en el Expediente Judicial Electrónico.
- Los documentos aportados por las partes y los profesionales al expediente, deberán llegar a las Oficinas Judiciales, donde se incorporarán al Expediente Judicial Electrónico, tanto si se trata de escritos de trámite como en el caso de documentos que dan origen a un nuevo asunto judicial.

Por parte de la Administración de Justicia, es un objetivo conseguir que los litigantes, sus representantes y demás profesionales presenten sus escritos en formato electrónico con las debidas garantías y que los procesos a los que den lugar se tramiten

[40] Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos. Artículo 32.1.

íntegramente en formato electrónico. Para ello es necesario fomentar las siguientes líneas de actuación:

- Realización de acuerdos con administraciones y organismos públicos y privados, como colegios profesionales para el intercambio de información inherente a los expedientes.
- Comunicaciones telemáticas seguras con los abogados y procuradores, cuerpos y fuerzas de seguridad, peritos, traductores, etc.
- Establecimiento de medios, tanto humanos como materiales para el proceso de digitalización en la sede, así como mecanismos para la firma digital.

Para poder interrelacionar a todos los usuarios de la Administración de Justicia, es imprescindible disponer de medios seguros. Es necesario acreditar quién está firmando los documentos, quién está realizando las presentaciones, que lo que figura en el Expediente Judicial Electrónico es realmente lo que se ha presentado, en resumen, quién y en qué condiciones está accediendo a la Administración de Justicia y es aquí donde la **firma digital** cobra todo su protagonismo.

Los documentos generados desde los sistemas de información de las Oficinas Judiciales deberán estar firmados digitalmente por los usuarios con autorización para ello, siendo estos inicialmente los secretarios, fiscales, jueces y magistrados. Del mismo modo las presentaciones que se realizan en el Juzgado deberán tener la validez que en cada momento sea necesario. Los documentos presentados en las sedes judiciales deben llevar una firma digital mediante una entidad certificadora que a modo de sello de entrada, certifique que ese es el documento que se ha presentado. De esta manera:

- En las comunicaciones telemáticas de abogados y procuradores serán los profesionales quienes firmen el proceso de presentación de la documentación.
- En la presentación de documentación mediante medios digitales en la propia sede deberá existir, en la incorporación al expediente de los documentos digitalizados, un proceso por el cual en el momento de la anexión de documentos al expediente, éstos quedarán firmados mediante lo que se denomina certificado digital de aplicación.
- En los documentos que se presenten en formato físico en la propia sede y que el departamento de digitalización proceda a su escaneo, será el propio proceso de escaneo y anexión al Expediente Judicial Electrónico quien firme el documento mediante el certificado digital de aplicación.

La existencia del Expediente Judicial Electrónico facilitará también, dentro de la nueva organización, la interrelación de las Unidades Procesales de Apoyo Directo y los Servicios Comunes y los diferentes órganos de la estructura judicial, tanto si se trata de asuntos entro órganos de la misma provincia (elevaciones, recursos, inhibiciones), como entre órganos de distintas ubicaciones geográficas (recursos al Tribunal Supremo, envíos a la Audiencia Nacional y los auxilios judiciales o exhortos).

El Consejo General del Poder Judicial ha creado un Test de Compatibilidad que define los protocolos para las comunicaciones telemáticas de exhortos entre distintos sistemas informáticos judiciales, tanto para los envíos como para la recepción por el órgano de destino. Del mismo modo, ha puesto a disposición de las comunidades una plataforma para el intercambio de información del Test de Compatibilidad[41].

La implantación de las Tecnologías de la Información y las Comunicaciones en el ámbito de la Justicia permitirá aumentar la agilidad y la eficacia de la Administración de Justicia, con medidas como la instauración del uso generalizado del Expediente Judicial Electrónico y su circulación entre las distintas unidades de la Oficina Judicial a través de las redes de comunicación para que cada integrante del proceso de tramitación acceda a la información correspondiente.

La nueva Oficina Judicial y el Expediente Judicial Electrónico abrirán el camino hacia un modelo de Justicia en Red y a su mejora administrativa.

7.3.-ARCHIVO ELECTRÓNICO

El artículo 31 de la Ley 11/2007 se encarga de regular el Archivo electrónico de documentos y en él se establecen las siguientes disposiciones:

- Podrán almacenarse por medios electrónicos todos los documentos utilizados en las actuaciones administrativas.
- Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar

[41] En cumplimiento del mandato del artículo 230 de la Ley Orgánica 16/94 de Reforma de la LOPJ que establece que los programas y aplicaciones informáticos que se utilicen en la Administración de Justicia deberán ser previamente aprobados por el CGPJ, quien garantizará su compatibilidad.

los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.

- Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

La Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos establece una serie de **requisitos** que debe cumplir el archivo electrónico de documentos:

- Deberá ser capaz de conservar en formato electrónico todo documento electrónico que forme parte de un expediente y/o que afecte a derechos o intereses de los ciudadanos (artículos 31.1 y 31.2).
- Deberá tener en cuenta que el interesado o las Administraciones Públicas podrán emitir copias auténticas siempre que el documento original esté en manos de la Administración y que la información sobre **firma electrónica** (o **sellado de tiempo** si procede) permitan comprobar la coincidencia con el original (artículo 30.1).
- El almacenamiento debe ser seguro (archivo **securizado**). En particular se deberá asegurar la identificación y el control de accesos (artículo 31.3).
- El almacenamiento de los documentos deberá ser en un soporte que se pueda convertir a otros formatos accesibles desde distintas aplicaciones (artículo 31.2).
- Deberá entender como expediente al conjunto de documentos electrónicos correspondientes a un procedimiento. Deberá ser posible que un documento pueda formar parte de distintos expedientes electrónicos (artículos 32.1 y 32.2).
- Deberá tener en cuenta que los expedientes deberán llevar un **índice electrónico** firmado por la Administración (artículo 32.2).

8.-IDENTIFICACIÓN ELECTRÓNICA.

Para poder cumplir con los sistemas o formas de identificación y autenticación propuestos en la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, es necesario remitirnos a los conceptos de firma electrónica y certificado electrónico.

Cuando la Ley 11/2007, en el artículo 13, se ocupa de regular las formas de identificación y autenticación, establece que las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica y nos remite a la Ley de Firma Electrónica [42]para determinar lo que se debe entender por dicho concepto de firma electrónica. Además, a continuación establece una relación de sistemas de firma electrónica aceptados legalmente, distinguiendo entre los que pueden utilizar los ciudadanos y los que pueden utilizar las Administraciones Públicas:

- **Los ciudadanos podrán utilizar en sus relaciones con las Administraciones Públicas:**
  - Sistemas de firma electrónica incorporados al Documento Nacional de Identidad para personas físicas.
  - Sistemas de firma electrónica avanzada[43], incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones Públicas.
  - Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen.

Las personas físicas podrán, en todo caso y con carácter universal, utilizar los sistemas de firma electrónica incorporados al Documento Nacional de Identidad en su relación por medios electrónicos con las Administraciones Públicas. El régimen de utilización y efectos de dicho documento se regirá por su normativa reguladora.

Los ciudadanos, además de los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, podrán utilizar sistemas de firma electrónica avanzada para identificarse y autenticar sus documentos.

[42] Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
[43] El artículo 3 de la LFE la define como la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

La relación de sistemas de firma electrónica avanzada admitidos, con carácter general, en el ámbito de cada Administración Pública, deberá ser pública y accesible por medios electrónicos e incluirá, al menos, información sobre los elementos de identificación utilizados así como, las características de los certificados electrónicos admitidos, los prestadores que los expiden y las especificaciones de la firma electrónica que puede realizarse con dichos certificados.

Los certificados electrónicos expedidos a Entidades sin personalidad jurídica, previstos en la Ley de Firma Electrónica podrán ser admitidos por las Administraciones Públicas en los términos que estas determinen.

Además de esto, la Ley 11/2007, en su artículo 16, admite la posibilidad de utilización de otros sistemas de firma electrónica tales como

- Las **Claves concertadas**, al establecer que las Administraciones Públicas podrán determinar, teniendo en cuenta los datos e intereses afectados, y siempre de forma justificada, los supuestos y condiciones de utilización por los ciudadanos de este sistema de claves concertadas, en un registro previo, aportación de información conocida por ambas partes u otros sistemas no criptográficos.
- En los supuestos en que se utilicen estos sistemas para confirmar información, propuestas o borradores remitidos o exhibidos por una Administración Pública, ésta deberá garantizar la **integridad** y el **no repudio** por ambas partes de los documentos electrónicos concernidos.
- Las Administraciones Públicas deben certificar la existencia y contenido de las actuaciones de los ciudadanos en las que se hayan usado las formas de identificación y autenticación mencionadas.

- **Las Administraciones Públicas podrán utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzcan:**
  - Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede electrónica y el establecimiento con ella de comunicaciones seguras.
  - Sistemas de firma electrónica para la actuación administrativa automatizada.
  - Firma electrónica del personal al servicio de las Administraciones Públicas.

- Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes.

En lo que se refiere a las **Sedes electrónicas,** la Ley 11/2007, en su artículo 17, prevé para su identificación y para garantizar una comunicación segura con las mismas, sistemas de firma electrónica basados en certificados de dispositivo seguro o medio equivalente.

Así mismo, en el artículo 18, establece los siguientes sistemas de firma electrónica, tendentes a la identificación y autenticación, que pueden adoptar las Administraciones Públicas en el ejercicio de su actividad administrativa automatizada:

- **Sello electrónico** de Administración Pública, órgano o entidad de derecho público, basado en **certificado electrónico** que reúna los requisitos exigidos por la legislación de firma electrónica
- **Código seguro de verificación** vinculado a la Administración Pública, órgano o entidad y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Hay que tener en cuenta que los **certificados electrónicos** mencionados en el primer apartado deben incluir el número de identificación fiscal y la denominación correspondiente, pudiendo contener la identidad de la persona titular en el caso de los **sellos electrónicos** de órganos administrativos.

La relación de **sellos electrónicos** utilizados por cada Administración Pública, incluyendo las características de los **certificados electrónicos** y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos. Cada Administración Pública debe adoptar las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.

8.1.-FIRMA ELECTRÓNICA DEL PERSONAL AL SERVICIO DE LA ADMINISTRACIÓN DE JUSTICIA.

En España, la Ley reguladora de la firma electrónica (Ley 59/ 2003 de 19 de diciembre), define la firma electrónica como “el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante”. (artículo. 3.1 de la Ley).

De esta definición deducimos una serie de características que debe cumplir la firma electrónica:

- ✓ identificar al titular de la firma.
- ✓ autenticar el contenido del documento.
- ✓ garantizar la integridad del documento.
- ✓ logar la seguridad jurídica en la conservación del documento.

El artículo 3 sigue desarrollando el concepto fijado en el apartado 1 dando lugar a lo que podríamos llamar "dos tipos cualificados" de firma electrónica:

- **firma electrónica avanzada**: *"es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control"*. (artículo. 3.2 LFE).
- **firma electrónica reconocida***: "firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma"*. (artículo. 3.3 LFE).

Estos conceptos de firma electrónica incorporan dos tipos de tecnología de cifrado: la Criptografía de Clave Única o Simétrica y la Criptografía de Clave Pública o Asimétrica.

El concepto de **firma electrónica** sólo exige que los datos que la componen permitan identificar al firmante.

La **firma electrónica avanzada** introduce la necesidad de contar con un par de claves, es decir, tecnología de cifrado asimétrico o Infraestructura de Clave Pública. Se precisa de una clave privada que el firmante nunca hace pública.

La **firma electrónica reconocida** añade al concepto anterior la necesidad de estar basada en un certificado reconocido y haber sido generada mediante un dispositivo seguro de firma.

La Criptografía de Clave Pública o Asimétrica es un método para el intercambio seguro de mensajes basado en la asignación de dos claves complementarias, una pública y otra privada, a los particulares implicados en una transacción. Se utiliza la clave privada para cifrar los datos y la pública para descifrar los mismos.

Por lo tanto, para que pueda utilizarse la firma electrónica reconocida es necesario una Infraestructura de Clave Pública (PKI[44]). Podemos decir que es una combinación de hardware, software y procedimientos de seguridad que permiten ejecutar con garantías operaciones criptográficas; permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad para cifrar y descifrar mensajes, firmar digitalmente y garantizar el no repudio de un envío.

- En este tipo de tecnología de cifrado intervienen como mínimo las siguientes partes:
  - ✓ usuario iniciador de la operación.
  - ✓ sistemas servidores que dan fe de la operación y garantizan la validez de los certificados implicados (Autoridad de Certificación, Autoridad de Registro y Sistema de sellado de Tiempo).
  - ✓ destinatario de los datos enviados por el usuario iniciador de la operación.

- Por lo tanto, los componentes de este sistema serían:
  - ✓ **la autoridad de certificación**: es la encargada de emitir y revocar los certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.
  - ✓ **la autoridad de registro**: es la responsable de verificar el enlace entre los certificados y la identidad de sus titulares.
  - ✓ **los repositorios**: son las estructuras encargadas de almacenar la información relativa a la PKI. Los mas importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados (se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecida dentro del mismo certificado).
  - ✓ **la autoridad de validación**: es la encargada de comprobar la validez de los certificados.
  - ✓ **la autoridad de sellado de tiempo**: es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo.
  - ✓ **los usuarios y entidades finales**: aquellos que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública.

[44] **PKI**: Public Key Infraestructure

Quiero reseñar que todo certificado válido ha de ser emitido por una autoridad de certificación reconocida, que garantice la validez de la asociación entre el tenedor del certificado y el certificado en sí.

El poseedor de un certificado es responsable de la conservación y custodia de la clave privada asociada al certificado.

Las entidades de registro se encargan de la verificación de la validez y veracidad de los datos de quien pide un certificado

Quiero profundizar un poco diciendo que los datos de creación de firma son datos únicos que el signatario utiliza para crear la firma electrónica, aplicándolos mediante un programa o aparato informático que la LFE denomina "dispositivo de creación de firma", que cuando cumple con unos requisitos establecidos en la ley, se le reconoce como dispositivo "seguro" de creación de firma; por otro lado, la firma electrónica es verificada por unos datos, que se conocen como dispositivos de verificación de firma.(artículos 24 y 25 de la LFE).

El artículo 3 cualifica esta firma electrónica reconocida concediéndole el mismo valor, respecto de los datos consignados en forma electrónica, que la firma manuscrita. A esta firma electrónica reconocida se le otorga la característica del *"no repudio"*, y por lo tanto hace prueba.

En conclusión, de la lectura de este precepto de la LFE deducimos que es necesaria una firma electrónica reconocida, basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, para que tenga el mismo valor jurídico que la firma manuscrita. Quiero comentar que el certificado reconocido debe ser expedido por un Prestador de Servicios de Certificación, y que estos certificados reconocidos que emiten estos prestadores tienen que contener unos requisitos mínimos.

El artículo.3 de la LFE en su apartado 8 establece que en los casos en que se impugne en juicio la autenticidad de la firma electrónica reconocida se podrá aportar como prueba documental el soporte en que se hallen los datos firmados electrónicamente. En estos casos se procederá a comprobar que el Prestador de Servicios de Certificación ha cumplido todos los requisitos establecidos en la ley.

No obstante, a la firma electrónica simple y a la avanzada se le reconocen efectos jurídicos y también podrán ser utilizadas como prueba en juicio, si bien no gozan de los mismos efectos jurídicos atribuidos a la firma electrónica reconocida (artículo. 3.9 LFE).

De hecho el artículo. 3.8 de la LFE establece que si se impugna la autenticidad de la firma electrónica avanzada, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil.

Por otra parte, un PSC (Prestador de Servicios de Certificación), según el Art.2.2 de la Ley 59/2003 de Firma Electrónica, puede ser una persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica. Tendríamos que distinguir entre PSC nacionales, comunitarios e internacionales.

La actividad de prestación de servicios de certificación no está sujeta a autorización previa y se realizará en régimen de libre competencia, según establece el artículo 5 de la Ley de Firma Electrónica que establece además que la prestación al público de servicios de certificación por las Administraciones Públicas, sus organismos públicos o las entidades dependientes o vinculadas a las mismas se realizará con arreglo a los principios de objetividad, transparencia y no discriminación.

Un PSC puede prestar diferentes servicios. Su función básica es la emisión de certificados, pero se deja abierta la posibilidad de que no expidan certificados al público, sino que presten otros servicios relacionados con la firma electrónica.

El Art.18 de la ley de firma electrónica define las obligaciones de los PSC que expiden certificados electrónicos y distingue aquellos PSC que puedan prestar otros servicios relacionados con la firma electrónica.

Cuando se trata de PSC que expiden certificados electrónicos reconocidos, tendrán que cumplir además de las obligaciones generales (Art.20), las obligaciones derivadas de la expedición de estos certificados reconocidos (Art.12) y las de comprobación de la identidad y demás circunstancias personales de los solicitantes (Art.13).

En cuanto al concepto de **certificado electrónico**, el artículo 6 de la LFE lo define como el "documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad".

El mismo artículo ofrece también una definición del concepto de firmante como "la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.

Los certificados electrónicos reconocidos, mencionados arriba, son definidos por la Ley de Firma Electrónica, en su artículo 11, como "los certificados expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten". Además, se especifica que deben incluir una serie de datos tales como:

- la indicación de que se expiden como tales
- el código identificativos único del certificado.
- la identificación y la firma electrónica avanzada del prestador de servicios de certificación que expide el certificado y su domicilio.
- la identificación del firmante por su nombre, apellidos y número de DNI en el caso de personas físicas y por su denominación o razón social y su código de identificación fiscal en el caso de personas jurídicas.
- los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.
- el comienzo y el fin del período de validez del certificado.
- limites de uso del certificado y límites del valor de las transacciones para las que puede utilizarse el certificado.
- cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite.
- en los casos de relaciones de representación deben incluir la indicación del documento público que acredite fehacientemente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente.

Además de esto, los Prestadores de Servicios de Certificación, deben cumplir con una serie de obligaciones antes de expedir estos certificados reconocidos, contempladas como ya he dicho anteriormente en los artículos 12 y 13 de la Ley de Firma Electrónica.

El artículo 19 de la Ley 11/2007, deja bien claro que la identificación y autenticación del ejercicio de la competencia de la Administración Pública, órgano o entidad actuante, cuando utilice medios electrónicos, se realizará mediante firma electrónica del personal a su servicio.

La Ley 11/2007 [45]deja en manos de la Administración Pública correspondiente la potestad de proveer a su personal de sistemas de firma electrónica; estos sistemas pueden identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en el que presta sus servicios.

El mismo artículo de la Ley también contempla la posibilidad de que el personal al servicio de una Administración Pública pueda utilizar el sistema de firma electrónica basada en el Documento Nacional de Identidad.

Además, en la actualidad se están desarrollando proyectos en común entre el Ministerio de Justicia, el Consejo General del Poder Judicial, Agencias de certificación y Colegios profesionales, para intentar lograr que las notificaciones y presentaciones telemáticas en los juzgados se hagan mediante la plataforma Lexnet. Para esto se requiere la certificación digital o la **firma electrónica reconocida**[46], para asegurar la confidencialidad, la identidad y la integridad de los mensajes de los emisores y receptores.

De hecho, el RD84/2007, de 26 de enero sobre implantación en la Administración de Justicia del sistema informático de telecomunicaciones Lexnet, en su artículo 2 establece que el sistema Lexnet es un medio de transmisión seguro de información, que mediante el uso de firma electrónica reconocida, en los términos establecidos en la Ley de Firma electrónica, satisface por un lado, las características de autenticación, integridad y no repudio y mediante los mecanismos técnicos adecuados las de confidencialidad y sellado de tiempo conforme a lo establecido en el artículo 230 de la Ley Orgánica del Poder Judicial, y por otro, el cumplimiento de los requisitos exigidos en las leyes procesales.

Actualmente, en Oficinas Judiciales de algunas Comunidades Autónomas se están repartiendo entre los funcionarios de las mismas tarjetas criptográficas de firma electrónica, con el fin de que puedan realizar también trámites administrativos por vía telemática y que puedan interactuar de manera eficaz y segura en la tramitación de los asuntos judiciales. La intención es que cada usuario las utilice como su identificación digital para acceder al expediente digital, interactuar con la Oficina Judicial y pedir información a la Oficina Judicial o a la Administración de Justicia.

[45] En el artículo 19, dentro de la Sección 3ª dedicada a la Identificación electrónica de las Administraciones Públicas y Autenticación del ejercicio de su competencia.
[46] Ya vimos que es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. Tiene el mismo valor jurídico que la firma manuscrita e incluso más ya que una de sus características es el "no repudio".

La Ley 11/2007 prevé también la circunstancia de que se produzcan transmisiones[47] de documentos electrónicos en entornos cerrados de comunicaciones entre Administraciones Públicas, órganos y entidades de derecho público, y establece para estos casos que serán válidos a efectos de autenticación e identificación de los emisores y receptores.

Si los participantes en esas comunicaciones pertenecen a una misma Administración Pública, ésta determinará las condiciones y garantías por las que se regirá que, al menos, comprenderá la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.

Si los participantes pertenecen a distintas administraciones, las condiciones y garantías citadas se establecerán mediante convenio.

En cualquier caso es necesario garantizar la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan.

[47] El artículo 20 de la Ley regula el intercambio electrónico de datos en entornos cerrados de comunicación.

9.-PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

9.1.-INTRODUCCIÓN Y DEFINICIÓN DE CONCEPTOS.

El Art. 18.4 de la Constitución española emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos.

La **intimidad** como vemos está suficientemente protegida por este artículo constitucional y las leyes que la desarrollan pero la **privacidad,** como derecho fundamental autónomo e independiente del derecho a la intimidad está amenazado por las tecnologías informáticas, lo que hace preciso establecer una frontera que garantice sus limites.[48]

En épocas pasadas el tiempo y el espacio actuaban como factores de salvaguarda de la privacidad de la persona, pero hoy en día, estos límites han desaparecido, y las modernas técnicas informáticas permiten obtener un determinado perfil de la persona, configurar una determinada reputación o fama, que es una cierta manifestación del honor de una persona, y este perfil puede resultar luego valorado, favorable o desfavorablemente, para las diferentes actividades públicas o privadas.

Hay que entender que la privacidad constituye un conjunto más amplio, más global de facetas de la personalidad del individuo, que coherentemente enlazadas entre si nos ofrecen un retrato de su personalidad; sería como el perfil que se puede obtener de un individuo con el tratamiento informatizado de la información, un perfil, por cierto, que el mismo puede llegar a desconocer.

La Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre indica claramente que el "derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos…" y asimismo "garantiza a los individuos u poder de disposición sobre sus datos que nada vale si el afectado desconoce qué datos son los que poseen terceros, quiénes los poseen y con qué fin".

Hay que tener también en cuenta que los ciudadanos son cada vez más conscientes de la importancia de protegerse del uso indebido de sus datos personales y los

[48] Exposición de Motivos de la LO 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

responsables de su tratamiento, de la incidencia que sobre su imagen tiene la política de privacidad que apliquen, además de la necesidad de cumplir con las obligaciones legales.

Teniendo en consideración todo esto, el legislador establece el Art. 1 de la Ley Orgánica de Protección de Datos de Carácter Personal[49], donde deja constancia, del objeto que persigue con esta ley. Hoy en día se considera protección de datos "*el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esta forma confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional*".

Podemos estructurar el análisis y estudio de la Protección de Datos como un triángulo en cuyos vértices se sitúan los principios de dicha protección, los derechos que emanan de dichos principios y los procedimientos que garantizan el ejercicio efectivo de dichos derechos. [50]De esta manera, podemos decir que existen unos principios que hay que cumplir por el responsable del fichero o tratamiento, unos derechos que, mediante su ejercicio, dan efectivo contenido a los principios recogidos en la norma y un procedimiento que tutela al interesado cuando por el responsable del fichero o tratamiento no se cumplen los principios o se le pone algún impedimento para ejercer los derechos.

A continuación voy a dedicar unas líneas a definir algunos conceptos fundamentales que utilizaré muy frecuentemente en los siguientes apartados a desarrollar, y que creo fundamental, esclarecer en este momento:

- **Datos de carácter personal**
  - ✓ la LOPD los define como "cualquier información concerniente a personas físicas identificadas o identificables"
  - ✓ el RD 1720/2007 los define como "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"
- **Fichero**: la LOPD lo define como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".

[49] Ley Orgánica 15/1999, de 13 de diciembre.
[50] Prof. Miguel Ángel Davara Rodríguez.

Como vemos, de esta definición que ofrece la LOPD, ha desaparecido el término automatizado, por lo tanto, el ámbito de aplicación de la presente ley se extiende también a los ficheros manuales.

- **Afectado o interesado**: según la LOPD es la "persona física titular de los datos que sean objeto del tratamiento". Podemos decir, por tanto, que afectados son potencialmente todos los ciudadanos y que de esta manera, queda delimitado el ámbito subjetivo de aplicación de la LOPD, quedando claramente incluidas las personas físicas y excluidas las personas jurídicas de la protección conferida por sus disposiciones.
- **Tratamiento de datos**: la LOPD lo define como "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencia"
- **Responsable del Fichero o tratamiento**: según la LOPD, sería toda "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".
- **Encargado de Tratamiento**: la LOPD lo define como "la persona física o jurídica, autoridad pública, servicio o cualquier organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento". En ciertas ocasiones, la persona que realiza un tratamiento de datos es distinta del responsable del fichero, como en los casos del acceso a los datos por terceros; se crea pues una nueva figura, que sin ser titular ni responsable del fichero puede tratar los datos por cuenta de aquél.
- **Consentimiento del interesado**: para la LOPD sería "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen". El consentimiento es una de las condiciones de licitud para el tratamiento de los datos de carácter personal. Siempre se requerirá el consentimiento del interesado para el tratamiento de sus datos de carácter personal, salvo que la ley disponga lo contrario.
- **Cesión o comunicación de datos**: según la LOPD, sería "toda revelación de datos realizada a una persona distinta del interesado". Podría ser considerada como cesión la simple consulta que un tercero realice a los datos, aunque sea a distancia y sin

creación de un fichero o tratamiento nuevo; la cesión es un punto conflictivo en las teorías sobre protección de datos ya que se deja abierta la posibilidad de que el interesado pierda el control sobre sus propios datos al haber sido comunicados a un tercero al que es muy probable que ni tan siquiera conozca. Por todo ello, la cesión, salvo las excepciones que marca la norma, deberá ser siempre con consentimiento.

- **Fuentes accesibles al público**: la LOPD las define como "aquellos ficheros cuya consulta puede ser realizada, por cualquier persona no impedida por una norma limitativa o sin más exigencia que el abono de una contraprestación", ofrece una relación cerrada de ellas estableciendo que "exclusivamente el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, los diarios y boletines oficiales y los medios de comunicación".
- **Bloqueo de los datos**: según el RD 1720/2007 [51]sería "la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades".

La LOPD, en su artículo 16, cuando regula el ejercicio de los derechos de rectificación y cancelación, establece que "la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales", pero en ningún momento define ni explica en qué consiste dicho bloqueo.

9.2.-GESTIÓN DE FICHEROS

9.2.1.-Ficheros de carácter personal dependientes de los Órganos Judiciales.

En el Acuerdo de creación de ficheros de carácter personal dependientes de los órganos judiciales, el Consejo General del Poder Judicial distingue dos tipos de ficheros:

[51] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LO 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.

los jurisdiccionales y los gubernativos. Vamos a centrarnos en los Jurisdiccionales, que a su vez se clasifican en:

- **Ficheros de Asuntos Jurisdiccionales**
  - ✓ El Responsable del Fichero será el órgano judicial encargado del conocimiento del procedimiento. A él le corresponde determinar la finalidad, contenido y uso que se le da al tratamiento con sujeción a las normas procesales aplicables y a las funciones y competencias que la Ley Orgánica del Poder Judicial atribuye a Jueces, Tribunales y Secretarios al configurar el diseño de la Oficina Judicial, "quedando su funcionamiento bajo la dependencia directa del secretario judicial".
  - ✓ El Encargado de Tratamiento serán las Administraciones Públicas competentes en la dotación de los medios materiales, al ser las responsables de los centros de tratamiento, locales, equipos, sistemas, programas, así como del personal técnico que interviene en el tratamiento.
- **Ficheros de Registro de Asuntos**
  - ✓ El Responsable del Fichero será el Secretario Judicial encargado del registro.
  - ✓ El Encargado de Tratamiento serán las Administraciones Públicas.

En cuanto a la responsabilidad por las infracciones recogidas en la LOPD (artículos 9 y 10), que hacen referencia a la no adopción de medidas de índole técnica y organizativa que garanticen la seguridad (que afectan al Responsable del Fichero y al Encargado del Tratamiento) y a la falta del deber de secreto (que afecta al Responsable del Fichero y a cualquier persona que intervenga en cualquier fase del tratamiento).

Son varias las resoluciones de la Agencia Española de Protección de Datos que en el ámbito judicial fijan un criterio y profundizan en la cuestión. De ellas se desprenden la siguiente línea de actuación:

- En el caso de **Ficheros de Asuntos Jurisdiccionales**, la Agencia de Protección de Datos analiza la LOPD y el régimen asignado a los ficheros por el Consejo General del Poder Judicial. En sus resoluciones fija el régimen de distribución de responsabilidades y señala que:

- ✓ El Responsable del Fichero: es el Consejo General del Poder Judicial, como creador del mismo. Si bien podría ser autor de las infracciones de los artículos 9 y 10 de la LOPD, no ha sido sancionado ya que la Agencia de Protección de Datos considera que este organismo ha sido "diligente en orden a concienciar e instruir a los usuarios de los sistemas informáticos de gestión judicial sobre como cumplir con la LOPD".

La Agencia ha tenido en cuenta dos datos importantes:

- o la aprobación del "*Código de Conducta para usuarios de equipos y sistemas informáticos al servicio de la Administración de Justicia*"[52], remitido a todos los órganos judiciales, y donde se establecen pautas de conducta tendentes a concienciar a los usuarios sobre la seguridad de los equipos informáticos y de las comunicaciones. Se entiende por usuario todo profesional que presta sus servicios en los órganos judiciales.
- o la aprobación de los "*Criterios Generales de Seguridad en los Sistemas de Información al Servicio de la Administración de Justicia*". [53]Contiene medidas que mejoran y permiten homogeneizar el nivel de seguridad existente en los sistemas de gestión procesal.

En los casos en que se produzca un menoscabo en la implantación de las medidas de seguridad, solo podría imputarse a quien por mandato de la ley debe establecer dichos medios necesarios para garantizar esa implantación. Por lo tanto:

- ✓ El Responsable de Fichero: será el órgano judicial que conozca del procedimiento.
- ✓ El Encargado del Tratamiento: será la Administración Pública competente en la dotación de bienes materiales.

Es evidente que lo dispuesto en la LOPD no tiene fácil traslado al ámbito judicial, ya que en este ámbito, el Responsable del Fichero (órgano judicial), no puede ni seleccionar al Encargado de Tratamiento pues este viene predeterminado por la estructura del Estado y por quien ejerza la competencia en materia de medios materiales en la

[52] Aprobado por la Instrucción 2/2003, de 26 de febrero, del Pleno del Consejo General del Poder Judicial.
[53] Aprobados por el Acuerdo adoptado por el Pleno del Consejo General del Poder Judicial en sesión de 13 de septiembre del 2007.

Administración de Justicia, ni darle las pautas contempladas en el artículo 12 de la LOPD, ya que estas están predeterminadas normativamente por el Consejo General del Poder Judicial.

9.2.2.-Papel del Secretario Judicial en el ámbito de los Ficheros de Datos de carácter personal.

En el nuevo modelo de Oficina Judicial, el Secretario Judicial ostenta un papel relevante desde el punto de vista de la dirección técnico procesal que le es propia, y ahora se ve incrementado en la medida en que se le adjudican, en determinados ámbitos, las funciones de impulso formal del procedimiento que desempeñaba hasta ahora y otras que le van a permitir la adopción de decisiones sobre materias colaterales a la función jurisdiccional, pero que son indispensables para la misma.

La legislación reguladora del nuevo modelo de Oficina Judicial tampoco atribuye una relación específica de cometidos concretos al Secretario Judicial.

El Fichero de Asuntos Jurisdiccionales es un soporte automatizado que opera al servicio de todos los usuarios y sobre cuyo funcionamiento el Secretario Judicial no tiene ni conocimientos apropiados ni competencia decisoria pues:

- La finalidad del fichero es atribución exclusiva del Consejo General del Poder Judicial.
- El contenido del fichero se delimita por los sistemas de gestión procesal diseñados por cada Administración de Justicia y que deben cumplir el test de compatibilidad que fija el Consejo General del Poder Judicial.
- Su uso viene fijado también por el Consejo General del Poder Judicial en el "Código de conducta para usuarios de equipos y sistemas informáticos al servicio de la Administración de Justicia" que vincula a todo usuario. El funcionamiento del fichero operará automáticamente y bajo las prescripciones técnicas de quienes lo han diseñado. El Secretario Judicial, como usuario del fichero lo utilizará ejerciendo las facultades jurídicas que le son propias pero debe desvinculársele de cualquier dependencia sobre el en la medida en que no tiene ninguna capacidad operativa, ni de decisión, etc.… sobre cual debe ser su funcionamiento.

Recientemente, en mayo del 2010, se ha firmado un Convenio para reforzar la protección de datos en la Administración de Justicia, entre el Consejo General del Poder Judicial y la Agencia Española de Protección de Datos. Este Convenio contempla la creación de una Comisión de Seguimiento, que tendrá entre sus funciones, el fomento de

actividades que contribuyan al desarrollo de los derechos de los ciudadanos y reuniones periódicas de representantes de ambas instituciones con el objetivo de desarrollar iniciativas que impulsen la aplicación efectiva de la normativa de protección de datos en el ámbito de la Administración de Justicia.

La participación en dichas iniciativas de representantes del Ministerio de Justicia y de las Consejerías competentes de las Comunidades Autónomas y de otras Administraciones y organizaciones, conduciría a buen puerto este impulso a la normativa de protección de datos en el ámbito de la Justicia. En este sentido, sería muy valiosa la participación de las asociaciones profesionales del Cuerpo de Secretarios Judiciales, sobre todo a la hora de sacar a la luz un documento unificador que fije las pautas a seguir a la hora de destruir documentos por los órganos judiciales y la dotación imprescindible de destructoras en todos ellos.

La implantación de la Nueva Oficina Judicial en este año 2010 y el cambio estructural que ello supone aconseja que se revise algún que otro aspecto del "Código de conducta para usuarios de equipos sistemas informáticos al servicio de la Administración de Justicia" que permita adaptarlo a las nuevas circunstancias tecnológicas que va a instaurar el expediente judicial digital.

9.2.3.- Creación, modificación o supresión de ficheros de titularidad pública.

El Capítulo I del Título IV de la Ley Orgánica 15/1999, de 13 de Diciembre de Protección de Datos de Carácter Personal (LOPD, en adelante) se encarga de regular los Ficheros de Titularidad Pública.

El **artículo 20** nos indica los pasos y trámites a seguir para la **creación, modificación o supresión** de este tipo de ficheros:

- la creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el B.O.E o diario oficial correspondiente.
- las disposiciones de creación o de modificación de ficheros deberán indicar:

a) La finalidad del fichero y los usos previstos para el mismo.
b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
f) Los órganos de las Administraciones responsables del fichero.
g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

- en las disposiciones que se dicten para la supresión de los ficheros se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Es importante tener en cuenta el **artículo 21** de la LOPD donde se regula **la Comunicación de los datos entre Administraciones Públicas:**

- los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
- podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra.
- a pesar de lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.
- en los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

Cuando entra en vigor la LO 15/1999 de Protección de Datos de Carácter Personal, la disposición adicional primera de dicha ley establecía que los ficheros y tratamientos automatizados inscritos o no en el Registro General de Protección de Datos

deberían adecuarse a las exigencias derivadas de la nueva ley, entre las que destacaba la necesaria adopción de medidas de seguridad de distinto nivel (básico, medio y alto);además encomendaba a las Administraciones Públicas responsables de ficheros de titularidad pública que aprobaran la pertinente disposición de regulación del fichero o adaptaran la existente.

En aquel momento, la separación de los Ministerios de de Interior y Justicia aconsejaba afrontar el correspondiente deslinde de los Ficheros gestionados por uno u otro Departamento.

Todas estas circunstancias aconsejaban elaborar un nuevo texto que recogiera de forma completa y sistematizada la regulación de los ficheros automatizados con datos de carácter personal gestionados por el Ministerio de Justicia y por sus Organismos Públicos adscritos, derogando al mismo tiempo, en el ámbito del Ministerio de Justicia, las disposiciones que hasta ese momento regulaban dichos ficheros.

En este contexto entra en vigor la Orden JUS/1294/2003 de 30 de Abril por la que se regulan los ficheros automatizados con datos de carácter personal gestionados por el Ministerio de Justicia y sus Organismos Públicos, conteniendo en dos anexos la relación y descripción de los distintos ficheros automatizados. Dicha orden ha sido modificada en diferentes ocasiones:

- Por la Orden JUS 4166/2004 de 30 de Noviembre.
- Por la Orden JUS 283/2006 de 1 de Febrero.
- Por la Orden JUS 837/2007 de 29 de Marzo, con objeto de crear un nuevo fichero relativo a los expedientes tramitados en los Registros Civiles y modificar algunos extremos de los ficheros de nacionalidad e INFOREG1 preexistentes.
- Por la Orden JUS 2474/2007 de 27 de Julio
- Por la Orden JUS 2714/2009, de 25 de Septiembre, con objeto de crear nuevos ficheros referidos a la consulta de documentación del archivo general, a la gestión de publicaciones, a la prevención de riesgos laborales etc., etc. Asimismo modifica algunos extremos de los archivos preexistentes.

Uno de los Ficheros automatizados con datos de carácter personal que contempla esta Orden JUS/1294/2003 de 30 de abril es el de *Nominas de Personal-DSJE.* Me parece interesante profundizar en la estructura de este fichero, para ponerlo como ejemplo de ficheros automatizados que podemos encontrarnos en una Oficina judicial:

1-Finalidad y usos previstos: pago de haberes y gestión de personal.

2-Personas y colectivos afectados: funcionarios y personal laboral.

3-Procedimiento de recogida de datos: registros públicos y formularios cumplimentados por el interesado.

4-Estructura básica del Fichero:

- datos identificativos.
- datos de características personales.
- datos especialmente protegidos (afiliación sindical y salud).
- datos de empleo y carrera administrativa:
- datos de transacciones.
- datos económico-financieros.
- datos de circunstancias sociales.

5-Cesión de datos que se prevé:

- A unidades en materia de gestión, en virtud de lo establecido en los artículos ll.2.c) y 21.1 de la LOPD.
- A las entidades bancarias encargadas del abono de la nómina y aquellas en que el interesado hubiera ordenado su domiciliación conforme al artículo 11.2.c) de la LOPD, limitándose la cesión a los datos necesarios para el abono de la nómina.

6-Órgano administrativo responsable: Abogacía General del Estado-Dirección del Servicio Jurídico del Estado.

7-Órgano ante el que puede ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Abogacía General del Estado-Dirección del Servicio Jurídico del Estado.

8-Medidas de Seguridad: Nivel alto.

Otro ejemplo de fichero que podemos encontrarnos, en el ámbito de la organización de Justicia que me parece interesante destacar es el de Quejas y Sugerencias, que incorpora la Orden JUS 2714/2009 de 25 de Septiembre:

1-Finalidad y usos previstos: ejercer las funciones de gestión y control de las quejas y sugerencias presentadas por los ciudadanos en relación con los servicios del Ministerio de Justicia.

2-Personas y colectivos afectados: los ciudadanos que han presentado quejas y sugerencias destinatarios de los servicios facilitados por el Ministerio de Justicia, así como los empleados públicos afectados por las quejas.

3-Procedimiento de recogida de datos: datos aportados por los interesados mediante declaración escrita, telefónica o comunicación electrónica, así como también los aportados en los informes y respuestas que facilitan las unidades afectadas.

4-Estructura básica del fichero: Sistema de información y tratamiento de los datos automatizado. Fecha de presentación de las quejas o sugerencias. Nombre y apellidos de los interesados, DNI, NIF, NIE, Pasaporte, teléfono de contacto, e-mail, firma y rúbrica de los interesados, nombre y apellidos de los funcionarios afectados, datos de la empresa o colectivo en caso de actuar.

5-Cesión de datos que se prevé: ninguna.

6-Órgano administrativo responsable: Subsecretaría del Ministerio de Justicia.

7-Órgano ante el que pueden ejercitarse los derechos ARCO: Subdirección General de Información **Administrativa e Inspección General de Servicios.**

8-Medidas de Seguridad: nivel medio.

9.2.4.- Notificación e inscripción de ficheros de titularidad pública

El Capítulo II del Título V del RD 1720/2007 establece que:

- todo fichero de datos de carácter personal de titularidad pública debe ser notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.
- Cuando se trate de ficheros que estén bajo la responsabilidad de una Comunidad Autónoma que haya creado su propio registro de ficheros, la notificación se realizará a la autoridad autonómica competente, que dará traslado de la inscripción al Registro General de Protección de Datos.
- La notificación se realizará conforme al procedimiento establecido en la sección primera del Capítulo IV del Título IX del presente reglamento.

- Cuando los datos de carácter personal objeto de tratamiento estén almacenados en diferentes soportes, automatizados y no automatizados o exista una copia en soporte no automatizado de un fichero automatizado sólo será precisa una sola notificación, referida a dicho fichero.
- Si existen varios responsables, cada uno de ellos deberá notificar, a fin de proceder a su inscripción en el Registro General de Protección de Datos y, en su caso, en los Registros de Ficheros creados por las autoridades de control de las comunidades autónomas, la creación del correspondiente fichero.
- La inscripción del fichero deberá encontrarse actualizada en todo momento. Se notificará a la Agencia Española de Protección de Datos o, en su caso, a las autoridades de control autonómicas correspondientes cualquier modificación que afecte a la inscripción de un fichero.
- Del mismo modo, la supresión de un fichero también deberá ser notificada a fin de que se proceda a la cancelación de la inscripción en el registro correspondiente.
- Como estamos tratando con ficheros de titularidad pública, cuando se pretenda la creación, modificación o supresión de los ficheros se deberá adoptar con carácter previo a la notificación la correspondiente norma o acuerdo en los términos previstos en el capítulo I del presente título.
- La Agencia Española de Protección de Datos facilitará, de manera gratuita a través de su página Web, los correspondientes modelos o formularios electrónicos de notificación de creación, modificación o supresión de ficheros[54], que permitan su presentación a través de medios telemáticos o en soporte papel, así como, previa consulta de las autoridades de protección de datos de las comunidades autónomas, los formatos para la comunicación telemática de ficheros públicos por las autoridades de control autonómicas.
- El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución acordando la inscripción, una vez que se haya cumplido con el procedimiento previsto en el Capítulo IV del Título IX.
- Esta inscripción debe contener:
    - ✓ el código asignado por el Registro
    - ✓ la identificación del responsable del fichero.

[54] La AEPD aprobó el Sistema de Notificaciones Telemáticas NOTA mediante Resolución de 12 de julio de 2006

- ✓ la identificación del fichero o tratamiento.
- ✓ la descripción de su finalidad y usos previstos.
- ✓ el sistema de tratamiento empleado.
- ✓ el colectivo de personas sobre el que se obtienen los datos.
- ✓ procedencia de los datos.
- ✓ categorías de datos.
- ✓ servicio o unidad de acceso.
- ✓ indicación del nivel de medidas de seguridad exigible.
- ✓ identificación del encargado del tratamiento en donde se encuentre ubicado el fichero
- ✓ destinatarios de cesiones y transferencias internacionales.
- ✓ referencia de la disposición general por la que ha sido creado o modificado el fichero.

- La inscripción de un fichero en el Registro General de Protección de Datos, no exime al responsable del cumplimiento del resto de las obligaciones previstas en la LOPD y demás disposiciones reglamentarias.
- El Director de la Agencia de Protección de Datos, previa tramitación del procedimiento establecido en la sección primera del capítulo IV del título IX, dictará resolución acordando la cancelación de la inscripción correspondiente al fichero, cuando el responsable del fichero le comunique la supresión del fichero.
- Del mismo modo, el Director de la Agencia de Protección de Datos, podrá acordar de oficio la cancelación de la inscripción de un fichero cuando concurran circunstancias que acrediten la imposibilidad de su existencia, cumpliendo siempre el procedimiento establecido en la sección segunda del capítulo IV del título IX del presente reglamento.
- El Registro General de Protección de Datos podrá rectificar en cualquier momento, de oficio o a instancia de parte, los errores materiales que pudieran existir en las inscripciones.
- Se contempla la posibilidad de la inscripción de oficio de un determinado fichero en el Registro General de Protección de Datos:
  - ✓ en supuestos excepcionales
  - ✓ con el fin de garantizar el derecho a la protección de datos de los afectados

- ✓ sin perjuicio de la obligación de notificación.
- ✓ es requisito indispensable que la correspondiente norma o acuerdo regulador de los ficheros con datos de carácter personal haya sido publicada en el correspondiente diario oficial y cumpla con los requisitos establecidos en la LOPD y el presente reglamento.
- ✓ El Director de la Agencia de Protección de Datos, a propuesta del Registro General de Protección de Datos, podrá acordar la inscripción del fichero de titularidad pública en el Registro, notificando dicho acuerdo al órgano responsable del fichero
- ✓ si la inscripción se refiere a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, se comunicará a la referida autoridad para que proceda a la inscripción de oficio.

- Se prevé la posibilidad de que se celebren convenios de colaboración entre el Director de la Agencia de Protección de Datos y los directores de las autoridades de control de las Comunidades Autónomas para garantizar la inscripción en el Registro de los ficheros sometidos a la competencia de dichas autoridades autonómicas.

9.3.-TRANSFERENCIAS INTERNACIONALES DE DATOS.

Un primer análisis de las Transferencias Internacionales de Datos nos permite clasificarlas en base a dos criterios:

1-Por el país de Destino; podemos diferenciar a su vez tres supuestos distintos. En los dos primeros casos la Transferencia Internacional de datos puede realizarse del mismo modo que las comunicaciones, o en su caso prestaciones de servicios, dentro del país comunitario origen de los datos, es decir, no requiere autorización previa de la Agencia Española de Protección de datos, aunque si debe constar en el documento de inscripción del fichero en concreto.

- ✓ un país de la Unión Europea o del Espacio Económico Europeo.
- ✓ un país declarado con un nivel adecuado de protección.
- ✓ un tercer país.

2-Por la finalidad

- ✓ una comunicación a un tercero
- ✓ un encargo o prestación de servicios.

Atendiendo a lo dispuesto en la LOPD, en el Título V, la **norma general** en materia de Transferencia Internacional de Datos es:

- la prohibición de transferencias a terceros países que no proporcionen un nivel de protección equiparable al que presta la LOPD.
- Obtención de autorización previa del Director de la Agencia de Protección de Datos para poder realizar la transferencia, autorización que se otorgará con base a la concurrencia de garantías adecuadas y la evaluación del nivel de protección del país de destino.

Es la Agencia de Protección de Datos quien debe valorar el carácter adecuado del nivel de protección que ofrece el país de destino, atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos; en particular se tomarán en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Esta norma general viene acompañada de unas **excepciones** previstas en el artículo 34 de la LOPD:

- Cuando resulte de la aplicación de tratados o convenios en los que sea parte España.
- Cuando se haga a efectos de prestar o solicitar auxilio judicial internacional.
- Cuando sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios.
- Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
- Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

- Cuando sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
- Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
- Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tienen esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- Cuando se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.
- Cuando tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

9.4-ADOPCIÓN DE MEDIDAS DE SEGURIDAD

Aconsejo hacerlo desde el mismo momento de la recogida de datos.

9.4.1.-Niveles de Seguridad

El artículo 9 de la LOPD establece que corresponde al Responsable de Fichero y, en su caso, al Encargado de Tratamiento la adopción de medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

En dicha adopción se debe tener en cuenta la naturaleza de los datos, los riesgos a los que están expuestos (provengan de la acción humana o del medio natural) y el estado de la tecnología.

El artículo 9 encarga que se regulen reglamentariamente los requisitos y condiciones que deben reunir los ficheros, centros de tratamiento, locales, equipos,

sistemas, programas, personas que tengan acceso a ellos, con respecto a su integridad y seguridad.

Obedeciendo a este encargo de la LOPD **el Título VIII del RD 1720/2007** de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la LOPD (en adelante RD 1720) regula las medidas de seguridad en el tratamiento de datos de carácter personal.

El RD 1720 distingue entre dos tipos de ficheros o tratamientos de datos de carácter personal:

- Los Ficheros y tratamientos automatizados. Dedica el Capítulo III a regular las medias de seguridad aplicables a estos ficheros.

- Los Ficheros y tratamientos no automatizados o manuales estructurados. Dedica el Capítulo IV a regular las medidas de seguridad aplicables a estos ficheros.

Hay que decir que independientemente del tipo de fichero de que se trate, las medidas que se adopten en cada uno de ellos se caracterizan por ser:

- **Mínimas:** El Responsable de Fichero o el Encargado de tratamiento tienen que adoptar las medidas "necesarias" que garanticen la seguridad de los datos, es decir evitar la pérdida, destrucción o manipulación de los datos. Cumpliendo con las medidas de seguridad reglamentarias, cumpliríamos con los mínimos exigidos por el reglamento pero no con el objetivo final de seguridad de los datos, por eso el Responsable de Fichero o el Encargado de Tratamiento tienen que hacer lo que sea para no perder esos datos.
- **Acumulativas**: Ya veremos como el reglamento prevé 3 niveles de seguridad. Todos los ficheros deben adoptar el nivel básico y si se cumplen ciertos requisitos adoptarán adicionalmente el resto de niveles.

El artículo 80 del RD 1720 establece los tres niveles en los que se clasifican las medidas de seguridad exigibles a los ficheros y tratamientos de datos de carácter personal:

- Nivel Básico.
- Nivel Medio.
- Nivel Alto.

En cuanto a la aplicación de estos niveles de seguridad, debemos atenernos a lo regulado en el artículo 81 del RD 1720, que establece lo siguiente:

- Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad de **nivel básico**.
- Además de estas medidas de **nivel básico**, se implantarán las de **nivel medio** en los siguientes ficheros o tratamientos de datos de carácter personal:
    - ✓ Los relativos a la comisión de infracciones administrativas o penales.
    - ✓ Ficheros sobre solvencia patrimonial y crédito, regulados en el artículo 29 de la LOPD.
    - ✓ Los que se encuentren bajo la responsabilidad de las Administraciones Tributarias.
    - ✓ Los que se encuentren bajo la responsabilidad de entidades financieras para finalidades relacionadas con la prestación de servicios financieros.
    - ✓ Los que se encuentren bajo la responsabilidad de las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias, y del mismo modo aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
    - ✓ Los que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y permitan evaluar determinados aspectos de la personalidad o comportamiento de los mismos.
- Además de las medias de **nivel básico y medio**, se aplicarán las medidas de **nivel alto** a los siguientes ficheros o tratamientos de dato de carácter personal:
    - ✓ Los que contengan datos referidos a la ideología, afiliación sindical, religión, creencias, origen racial, salud, o vida sexual.
    - ✓ Los que se contengan datos recabados para fines policiales sin consentimiento de las personas afectadas.
    - ✓ Los que contengan datos referentes a actos de violencia de género.

- A los ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual se les aplicará las medidas de seguridad de nivel básico, cuando se den las siguientes circunstancias:
    - ✓ el tratamiento de estos datos tenga como única finalidad realizar transferencias dinerarias a las entidades de las que los afectados sean asociados o miembros.
    - ✓ se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.
- También podrán adoptarse medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.
- Es importante tener en cuenta que las medidas de seguridad de cada uno de los niveles mencionados tienen la condición de **mínimos exigibles**, por lo tanto debemos plantearnos la posibilidad de que puedan ser ampliadas o complementadas con otras establecidas por disposiciones legales, reglamentarias o por la iniciativa del Responsable del Fichero, cuando así lo exija el objetivo principal de salvaguardar la seguridad de los datos.
- El artículo 81 también prevé la posibilidad de que en un sistema de información existan determinados ficheros que debido a su finalidad, uso concreto o naturaleza de los datos que contienen, requieran la adopción de un nivel de seguridad diferente al del sistema principal. En estos casos, y siempre que se puedan delimitar los datos afectados, los usuarios con acceso a los mismos, y que se haga constar en el documento de seguridad, se podrán aplicar a estos ficheros un nivel de medidas de seguridad, distinto al del sistema principal, adecuado o correspondiente debido a sus características.

9.4.2.-Medidas de Seguridad (Título VIII del RD 1720)

❖ **Aplicables a ficheros y tratamientos automatizados** (Capítulo III RD 1720)

Medidas de Seguridad de Nivel Básico: (Sección 1ª, Capítulo III del RD 1720)

- Funciones y obligaciones del personal: deberán definirse y documentarse claramente en el documento de seguridad.

- Registro de incidencias: a través de un procedimiento de gestión y control de las incidencias que afecten a los datos de carácter personal, donde se haga constar el tipo de incidencia, el momento en que se ha producido o detectado, persona que la detecta y a quien se le comunica, efectos que se hubieran derivado de la misma y medidas correctoras aplicadas.
- Control de acceso: a través del establecimiento de un sistema que permita el acceso únicamente a los datos que se precisen para el desarrollo de sus funciones (con una relación de usuarios y perfiles de usuarios y los accesos autorizados para cada uno de ellos).
- Gestión de soportes y documentos: deberán permitir identificar el tipo de información contenida, ser inventariados y solo serán accesibles por el personal autorizado. La salida o traslado de estos, deberá autorizarse por el responsable del fichero o contemplarse en el documento de seguridad, además deberán adoptarse las medidas necesarias para impedir su sustracción, perdida o acceso indebido durante el transporte, o para impedir el acceso o recuperación de la información contenida en ellos cuando se proceda a su destrucción o borrado.
- Identificación y autenticación: el responsable de fichero adoptará los mecanismos que permitan la identificación inequívoca y personalizada de todo usuario que acceda al sistema y la verificación de su autorización. Si el mecanismo de autenticación se basa en contraseñas, existirá un procedimiento de asignación, distribución y almacenamiento que garantice la confidencialidad e integridad. Estas contraseñas se cambiarán como mínimo cada año y se almacenarán de forma ininteligible.
- Copias de respaldo y recuperación: se realizarán como mínimo semanalmente, salvo que no hubiera actualización de los datos. Deberán establecerse procedimientos de recuperación de datos que garanticen la reconstrucción en caso de pérdida o destrucción. Se verificará cada seis meses el correcto funcionamiento de este procedimiento.

Medidas de Seguridad de Nivel Medio: (Sección 2ª Capítulo III del RD 1720)

- Responsable de Seguridad: se designarán en el documento de seguridad uno o varios responsables de seguridad que coordinen y controlen las medidas definidas

en el mismo. La designación puede ser única para todos los ficheros o diferenciada según los sistemas de tratamiento utilizados.

- Auditoria: se realizará cada dos años, o extraordinariamente cuando se produzcan modificaciones sustanciales.
- Gestión de soportes y documentos: estableciendo un sistema de registro de entrada de soportes que permita conocer el tipo de documento o soporte, fecha y hora, el emisor, el número de documentos o soportes incluidos en el envió, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción. De la misma manera se establecerá un sistema de registro de salida de soportes.
- Identificación y autenticación: estableciendo un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema.
- Control de acceso físico: exclusivamente el personal autorizado en el documento de seguridad podrá acceder a los lugares donde se encuentren ubicados los equipos físicos que dan soporte a los sistemas de información.
- Registro de incidencias: en el se harán constar los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y cuando se de el caso, los datos que haya sido necesario grabar manualmente en el proceso de recuperación.

Medidas de Seguridad de Nivel Alto (Sección 3ª, Capítulo III RD 1720)

- Gestión y distribución de soportes: se utilizarán sistemas de etiquetado comprensibles para los usuarios con acceso autorizado, pero que dificulten la identificación al resto de personas. Se cifrarán los datos contenidos en los soportes cuando se proceda a su traslado o cuando se encuentren en instalaciones que estén fuera del control del responsable de fichero.
- Copias de respaldo y recuperación: deberá conservarse una en un lugar diferente de aquel en que se encuentren los equipos informáticos.
- Registro de accesos: se guardará la identificación del usuario, fecha y hora, fichero accedido, tipo de acceso y si ha sido denegado o autorizado. Si el acceso es autorizado, se guardará la información que identifique el registro accedido. Se conservarán los datos registrados por un periodo mínimo de dos años.

- Telecomunicaciones: la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

❖ **Aplicables a ficheros y tratamientos no automatizados** (Capítulo IV RD 1720)

Medidas de Seguridad de Nivel Básico (Sección 1ª)

- Criterios de archivo: deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.
- Dispositivos de almacenamiento: deberán disponer de mecanismos que obstaculicen su apertura. En todo caso se adoptarán medidas que impidan el acceso de personas no autorizadas.
- Custodia de los soportes: en los casos en que la documentación con datos de carácter personal no se encuentre archivada en dispositivos de almacenamiento, se deberá custodiar e impedir en todo momento que pueda ser accedida por persona no autorizada, por la persona que se encuentre al cargo de la misma.

Medidas de Seguridad de Nivel Medio (Sección 2ª)

- Responsable de seguridad: se designarán uno o varios responsables en los términos y con las funciones previstas para los ficheros y tratamientos automatizados.
- Auditoria: se someterán cada dos años a auditoria interna o externa.

Medidas de Seguridad de Nivel Alto (Sección 3ª)

- Almacenamiento de la información: los armarios en los que se almacenen este tipo de ficheros deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave o dispositivo equivalente. En el caso de no ser posible por las características de los locales se adoptarán medidas alternativas.
- Copia o reproducción: sólo podrá realizarse bajo el control del personal autorizado en el documento de seguridad. Se procederá a la destrucción de las

copias o reproducciones desechadas para evitar el acceso o recuperación de la información.

- Acceso a la documentación: se limitará exclusivamente al personal autorizado. Deben establecerse mecanismos que permitan identificar los accesos realizados en el caso de documentos utilizados por múltiples usuarios.
- Traslado de documentación: deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información trasladada.

9.4.3.-Documento de seguridad.

Se elaborará un **Documento de Seguridad** [55]que recogerá las medidas de índole técnica y organizativa que será de obligado cumplimiento para todo el personal que tenga acceso a datos de carácter personal.

Este documento podrá ser único para todos los ficheros o tratamientos, o también podrá ser individualizado para cada fichero o tratamiento. Del mismo modo, podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado, o bien atendiendo a los criterios organizativos del responsable. En cualquier caso hay que tener en cuenta que se trata de un documento interno de la organización.

Este documento debe poseer el siguiente contenido mínimo:

- Ámbito de aplicación. Deben especificarse detalladamente los recursos protegidos.
- Medidas, normas, procedimientos de actuación encaminados a garantizar el nivel de seguridad exigido.
- Funciones y obligaciones del personal.
- Estructura de los Ficheros de datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta a las incidencias.
- Procedimiento de realización de copias de respaldo y recuperación de datos.
- Medidas necesarias para el transporte de soportes y documentos así como para su destrucción o reutilización.

Cuando son aplicables también las medidas de seguridad de nivel medio y alto, el documento deberá incluir además:

[55] Regulado en el Capítulo II del Título VIII del RD 1720/2007.

- Identificación del Responsable de Seguridad.
- Controles periódicos para verificar el cumplimiento de lo dispuesto por el documento.

Como existe también tratamiento de datos por cuenta de terceros, el documento debe contener también:

- Identificación de los ficheros o tratamientos que se traten con referencia expresa al contrato o documento que regula las condiciones del encargo, así como la identificación del responsable y del período de vigencia del encargo.
- Mención de los supuestos en que los datos personales del fichero o tratamiento se incorporen y traten en los sistemas del encargado.

El documento de seguridad se mantendrá actualizado en todo momento y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o como consecuencia de los controles periódicos. Se entiende que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

El contenido del documento de seguridad deberá adecuarse, en todo momento a las disposiciones vigentes en materia de seguridad de datos de carácter personal.

9.5.-AUDITORIA DE LA OFICINA JUDICIAL EN LAS FASES DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL.

Un tratamiento de datos de carácter personal, a efectos del cumplimiento de la normativa sobre protección de datos, debe realizarse en tres fases:

1-**Recabar los datos**, bien sea directamente del propio interesado o de un tercero. Esta fase se tiene que caracterizar por su transparencia, es decir, los datos deben ser recabados de una manera leal y lícita, y por el conocimiento y consentimiento del afectado.

2-**Tratamiento de los datos**, queda definida en la letra c del Art. 3 de la LOPD. Los datos pueden cruzarse y relacionarse con otros datos, con el objetivo de obtener un perfil del afectado que incluso él mismo desconoce.

3-**Utilización y en su caso comunicación a terceros de los resultados del tratamiento**. A esta fase también se la conoce como "cesión o comunicación de datos". En esta fase vuelve a ser esencial el conocimiento y consentimiento del titular.

Un cumplimiento riguroso de la LOPD exige que se observen en todas y cada una de las tres fases los **principios** de la protección de datos regulados por la LOPD en los artículos 4 al 12 y se respeten en todo momento los **derechos** de las personas, regulados en los artículos 13 al 19. También es importante que se articulen los **procedimientos** que permitan a los ciudadanos ejercer esos derechos.

FASE DE RECOGIDA:

1-Principio de Información (artículo 5 LOPD):

- Debemos informar a cada ciudadano de quien se recaben datos de modo "expreso, preciso e inequívoco".
- Contenido de esa información:
  - ✓ Existencia del Fichero, Finalidad de la recogida y Destinatarios de la información.
  - ✓ Carácter obligatorio o facultativo de la respuesta a las preguntas planteadas. No será necesaria esta información cuando se deduzca de la naturaleza de los datos o de las circunstancias en que se recaba.
  - ✓ Consecuencias de la obtención de los datos o de la negativa a suministrarlos. No será necesario cuando se deduzca de la naturaleza de los datos o de las circunstancias.
  - ✓ Posibilidad de ejercitar los Derechos ARCO (derechos de acceso, rectificación, cancelación y oposición). No será necesario cuando se deduzca de la naturaleza de los datos o de las circunstancias.
  - ✓ Identidad y Dirección del Responsable de Fichero.
- Si se utilizan cuestionarios o formularios en la recogida de datos, estos deben contener, de manera claramente legible los anteriores puntos.
- Los datos pueden recogerse del propio titular o de un tercero:
  - ✓ Del titular: debe informarle con carácter previo a la recogida

- ✓ De un tercero: debe informar al titular dentro de los tres meses siguientes al registro de los datos. Hay excepciones a esta regla general reguladas en el Art.5.4 y 5.5: que ya hubiese sido informado, que lo prevea una ley, cuando el tratamiento tenga fines históricos, estadísticos o científicos, que resulte imposible o esa información exija esfuerzos desproporcionados, que los datos procedan de fuentes accesibles al público.

2-Principio de consentimiento (artículo 6 LOPD)**:**

- Regla general: Es fundamental contar con el consentimiento del afectado.
- En el caso que nos ocupa, se pueden recabar **datos especialmente protegidos**:
  - ✓ relativos a la ideología, afiliación sindical, religión y creencias. Es necesario el consentimiento expreso y por escrito del afectado, además se le debe informar previamente de su derecho a no prestarlo.
  - ✓ Relativos al origen racial, salud y vida sexual. Sólo podrán recabarse, tratarse o cederse cuando el afectado consienta expresamente o cuando lo disponga una ley.
  - ✓ Relativos a la comisión de infracciones penales o administrativas. Sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las normas reguladores correspondientes.
- Excepciones a la regla general:
  - ✓ Que la ley disponga otra cosa.
  - ✓ Que los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias.
  - ✓ Que los datos se refieran a las partes de un contrato, precontrato etc. y sean necesarios para su mantenimiento o cumplimiento.
  - ✓ Que el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado (prevención, diagnóstico médico, prestación de asistencia sanitaria, tratamientos médicos o gestión de servicios sanitarios) siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sometida a una obligación equivalente al secreto.
  - ✓ Que los datos figuren en fuentes accesibles al público.

- Creo conveniente informar del carácter revocable de este consentimiento del interesado para otorgar sus datos. Para ello el interesado debe alegar una causa justificada y que en cualquier caso esta revocación carece de efectos retroactivos.

3-Calidad de los Datos (artículo 4 LOPD)**:**

- Sólo debemos recabar los datos que sean necesarios para el cumplimiento de sus finalidades legítimas, explícitas y determinadas. Los datos recabados, por lo tanto, deben ser "adecuados, pertinentes y no excesivos" en relación con estas finalidades[56].
- Recabaremos los datos de manera lícita y leal. El Art. 4.7 prohíbe recoger datos por medios fraudulentos, desleales o ilícitos. Por lo tanto deberá cumplir con todo lo estipulado en la LOPD acerca de la recogida, que precisamente estoy analizando.

4-Deber de Secreto (artículo 10 LOPD):

- El Responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos están sometidos a la obligación de secreto profesional y al deber de guarda y custodia de los mismos incluso después de finalizar la relación laboral.
- Es obligación mantener informados y formados a todos los empleados, en este caso funcionarios a su servicio, que tengan acceso a datos de carácter personal en este deber de custodia. Sería aconsejable hacerlo de la siguiente forma:
    - ✓ cuando se trate de funcionarios de nueva incorporación, redactando una cláusula que lo contemple o un documento anexo que se incluirá en el procedimiento de integración del funcionario al servicio de la Administración de Justicia. El funcionario debe firmarlo y a partir de ese momento quedará sujeto a este deber que subsistirá incluso después de acabar su relación laboral con la Oficina Judicial.
    - ✓ cuando se trate de antiguos funcionarios. Por ejemplo: adjuntando a la nómina un documento de compromiso a este deber de secreto; publicándolo en los tablones de anuncios, en la intranet o por medio de sindicatos.

[56] El artículo 4.2 de la LOPD establece claramente que los datos de carácter personal no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

5-Seguridad de los Datos. (Artículo 9 LOPD). Queda configurada como una obligación del Responsable del Fichero la adopción de las medidas técnicas y organizativas necesarias que garanticen la seguridad de los datos y eviten la alteración, pérdida y tratamiento o acceso no autorizado, teniendo en cuenta la naturaleza de los datos y los riesgos a que están expuestos. Nos remite al Título VIII del RD 1720/2007.

6-Ejercicio de Derechos: Cuando he analizado anteriormente el principio de información, ya he mencionado como el artículo 5.1b) regulaba el deber de informar a los interesados a los que se le soliciten datos personales, de modo expreso, preciso e inequívoco de la posibilidad de ejercitar los derechos ARCO (Derecho de Acceso, Derecho de Rectificación, Derecho de Cancelación y Derecho de Oposición). Por tanto, en esta fase es importante que el interesado tenga conocimiento de la existencia de estos derechos y del contenido de los mismos.

FASE DE TRATAMIENTO:

1-Información al interesado:

- Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco.
- Ya vimos en la fase anterior, que cuando los datos no se recaban del interesado se dan una serie de excepciones al principio de información al interesado. En cualquier caso, en cada comunicación que se dirija al interesado se le debe informar del origen de los datos y de la identidad del responsable del tratamiento así como los derechos que le asisten.

2-Consentimiento del interesado:

- es imprescindible para poder llevar a cabo cualquier tratamiento de datos de carácter personal; puede recabarse de manera expresa o tácita (se debe informar al interesado en cada comunicación, de la existencia del fichero y de sus derechos).
- carácter revocable del consentimiento cuando exista causa justificada y no se le atribuyan efectos retroactivos.
- en el caso de **datos especialmente protegidos** ya vimos que es necesario:

- ✓ el consentimiento expreso y por escrito para poder tratar los datos relativos la ideología, afiliación sindical, religión y creencias.
- ✓ el consentimiento expreso en el caso de los datos relativos al origen racial, a la salud y a la vida sexual.

3-Calidad de los datos:

- Adecuación a la finalidad: Los datos no podrán usarse para finalidades incompatibles con aquellas para las que se recabaron los datos. No obstante podrán ser usados con fines históricos, estadísticos o científicos, ya que estos no se consideran incompatibles con la finalidad.
- Mantenimiento de los datos exactos y puestos al día: nos tenemos que regir por la situación actual del interesado. Esto implica una serie de obligaciones :
  - ✓ Deber de cancelar los datos cuando se le den casos de datos inexactos o incompletos. Ya veremos como este deber de cancelación en la práctica se traduce en un deber de bloqueo.
  - ✓ Deber de sustituir los datos inexactos o incompletos por otros que respondan con veracidad a la situación actual del interesado.
  - ✓ Deber de cancelación con respecto a los datos que hayan dejado de ser necesarios para la finalidad de las actividades llevadas a cabo en la Oficina Judicial. La ley prohíbe conservar datos durante un período superior al necesario para el cumplimiento de esa finalidad.
  - ✓ Este deber de cancelación/sustitución se ejerce "de oficio". Debe tomar la iniciativa en cuanto tenga conocimiento de estas situaciones mencionadas.

- Se deben almacenar los datos de manera que se permita el ejercicio, por el titular de los datos, de los Derechos ARCO.

4-Deber de secreto: En esta fase es fundamental la prestación de formación a los funcionarios para evitar que estos realicen tratamientos inadecuados de los datos de carácter personal que puedan originar responsabilidades a la organización.

Será de vital importancia diseñar un **Plan de Formación** en materia de protección de datos de carácter personal que se aplique al ámbito de la Oficina Judicial. Teniendo en cuenta la diversa naturaleza de los agentes que participan en la Administración de Justicia, es necesario que ese Plan de Formación esté estructurado por niveles.

La LO 6/1985 de 1 de Julio del Poder Judicial, bajo la denominación de personal al servicio de la Administración de Justicia, agrupa a los Secretarios Judiciales, Médicos Forenses, los Oficiales, Auxiliares y Agentes Judiciales así como los miembros de los Cuerpos que puedan crearse, por ley, para el auxilio y colaboración con los Jueces y Tribunales.

En el sistema judicial español nos encontramos, por tanto con las siguientes figuras de "empleados":

- ✓ Jueces y Magistrados.
- ✓ Fiscales.
- ✓ Secretarios Judiciales.
- ✓ Jueces de Paz
- ✓ Personal Administrativo: Oficiales, Auxiliares, Agentes y Médicos Forenses.

Por tanto el Plan de Formación que se implante en la Oficina Judicial, se estructurará teniendo en cuenta estos niveles o categorías mencionados. Es decir, se compondrá de unas medidas formativas genéricas o comunes a todos los niveles y otras específicas en función del nivel o categoría funcionarial.

Las competencias respecto de todo el personal al servicio de la Administración de Justicia, corresponde al Ministerio de Justicia, en todas las materias relativas a su Estatuto y régimen jurídico, comprendidas la selección, formación y perfeccionamiento, así como la provisión de destinos, ascensos, situaciones administrativas y régimen disciplinario.

5-Seguridad de los Datos: En esta fase la regulación de este apartado es la misma que la que he analizado en la fase anterior. Solo quiero añadir que en esta fase he contemplado el principio de Acceso a Datos por Terceros (Art. 12 LOPD), y que esta circunstancia debe ser contemplada en el Documento de Seguridad.

6-Acceso a los datos por cuenta de terceros (Artículo 12 de la LOPD):

- Tiene que darse una situación de necesidad por la cual se precise de los servicios de un tercero que llamaremos Encargado de Tratamiento.
- Esta relación por la cual el Encargado de Tratamiento presta un servicio a la Oficina Judicial tiene que regularse en un contrato. Yo aconsejaría que se hiciese por escrito, aunque la ley permite cualquier forma que permita dejar constancia de su celebración y contenido. En este contrato debe especificarse:

- ✓ Que el R.F [57]de la Oficina Judicial será quien decida sobre la finalidad del tratamiento que realizará el Encargado de Tratamiento, por lo tanto este último está obligado a seguir las instrucciones del R.F de la Oficina Judicial y no podrá utilizar los datos a los que tiene acceso para fines distintos a los especificados ni podrá comunicar estos datos ni siquiera para su conservación.
- ✓ las medidas de seguridad que debe adoptar el Encargado de Tratamiento.
- ✓ una cláusula en la que se indique que una vez cumplida la prestación del servicio por el Encargado de Tratamiento, éste debe destruir los datos y los soportes o documentos en los que consten o devolverlos a la Oficina Judicial. Aconsejaría que se añadiera una disposición a esta cláusula que permitiera a la Oficina Judicial elegir sobre las dos opciones a las que está obligado el Encargado.

• en caso de incumplimiento de lo estipulado en el mencionado artículo 12 de la LOPD por parte del Encargado de Tratamiento deberá responder por tal incumplimiento.

7-Ejercicio de Derechos:

DERECHOS ARCO: Este conjunto de derechos que analizaré a continuación tienen una serie de características comunes:

- Son derechos personalísimos, por lo tanto sólo podrán ejercerse por el afectado o por su representante legal o voluntario. Todos deberán acreditar su identidad (Art. 23 RD 1720).
- Son derechos independientes: el ejercicio de uno de ellos no es requisito previo para el ejercicio de los otros.
- Se debe ofrecer un medio sencillo y gratuito para el ejercicio de estos derechos por parte del interesado, que en ningún caso le suponga un ingreso adicional. Por ejemplo no podrá imponer como medio para el ejercicio de estos derechos al interesado el envío de cartas certificadas, utilización de servicios de

[57] R.F: Responsable de Fichero. Ya vimos como en el caso de los Ficheros Jurisdiccionales, podía ser el órgano judicial (Ficheros de Asuntos Jurisdiccionales), o el secretario judicial (Ficheros de Registro de Asuntos).

telecomunicaciones que impliquen tarificación adicional o cualquier otro medio que suponga un coste excesivo para el interesado.

- Si se dispusiese de un Servicio de Atención al ciudadano puede conceder la posibilidad al interesado de ejercitar sus derechos ARCO a través de dicho servicio.
- Se deberá atender siempre las solicitudes del interesado, cuando éste haya utilizado un medio que permita acreditar el envío y recepción de la solicitud y esta contenga unos requisitos que analizaré en el siguiente punto.
- Salvo en los supuestos en que el interesado utilice el Servicio de Atención al Ciudadano de la Oficina Judicial para ejercitar sus Derechos ARCO., este debe dirigirse a la Oficina Judicial a través de una **Solicitud** (de Acceso, de Rectificación, de Cancelación o de Oposición) que debe recoger:
  - ✓ Nombre y Apellidos del interesado. Debe adjuntar una fotocopia del documento que acredite su identidad salvo que utilice la vía de la firma electrónica.
  - ✓ Petición en que se concreta su solicitud.
  - ✓ Dirección. Fecha y firma.
  - ✓ Documentos acreditativos de la petición que formula.

- Si la Solicitud del interesado no reúne los requisitos fijados, es preciso ponerse en contacto con él para que lo corrija.
- Es importante que se guarde prueba del cumplimiento del deber de respuesta.
- Se Formará e Informará a todos los funcionarios para que estos puedan asesorar a los ciudadanos acerca de los procedimientos a seguir para el ejercicio de los D. ARCO.

A) DERECHO DE ACCESO:

- Se concreta en un derecho del ciudadano titular de los datos de carácter personal a obtener información sobre si sus datos están siendo objeto de tratamiento, finalidad de dicho tratamiento, origen de dichos datos, y comunicaciones previstas o realizadas.

- Se puede solicitar al interesado que ejerce este derecho la especificación de los ficheros respecto de los cuales quiere obtener dicha información, para eso debe facilitársele una relación de todos los ficheros en los que haya datos suyos.
- El interesado puede optar por recibir la información a través de varios sistemas de consulta: por escrito, copia o fotocopia, visualización en pantalla, correo electrónico etc. Estos sistemas pueden restringirse, pero siempre deben ser gratuitos y debe garantizarse la comunicación escrita.
- Se debe cumplir, al facilitar el acceso, lo establecido en el Título VIII del RD 1720 que regula las medidas de seguridad.
- Se debe responder en el plazo máximo de 1 mes, tanto si tiene datos del interesado como si no los tuviese. La información que en su caso se proporcione debe ser inteligible y comprenderá tanto los datos de base como los resultantes del tratamiento.
- Se puede denegar el acceso cuando lo disponga una ley o si ya se ha ejercido en los 12 meses anteriores, salvo que el interesado acredite un interés legítimo.

B) DERECHO DE RECTIFICACIÓN Y CANCELACIÓN: Voy a analizarlos en el mismo apartado ya que tienen varios puntos en común.

- **El Derecho de Rectificación** es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos. Cuando se solicite por el interesado la rectificación de determinados datos éste debe indicar en la solicitud a que datos se refiere y la corrección que quiere que se practique y deberá aportar la documentación justificativa.
- **El Derecho de Cancelación** es el derecho del afectado a que se supriman los datos que resulten ser inexactos, incompletos, inadecuados o excesivos en relación con la finalidad, y también los que hayan dejado de ser necesarios para el fin para el cual se recabaron. Ya veremos como en la mayoría de los casos implica un *deber de bloqueo*[58]. El interesado debe indicar en su solicitud de cancelación a qué datos se refiere y deberá aportar también la documentación justificativa.

[58] deber de conservarlos para ponerlos a disposición de las Administraciones Públicas, de los Jueces y Tribunales para atender a las posibles responsabilidades nacidas del tratamiento durante los plazos de prescripción de éstas. Cumplidos los citados plazos ya puede proceder a la **Supresión** de los datos.

- Se dispone de un plazo máximo de 10 días desde la recepción para resolver sobre una solicitud de Cancelación o Rectificación. Debe responderse en todo caso, tanto si tiene datos del afectado como si no.
- Es importante comunicar la Cancelación o Rectificación de los datos en los casos en que hubiese habido cesión o comunicación. Por lo tanto tiene que comunicar a sus cesionarios de datos para que estos en el mismo plazo de 10 días procedan a practicar a los datos cedidos esa cancelación o rectificación.
- Se puede denegar los derechos de Cancelación o Rectificación:
  - ✓ Cuando así lo prevea una ley o una norma de d. comunitario.
  - ✓ Cuando los datos deban ser conservados por la existencia de una relación contractual que justificó el tratamiento.

- Quiero hacer un inciso para explicar que nunca se deben cancelar o suprimir los datos directamente. Una vez que responde afirmativamente a una Solicitud de Cancelación debe proceder al **Bloqueo de los datos**, es decir, debe conservarlos pero únicamente para ponerlos a disposición de las Administraciones Públicas, de los Jueces y Tribunales para atender a las posibles responsabilidades nacidas del tratamiento durante los plazos de prescripción de éstas. Cumplidos los citados plazos ya puede proceder a la **Supresión** de los datos.

C) DERECHO DE OPOSICIÓN:

- La ley y su Reglamento [59]definen este derecho como la facultad que asiste al afectado para impedir el tratamiento de sus datos personales o se cese en el mismo cuando se den los siguientes supuestos:
  - ✓ En los casos en que no sea necesario su consentimiento para el tratamiento y alegue un motivo fundado y legítimo referido a una concreta situación personal, siempre que la ley no establezca lo contrario.
  - ✓ Cuando se trata de Ficheros con finalidades de publicidad y prospección comercial.

[59] LOPD y RD 1720/2007

- ✓ Cuando se trate de tratamientos destinados a la adopción de decisiones con efectos jurídicos basadas únicamente en un tratamiento automatizado de sus datos.

- Se dispone de un plazo de 10 días, desde la recepción de la solicitud de oposición. Debe responder al afectado en todo caso, aunque sólo sea para comunicarle que en sus ficheros no constan sus datos personales.

DERECHO DE TUTELA:

- Es el derecho que asiste al interesado para solicitar la debida protección ante la Agencia Española de Protección de Datos cuando se encuentre ante una situación de desamparo debido a:
  - ✓ Actuaciones contrarias a lo dispuesto en la LOPD.
  - ✓ Cuando no se responda debidamente ante el ejercicio de sus D. ARCO. Es decir, cuando se le deniegue total o parcialmente su solicitud de acceso, rectificación, cancelación u oposición, o cuando no se le responda o se le responda fuera de plazo.

- Siempre que se deniegue, total o parcialmente, alguno de los derechos ARCO que ejercita el interesado, deberá incluir en la ya mencionada *obligatoria respuesta* al afectado la debida información referida al derecho que le asiste a recabar la tutela de la AEPD recogido en el Art. 18 de la LOPD.
- Quiero mencionar que la AEPD dispone de 6 meses para pronunciarse sobre la concesión de tutela.

DERECHO DE CONSULTA AL REGISTRO GENERAL DE PROTECCIÓN DE DATOS:

- El derecho que asiste a cualquier ciudadano a dirigirse al mencionado Registro y recibir información acerca de si sus datos de carácter personal están siendo objeto de algún tratamiento, finalidades de ese tratamiento y la identidad del responsable de ese tratamiento. Está regulado en el artículo 14 de la LOPD.
- La consulta a este Registro se caracteriza por ser pública y gratuita.

DERECHO DE INDEMNIZACIÓN: Art. 19 LOPD.

- Cuando a consecuencia del incumplimiento de lo dispuesto en la LOPD algún ciudadano (persona física) sufra daño o lesión en sus bienes o derechos, tendrá derecho a ser indemnizado.
- Al tratarse de ficheros de titularidad pública, la responsabilidad debe exigirse de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas, en este caso, de la Administración de Justicia.

DERECHO DE IMPUGNACIÓN DE VALORACIONES: Art. 13 LOPD.

- Podemos definirlo como el derecho que asiste al ciudadano a no verse sometido a decisiones con efectos jurídicos basadas únicamente en tratamientos de datos que tengan como objetivo valorar o evaluar aspectos de su personalidad.
- En estos casos el ciudadano podrá impugnar esas decisiones o actos administrativos.
- Además, el ciudadano, tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizado en el tratamiento que sirvió para adoptar la decisión.
- Los resultados de esas valoraciones o evaluaciones obtenidas del tratamiento de esos datos, únicamente tendrá valor probatorio a petición del interesado o afectado.

FASE DE UTILIZACIÓN/COMUNICACIÓN DE LOS RESULTADOS DEL TRATAMIENTO.

Si la Oficina Judicial tiene previsto realizar algún tipo de Comunicación o Cesión de los datos contenidos en sus Ficheros es esencial que lo haga saber a los titulares de los mismos a fin de que estos den su consentimiento. Como vemos en esta fase vuelve a ser esencial el **Principio de información** al interesado. A tal punto es importante, que la Ley contempla la posibilidad de declarar nulo el consentimiento prestado para la comunicación de datos a un tercero cuando la información previa dada al interesado no sea suficiente para conocer la finalidad o el tipo de actividad a que se destinarán los datos.

Aquel a quien se comuniquen los datos se obliga, por el sólo hecho de la comunicación o cesión a la observancia de las mismas disposiciones que marca la LOPD. Por lo tanto en esta fase rige también los apartados que ya he analizado en las fases anteriores, como la Adopción de medidas de seguridad, el Deber de secreto, el Acceso a Datos por cuenta de Terceros, etc.

1-Principio de información: Es necesario mantener al interesado correcta y adecuadamente informado de toda revelación, comunicación o cesión de sus datos de carácter personal.

2-Principio del Consentimiento:

- Es preciso contar con el consentimiento previo del interesado para llevar a cabo una comunicación o cesión de datos. Hay una serie de excepciones a esta regla general reguladas en el Art. 11 de la LOPD, que pueden afectar a la Oficina Judicial en el caso que nos ocupa:
    - ✓ Que la cesión esté autorizada por Ley.
    - ✓ Que se trate de datos procedentes de Fuentes accesibles al público.
    - ✓ Cuando exista una relación jurídica, libre y legítimamente aceptada que implique dicha conexión de ficheros.
    - ✓ Cuando la comunicación tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será necesario el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
    - ✓ Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
- También quiero mencionar que la Oficina Judicial debe prever supuestos de revocación del consentimiento por parte del interesado cuando este quiera ejercer su derecho de oposición.
- El consentimiento para la comunicación de datos de carácter personal a un tercero será nulo, cuando la finalidad a la que se destinan esos datos o el tipo de actividad a

la que se dedica el cesionario no quedan suficientemente claras en la información que se debe facilitar al interesado.

- Si la Oficina Judicial realiza comunicación de datos utilizando previamente procedimientos de disociación, que impidan asociar esos datos con una persona física identificada o identificable no es necesario que se ajuste a lo dispuesto en el mencionado Art.11.

3-Calidad de los datos:

- En esta fase también tiene su protagonismo el principio de calidad de los datos ya que la ley exige que la comunicación de los datos reúna el *requisito de la adecuación al fin.* En el Art. 11 de la LOPD claramente se especifica que "*los datos de carácter personal objeto de tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y cesionario"*.
- En esta fase sigue persistiendo la obligación de mantener los datos exactos y puestos al día, con las obligaciones que esto implica tanto al cedente como al cesionario, de cancelar y sustituir los datos que resulten ser inexactos o incompletos, cancelar los datos que dejen de ser necesarios al fin de la comunicación etc., etc.
- Los datos deben ser almacenados de manera compatible con el ejercicio de los Derechos ARCO por parte del interesado.

4-Datos especialmente protegidos:

- El artículo 7 de la LOPD nos remite al artículo 16.2 de la Constitución Española en el que se especifica que nadie puede ser obligado a declarar sobre su ideología, religión y creencias, y por lo tanto cuando se proceda a recabar el consentimiento del interesado para proceder a la cesión o comunicación de sus datos se le advertirá del derecho que le asiste a no prestarlo.
- En el artículo 7 se distinguen dos grupos de datos de esta índole
    - ✓ Ideología, afiliación sindical, religión y creencias, exige el consentimiento expreso y por escrito del afectado.

- ✓ origen racial, a la salud y a la vida sexual, es preciso el consentimiento expreso del afectado salvo que una ley disponga otra cosa por razones de interés general.

- los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

5-Seguridad de los Datos y deber de Secreto: En esta fase la regulación de este apartado es la misma que la que he analizado en las fases anteriores. Solo quiero añadir que en esta fase he contemplado el principio de Comunicación de datos (artículo 11 LOPD), y que esta circunstancia debe ser contemplada en el Documento de Seguridad.

6-Comunicación de datos (artículo 11 de la LOPD):

- Los datos de carácter personal objeto de tratamiento pueden ser comunicados a terceros siempre que se cumplan unos requisitos:
  - ✓ que la finalidad de esa comunicación sea el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.
  - ✓ que se cuente con el consentimiento previo del interesado. Ya vimos como esta necesidad de consentimiento tenía una serie de excepciones.
- Es importante tener en cuenta que el cesionario de esos datos de carácter personal se obliga, con esa comunicación, a la observancia de las disposiciones de la LOPD.
- Si la comunicación se realiza precedida de un procedimiento de disociación que impida relacionar esos datos con sus titulares, no será aplicable lo establecido en los apartados anteriores de este artículo 11 de la LOPD.

7-Acceso a los datos por cuenta de un tercero (artículo 12 LOPD): En esta fase también puede darse la circunstancia de que se plantee la necesidad de prestación de un servicio a los responsables del tratamiento. Esta prestación de servicios por parte de un tercero que pueda tener acceso a los datos no se considera una comunicación de datos. Ya

vimos en la anterior fase como esta relación debe regularse en un contrato que debe tener ciertas características, por lo que me remito a lo desarrollado ya con anterioridad.

8-Ejercicio de Derechos: En esta fase el interesado puede ejercer todos y cada uno de los derechos que ya he analizado en la Fase anterior, pero quiero hacer hincapié en uno que apenas he comentado y que creo que es más propio de esta Fase:

DERECHO DE IMPUGNACIÓN DE VALORACIONES:

- Regulado en el Art. 13 de la LOPD y en el 36 del RD 1720, consiste en el derecho de los interesados a no verse sometidos a decisiones con efectos jurídicos que se basen únicamente en tratamiento automatizado de datos destinados a evaluar aspectos de su personalidad como su rendimiento laboral, crédito, fiabilidad o conducta. De acuerdo con este derecho el interesado podrá impugnar este tipo de decisiones.
- la Oficina Judicial tiene que prever que el interesado pueda solicitarle información sobre los criterios de valoración y el programa que ha utilizado en los tratamientos por los cuales ha adoptado tales decisiones. La Oficina Judicial tendrá que facilitarle dicha información.
- No obstante el RD 1720 contempla en el Art.36.2 una serie de excepciones a este derecho:
    - ✓ que exista un contrato, a petición del interesado. En este caso se debe dar al interesado la posibilidad de formular alegaciones a fin de defender sus derechos e intereses. La Oficina Judicial deberá informar al interesado, de forma clara precisa, de que se van a adoptar este tipo de decisiones referidas a él.
    - ✓ que esté autorizado por ley. En este caso deben contemplarse también por ley medidas que garanticen el interés legítimo del interesado.

9.6.-PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EN EL ÁMBITO DEL SISTEMA INFORMÁTICO DE TELECOMUNICACIONES LEXNET.

El artículo 3 del RD 84/2007, de 26 de Enero, sobre implantación en la Administración de Justicia del sistema informático de telecomunicaciones Lexnet para la presentación de escritos y documentos, el traslado de copias y la realización de actos

de comunicación procesal por medios telemáticos, establece que es preciso adaptar la aplicación de este Real Decreto a la LOPD y su normativa de desarrollo.

Además de esto, siguiendo el mandato del artículo 20 de la LOPD, el RD 84/2007 procede a crear los ficheros automatizados previstos en el Anexo I del mismo:

- **Nombre del Fichero**: Custodia de la información acreditativa de las transacciones realizadas
  - **Finalidad y usos previstos del fichero**: Registro, custodia y conservación segura de los documentos electrónicos acreditativos de las transacciones telemáticas.
  - **Personas o colectivos titulares de los datos**: Los usuarios del sistema y cualquier sujeto interviniente en los procesos judiciales.
  - **Procedimiento de recogida de los datos**: Los datos que figuran en los resguardos electrónicos que se generan automáticamente por el sistema proceden de las relaciones de campos a cumplimentar por los usuarios.
  - **Estructura básica del fichero y descripción de los tipos de datos incluidos**: Datos e información contenida en los resguardos electrónicos referente a:

    - ✓ la identidad del remitente y del destinatario de cada mensaje,
    - ✓ fecha y hora de su efectiva realización proporcionada por el sistema,
    - ✓ proceso judicial al que se refiere, indicando tipo de procedimiento, número y año, así como los escritos y notificaciones, los acuses de recibo, diligencias, recibís o cualquier otro mensaje procesal transmitido por medios telemáticos a que se refiere el apartado 4 del artículo 6 de este real decreto.

  - **Cesiones de datos o transferencia**: No se prevén.
  - **Órganos de las Administraciones responsables del fichero**: Subdirección General de Nuevas Tecnologías de la Justicia. Dirección General de Relaciones con la Administración de Justicia. Secretaría de Estado de Justicia. Ministerio de Justicia.
  - **Servicios o unidades ante los que ejercer los derechos de acceso, rectificación, cancelación y oposición**: Subdirección General de Nuevas Tecnologías de la Justicia. Dirección General de Relaciones con la Administración de Justicia. Secretaría de Estado de Justicia. Ministerio de Justicia.
  - **Las medidas de seguridad, con indicación del nivel exigible**: Se adoptarán todas las medidas de seguridad correspondientes al nivel alto, previstas en el RD

994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

- **Nombre del Fichero**: Gestión de usuarios del sistema Lexnet
  - **Finalidad y usos previstos del fichero**: Disponer de una relación actualizada de usuarios que tengan acceso autorizado al sistema Lexnet, a efectos de la actividad de gestión de usuarios y de establecer mecanismos o procedimientos de identificación y autenticación para dicho acceso.
  - **Personas o colectivos titulares de los datos**: Los relacionados en el Anexo II de este Real Decreto.
  - **Procedimiento de recogida de los datos**: Suministrados por el propio interesado a través de proceso de alta.
  - **Estructura básica del fichero y descripción de los tipos de datos incluidos**:
    - ✓ Datos de identificación y de contacto: DNI o NIE, nombre, apellidos, dirección de correo electrónico y parte pública del certificado de usuario.
    - ✓ Datos profesionales indicadores de la calidad de la intervención en el proceso judicial: Cuerpo, Escala, Carrera o Colectivo profesional de pertenencia. Órgano, Unidad de destino o adscripción.
  - **Cesiones de datos o transferencia**: No se prevén.
  - **Órganos de las Administraciones responsables del fichero**: Subdirección General de Nuevas Tecnologías de la Justicia. Dirección General de Relaciones con la Administración de Justicia. Secretaría de Estado de Justicia. Ministerio de Justicia.
  - **Servicios o unidades ante los que ejercer los derechos de acceso, rectificación, cancelación y oposición:** Subdirección General de Nuevas Tecnologías de la Justicia. Dirección General de Relaciones con la Administración de Justicia. Secretaría de Estado de Justicia. Ministerio de Justicia.
  - **Las medidas de seguridad, con indicación del nivel exigible**: Se adoptarán todas las medidas de seguridad correspondientes al nivel básico previstas en el RD 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

A estos ficheros de datos de carácter personal que resultan de la utilización por parte de los usuarios del sistema Lexnet, se les debe aplicar la normativa establecida en la LOPD.

9.7.-PROBLEMÁTICA DE PROTECCIÓN DE DATOS QUE PLANTEA EL DNI ELECTRÓNICO Y LA PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN.

Una de las características que plantea el DNI electrónico es que toda la información relevante de la persona se encuentra reflejada en dicho documento de dos maneras diferentes:

- Por un lado tenemos los datos relativos al titular impresos en la tarjeta como si de un DNI normal se tratara, lo que facilita conocer la identidad de una persona.
- Por otro lado la tarjeta incluye un chip donde se incluyen los datos personales, la fotografía, firma manuscrita digitalizada y huella dactilar digitalizada, junto con los certificados de autenticación y de firma electrónica, que son los datos que hacen posible la confirmación electrónica de que el titular cuyos datos aparecen en la tarjeta, es quien dice ser.

En dicho chip también encontramos el certificado electrónico de que la autoridad emisora de la autenticación y la firma electrónica está autorizada para conceder los mismos. De la misma manera, se incluyen las dos claves de cada certificado electrónico, la clave pública y la clave privada. Estos datos se alojan en dos zonas diferentes del chip: zona pública y zona privada. En la primera se alojan los datos básicos de los certificados y la clave pública y para acceder a la misma no hay restricción alguna. En la segunda se encuentran las claves privadas del ciudadano, el certificado de identidad del mismo y el certificado de firma correspondiente; esta zona será únicamente accesible por contraseña o a través de los datos biométricos del titular del mismo.

Existe también una zona de seguridad que es únicamente accesible por el ciudadano a través de su número de identificación personal o PIN[60], existiendo un procedimiento de acceso a disposición de la Administración. En esta zona se detecta la siguiente información: datos biométricos[61], datos de filiación del ciudadano y el número de serie de la tarjeta.

[60] PIN: Personal Identification Number o Número de Identificación Personal.
[61]. En las TIC la autenticación biométrica se refiere a las tecnologías para medir y analizar las características físicas y del comportamiento de la persona para poder autentificar.

La Ley 59/2003 de Firma Electrónica define en el artículo 15 el DNI electrónico como "el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos", agregando además que "todas las personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los distintos dispositivos de firma electrónica en él incluidos".

Según este precepto, los certificados electrónicos incorporados en el DNI electrónico cumplen una doble función:

- ✓ identificar a su titular en las relaciones telemáticas.
- ✓ garantizar la autenticidad e integridad de los documentos rubricados.

En cuanto a sus requisitos y características, la ley de Firma Electrónica es clara al establecer que:

- Los órganos competentes del Ministerio del Interior, para la expedición del DNI electrónico cumplirán las obligaciones que la presente ley impone a los prestadores de servicios de certificación que expidan certificados reconocidos con excepción de la relativa a la constitución de la garantía a la que se refiere el artículo 20.2.
- La Administración General del Estado empleará en la medida de lo posible, sistemas que garanticen la compatibilidad de los instrumentos de firma electrónica incluidos en el DNI electrónico con los distintos dispositivos y productos de firma electrónica generalmente aceptados.

Los artículos 13 y 14 de la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos admitían como medio de identificación y autenticación de los ciudadanos para relacionarse por medios electrónicos con las Administraciones Públicas los sistemas de firma electrónica incorporados al DNI electrónico para personas físicas.

Efectivamente, el DNI electrónico se ha convertido en una herramienta de gran utilidad para facilitar la gestión informativa referente a personas físicas, pero puede plantear problemas de confrontación con la normativa de protección de datos de carácter personal.

Los datos de carácter personal necesarios para la expedición del DNI electrónico son recabados por la Dirección General de la Policía, la cual, según lo previsto en el artículo 3.2 del RD 1553/2005 por el que se regula la expedición del DNI electrónico y sus certificados de firma electrónica, es responsable de la emisión de los certificados de firma electrónica reconocidos y de la custodia de los archivos y ficheros, automatizados o no, relacionados con el DNI. Por lo tanto, la Dirección General de la Policía quedará sometida a las obligaciones impuestas al Responsable de Fichero por la LOPD.

Ya vimos como el DNI electrónico incluía dos tipos de certificados reconocidos: un certificado de autenticación dirigido a identificar al usuario de un servicio y un certificado de no repudio que permite firmar electrónicamente documentos electrónicos. En ambos casos se precisa la figura de una tercera parte de confianza: el prestador de servicios de certificación, que expide los certificados a los usuarios y debe responder de que los mismos se generen de forma segura y de la vigencia de éstos, según establece el artículo 10 de la Ley de Firma Electrónica.

Es muy probable que se de la circunstancia de que los titulares de los datos de carácter personal de esos certificados contenidos en el DNI electrónico desconozcan la información contenida en ellos y las interconexiones de informaciones que se originan cuando conectan su DNI electrónico a un lector de tarjetas de un terminal.

La Ley 59/2003 de Firma Electrónica ya preveía esto, cuando en su artículo 17 establecía que:

- El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta ley se sujetará a lo dispuesto a la LOPD.
- Para la expedición de certificados electrónicos al público, los prestadores de servicios de certificación únicamente podrán recabar datos personales directamente de los firmantes o previo consentimiento expreso de estos.

Los datos requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado electrónico y la prestación de otros servicios en relación con la firma electrónica, no pudiendo tratarse con fines distintos sin el consentimiento expreso del firmante.

- Los prestadores de servicios de certificación que consignen un seudónimo en el certificado electrónico a solicitud del firmante deberán constatar su verdadera identidad y conservar la documentación que la acredite.

Dichos prestadores de servicios de certificación estarán obligados a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la LOPD.

- En cualquier caso, los prestadores de servicios de certificación no incluirán en los certificados electrónicos que expidan, los datos a los que se hace referencia en el artículo 7 de la LOPD (datos especialmente protegidos).

9.8.-CAMARAS DE VIDEOVIGILANCIA

La imagen de una persona obtenida a través de una cámara de video vigilancia constituye un dato de carácter personal, y por lo tanto, su tratamiento debe estar sometido a las disposiciones de la LOPD y su normativa de desarrollo.

La LOPD establecía en su primer artículo que su objeto era garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

En lo que se refiere al ámbito de aplicación de esta norma, se determina que será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de esos datos por los sectores público y privado. Encontramos el concepto de dato de carácter personal definido en el artículo 3.a) de la citada norma cuando se nos dice que es “cualquier información concerniente a personas físicas identificadas e identificables”.

Ya hemos visto como la LOPD establece el concepto de tratamiento de datos al definirlo como “operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”. Como vemos, la garantía del derecho a la protección de datos precisa la existencia de una actuación que constituya un tratamiento de datos de carácter personal en el sentido definido por la Ley. Y si nos ajustamos a la definición de tratamiento que ofrece la LOPD la grabación de imágenes de personas en espacios públicos constituye un tratamiento de datos personales que entra dentro del ámbito de aplicación de la norma.

El artículo 3 de la Instrucción 1/2006 de la Agencia de Protección de datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras establece que los responsables que cuenten con sistemas de video vigilancia deberán cumplir con el deber de información previsto en el artículo 5 de la LOPD, de tal modo que deberán:

- ✓ colocar en las zonas video vigiladas un distintivo informativo colocado en un lugar suficientemente visible, tanto en espacios abiertos como cerrados.
- ✓ tener a disposición de los interesados impresos en los que se detalle la información prevista en el artículo 5.1 de la LOPD.

• Un ejemplo de Cláusula de video vigilancia sería el siguiente:

De conformidad con lo dispuesto en el artículo 5.1de la LO 15/1999 de 13 de diciembre de Protección de Datos de Carácter personal se informa:

1.que sus datos personales se incorporarán al fichero denominado…y/o serán tratados con la finalidad de seguridad a través de un sistema de video vigilancia.

2.que el destinatario de sus datos personales es:

- **la empresa de seguridad.**
- **responsable de la Oficina Judicial.**

Como vemos, es muy importante identificar a la autoridad responsable del control de las imágenes, de está manera, el interesado sabrá a donde dirigirse en caso de que quieran conocer sus derechos.

La instalación de sistemas de video vigilancia tendrá lugar, según la previsión legal, cuando la vigilancia no pueda realizarse por otros medios, y deberá llevarse a cabo por servicios técnicos autorizados.

Bajo ningún concepto se pueden grabar imágenes de zonas ajenas a las instalaciones donde está situada la cámara, es decir, que no podremos dirigir la posición de la cámara hacia la calle, por ejemplo.

Las imágenes captadas por las cámaras deberán ser destruidas en el plazo de un mes, después de ser grabadas (artículo 8 de la LO 4/1997 [62]por la que se regula la

[62] LO 4/1997 de 4 de agosto por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

utilización de las videocámaras), ya que se consideran datos de carácter personal, y por lo tanto, solo podrán ser tratadas por el responsable o autoridades competentes, quedando prohibida su utilización y acceso a terceros.

Según el mismo artículo 8 "cualquier persona que por el ejercicio de sus funciones tenga acceso a las grabaciones deberá observar la debida reserva, confidencialidad y sigilo en relación con las mismas, siéndole de aplicación, en caso contrario, lo dispuesto en el artículo 10 de la presente Ley"

Hay que tener en cuenta que la cámara aunque no grabe, recoge las imágenes lo que supone un tratamiento de datos en los términos contemplados por la LOPD en el artículo 3.c), y además si tenemos en cuenta el artículo 6.1 de la Ley afirmaremos que es imprescindible el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

La utilización de videocámaras para la vigilancia será posible siempre que no exista identificación de las personas que aparecen en las mismas o en caso de existir que no sean incorporadas a un fichero, ya que si no necesitaríamos el consentimiento del interesado y por lo tanto habría que informar de esta circunstancia a quienes pudieran aparecer en las imágenes, debiendo además el fichero resultante, ser inscrito en el Registro General de Protección de Datos como establece el artículo 26 de la LOPD.

La video vigilancia puede plantear un conflicto entre dos derechos: el derecho a la intimidad y el de la vigilancia de la seguridad ciudadana.

Efectivamente, el derecho fundamental al honor, la intimidad y la propia imagen, contemplado en el artículo 18.1 de la Constitución como tal derecho fundamental, y en el artículo 20 como límite al ejercicio de las libertades contempladas en el artículo, puede en algunos casos llegar a situaciones de confrontación con el derecho a la seguridad, a la integridad, e incluso a la propia vida que los poderes públicos deben proteger. Por ello, es inevitable, que en caso de conflicto de derechos, se estudien las circunstancias de cada caso en concreto y valorar si en determinadas situaciones es preferible perder un poco de intimidad si con ello logramos encontrarnos más seguros, ya que hay que tener en cuenta que la inseguridad también supone una pérdida de libertad personal.

Como ya he mencionado anteriormente, es necesario, en todo caso, informar al ciudadano de la existencia de las cámaras, aunque no de su ubicación, y la autoridad responsable de su control tal y como dispone el artículo 9.1 de la LO 4/1997 por la que se regula la utilización de las videocámaras.

La no información del emplazamiento se debe a razones de seguridad y de eficacia, aunque en la mayoría de los casos suelen ser fácilmente localizables.

También es interesante resaltar que el artículo 9.2 de la Ley prevé el derecho de acceso y cancelación por cualquier interesado, pero se establecen una serie de garantías de la seguridad para que no surta efecto ese derecho de acceso.

10.-SISTEMA INFORMÁTICO LEXNET. COMERCIO ELECTRÓNICO

El RD 84/2007, de 26 de Enero, implanta en la Administración de Justicia el sistema informático de telecomunicaciones Lexnet para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos.

La Administración de Justicia acomete un proceso de modernización de su estructura y sus medios con el fin de dar servicio a los ciudadanos con mayor agilidad, calidad y eficacia, aplicando los métodos de organización e instrumentos procesales más modernos y avanzados a que se refiere el Preámbulo de la Carta de los Derechos de los Ciudadanos ante la Justicia[63].

La implantación del sistema informático Lexnet se enmarca en el Plan de Modernización de la Administración de Justicia,[64] que exige, para lograr una realidad judicial informatizada, la incentivación del uso de nuevas tecnologías en los sistemas de gestión procesal, para que las formas de trabajo desempeñadas en las Oficinas Judiciales evolucionen y se adapten a la Sociedad de la Información, requisito imprescindible para alcanzar una atención de calidad a los ciudadanos.

El artículo 230.2 de la Ley Orgánica del Poder Judicial establecía la posibilidad de que tanto los órganos judiciales, como las personas que demanden ante ellos la tutela judicial de sus derechos e intereses utilicen en sus relaciones cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, compatibles entre si, siempre que estas se produzcan en condiciones de seguridad, autenticidad, integridad, constancia fehaciente de su realización y del momento en que se efectúen, con garantías de confidencialidad de los datos de carácter personal, así como con respeto de las garantías y requisitos previstos en las leyes de procedimiento.

El sistema Lexnet está constituido por un sistema basado en correo electrónico securizado que proporciona máxima seguridad y fiabilidad en la comunicación mediante el empleo de **firma electrónica reconocida**. A las garantías de autenticidad, integridad y no repudio que proporciona la firma electrónica reconocida, el sistema añade, mediante los mecanismos técnicos adecuados, la de confidencialidad en las comunicaciones y la de sellado de tiempo.

[63] Proposición no de Ley aprobada por el Pleno del Congreso de los Diputados en abril del 2002.

[64] Aprobado por el Consejo de Ministros el 18/09/2009.

En cualquier caso, la utilización y funcionamiento del sistema Lexnet se regirá, en lo que resulte aplicable, por la Ley Orgánica del Poder Judicial, por la Ley de Enjuiciamiento Civil, por la LOPD, por la Ley de Firma Electrónica y por la Instrucción 2/2003 del Pleno del Consejo General del Poder Judicial por la que se aprueba el Código de conducta para usuarios de equipos y sistemas informáticos al servicio de la Administración de Justicia y por lo establecido en la demás normativa que pudiera resultar de aplicación en el ámbito de la Administración de Justicia.

La instauración de la vía telemática para la realización de determinados actos procesales, no excluye la utilización de la ya existente en la actualidad, sino que constituye una opción más que abre otras posibilidades a los litigantes, a los profesionales que les asistan, y a los demás intervinientes en el proceso en sus relaciones con la Administración de Justicia. Con ello, quedan ampliados y facilitados los cauces en el acceso a la tutela judicial.

En el ámbito de la Administración de Justicia, los interlocutores en las comunicaciones telemáticas son los sujetos intervinientes en los procesos judiciales. En un lado de la relación están los Secretarios Judiciales y los funcionarios de los cuerpos al servicio de la Administración de Justicia que desempeñan sus funciones en la Oficina Judicial, y en el otro, las personas que demandan la tutela judicial, los profesionales que les asisten y otras personas e instituciones que también se relacionan con los Juzgados y Tribunales. Como vemos, esta regulación no contiene ninguna exclusión al respecto.

El artículo 162.1 de la Ley de Enjuiciamiento Civil, impone a las partes y a los profesionales que intervengan en el proceso el deber de comunicar a su interlocutor el hecho de disponer de los indicados medios y su dirección y, por otro lado, que razones técnicas y de prudencia aconsejan abordar la instauración, admitiendo inicialmente como usuarios sólo a algunos interlocutores de la Administración de Justicia, sin perjuicio de que en el futuro puedan incorporarse otros colectivos.

Es interesante constatar, como el artículo 4 del RD 84/2007 [65]establece que la utilización del sistema Lexnet será obligatoria para los Secretarios judiciales y para los funcionarios de los Cuerpos al servicio de la Administración de Justicia, destinados en aquellas Oficinas Judiciales que dispongan del sistema y estén dotadas de los medios técnicos necesarios

[65] RD 84/2007 de 26 de enero, sobre implantación en la Admon de Justicia del sistema informático de telecomunicaciones Lexnet para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos.

Entre los usuarios del sistema Lexnet destaca el especial régimen de utilización atribuido a los Colegios de Procuradores. El mencionado artículo 4 establece que el sistema también será obligatorio para los Colegios de Procuradores que cuenten con los medios técnicos necesarios.

El Anexo II del RD 84/2007 establece una relación de usuarios del sistema, y entre ellos nos encontramos:

- ✓ Funcionarios del Cuerpo Superior Jurídico de Secretarios Judiciales.
- ✓ Otros funcionarios al servicio de la Administración de Justicia: Gestión Procesal y Administrativa, Tramitación Procesal y Administrativa, Auxilio Judicial.
- ✓ Abogacía del Estado.
- ✓ Ministerio Fiscal.
- ✓ Procuradores de los Tribunales.
- ✓ Abogados.
- ✓ Graduados sociales.
- ✓ Administrador del Colegio de Procuradores.
- ✓ Órganos de la Administración General del Estado y sus organismos públicos, así como otras Administraciones e instituciones que habitualmente se relacionen con la Administración de Justicia.

La implementación del sistema Lexnet se producirá en las Oficinas Judiciales de forma gradual en función de las posibilidades técnicas y presupuestarias y ello sin perjuicio de la extensión y utilización del sistema en las Comunidades Autónomas con competencias asumidas en materia de Justicia en el marco de los correspondientes convenios de cooperación tecnológica que puedan celebrarse con este objeto.

El RD 84/2007 encarga al Ministerio de Justicia la responsabilidad de administrar y mantener el entorno operativo y disponibilidad del sistema y la realización de las tareas necesarias que garanticen el correcto funcionamiento, la custodia y la seguridad del sistema, sin perjuicio de las atribuciones correspondientes a las Comunidades Autónomas con competencias asumidas en materia de Justicia en los términos de los convenios de cooperación tecnológica suscritos con éstas. Dichos convenios se ajustarán a las características del sistema y respetarán las garantías establecidas en este Real Decreto (artículo 5)

En cuanto a la disponibilidad de este sistema, el artículo 6 del RD 84/2007 establece que deberá estar en funcionamiento durante las veinticuatro horas del día, todos los días del año. Este mismo artículo prevé que en ningún caso, la presentación telemática de escritos y documentos o la recepción de actos de comunicación por medios telemáticos implicará la alteración de lo establecido en las leyes sobre el tiempo hábil para las actuaciones procesales, plazos y su cómputo, ni tampoco supondrá ningún trato discriminatorio en la tramitación y resolución de los procesos judiciales.

Quiero mencionar también, por su importancia, que muchas de las actividades que se realizan en el sistema Lexnet, implican un tratamiento de datos de carácter personal que determinan la existencia en el sistema de ficheros automatizados de datos de carácter personal, por eso el RD 84/2007 acuerda la creación de estos ficheros de conformidad con lo dispuesto en el artículo 20 de la LOPD.

- Para abordar el capítulo correspondiente al **Comercio Electrónico** he planteado el siguiente supuesto hipotético: el sistema Lexnet sería la herramienta utilizada por la Oficina Judicial para comunicarse no sólo con los usuarios mencionados anteriormente, previstos legalmente, sino también con cualquier ciudadano que precisase dirigirse a la Justicia. Es decir, quiero plantear la **hipótesis** de que el sistema Lexnet tuviese también la funcionalidad de una dirección electrónica disponible para el ciudadano para relacionarse con la Administración de Justicia con todas las garantías necesarias; que ofreciese un marco de comunicación e interacción con el ciudadano en relación con los servicios ofrecidos por la Oficina Judicial.

Imaginemos, por ejemplo, que a través del sistema Lexnet, cualquier ciudadano pudiera tener acceso telemático a las resoluciones judiciales o sentencias (siempre que estas fuesen públicas), realizar el pago de las costas judiciales o de las tasas administrativas por la expedición de certificados, etc., etc.

Con los datos de que disponemos, ¿podemos decir que la Administración de Justicia a través de la implantación del sistema LEXNET entraría dentro del ámbito de aplicación de la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico?[66]

Debemos analizar si se cumplen con todos los requisitos que enumera la Ley 34/2002 al respecto:

[66] LSSI: Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

- Atendiendo a la actividad que desarrolla, a los efectos de la Ley, se considera un "servicio de la sociedad de la información" si es prestado:
    - ✓ **a título oneroso**. Este requisito no es imprescindible para caracterizar un servicio como de la sociedad de la información. El carácter que debe tener es el de suponer al que lo presta una actividad económica, aunque sea indirecta, esto es, aunque no provenga directamente del destinatario del servicio.
    - ✓ **a distancia**; la prestación de servicios se realiza sin presencia física simultánea de prestador y destinatario en el mismo lugar.
    - ✓ **por vía electrónica**; se deben utilizar medios electrónicos en la prestación.
    - ✓ **a petición individual del destinatario**; se debe primar la voluntad del destinatario de recibir el servicio previa solicitud y respetando en todo momento su libertad de elección.

La ley acoge un concepto amplio de "servicios de la sociedad de la información", que engloba la contratación de bienes y servicios por vía electrónica, el suministro de información por dicho medio, las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios, siempre que represente una actividad económica para el prestador. Estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico.

- Se trata de una Administración Pública u organismo establecido en territorio español, y los servicios prestados por la misma se llevan a cabo en territorio español (tendríamos que entrar a analizar el artículo 2 de la LSSI para comprobar que entramos dentro del ámbito de aplicación de la ley).

- los servicios prestados por la Administración de Justicia a través del sistema LEXNET ¿están dentro de los supuestos de exclusión contemplados por el artículo 5 de la Ley? Este artículo establece que se regirán por su normativa específica una serie de actividades y servicios de la sociedad de la información:
    - ✓ los servicios prestados por notarios y registradores de la propiedad y mercantiles en el ejercicio de sus respectivas funciones públicas.
    - ✓ los servicios prestados por abogados y procuradores en el ejercicio de sus funciones de representación y defensa en juicio.

Ya hemos visto como el Anexo II del RD 84/2007 incluía como usuarios del sistema Lexnet, a los abogados, procuradores y otros órganos de la Administración General del Estado y sus organismos públicos, así como otras Administraciones e Instituciones que habitualmente se relacionen con la Administración de Justicia, pero en el caso que nos ocupa es la Administración de Justicia quien presta el servicio, estos colectivos sólo son usuarios del sistema o servicio ofrecido.

El Capítulo I del Título II de la LSSI desarrolla el principio de de libre prestación de servicios:

-**El artículo 6** establece que la prestación de servicios de la sociedad de la información no está sujeta a autorización previa, por lo que la Administración de Justicia no está obligada a recabar ninguna autorización al respecto.

-**El artículo 7** permite que la Administración de Justicia pueda realizar su actividad en el ámbito de la sociedad de la información en régimen de libre prestación de servicios, sin que pueda establecerse ninguna restricción a los mismos salvo los supuestos establecidos en el artículo 8.

-**El artículo 8** establece un número de restricciones a la prestación de servicios, ninguna de las cuales afecta a la actividad desarrollada por el sistema Lexnet.

Una vez determinado, que se trata de un servicio que entra dentro del ámbito de aplicación de la LSSI, la Oficina Judicial, como prestador de servicios de la sociedad de la información estará sujeta a las **obligaciones** establecidas en la Sección 1ª del Capítulo II de la LSSI, entre ellas, a disponer de los medios que permitan tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la información relacionada en el artículo 10 de la LSSI:

- Sin perjuicio de los requisitos que en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:
    - ✓ Su nombre o denominación social; su residencia o domicilio o en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.
    - ✓ Los datos de su inscripción en el Registro Mercantil.
    - ✓ Si su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.
    - ✓ El número de identificación fiscal correspondiente.
    - ✓ Información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío.
    - ✓ Códigos de conducta a los que esté adherido y la manera de consultarlos electrónicamente.

El artículo 9 de la LSSI impone la obligación de comunicar al Registro Mercantil o a otro registro público en el que se encuentre inscritos los prestadores de servicios de la sociedad de la información, un nombre de dominio o dirección de Internet así como todo acto de sustitución o cancelación del mismo.

También deberá colaborar con los prestadores de servicios de intermediación en los términos establecidos en el Art.11 y a retener los datos de tráfico relativos a las comunicaciones electrónicas como estipula el Art. 12.

En el caso que nos ocupa, la presentación de escritos ante las Oficinas Judiciales y la recepción de los actos de comunicación que éstas cursaren, y otras actividades por las que los ciudadanos se interrelacionan con la Administración de Justicia, podrá ser realizada mediante la conexión a la dirección Web lexnet.justicia.es que se calificaría como una **página dinámica contractual** ya que permitiría la realización de actividades de comercio electrónico.

Las páginas Web se clasifican en:

- **Páginas estáticas**: sólo constan de una página. Pueden consistir solamente en ofrecer información sobre su identidad, dirección y contenido de los productos o servicios que ofrece, pero de una forma que denominados estática porque no alcanza a ningún tipo de interrelación con el destinatario de la información que vaya más allá de proporcionarle esa información cuando lo solicita, esto es, cuando se conecta a su página Web y lee lo que en ella figura.
- **Páginas dinámicas**; realizan una actividad bidireccional en el sentido de conversar o establecer una relación dinámica con el destinatario del servicio llegando, en el caso extremo, incluso a la contratación electrónica. Dentro de estas páginas dinámicas podemos diferenciar a su vez:
  - ✓ *conversacionales*: se conversa entre usuario y empresa. El servicio que se ofrece va más allá de la simple información pero no llega a suponer una contratación electrónica. Podemos decir que se trata de un prestador de servicios intermedio entre el estático y el dinámico contractual, como por ejemplo un prestador que ofrece un diálogo con el usuario sin llegar a posibilitar una verdadera contratación electrónica (es el caso de un servicio de asesoramiento sobre la utilización de un producto o servicio).
  - ✓ *contractuales:* aparte de la conversación se llega a la contratación. Aquí si habría comercio electrónico.

- Si la Administración de Justicia llegara a realizar **contratos on-line** a través del sistema Lexnet deberá incluir la siguiente información con carácter previo a la contratación:

  - ✓ Trámites que deben seguirse para contratar on-line.
  - ✓ Si el documento electrónico del contrato se va a archivar y si éste será accesible.
  - ✓ Medios técnicos para identificar y corregir errores en la introducción de datos.
  - ✓ Lengua o lenguas en que podrá formalizarse el contrato.
  - ✓ Condiciones generales a que, en su caso se sujete el contrato, de manera que estas puedan ser almacenadas y reproducidas por el destinatario.

Posteriormente deberá confirmar la recepción de la aceptación:

- Se deberá confirmar la celebración del contrato por vía electrónica, en el plazo de las 24 horas siguientes a la recepción de la aceptación, y además, se debe confirmar a los destinatarios la recepción de la aceptación mediante el envío de
  - ✓ un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente.
  - ✓ un medio equivalente al utilizado en el procedimiento de contratación, tan pronto como el aceptante lo haya completado siempre que dicha confirmación pueda ser archivada por su destinatario.

El artículo 9 de la LSSI impone la obligación de comunicar al Registro Mercantil o a otro registro público en el que se encuentre inscritos los prestadores de servicios de la sociedad de la información, un nombre de dominio o dirección de Internet así como todo acto de sustitución o cancelación del mismo.

La LSSI se aplica al comercio electrónico y a otros servicios de Internet cuando sean parte de una actividad económica.

En el caso que nos ocupa, la presentación de escritos ante las Oficinas Judiciales y la recepción de los actos de comunicación que éstas cursaren, podrá ser realizada mediante la conexión a la dirección Web lexnet.justicia.es; ello sin perjuicio de la posibilidad de que la conexión pueda establecerse a través de otras vías, como los portales profesionales, reconocidos por el Ministerio de Justicia, de los distintos operadores jurídicos, o a través de la intranet administrativa de las Administraciones públicas. Así lo establece el apartado 4 del Anexo IV del RD84/2007.

Como paso o requisito previo a la utilización del sistema Lexnet, el apartado 3 del mismo Anexo IV, establece que los usuarios deberán solicitar el alta en el mismo con su **certificado de usuario** [67]mediante la conexión a la dirección Web lexnet.justicia.es, salvo en aquellos casos en que la conexión pueda establecerse a través de los portales profesionales de los distintos operadores jurídicos reconocidos por el Ministerio de Justicia. Esta solicitud de alta deberá ser validada por los administradores competentes de los colectivos de usuarios autorizados como garantía de pertenencia a un determinado colectivo. Sin dicha validación, el usuario no podrá utilizar el sistema.

[67]El sistema está basado en el empleo de **firma electrónica reconocida** como ya vimos.

El Anexo VI del RD 84/2007 regula el **procedimiento** que utiliza el sistema Lexnet para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal y establece lo siguiente:

- tanto la presentación de escritos y documentos, el traslado de copias como la realización de actos de comunicación a través del sistema telemático requerirá por parte de los usuarios del sistema la previa cumplimentación de todos los campos de datos obligatorios que aparecen relacionados en el Anexo III.
- el usuario podrá incorporar, además del documento electrónico anexo, en el que se contenga el propio acto procesal objeto de transmisión, otros anexos, uno por cada uno de los documentos electrónicos que se deban acompañar.
- el usuario podrá visualizar los documentos electrónicos incorporados como anexos, a efectos de comprobación, antes de proceder a su envío.
- cuando, por las singulares características de un documento, el sistema no permita su incorporación como anexo para su envío en forma telemática, el usuario hará llegar dicha documentación al destinatario por otros medios, en la forma que establezcan las normas procesales, y deberá hacer referencia a los datos identificativos del envío telemático al que no pudo ser adjuntada.
- el usuario remitente utilizará firma electrónica reconocida para realizar el envío. Los documentos electrónicos anexos también serán firmados electrónicamente.

Llegado este punto me parece interesante detenerme en el artículo 7 del RD 84/2007, donde se trata la **operativa funcional del sistema Lexnet**; el artículo nos remite al Anexo VI ya visto para determinar el procedimiento del sistema, y además establece los siguientes puntos:

- Para la acreditación de la presentación telemática de escritos y documentos el sistema devolverá al usuario un resguardo electrónico acreditativo de la correcta transmisión y, en todo caso, de la fecha y hora de la efectiva realización de la presentación en la Oficina Judicial.
- Si el envío se realiza correctamente, el acto de comunicación se recibe en el buzón del destinatario y queda depositado en el mismo a su disposición. En este supuesto, el sistema devolverá al remitente un resguardo electrónico, acreditativo de la remisión y puesta a disposición, en el que consten los siguientes datos: identidad del remitente y del destinatario, fecha y hora de su

efectiva realización proporcionada por el sistema y tipo de procedimiento judicial, número y año al que se refiere.

- Cuando el destinatario acceda al acto de comunicación y documentos anexos depositados en su buzón virtual, el sistema genera un resguardo electrónico dirigido al remitente, reflejando el hecho de la recepción y la fecha y hora en que ha tenido lugar, quien así tendrá constancia de la recepción.
- En el caso de los procuradores, cuando se produzca el acceso al buzón virtual del Colegio de Procuradores se generará el correspondiente resguardo, que bastará para acreditar la recepción a los efectos previstos en la ley.
- El sistema confirmará al usuario la recepción del mensaje por el destinatario. La falta de confirmación implicará que no se ha producido la recepción. En aquellos casos en que se detecten anomalías en la transmisión telemática, el propio sistema lo pondrá en conocimiento del usuario, mediante los correspondientes mensajes de error, para que proceda a la subsanación, o realice el envío en otro momento o utilizando otros medios.

  El mensaje de indicación de error o deficiencia de la transmisión podrá ser imprimido en papel, archivado por el usuario, y en su caso, integrado en los sistemas de gestión procesal, a efectos de documentación del intento fallido.

En cuanto a las **funcionalidades** del sistema Lexnet, el Anexo V del RD 84/2007 es muy claro al establecer que este sistema deberá garantizar la prestación de los siguientes servicios:

- La presentación, transporte de escritos procesales y documentos que con los mismos se acompañen, así como su distribución y remisión a la Oficina Judicial encargada de su tramitación.
- La gestión del traslado de copias, de modo que quede acreditado en las copias la fecha y hora en que se ha realizado el traslado y que éste se ha efectuado a los restantes Procuradores personados, de conformidad con lo previsto en las leyes procesales.
- La realización de actos de comunicación procesal conforme a los requisitos establecidos en las leyes procesales.
- La expedición de resguardos electrónicos, integrables en las aplicaciones de gestión procesal, acreditativos de la correcta realización de la presentación de

escritos y documentos anexos, de los traslados de copias y de la correcta remisión y recepción de los actos de comunicación procesal y, en todo caso, de la fecha y hora de la efectiva realización.

- La constancia de un asiento por cada una de las transacciones telemáticas a que se refieren las letras a), b), c) y d) de este anexo, realizadas a través del sistema, identificando cada transacción los siguientes datos: identidad del remitente y del destinatario de cada mensaje, fecha y hora de su efectiva realización proporcionada por el sistema, y proceso judicial al que se refiere, indicando tipo de procedimiento, número y año.

11.-PAGO ELECTRÓNICO

Siguiendo con el desarrollo del hipotético caso planteado sobre la posibilidad de utilizar lexnet.justicia.es como medio de comunicación e interrelación entre la Administración de Justicia y cualquier ciudadano que precise acceder a ella, por ejemplo para el pago de tasas administrativas o costas judiciales, he tomado como punto de partida una disposición normativa real para abordar el tratamiento de este capítulo del pago electrónico.

La Resolución de 10 de enero de 2008 de la Subsecretaria del Ministerio de Justicia por la que se establece la aplicación del procedimiento para el pago por vía telemática de las tasas administrativas del Ministerio de Justicia tiene por objeto establecer el procedimiento para la presentación de la autoliquidación y las condiciones para el pago por vía telemática de las "tasas administrativas del Ministerio de Justicia" que gravan los siguientes hechos imponibles:

- ✓ expedición de certificados por el Registro Central de Penados y Rebeldes y por el Registro General de Actos de Última Voluntad.
- ✓ expedición de certificados por el Registro de Contratos de Seguro de Cobertura de fallecimiento.

En esta Resolución se establecen los siguientes requisitos para el pago telemático de estas tasas:

- disponer de NIF o CIF, según corresponda.
- disponer de firma electrónica avanzada basada en un certificado de usuario admitido por la Agencia Tributaria.
- tener una cuenta abierta en una entidad colaboradora en la gestión recaudatoria.

El procedimiento a seguir establecido en esta norma, y que podríamos adoptar para el pago de cualquier servicio que precisáramos de la Administración de Justicia sería el siguiente:

1. el interesado accederá a lexnet.justicia.es [68]a través de Internet y cumplimentará el formulario [69]de pago telemático de las tasas.

[68] Continúo con el desarrollo del supuesto hipotéticamente planteado, ya que en realidad la Resolución prevé que la dirección web sea www.mjusticia.es.
[69] Formulario 790 de pago telemático de las tasas con código 006.

2. Cumplimentados todos los campos solicitará la realización del pago telemático.
3. A continuación se accederá a través de un enlace, a la página Web de la Agencia Tributaria en la cual se podrá proceder al pago telemático de la tasa a través del sistema de cargo en cuenta o mediante la utilización de tarjetas de débito o crédito.
4. Si la declaración o el pago son aceptados, la entidad financiera colaboradora facilitará el Número de Referencia Completo (NRC), que se entregará al Ministerio de Justicia.
5. Comprobado el NRC por el Ministerio de Justicia se generará al interesado un mensaje de confirmación de la realización del ingreso, que junto al registro telemático posterior permitirá la impresión del modelo de formulario de pago, el cual, junto al NRC servirá de justificante del pago.

El concepto de pago de una deuda que establece el Código Civil en el artículo 1157 requería la entrega de la cosa o la realización de la prestación en que consistía la obligación en cuestión.

Si esa entrega o prestación se realiza por medios electrónicos, no sólo por Internet, estamos ante un pago electrónico. Por tanto, se entiende por pago electrónico aquel que se realiza por medios electrónicos.

Podemos encontrarnos con varios medios de pago electrónico, entre ellos, los más importantes serían:

- ✓ tarjetas: de crédito, débito o de pago.
- ✓ micropagos.
- ✓ cheques electrónicos.
- ✓ monederos electrónicos.

No obstante, en la contratación electrónica, y más concretamente en la contratación en Internet, asimilamos el pago electrónico con el pago mediante tarjetas ya que es el medio más utilizado en este ámbito. Por eso vamos a profundizar, con más detenimiento en este medio de pago.

Las tarjetas electrónicas podrían definirse como el "documento mercantil, instrumental y electrónico, que permite a su titular, mediante compromiso contractual con el emisor, servir como documento de pago a la vez que beneficiarse de una línea de crédito limitada, que podrá utilizar en la compra de bienes o servicios en

establecimientos adheridos al sistema, o en el acceso a cantidades limitadas de dinero en bancos o entidades financieras que hayan concertado el servicio".

Las tarjetas cumplen una serie de funciones:

- Función identificativa: podemos decir que la principal función de una tarjeta es la identificación de su titular.
- Instrumento de pago: a través de ellas, satisfacemos el pago o aplazamos el mismo, dependiendo del tipo de tarjeta.
- Instrumento de crédito al consumo: cumplen la función de financiación.

La seguridad en las transacciones electrónicas es uno de los temas que más preocupan y que más atención y estudio ha acaparado. Podríamos decir que se desvía un poco de los temas legislativos y se centra en las herramientas tecnológicas disponibles para garantizar esa seguridad.

Para garantizar un correcto desarrollo de la utilización de los medios de pago tanto en Internet como en el comercio electrónico en general aparece la figura de los **protocolos de seguridad**. Estos son medidas de carácter técnico que tratan de dar solución a cuestiones concretas, asegurando la realización de transacciones económicas y del pago por la adquisición de bienes y servicios. **SSL y SET** son los protocolos de seguridad más generalizados:

- **SSL (Secure Sockets Layer)** fue creado en 1994 por Netscape Communications Corporation.
  - es un protocolo de carácter general para conseguir comunicaciones electrónicas seguras.
  - no exige ninguna capacidad específica en el servidor para el comerciante. Basta con que utilice como mínimo un canal seguro para transmitir la información de pago.
  - proporciona un canal seguro por el que se transmite la información de pago, pero carece de una estructura comercial integrada (el comerciante tiene que gestionar previamente las compras con la entidad financiera).
  - no es un protocolo multiparte: sólo protege las transacciones entre dos partes (garantiza la confidencialidad en la transmisión de datos mediante encriptación, pero sólo entre el usuario y comerciante), no contempla la relación tripartita que se

da en toda transacción con tarjeta de crédito. Autentica el servidor, pero no al comprador ni al banco del comerciante.

- tiene deficiencias en cuanto a seguridad: por eso se habla del SSL como un protocolo de seguridad general, pero no de pago seguro. No hace uso de firmas electrónicas, por lo que la integridad no queda garantizada, no garantiza el no repudio del envío del mensaje.
- es más apropiado para realizar operaciones que impliquen pagos de poco valor.
- su utilización es masiva.

➢ **SET (Secure Electronic Transaction)** fue creado en 1995 por VISA y MasterCard.

- posee numerosas especificaciones técnicas que garantizan la seguridad en la transacción electrónica: hace uso de firmas electrónicas, por lo que la integridad queda asegurada, garantiza el no repudio del envío entre las partes, proporciona confidencialidad en la transmisión de datos mediante encriptación entre todas las partes.
- su implantación requiere de unos requisitos tecnológicos específicos. hay que implantar un software específico en los ordenadores del comerciante y del comprador, además es necesario que exista compatibilidad entre todos los productos que forman este software de instalación, se tiene que elegir un PSC (Prestador de Servicios de Certificación), y utilizar unos circuitos cerrados de intercambio financiero.
- se apoya en una Infraestructura de Clave Pública [70]que le permite la autenticación de todas las partes implicadas, confidencialidad e integridad.
- es un protocolo multiparte: autentica el servidor al que se conecta el usuario para efectuar la transacción, autentica al comprador y también a otros terceros que intervienen en la transacción, como por ejemplo, los bancos de las partes.
- resulta inadecuado para realizar un gran número de transacciones de poco valor.
- su utilización está menos generalizada; su implantación lleva aparejados problemas de gestión que dificultan el dinamismo de este tipo de transacciones electrónicas.

[70] PKI: método para el intercambio seguro de mensajes, basado en la asignación de dos claves complementarias, una pública y otra privada, a los particulares implicados en una transacción. El más conocido es el RSA.

12.-FACTURA ELECTRÓNICA

También quiero contemplar la posibilidad de que la Oficina Judicial pueda emitir o recibir facturas electrónicas por los servicios prestados o recibidos.

La factura electrónica es un documento electrónico que cumple con los requisitos legal y reglamentariamente exigibles a las "facturas-papel" y que, además garantiza la autenticidad de su origen y la integridad de su contenido lo que impide el repudio de la factura por su emisor. Así lo establece el Art.1 de la Ley 56/2007 de 28 de Diciembre de Medidas de Impulso de la Sociedad de la Información.

De esta definición de factura-e que hace el Art. 1 podemos extraer una serie de características que debe cumplir este tipo de documento electrónico:

- La factura electrónica debe consignarse en un formato determinado cuyas características son:
  - ✓ cumple con los requisitos legales vigentes y las condiciones establecidas por la Agencia Tributaria para la facturación telemática.
  - ✓ es universal: lo pueden utilizar todas las entidades y sus clientes.
  - ✓ es de libre uso: su utilización no está sujeta al pago de cánones ni a una autorización previa.
  - ✓ es gratuito: se distribuye gratuitamente a las entidades y sus clientes.
  - ✓ cumple con la garantía de convergencia con los formatos que se definan en los foros europeos.

- La factura electrónica precisa de su transmisión telemática (es decir, es necesario un ordenador emisor y un ordenador receptor).
- Es necesario garantizar la integridad y autenticidad de este documento electrónico a través de sistemas de firma electrónica reconocida[71]. La validez legal y fiscal de la factura electrónica la aporta la firma electrónica reconocida que debe incorporarse a la factura.
- Es fundamental el consentimiento de ambas partes (emisor y receptor). El artículo 2 de la Orden EHA 962/2007 de 10 de abril por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas

[71] Basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. Tiene la misma eficacia jurídica que la firma manuscrita.

contenidas en el RD 1496/2003 establece que el consentimiento podrá formularse de forma expresa por cualquier medio, verbal o escrito.

La utilización de la factura-e implica una serie de obligaciones tanto para el emisor como para el receptor:

- **Obligaciones para el Emisor:**
  - debe disponer del consentimiento del receptor, de forma expresa, por cualquier medio, verbal o escrito.
  - firmar las facturas con firma electrónica con certificado reconocido (firma-e reconocida).
  - crear la factura con una aplicación informática que observe los contenidos obligatorios mínimos requeridos.
  - hacerlas llegar al destinatario telemáticamente.
  - conservar copia o matriz enviado durante el periodo de prescripción.
  - contabilización y anotación en los registros del IVA.
  - garantía de accesibilidad completa: acceso completo a datos (visualización, búsqueda selectiva, copia, descarga en línea, e impresión).
  - todas las actividades anteriores se pueden subcontratar a un tercero sin perder la responsabilidad. (Art. 5.1 del RD 1496/2003).

- **Obligaciones para el Receptor:**
  - recepción de la factura por medios electrónicos.
  - asegurar la legibilidad en el formato original.
  - validar firma y certificado.
  - conservar formato original recibido durante el periodo de prescripción.
  - conservar mecanismos de validación de los contenidos mínimos exigibles.
  - contabilización y anotación en los registros del IVA.
  - gestionar la factura de modo que se garantice su accesibilidad completa.
  - todas las actividades anteriores se pueden subcontratar a un tercero sin perder la responsabilidad.

El RD 1496/2003 de 28 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación y se modifica el Reglamento del IVA establece en el artículo 6 el contenido mínimo que debe observar una factura.

Podemos predecir que la factura electrónica fomentará el desarrollo del comercio electrónico y en consecuencia la integración definitiva de la Administración de Justicia en la Sociedad de la Información.

13.-LEXNET.JUSTICIA.ES COMO NOMBRE DE DOMINIO.

Ya hemos visto como mediante la conexión a la dirección Web Lexnet.Justicia.es se puede realizar la presentación de escritos ante las Oficinas Judiciales y materializar la recepción de los actos de comunicación que éstas cursaren, ello sin perjuicio de la posibilidad de que la conexión pueda establecerse a través de otras vías, como los portales profesionales, reconocidos por el Ministerio de Justicia, de los distintos operadores jurídicos, o a través de la intranet administrativa de las Administraciones públicas. Así lo establece el apartado 4 del Anexo IV del RD84/2007 que implanta en la Administración de Justicia el sistema informático de telecomunicaciones Lexnet.

También sabemos que el acceso al sistema Lexnet es un acceso que podemos llamar "restringido" ya que, por un lado, la relación de usuarios del mismo esta limitada a funcionarios del la Administración de Justicia, al ministerio fiscal, a profesionales de la Justicia como abogados, procuradores, graduados sociales y otros organismos de las Administraciones Públicas, y además, el acceso al mismo requiere un "alta previa". La utilización de Lexnet precisa la utilización de tarjetas criptográficas que incluyen certificados digitales de firma electrónica reconocida.

Ya hemos visto como planteábamos la hipótesis de que Lexnet ampliase su funcionalidad para permitir también el acceso al sistema a los ciudadanos que precisasen dirigirse a la Administración de Justicia.

Los nombres de dominio son un elemento básico dentro del ámbito del comercio electrónico que permite la identificación de una entidad en la red.

El ingente desarrollo de Internet en los últimos años determinó la necesidad de identificar a las partes intervinientes o conectadas a la red. Podemos decir que los nombres de dominio pasaron de identificar a ordenadores a ser identificadores comerciales de las entidades que los poseían.

De esta manera, las direcciones IP(Internet Protocol)que originariamente identificaban las máquinas de origen y destino de la información, y que estaban compuestas por cuatro números, separados por puntos, comprendidos en un rango de entre 0 y 255, fueron sometidas a un tratamiento que identificaba estas direcciones IP con unos términos comprensibles e identificables por las personas. En este momento nace el Sistema de Nombres de Dominio (NDS: Domain Name System). Con este sistema, para poder conectarnos a la red y comunicarnos con los ordenadores, pasamos

de tener que memorizar números (en una situación similar a cuando marcamos un número de teléfono) a recordar nombres que ya conocíamos previamente.

En un principio los nombres de dominio se clasificaban en dos grupos: nombres de dominio de primer nivel y nombres de dominio de segundo nivel. Actualmente ha aparecido una tercera categoría: los nombres de dominio de tercer nivel.

- **Nombres de Dominio de primer nivel**: podemos decir que se encuentran en el nivel más alto de la jerarquía; se conocen por las siglas TLD (Top Level Domain); se sitúan al final de la dirección después del último punto. Se dividen en dos grupos.

  - ***Nombres de dominio de primer nivel genérico***: conocidos por gTLD, algunos de estos son de acceso libre (.com; .net; .org; .info; .biz), es decir, no será necesario ningún requisito para acceder a uno de estos nombres salvo realizar la solicitud.

  Otros son de acceso restringido, es decir el solicitante tendrá que demostrar ciertas peculiaridades (.mil; .int;.edu;.gov;.pro;.name;.coop;.aero;.museum;.travel;.jobs;.mobi).

  La Entidad encargada de gestionar estos nombres de dominio es la **ICANN**.

  - ***Nombres de dominio de primer nivel del código de país***: Conocidos por ccTLD, están compuestos de dos caracteres que se corresponden con las siglas de las normas ISO-3166. Por ejemplo, en el caso de España, los caracteres serían ".es".

  La Entidad gestora es la **ESNIC**, y en el caso de España sería "**Red.es**".

Hay que hacer una mención especial, dentro de este epígrafe de los nombres de dominio de primer nivel, a los **Nombres de Dominio bajo el Código europeo ".eu"**, que tienen como objetivo acelerar el comercio electrónico en el marco de la Unión Europea, y promover el uso y acceso tanto de las redes como del mercado virtual basado en Internet.

- **Nombres de Dominio de segundo nivel**: conocidos por las siglas SLD (Second Level Domain), podemos decir que son los que se equiparan a la marca o al nombre comercial; serán aquellos que se puedan registrar bajo un nombre de dominio de

primer nivel y que coincidirán con el concepto que el solicitante desea que sea conocido en la red.

- **Nombres de Dominio de tercer nivel**: el Plan Nacional ha creado los indicativos ".com.es", ".nom.es", ".org.es",".gob.es" y ".edu.es", permitirán a los solicitantes ubicarse en un espacio adecuado a su actividad o al tipo de entidad que constituyan y a los usuarios, distinguir unas de otras de forma intuitiva.

En lo que se refiere a la clasificación de Lexnet.justicia.es como hipotético nombre de dominio de la Oficina Judicial, podría servirnos la regulación que hace el artículo 17.2 del RD 1671/2009 [72]de la identificación de las sedes electrónicas al establecer que para facilitar su identificación, *"las sedes electrónicas seguirán las disposiciones generales que se establezcan para la imagen institucional de la Administración General del Estado y su dirección electrónica incluirá el nombre de dominio de tercer nivel -gob.es"*. Por tanto calificaríamos a Lexnet.justicia.es como nombre de dominio de tercer nivel.

13.1.-CONFLICTOS DE USURPACIÓN DE NOMBRES DE DOMINIO

Debemos decir que como punto de partida, u origen del problema está la filosofía que reina en Internet de *"todo vale"*. Internet representa el reino de las libertades y la autorregulación del mercado.

Las entidades encargadas de la regulación de los nombres de dominio se rigen por unos principios basados en la divisa de que *el primero que llega es el primero que se sirve* ("first come, first served").

A todo esto se añade el agravante de la falta de legislación y la ausencia de un órgano central de autoridad y control en la Red.

Podemos decir que en Internet no existen los límites en cuanto al contenido o derechos de registro de un nombre de dominio. Por otro lado, sería prácticamente imposible que cualquier institución pudiera determinar a priori el mejor derecho de una parte para registrar un nombre de dominio frente a otra: entrarían en conflicto legislaciones de diferentes lugares del mundo y sería necesario arbitrar un sistema de

[72] RD 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007 de22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

análisis de las legislaciones y estudio de los documentos que aportase cada una de las partes para poder determinar su derecho al nombre de dominio en conflicto. No hace falta ser muy avispado en la materia para predecir que esto afectaría gravemente la dinámica imperante en la Red: la inmediatez y la rapidez de su funcionamiento.

Por todo esto se otorga un poder casi absoluto al registro, como presunción iuris tantum[73] de posesión de un derecho: el simple hecho del registro se constituía en el derecho para la utilización del nombre de dominio frente a cualquiera.

A medida que el uso de Internet se desborda se plantea la necesidad de regular el registro y la utilización de los nombres de dominio.

Se promulgan las primeras **Normas de Resolución de Conflictos sobre Nombres de Dominio** para los gTLD (nombres de dominio genéricos) y aquellos ccTLD (nombres de dominio de código de país) que las adoptaren como medio de resolución de conflictos (para los ccTLD de la mayoría de los países son los propios Estados los que dictan las normas por las que se regirán debido a su carácter territorial)

También se crean órganos arbitrales de resolución de controversias. Se establece, llegado a este punto, que como resoluciones arbitrales que son, son susceptibles de recurso ante la jurisdicción que corresponda, comprometiéndose el registrador, en los casos de recurso jurisdiccional, a impedir la transmisión del nombre de dominio en conflicto por parte del titular, para facilitar la legitimación pasiva del titular en el procedimiento judicial.

La ICANN (entidad encargada del registro y asignación de nombres de dominio) decidió promulgar una serie de normas de obligado cumplimiento para todas aquellas personas usuarias de algún gTLD o nombre de dominio genérico y para aquellos ccTLD o nombres de dominio de código de país que se quisieran adherir a ellas, mientras que en la mayoría de los países se dictaban normas de registro y protección de sus propios dominios.

El 26 de agosto de 1999 aprobó una **Política Uniforme de Solución de Controversias** en materia de nombres de dominio. Esta política está en vigor y se aplica para la solución de controversias relacionadas con los nombres de dominio genéricos o gTLD, incluso con efectos retroactivos.

[73] Admite prueba en contrario.

Establece las cláusulas y condiciones en relación con una controversia que surja entre la persona que registró un dominio y cualquier otra parte distinta al propio registrador sobre el registro y utilización de un nombre de dominio de Internet registrado por esa persona, y el procedimiento lo establece en el "Reglamento de la Política Uniforme de solución de controversias en materia de nombres de dominio" y el Reglamento Adicional del proveedor del servicio de solución de controversias administrativas seleccionado.

Los pasos que deberé seguir según la ICANN son los siguientes:

1- Iniciación del Procedimiento: cualquier persona o entidad podrá iniciar un procedimiento administrativo presentando una demanda a cualquier proveedor aprobado por la ICANN de conformidad con la Política Uniforme de Solución de Controversias y su Reglamento. Son cuatro los órganos ante los que se pueden presentar las controversias (el que mayor número de controversias resuelve es el Centro de Mediación y Arbitraje de la **OMPI**[74]).

La presentación deberá hacerse de manera electrónica y habrá que efectuar las solicitudes y especificar la forma preferida para efectuar las comunicaciones al demandante.

El demandado estará obligado a someterse a un procedimiento administrativo en caso de que el demandante sostenga ante el proveedor competente que:

- ✓ posee un nombre de dominio idéntico o similar hasta el punto de crear confusión.
- ✓ no tiene derechos o intereses legítimos respecto del nombre de dominio.
- ✓ posee un nombre de dominio que ha sido registrado y se utiliza de mala fe.

2- Legislación Adicional: si las dos partes son del mismo país se podrán aplicar por parte del árbitro normas del país en cuestión para dirimir la controversia.

3- Pruebas: la carga de la prueba estará siempre del lado del demandante, que será quien tenga que demostrar los aspectos antes mencionados. Debe demostrar los tres aspectos señalados en el punto 1, de manera independiente y todos ellos. Si el

[74] OMPI: Organización Mundial de la Propiedad Intelectual. Organismo especializado de Naciones Unidas. Se estableció en 1967. Su sede se encuentra en Ginebra (Suiza).

demandante no es capaz de probar uno solo de ellos, el nombre de dominio seguirá siendo utilizado por el demandado.

4-Pruebas de registro y utilización de mala fe: la ICANN establece una serie de condiciones en el artículo 4.a) de la Política Uniforme de Solución de Controversias y si se da alguna de ellas, sólo una de ellas es suficiente, se entenderá que ha existido mala fe por parte de la persona que registró el nombre de dominio. Repito que es necesario probar todos los puntos, no sólo uno, del artículo 4.a). Si logramos demostrar la mala fe, habremos demostrado uno de los puntos mencionados en el apartado 1. La mala fe sin embargo la debemos demostrar en dos momentos, en el momento del registro del nombre de dominio, y en el momento de la utilización de ese nombre de dominio.

5-Cómo demostrar sus derechos y sus legítimos intereses sobre el nombre de dominio al responder una demanda; el demandado podrá probar su interés legítimo sobre el nombre de dominio objeto de controversia de alguna de las siguientes maneras:

- ✓ antes de haber recibido cualquier aviso de la controversia, usted ha utilizado el nombre de dominio, o ha efectuado preparativos demostrables para su utilización.
- ✓ ha sido conocido corrientemente por el nombre de dominio, aun cuando no haya adquirido derechos de marcas de productos o de servicios.
- ✓ hace un uso legítimo y leal o no comercial del nombre de dominio, sin intención de desviar a los consumidores de manera equívoca o de empañar el buen nombre de la marca de productos o de servicios en cuestión con ánimo de lucro.

Con probar uno solo de los aspectos señalados, el demandado demostrará su interés legítimo en el nombre de dominio, y desvirtuará toda posibilidad de traspaso al demandante.

6- Resolución y costas del procedimiento; las costas serán siempre de parte del demandante, y la solución que decida el órgano administrativo no podrá determinar nada en cuanto a las costas, sólo podrá decidir acerca del nombre de dominio:

- ✓ que siga utilizándolo el demandado, cuando entienda que no se han cumplido los tres puntos antes señalados
- ✓ que pase al demandante, cuando entienda que tiene derecho a ello.

- ✓ que se cancele el nombre de dominio cuando pueda resultar ofensivo para el demandante.

Las únicas costas que pueden ser de parte del demandado serán aquellas que hagan referencia a la intención de éste de ampliar el número de árbitros a tres.

7- Recursos: contra la resolución del órgano administrativo se pueden interponer recursos antes de iniciar el procedimiento administrativo o después de su conclusión.

8-Resumen: la persona, física o jurídica, que considere que tiene derecho a un nombre de dominio que haya registrado otra persona podrá interponer una demanda ante uno de los órganos administrativos seleccionados por la ICANN.
La carga de la prueba recaerá sobre el demandante.
El árbitro decidirá acerca del nombre de dominio tras la demanda y la contestación.

Las costas serán siempre de parte del demandante, salvo que el demandado solicite la ampliación de árbitros.

Contra esta resolución administrativa cabe la interposición de recursos ante la jurisdicción ordinaria, que paralizarían la ejecución de la resolución, o que impedirían la transmisibilidad del nombre de dominio, a fin de facilitar las cosas al órgano juzgador posterior.

14.-CONTRATACIÓN INFORMÁTICA EN EL ÁMBITO DE LA ADMINISTRACIÓN DE JUSTICIA.

La celebración de cualquier tipo de contrato por una Administración Pública, está sujeta a lo dispuesto en la Ley 30/2007 de 30 de octubre de Contratos del Sector Público y el Reglamento General de la Ley de Contratos de las Administraciones Públicas aprobado por RD 1098/2001 de 12 de Octubre.

También es muy importante tener en cuenta el Plan de medidas, recomendaciones y buenas prácticas en la adquisición y uso de programas de ordenador por las Administraciones Públicas de la Comisión Interministerial de Adquisición de Bienes y Servicios Informáticos del 12 de abril del 2000 y la Directiva 2004/18/CE del Parlamento Europeo y del Consejo sobre coordinación de los procedimientos de adjudicación de los contratos públicos de obras, suministro y servicios.

Para empezar, el artículo1 de la Ley 30/2007 señala que su objeto es "regular la contratación del sector público, a fin de garantizar que la misma se ajusta a los principios de libertad de acceso a las licitaciones, publicidad y transparencia de los procedimientos y no discriminación e igualdad de trato entre los candidatos, y de asegurar, en conexión con el objetivo de estabilidad presupuestaria y control del gasto, una eficiente utilización de los fondos destinados a la realización de obras, la adquisición de bienes y la contratación de servicios mediante la exigencia de la definición previa de las necesidades a satisfacer, la salvaguarda de la libre competencia y la selección de la oferta económicamente más ventajosa. Es igualmente objeto de esta ley la regulación del régimen jurídico aplicable a los efectos, cumplimiento y extinción de los contratos administrativos, en atención a los fines institucionales de carácter público que a través de los mismos se traten de realizar".

Una vez que la Ley fija su objeto, se ocupa de establecer los contratos que entran dentro de su ámbito de aplicación y determina que éstos serán los siguientes:

- los contratos onerosos, cualquiera que sea su naturaleza jurídica, que celebren los entes, organismos y entidades enumerados en su artículo 3.
- los contratos subvencionados por los entes, organismos y entidades del sector público que celebren otras personas físicas o jurídicas en los supuestos previstos

en el artículo 17, así como los contratos de obras que celebren los concesionarios de obras públicas en los casos del artículo 250.

- los contratos que celebren las Comunidades Autónomas y las entidades que integran la Administración Local, o los organismos dependientes de las mismas, así como a los contratos subvencionados por cualquiera de estas entidades.

La Sección III de la Ley hace la siguiente clasificación de los contratos del sector público en el artículo 18: "los contratos del sector público pueden tener carácter administrativo o carácter privado".

- **Contratos Administrativos**: los celebrados por una Administración Pública. El artículo 19 de la Ley ofrece una relación de los mismos. Se regirán en cuanto a su preparación, adjudicación, efectos y extinción por la presente Ley.
- **Contratos Privados**: los celebrados por los entes, organismos y entidades del sector público que no reúnan la condición de Administración Pública. Se regirán en cuanto a su preparación y adjudicación, en defecto de norma específica por la presente Ley. Artículo 20.

La Sección I del Capítulo II de la Ley regula una serie de Contratos Administrativos, de los cuales, hay dos que afectan a la contratación informática:

- **Contrato de Suministro** (artículo 9 de la Ley):
  - los que tienen por objeto la adquisición, el arrendamiento financiero o el arrendamiento, con o sin opción de compra, de productos o bienes muebles.
  - no tendrán esta consideración los contratos relativos a propiedades incorporales o valores negociables, sin perjuicio de lo dispuesto con respecto a los contratos que tengan por objeto programas de ordenador.
  - los que tengan por objeto la adquisición y el arrendamiento de equipos y sistemas de telecomunicaciones o para el tratamiento de la información, sus dispositivos y programas, y la cesión del derecho de uso de estos últimos, a excepción de los contratos de adquisición de programas de ordenador desarrollados a medida, que se considerarán contratos de servicios.

Siguiendo la referencia que se hace en este artículo a los contratos de servicios voy a analizar el artículo que los regula:

- **Contratos de Servicios** (artículo 10):
  - Son aquellos cuyo objeto son prestaciones de hacer consistentes en el desarrollo de una actividad o dirigidas a la obtención de un resultado distinto de una obra o un suministro.
  - Se dividen en las categorías enumeradas en el Anexo II, entre las cuales podemos destacar las siguientes:
    - ✓ servicios de mantenimiento y reparación.
    - ✓ servicios de telecomunicación.
    - ✓ servicios de informática y servicios conexos.
    - ✓ servicios jurídicos.
    - ✓ servicios de investigación y seguridad.
    - ✓ servicios de educación y formación profesional.´

Por otro lado hay que hacer mención a las nuevas tipologías de contratación exclusivamente electrónicas que introducen La Directiva Comunitaria 18/2004/CE de Contratación Administrativa y el Proyecto de Ley de Contratos del Sector Público:

- **La Subasta Electrónica**
- **Los Sistemas Dinámicos de Contratación.**

Como dato interesante, hay que mencionar que la Unión Europea ha establecido como objetivo para el año 2010 que el 50% de la contratación del conjunto de la Administración Pública europea se realice por procedimientos electrónicos.

- **La Subasta Electrónica**; es un procedimiento de selección de ofertas realizada por medios electrónicos, que permite que las empresas puedan revisar los precios de su oferta a la baja y modificar el valor de otros parámetros cuantificables.

La clasificación de las ofertas se efectuará automáticamente mediante una fórmula que incorpore la valoración de todos los criterios fijados para determinar la oferta económicamente más ventajosa.

A lo largo de las fases de la subasta se comunicará a los licitadores la información que les permita conocer su clasificación en cada momento.

Entre las características de la Subasta Electrónica deben encontrarse:

- ✓ la subasta puede referirse tanto al precio como al valor de otros parámetros cuantificables de la oferta.

- ✓ es precisa una fase previa de evaluación cualitativa de las ofertas., de esta manera las fases específicas de la subasta se desarrollarán automáticamente sobre la base de aquellos proveedores que hayan superado la fase de evaluación.

La subasta ha de ser anunciada en el Boletín Oficial correspondiente, que deberá contener las siguientes informaciones:

- ✓ definición de los parámetros sobre los que se ejecutará la subasta.
- ✓ variación mínima aceptable de tales parámetros a lo largo de la subasta, es el diferencial mínimo que ha de existir entre dos ofertas sucesivas de una misma empresa.
- ✓ naturaleza de las informaciones que serán comunicadas a las empresas participantes en la subasta y momentos concretos en que se facilitarán.
- ✓ forma en que se desarrollará la subasta.

El cierre de la subasta se fijará por alguno de los siguientes criterios:

- ✓ estableciendo fecha y hora concreta.
- ✓ cuando no existan nuevas ofertas
- ✓ por culminación del número de fases establecido.

➢ **Los Sistemas Dinámicos de Contratación;** son procedimientos de contratación exclusivamente electrónicos destinados a la adquisición de suministros y servicios de uso corriente. Es un procedimiento limitado en el tiempo, durante un máximo de 4 años, estando abierto a lo largo de este periodo a todas las empresas interesadas que hubieran satisfecho los criterios de selección y que hubieran presentado una oferta indicativa conforme a los criterios de consulta.

El proceso comienza con la publicación de los siguientes elementos:

- ✓ un anuncio precisando que se trata de un expediente de Sistema Dinámico de Contratación y estableciendo los criterios de adjudicación.
- ✓ especificaciones que determinen la naturaleza de los elementos a contratar, toda la información necesaria para incorporar al sistema y a los medios informáticos para el desarrollo de la contratación.

El proceso permanece abierto a todas las empresas que presentasen una oferta indicativa conforme a las especificaciones, pudiendo mejorar su oferta a lo largo del proceso.

El desarrollo del sistema y la adjudicación de los contratos deberán efectuarse exclusivamente por medios electrónicos, informáticos y telemáticos debiendo cumplirse los siguientes requisitos:

- ✓ durante la vigencia del sistema, todo empresario interesado podrá presentar una oferta a efectos de ser incluido en el mismo.
- ✓ cada contrato específico que se pretenda adjudicar deberá ser objeto de una licitación específica.
- ✓ las ofertas podrán mejorarse en cualquier momento siempre que permanezcan conformes a las especificaciones.

La Administración podrá utilizar la subasta electrónica en el contexto de un Sistema Dinámico de Contratación.

La Comisión Interministerial de Adquisición de Bienes y Servicios Informáticos (en adelante CIABSI[75]) es el organismo encargado de adoptar medidas y recomendar actuaciones tendentes a facilitar el uso adecuado de los programas de ordenador en los sistemas informáticos de las Administraciones Públicas. Estas medidas podrán estar relacionadas con las siguientes materias:

- Difusión de la información legal y técnica relacionada con la protección de la propiedad intelectual de los programas de ordenador.
- Recomendaciones a seguir en la adquisición de productos informáticos, especialmente programas de ordenador, para que queden suficientemente protegidos, por un lado los derechos de explotación que pueda adquirir la Administración Pública y por otro los derechos de propiedad intelectual y derechos de autor de los suministradores. Esta Comisión recomienda incluir, a estos efectos, "cláusulas tipo" en los contratos informáticos, donde se contemplen los intereses de las partes contratantes.
- Establecer conversaciones con la Empresas del sector industrial TIC, directamente o a través de sus representantes, con el objetivo de profundizar en la definición de nuevas fórmulas y condiciones de contratación, o cualquier otro tipo de acuerdo que aporte un ambiente de consenso y proteja los intereses de ambas partes.

[75] Creada por RD 2291/1983. Entre sus funciones está optimizar en todo su sentido la capacidad de inversión de la Administración Pública en materia informática.

- Estudios, análisis y pruebas de conformidad de herramientas y productos comerciales de interés para las Administraciones Públicas en materia de protección de la propiedad intelectual.
- Establecimiento de un Esquema General de Autodiagnóstico que contemple los procedimientos a seguir y las tareas a ejecutar por los centros directivos que deseen aplicar medidas de evaluación y adecuación de sus instalaciones.
- Soporte a las labores de autodiagnóstico de esos centros directivos, proporcionando información sobre el contenido del inventario de software (REINA) correspondiente a cada caso en concreto, aportando datos generales y estudios anuales específicos de la información recogida que proporcionen una visión analítica de la situación global de cada centro. Entre la información que se puede obtener de los inventarios REINA, podemos destacar:
    - ✓ listado completo del software instalado.
    - ✓ listado completo de los equipos instalados por tipo.
    - ✓ número total de licencias de software instaladas por grupo de software.
    - ✓ número total de sistemas instalados por tipo.
    - ✓ número de sistemas instalados por tipo en un periodo anual.
    - ✓ cociente número de licencias/número de sistemas.
    - ✓ cociente gasto hardware/gasto software.
- Diseño, elaboración y desarrollo de actividades de difusión y formación en materia de propiedad intelectual para los empleados públicos a través de los Planes de Estudio del Instituto Nacional de Administración Pública.
- Elaboración y puesta a disposición de los centros de anuncios electrónicos recordatorios de la legalidad vigente y cuya aparición automática se produzca en el momento de arranque de los equipos informáticos.

La Comisión Ministerial de Informática y Comunicaciones del Ministerio de Justicia (creada por la Orden JUS 764/2005 de 17 de marzo), es el organismo por el que el Ministerio de Justicia se relaciona con la CIABSI. Podemos decir que es el vínculo que permite la puesta en marcha y difusión de las actividades de la CIABSI en el ámbito del Ministerio de Justicia. Además de esto, entre sus actividades deberá:

- promover y observar los procesos de evaluación que voluntariamente, sean aplicados por los centros directivos de su Departamento.

- asesorarán a estos en la particularización del Esquema General de Autodiagnóstico antes mencionado.
- recogerán y custodiarán los resultados obtenidos para uso exclusivo de su departamento, para adoptar las medidas oportunas.
- trasladarán a la CIABSI los resultados, experiencias y recomendaciones obtenidas.

En primer lugar quiero aclarar que por **contratación informática** entendemos la contratación de **bienes o servicios informáticos**; no debemos confundir la contratación informática con la **contratación electrónica** que es aquella que se realiza por medios electrónicos e informáticos sin que su objeto sean bienes o servicios informáticos.

Con el término **bienes informáticos** nos referimos a " todos aquellos elementos que forman el sistema (ordenador) en cuanto al hardware, ya sea la unidad central de proceso o sus periféricos, y todos los equipos que tienen una relación directa de uso con respecto a ellos y que, en su conjunto, conforman el soporte físico del elemento informático, así como los bienes inmateriales que proporcionan las órdenes, datos, procedimientos e instrucciones, en el tratamiento automático de la información y que, en su conjunto, conforman el soporte lógico del elemento informático".

Con el término **servicios informáticos** nos referimos a "todos aquellos que sirven de apoyo y complemento a la actividad informática en una relación de afinidad directa con ella".

También debo aclarar que un **contrato informático** es aquel contrato en el que una parte se obliga a entregar un bien informático o a prestar un servicio informático a otra que se compromete a pagar por ello. Como contrato que es, su primera definición deriva del artículo 1254 del Código Civil que establece que "el contrato existe desde que una o varias personas consienten en obligarse respecto de otra u otras, a dar alguna cosa o prestar algún servicio".

Al tratarse de un tipo de contratos que carece de regulación específica en el derecho español, su estudio implica el examen de una diversidad de normas que les afectan. Y es que su carácter atípico no se salva con el principio de autonomía de la voluntad recogido en el artículo 1255 del Código Civil que establece que "las partes contratantes pueden establecer los pactos, cláusulas y condiciones que tengan por conveniente, siempre que no sean contrarios a las leyes, a la moral, ni al orden público".

Hay que tener en cuenta las peculiaridades de la contratación informática y estudiar su régimen jurídico extrayéndolo de una pluralidad de normas.

Se nos plantea el problema de ver en qué contrato típico lo vamos a encuadrar. Además, se trata de un tipo de contratos que implican una desventaja para una de las partes (una de las partes lo sabe todo mientras que la otra no sabe nada).

Es importante recalcar que lo primero que tenemos que hacer es especificar el resultado: "¿qué es lo que yo quiero?" pues eso es a lo que se obliga la parte experta. Esto es lo que conocemos como Teoría del Resultado.

Otro problema de los contratos informáticos es que son contratos de adhesión[76]. Cuando impera la autonomía de la voluntad es necesario determinar los siguientes puntos (ya que si no, la empresa o parte experta no se responsabilizaría):

- Objeto del contrato.
- Precio.
- Retención del Precio en garantía.
- Mantenimiento (puede ser on-line, por teléfono, o 24 horas los siete días de la semana, o sólo días laborables) si queremos un mantenimiento preventivo.
- Pago: (¿en qué momento?)
- Garantía: que plazo tengo de garantía.
- Pago en Garantía.
- Locales: van a ser mis locales o los locales de la empresa informática.
- La Entrega: la implementación
- Se pueden poner pruebas de aceptación
- Aceptación.
- Formación.
- Respuesta ante incidencias.
- Definiciones: es muy importante la claridad de los conceptos.
- Transferencia de personal.
- Compatibilidad: que todas las herramientas informáticas instaladas sean compatibles entre si.
- Confidencialidad y exclusividad.

[76] Las cláusulas son redactadas por una sola de las partes, con lo cual la otra se limita tan solo a aceptar o rechazar el contrato en su integridad. Entraríamos en la teoría de las **Condiciones Generales de la Contratación.**

Es preciso que se recojan, en un solo contrato o en varios, todos estos puntos o cláusulas anteriormente mencionados, ya que esto si otorgaría más seguridad jurídica a la relación que la Oficina Judicial o en su caso la Administración de Justicia tendría con la empresa informática; en caso de conflictos siempre será más fácil acudir a un solo contrato que a varios.

Es necesario que se redacten las cláusulas de ese contrato con la mayor claridad posible incluyendo la de Confidencialidad y Exclusividad para evitar que la empresa informática venda el programa informático desarrollado a medida para la Oficina Judicial o para la Administración de Justicia a otra entidad. El Pacto de Exclusividad reflejaría el compromiso del programador de no desarrollar programas idénticos para otros.

Hay que diferenciar esta cláusula de la de Confidencialidad que recogería el acuerdo por el que el proveedor de servicios se compromete a guardar la información de manera confidencial en la forma especificada en el acuerdo. Su finalidad es regular la confidencialidad de la información que se comunica al proveedor del servicio para que pueda prestar el servicio.

Por el mismo motivo expresado en el apartado anterior, se aconseja incluir en el mismo contrato una cláusula de mantenimiento del software. No es necesario pactarlo en un contrato a parte. Y siempre se contribuirá a la seguridad en la relación jurídica entre las partes intervinientes en el contrato.

Debe existir un compromiso de tiempo en el que el suministrador garantice prestar ese mantenimiento, por lo tanto se especificará detalladamente la duración pactada del mantenimiento, el lugar en el que se presta el servicio, la forma de pago del mismo si se incluye en el precio del contrato o no, el tiempo de respuesta estipulado y el responsable de este servicio de mantenimiento.

El mantenimiento implica unos controles periódicos de todas las partes del equipo con sustituciones preventivas de aquellos elementos que se considere que pueden tener un fallo o provocar una falta en una parte determinada del equipo.

Se utilizan dos criterios para agrupar los contratos informáticos:

- **el del objeto**: existen características especiales de los distintos objetos sobre los que tratan estos contratos (hardware, software, servicios de mantenimiento y formación, o llave en mano) que hacen que se precise un tratamiento y estudio individualizado.
- **el del negocio jurídico**: los contratos informáticos se llevan a cabo bajo la cobertura de una determinada figura jurídica en la que encuentran acomodo, aunque es necesario adecuar el objeto del contrato al negocio jurídico realizado. Por eso es conveniente conocer las características de ese objeto en relación con el negocio jurídico.

- **Por el Objeto**:
  - **Contratos de hardware**: entendiendo como hardware todo aquello que físicamente forme parte del equipo, incluyendo los equipos de comunicaciones u otros elementos auxiliares necesarios para el funcionamiento del sistema que se va a implementar.
  - **Contratos de software**: hay que distinguir el software de base o de sistema del software de utilidad o de aplicación o usuario. Este último responde a unas necesidades particulares que tendrán que especificarse claramente en el contrato.

Sin embargo, el software de base o de sistema y el de utilidad responden a unas características generales que son las del propio sistema o las de la utilidad a la que sirven y es un producto ya conformado de antemano no sometido a particularidades del usuario. Es necesario compatibilizar el software del usuario al de base y utilidad.

- **Contratos de instalación llave en mano:** en este tipo de contratos van incluidos tanto el hardware como el software, así como determinados servicios de mantenimiento y formación del usuario.
- **Contratos de servicios auxiliares:** tratarían el mantenimiento de equipos y programas o la formación de las personas que utilizarán la aplicación respecto a equipos, sistema o desarrollos.

- **Por el negocio jurídico**: existirán tantos tipos de contratos como negocios jurídicos se realicen sobre este objeto. Algunos de los más utilizados son los siguientes.
  - **Contratos de venta:** cuando el suministrador o vendedor se obliga a la entrega de una cosa determinada (en este caso un bien informático), y el comprador a pagar por ella un precio cierto. La compra-venta puede ser mercantil o civil por lo que se tendrá que atender a la regulación del Código civil o mercantil.
  - **Contratos de arrendamiento financiero**: o de leasing. Se requiere la participación de tres partes en dos contratos diferentes. Por un lado nos encontramos al suministrador (vendedor), una entidad o intermediario financiero (qué comprará el bien) y un usuario del bien que le utilizará en régimen de arrendamiento financiero hasta que haya cumplido con unos requisitos. Cumplidos estos requisitos (normalmente el pago) el equipo pasará a ser propiedad del usuario, transmitido por el propietario (la entidad financiera).
  - **Contrato de alquiler**: es un contrato tipo de los regulados en los artículos 1543 y siguientes del Código Civil. El suministrador se obliga a dar al usuario el uso y disfrute de un bien informático durante un tiempo determinado y por un precio cierto. El suministrador se obliga a efectuar las reparaciones necesarias para la conservación del bien respecto al uso al que ha sido destinado.
  - **Contrato de opción de compra**: tienen que darse tres requisitos; uno respecto al optante ya que se le debe conceder la decisión unilateral de la realización de la opción a compra; otro respecto al precio de la compra-venta, que debe quedar perfectamente señalado para el caso de que el optante decida acceder a dicha compraventa y un tercero respecto al plazo del ejercicio de la opción a compra, que debe quedar determinado con claridad en el acuerdo de las partes.
  - **Contrato de mantenimiento**: puede ser tanto de equipos como de programas o también mantenimiento integral en el que se puede incluir un servicio de formación, asesoramiento y consulta.
  - **Contrato de prestación de servicios**: incluiríamos análisis, especificaciones, horas máquina, tiempo compartido, programas, etc., que los podríamos calificar como contratos de arrendamiento de servicios. Estos se dan cuando una parte se obliga con la otra a prestarle unos determinados servicios, con independencia del resultado que se obtenga.

- **Contrato de arrendamiento de obra:** consiste en el compromiso de una de las partes (suministrador del bien o servicio informático) a ejecutar una obra y de la otra parte a realizar una contraprestación en pago por la obra. Es importante tener en cuenta, para diferenciarlo del contrato anterior, que en este tipo de contratos se ofrece terminar o realizar una obra determinada, independientemente del trabajo o los medios que se empleen.
- **Contrato de préstamo**: una parte entrega a otra el bien informático para que use de él durante un tiempo determinado y le devuelva una vez cumplido ese tiempo. Podemos diferenciar también el contrato de comodato como tipo de contrato de préstamo en el que el suministrador trasfiere el uso del bien informático prestado.
- **Contrato de depósito**: cuando una persona recibe una cosa ajena con la obligación de guardarla y restituirla; es un contrato gratuito salvo pacto en contrario. Esta regulado en los artículos. 1758 y siguientes del Código Civil. En el caso de cumplirse con los requisitos establecidos en el Código de Comercio, artículo. 303 se trataría de un depósito mercantil.

➢ Es importante hacer mención a los **Contratos informáticos en el Ámbito de Internet** y es que dentro de la "red de redes" están proliferando multitud de contratos dirigidos a cubrir las diferentes necesidades que se van originando con su uso.

Hay que tener presente que en el entorno de Internet deben extremarse las medidas de seguridad para garantizar que las transacciones se hagan en un entorno seguro. Algunas medidas propuestas son la utilización de la firma electrónica y los certificados digitales de firma.

Dentro de los contratos informáticos que pueden celebrarse dentro del ámbito de Internet figuran los siguientes:

- **Contratos de acceso a Internet**: a través de estos contratos se solicita el acceso a Internet a cambio de un Precio.
- **Contrato de correo electrónico**: se establece como requisito necesario darse de alta como usuario de correo electrónico que puede tener por objeto comunicaciones internas dentro de una misma empresa así como con el exterior.
- **Contrato de creación de página Web**: este contrato de carácter técnico y de diseño busca revestir el alojamiento de un sitio Web en la red.

- **Contrato de nombres de dominio**: a través de el se registra un nombre de dominio y se adquiere derecho a utilizarlo con exclusividad en la red.
- **Contrato de housing**: por el cual una de las partes se compromete a ubicar en sus instalaciones un determinado hardware y a prestar al cliente una serie de servicios además del alojamiento del hardware. Podemos decir que es un contrato de servicios de una empresa de tecnología a un cliente permitiéndolo alcanzar mayor nivel de competitividad sin necesidad de realizar inversiones en equipamiento tecnológico o en formación del personal informático propio.
- **Contrato de hosting**: por el cual un usuario de Internet que no puede mantener, por motivos técnicos o económicos, su propio servidor, alquila éste a un tercero. De esta manera, el proveedor pone a disposición del cliente, un espacio en su disco duro, para que éste pueda almacenar su información normalmente una página o sitio Web.

15.-PROPIEDAD INTELECTUAL

La Propiedad Intelectual es un tipo especial de propiedad cuya característica fundamental es la intangibilidad del objeto sobre el que recae. Esta característica del objeto hace que se precisen unas medidas de protección especiales.

Nos encontramos a menudo con el problema de que se entiende que cuando una creación intelectual ha sido puesta a disposición del público, ya le pertenece a éste.

La legislación entiende que el objeto de protección de la propiedad intelectual es *"una obra literaria, artística o científica"*, y la persona que gozará de la protección será su autor (como norma general se corresponde con una persona física, pero la ley contempla la posibilidad de que también pueda serlo una persona jurídica).

Se presume autor a quien *firme* la obra, salvo que se demuestre lo contrario, y este autor gozará de la protección de la ley.

También quiero mencionar los tipos de derechos de protección que atribuye la LPI;[77] estos se clasifican en dos tipos:

- **derechos personales:** son irrenunciables e inalienables.
- **derechos patrimoniales**: pueden transmitirse.

En lo que se refiere a la Oficina Judicial, creo que los dos tipos de protección contemplados en la Ley de Propiedad Intelectual, que nos pueden afectar serían:

- **la protección jurídica del software o programas de ordenador.**
- **la protección jurídica de las bases de datos.**

Efectivamente, en el ámbito de la Administración de Justicia, y concretamente de la Oficina Judicial, se persigue incrementar la productividad de ésta proporcionando herramientas al cuerpo de funcionarios al servicio de la misma que le permitan realizar sus tareas habituales de manera más fácil, rápida y ágil.

Con esto se pretende aumentar la calidad del servicio prestado al ciudadano ya que se consigue la apertura y agilización de la comunicación con éste y con los organismos y entidades que intervienen de una forma u otra en los procesos.

[77] LPI: Ley de Propiedad Intelectual. Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

Se requiere que en cada puesto de trabajo exista un ordenador personal que reúna las siguientes características:

- utilice un entorno gráfico (Windows).
- que esté conectado a la Red Judicial de Comunicaciones.
- que tenga acceso integrado al Sistema de Información Documental. Este Sistema permite dos tipos de consulta:
  - ✓ en Jurisprudencia Propia
    a. búsqueda asistida.
    b. búsqueda experta.
    c. histórico de búsqueda.
  - ✓ enlaces a otros sistemas de Jurisprudencia.
    a. Aranzadi.
    b. BOE.

Vemos pues, que en el desempeño de la actividad normal o habitual que se desarrolla en la Oficina Judicial, es imprescindible el uso de programas de ordenador y bases de datos hechos a medida, por lo que se tendrá que tener en cuenta el tipo de protección conferida a éstos.

15.1.-PROTECCIÓN JURÍDICA DE LOS PROGRAMAS DE ORDENADOR

El texto legislativo vigente en la materia es el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual (LPI).

La LPI dedica su Título VII a la protección de los programas de ordenador[78]. Tenemos que decir que la Ley incluye dentro del ámbito de protección conferido a los programas de ordenador la documentación preparatoria que acompaña al programa, entendiendo por tal los manuales técnicos y de uso de los programas de ordenador.

La protección conferida a los programas de ordenador se extiende también a las versiones sucesivas de un programa de ordenador original y los programas derivados del mismo, con la excepción de que el programa de ordenador haya sido creado para ocasionar algún efecto nocivo en un sistema informático.

[78] También conocida como la protección jurídica del software.

Se impone como requisito para esta protección que el programa de ordenador sea original, constituyendo así una creación intelectual propia de su autor, con independencia de la forma de expresión en que se manifiesta dicha creación intelectual.

El legislador español incluye los programas de ordenador como creaciones que se encontraban sujetas a los derechos de propiedad intelectual, conceptuándolas como "obras tecnológicamente avanzadas".

La ley define programa de ordenador como "toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación".

En nuestra legislación podemos encontrarnos con una serie de principios legales que rigen la protección jurídica del software o programas de ordenador:

- los programas de ordenador reciben la protección conferida para las obras literarias mediante derechos exclusivos sujetos a derechos de autor.
- se especifica legalmente quién es la persona titular de los derechos de propiedad intelectual, lo que conlleva en el RDLeg 1/1996 [79]a la enumeración de supuestos tasados en los que se determina quién es o quiénes son los titulares de los derechos de autor sobre los programas de ordenador.
- se determinan una serie de actos sujetos a restricciones que requieren la autorización del titular de los derechos y actos que no constituyen incumplimiento.
- se definen las condiciones para la protección del programa.

Existen otras normas en el ordenamiento jurídico que también ofrecen protección a los programas de ordenador, como el Código Penal de 1995 que regula esta protección en la sección correspondiente a los delitos contra la propiedad intelectual (Art. 270 a 272). Por tanto, el Código Penal protege los programas de ordenador con el mismo régimen previsto para los delitos cometidos contra la propiedad intelectual, tipificando expresamente en su Art.270 las conductas consistentes en la fabricación, puesta en circulación y tenencia de cualquier medio que se destine específicamente a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

[79] aprueba el Texto Refundido de la Ley de Propiedad Intelectual (LPI).

También hay que señalar que cuando un programa de ordenador forme parte de una patente o modelo de utilidad, disponemos de otra forma de protección otorgada por la normativa vigente en materia de protección industrial.

La Ley 11/1986 de Patentes también ofrece protección a los programas de ordenador, cuando estos formen parte de un procedimiento completo susceptible de ser patentado.

Existe una protección de carácter administrativo, concretamente registral, que posibilita que los programas de ordenador accedan al Registro de la Propiedad Intelectual, al igual que sus sucesivas versiones y los programas derivados. Hay que señalar que esta inscripción registral no tiene carácter constitutivo, sino que proporciona publicidad frente a terceros de los derechos inscritos y se convierte en una prueba cualificada sobre la existencia y pertenencia a su titular de los derechos en él inscritos, que podría ser utilizada en juicio. Cómo vemos es una protección más bien de carácter formal, ya que se crea una presunción sobre la existencia de derechos inscritos, si bien cabe prueba en contrario.

Quiero mencionar también los derechos exclusivos de la explotación de un programa de ordenador por parte de quien sea su titular. Según el Art. 99 de la LPI incluirán el derecho de realizar o de autorizar:

- la reproducción total o parcial, incluso para uso personal, de un programa de ordenador, por cualquier medio y bajo cualquier forma, ya fuere permanente o transitoria. Cuando la carga, presentación, ejecución, transmisión o almacenamiento de un programa necesiten tal reproducción deberá disponerse de autorización para ello, que otorgará el titular del derecho.
- la traducción, adaptación, arreglo o cualquier otra transformación de un programa de ordenador y la reproducción de los resultados de tales actos, sin perjuicio de los derechos de la persona que transforme el programa de ordenador.
- cualquier forma de distribución pública incluido el alquiler del programa de ordenador original o de sus copias.

Cuando se produzca cesión del derecho de uso de un programa de ordenador, se entenderá, salvo prueba en contrario, que dicha cesión tiene carácter no exclusivo e intransferible, presumiéndose que lo es para satisfacer únicamente las necesidades del usuario. La primera venta en la UE de una copia de un programa por el titular de los derechos o con su consentimiento, agotará el derecho de distribución de dicha copia, salvo el derecho de controlar el subsiguiente alquiler del programa o de una copia del mismo.

Quiero acabar mencionando que la duración de la protección de los derechos de autor es toda la vida del autor y 70 años después de su muerte o declaración de fallecimiento.

Cuando se trata de una persona jurídica serían 70 años desde el 1 de enero del año siguiente al de la divulgación lícita del programa o al de su creación si no se hubiera divulgado.

15.2.-PROTECCIÓN JURÍDICA DE LAS BASES DE DATOS.

Las bases de datos que son utilizadas por la Administración de Justicia para el tratamiento eficaz de la información que precisa en el desarrollo normal de su actividad son objeto de protección por la LPI.

Las bases de datos se definirían de una manera genérica como depósitos en los que se contiene información, que puede ser útil para distintos usuarios y que sea recuperable mediante distintas aplicaciones. Estos depósitos guardan la información de manera estructurada, añadiéndole el valor de una recuperación y tratamiento, automatizado o no, que permita una mayor utilidad de esa información.

El contenido de la base de datos será, por tanto, un conjunto de documentos o datos, y la propia base de datos, le otorga una estructura lógica que le confiere un valor añadido. Estos datos o documentos no tienen por qué ser propiedad de la misma persona que desarrolla la base de datos. Son objetos distintos y la protección otorgada también será distinta.

En función del tipo de acceso a las bases de datos, estas se pueden clasificar en dos grupos:

- bases de datos autónomas: o de acceso local, desde el lugar en que nos encontremos utilizando el ordenador. Normalmente se encontraran ubicadas en un CD-ROM o un DVD-ROM.

- bases de datos on-line: o de acceso remoto. Se encontrarán en un servidor común.

Las bases de datos, entendidas como estructura que contiene una información, son objeto de protección por la LPI al ser consideradas obras de creatividad intelectual (tanto en el momento de almacenamiento de la información como en el de recuperación de la misma de acuerdo a la consulta planteada). Podemos decir que el objeto de protección no es solamente la recopilación de información, sino todo el procedimiento de creación de la base de datos y el resultado del mismo.

Además de la LPI, la Ley 5/1998, de 6 de marzo de Incorporación al Derecho Español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo sobre la Protección Jurídica de las Bases de Datos, también otorga protección a las bases de datos en España. Se articula por tanto un doble ámbito de protección:

- el que otorga el derecho de autor.
- el derecho "sui generis" otorgado por la citada Ley 5/1998 que protegería la inversión sustancial evaluada cualitativa o cuantitativamente realizada por el fabricante de cualesquiera medios como tiempo, esfuerzo, energía, etc., para la obtención, verificación o presentación de su contenido.

16.-PLAN DE TRANSPARENCIA JUDICIAL. LA ESTADÍSTICA JUDICIAL.

16.1.-GÉNESIS DEL PLAN DE TRANSPARENCIA JUDICIAL.

El Plan de Transparencia Judicial[80] será, a partir de su publicación por el Gobierno, una herramienta decisiva para la mejora de la Administración de Justicia que demandan los ciudadanos. El Pacto de Estado para la Reforma de la Justicia suscrito el 28 de mayo de 2001 contempló en su apartado 13 la preparación de una Carta de Derechos de los Ciudadanos ante la Justicia, que debía atender a los principios de transparencia, información y atención adecuada y establecer los derechos de los usuarios de la Justicia.

La Comisión de Seguimiento del Pacto de Estado redactó por acuerdo unánime de todos sus integrantes dicha Carta de Derechos de los Ciudadanos ante la Justicia, que fue aprobada por el Pleno del Congreso de los Diputados en su sesión del día 22 de abril de 2002 como Proposición no de Ley.

Se trata de conseguir una Justicia moderna y abierta a los ciudadanos a la par que responsable ante ellos, dejando claro que los ciudadanos podrán formular sus quejas y sugerencias sobre el funcionamiento de la Justicia y exigir, en caso necesario, las reparaciones a que hubiera lugar. Se concebía y defiende para ello una Justicia transparente, comprensible, atenta con el ciudadano, responsable ante él, ágil y tecnológicamente avanzada y, por fin, protectora de los más débiles, como son, entre otros, las víctimas del delito, los menores, los discapacitados, los inmigrantes u otras capas desfavorecidas de la población.

El título I de la Carta de Derechos proclama que el ciudadano tiene derecho a recibir información general y actualizada sobre el funcionamiento de los juzgados y tribunales y sobre las características y requisitos genéricos de los distintos procedimientos judiciales.

El apartado 2 de la Carta de Derechos señaló el que tienen los ciudadanos a recibir información transparente sobre el estado, la actividad y los asuntos tramitados y pendientes de todos los órganos jurisdiccionales.

Se enumeraban además, dentro de tal objetivo de transparencia y de modo concreto:

[80] Aprobado por la Resolución de 28 de octubre de 2005, de la Secretaría de Estado de Justicia por la que se dispone la publicación del Acuerdo del Consejo de Ministros de 21 de octubre de 2005.

- El derecho de los ciudadanos a conocer el contenido actualizado de las leyes españolas y de la UE mediante un sistema electrónico de datos fácilmente accesible.
- El derecho a conocer el contenido y estado de los procesos en los que tengan interés legítimo de acuerdo con lo dispuesto en las leyes procesales.
- El acceso por los interesados a los documentos, libros, archivos y registros judiciales que no tengan carácter reservado; y la necesaria motivación por las autoridades y funcionarios de la denegación de acceso a una información de carácter procesal.

A través del Plan de Transparencia Judicial, las Cortes Generales, el Gobierno, las CCAA, el CGPJ y los propios ciudadanos deberían tener a su disposición una herramienta de información continua, rigurosa y contrastada acerca de la actividad y la carga de trabajo de todos los órganos jurisdiccionales del Estado, lo que a su vez permitiría el tratamiento estadístico y su aplicación en todo tipo de procesos de planificación y modernización de la Administración de Justicia, enlazando así con uno de los grandes ejes programáticos del Pacto de Estado para la Reforma de la Justicia.

De modo concreto establecía el apartado 1 del artículo 14 de la Ley 15/2003 [81]que el Plan de Transparencia Judicial constituye una herramienta básica de las Administraciones Públicas y del CGPJ para la planificación, desarrollo y ejecución de las políticas públicas relativas a la Administración de Justicia.

Disponía el artículo 14 de la Ley 15/2003 en su apartado 4 que el Plan de Transparencia Judicial sería aprobado por el Gobierno, a propuesta del Ministerio de Justicia, previo informe del CGPJ, del Fiscal General del Estado y de las CCAA que hubieran asumido el traspaso de funciones y servicios para la provisión de medios personales y materiales en materia de Justicia.

Así las cosas, se aprueba la LO 19/2003, de 23 de diciembre, de modificación de la LO 6/1985, del Poder Judicial, en cuyo artículo 461 se define a la Estadística Judicial como un instrumento básico al servicio de las Administraciones Públicas y del CGPJ para la planificación, desarrollo y ejecución de las políticas públicas relativas a la Administración de Justicia y, en particular, para atender las finalidades atinentes al ejercicio de la política legislativa del Estado en materia de Justicia, a la modernización de la organización judicial, a la planificación y gestión de los recursos

[81] Ley 15/2003, de 26 de mayo, reguladora del régimen retributivo de las carreras judicial y fiscal.

humanos y medios materiales al servicio de la Administración de Justicia y al ejercicio de la función de inspección sobre los juzgados y tribunales.

La Comisión Nacional de Estadística Judicial[82], está integrada por el Ministerio de Justicia, una representación de las CCAA con competencias en la materia, el CGPJ y la Fiscalía General del Estado, deberá aprobar los planes estadísticos, generales y especiales, de la Administración de Justicia y establecer criterios uniformes y de obligado cumplimiento para todos sobre la obtención, tratamiento informático, transmisión y explotación de los datos estadísticos del sistema judicial español, sin perjuicio de que las Administraciones Públicas con competencias en materia de Administración de Justicia puedan llevar a cabo las explotaciones de otros datos estadísticos que puedan ser recabados a través de los sistemas informáticos, siempre que las consideren necesarias o útiles para su gestión.

La propia reforma de la LOPJ prevé que la Estadística Judicial asegure, en el marco de un Plan de Transparencia, la disponibilidad permanente de una información actualizada, rigurosa y debidamente contrastada sobre la actividad y carga de trabajo de todos los órganos, servicios y oficinas judiciales de España y también sobre las características estadísticas de los asuntos sometidos al conocimiento de la Justicia.

16.2.-RAZONES DEL PLAN DE TRANSPARENCIA JUDICIAL

Las encuestas especializadas revelan sistemáticamente que la valoración de la población en general sobre la Administración de Justicia es más negativa que la que realizan quienes alguna vez han tenido que acudir a los tribunales.

Entre estos últimos, usuarios de la Justicia, prevalece el número de ciudadanos que cree que la Administración de Justicia funciona razonablemente frente a quienes consideran que funciona mal o muy mal.

Ahora bien, dicho servicio está lejos del nivel de excelencia reclamado por los ciudadanos, la opinión pública en general penaliza gravemente a la Administración de Justicia por la excesiva duración de los procesos, mientras que los usuarios del servicio público tienen una opinión mucho menos negativa, considerando que la calidad en la resolución de los litigios es más importante que la agilidad en su conclusión. Esta contradicción sólo podrá resolverse adecuadamente cuando se conozcan con rigor datos definitivos, oficiales y fiables sobre las duraciones reales de

[82] Regulada por el RD 1184/2006, de 13 de octubre. Sería el Órgano colegiado adscrito al Ministerio de Justicia que actúa con plena autonomía en el ejercicio de sus funciones.

la tramitación en los procedimientos judiciales en nuestro país, identificándose pormenorizadamente cuáles son las disfunciones que provocan dichos retrasos, sus causas reales y los responsables de las mismas, porque de no alcanzarse ese objetivo, la valoración del Servicio Público de la Administración de Justicia dependerá de informaciones sesgadas, rumores, realidades obsoletas y casos insólitos. El desconocimiento efectivo de datos definitivos, oficiales y fiables sobre las duraciones reales en los procedimientos judiciales y sus causas no sólo confunde a la opinión pública, sino que además impide a las distintas Administraciones responsables contar con los elementos de juicio necesarios para acometer reformas profundas que permitan agilizar estos procedimientos. Es exigible, por tanto, que los poderes públicos y los ciudadanos en general conozcan mediante instrumentos informáticos y en tiempo real la duración de los procesos en todas las jurisdicciones, así como los motivos concretos de los retrasos.

Debe despejarse, asimismo, qué causas motivan las impuntualidades en los procesos, así como dar a conocer las quejas de los usuarios sobre el trato recibido por cada uno de los intervinientes en el pleito, ya que la impuntualidad y el mal trato constituyen una piedra de toque para los usuarios sobre la calidad del servicio público de la Administración de Justicia, siendo exigible concretar también las pautas necesarias para medir tanto el volumen de trabajo de cada órgano jurisdiccional, como la calidad de las actuaciones de todos los intervinientes en el proceso.

Se garantizará, de este modo, la planificación presupuestaria en materia de retribuciones y la correcta gestión de los Cuerpos al servicio de la Administración de Justicia, contribuyendo finalmente a clarificar los costes reales de los procesos.

Debe conocerse finalmente si los servicios de justicia gratuita, cuyo coste aumenta geométricamente año tras año, atienden adecuadamente las demandas sociales de justicia, lo que obligará a identificar costes y resultados en todos los ámbitos del estado.

Será pertinente identificar, así mismo, todas las instalaciones y equipos de trabajo de la Administración de Justicia siendo necesario precisar si están en condiciones de permitir eficientemente el despliegue de la nueva oficina judicial. Habrá de permitirse también que los ciudadanos y los usuarios del servicio conozcan a través de recursos informáticos y en tiempo real cuál es el estado de las infraestructuras y medios de la Administración de Justicia.

Se impone, por otro lado, publicar en tiempo real el resultado de todos los litigios, permitiendo, de esta manera, que las Administraciones afectadas y los ciudadanos en general puedan conocer eficazmente el funcionamiento de nuestros Tribunales, así como la evaluación del funcionamiento de las normas legales y su capacidad de resolver los conflictos sociales.

Es necesario reconocer la calidad del desempeño de cada uno de los intervinientes en la Administración de Justicia, utilizando, a estos efectos, tanto los instrumentos de control interno de calidad en el funcionamiento de la Administración de Justicia, como los mecanismos de control externo, en los que los usuarios del Servicio Público jugarán un papel determinante.

Los rasgos que caracterizan la existencia de una buena Justicia son la independencia, la imparcialidad, la competencia, la asequibilidad, la eficiencia, la eficacia, la duración razonable, la calidad, la previsibilidad, la igualdad y la responsabilidad, garantizándose, en cualquier caso, que el coste público de la Administración de Justicia se corresponde con los resultados del servicio público, debe conocerse necesariamente por las Cortes Generales, el Gobierno, las CCAA, el CGPJ, la Fiscalía General del Estado, los ciudadanos en general, si la Justicia española supera efectivamente el nivel exigible en cada uno de tales rasgos, ya que el conocimiento efectivo en tiempo real y por medios informáticos de dichos extremos permitirá a los responsables públicos, la modernización de la organización judicial, la planificación y gestión de los recursos humanos y medios materiales al servicio de la Administración de Justicia y el desarrollo de la función de inspección sobre juzgados y tribunales, así como el control sobre el funcionamiento de todos los intervinientes en el proceso y la calidad de sus intervenciones, contribuyendo, por otra parte, a la gestación de una opinión pública informada que pueda influir razonablemente en el control efectivo de la Administración de Justicia, sus responsables y los intervinientes en ella.

Éstas son, por tanto, las razones justificadoras del Plan de Transparencia Judicial que el Gobierno aprobó a propuesta del Ministerio de Justicia, previo informe del CGPJ, el Fiscal General del Estado y las CCAA con competencias asumidas en materia de Justicia, cumpliéndose el mandato del artículo 14 de la Ley 15/2003 reguladora del régimen retributivo de las carreras judicial y fiscal.

16.3.-PRINCIPIOS DE LA ESTADÍSTICA JUDICIAL QUE HA DE OPERAR EN EL MARCO DEL PLAN DE TRANSPARENCIA JUDICIAL.

Tanto el Pacto Internacional de Derechos Civiles y Políticos [83]en su artículo 14.1 como el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales[84] en su artículo 6 y la Constitución española en el artículo 24 reconocen, con distintas formulaciones, el derecho de todas las personas a obtener la tutela efectiva de los tribunales en un proceso público sin dilaciones indebidas y con todas las garantías. También el artículo 120 de la Constitución resalta el carácter público de las actuaciones judiciales, con las excepciones que prevean las leyes de procedimiento, y añade la obligación de que las sentencias sean siempre motivadas y se pronuncien en audiencia pública.

El primer principio del Plan de Transparencia Judicial es el relativo a la necesaria publicidad de las actuaciones judiciales, que deberá cumplir al menos dos objetivos: proteger a los ciudadanos de una Justicia sometida al control y conocimiento públicos y mantener la confianza de la comunidad en sus tribunales. La transparencia judicial, en su vertiente de publicidad del proceso, no debe perder de vista la necesaria protección de derechos e intereses legítimos que puedan verse afectados por la falta de autorregulación de los medios de comunicación sobre los límites que no han de sobrepasarse en una sociedad avanzada. Además de ello, la idea de transparencia judicial ha de relacionarse necesariamente con lo establecido en el artículo 9 de la Constitución Española, para ello, es preciso que se pueda conocer no sólo el contenido de las resoluciones judiciales, sino también el tiempo medio en que éstas deberían haber sido dictadas, lo que dará un parámetro suficiente acerca de si el funcionamiento de la Administración de Justicia ha sido, en su caso, anormal y por tanto tributario de una indemnización con cargo al Estado y conforme a la Ley.

16.4.-OBJETIVOS DEL PLAN DE TRASPARENCIA JUDICIAL

El Plan de Transparencia Judicial, en íntima conexión con la Estadística Judicial tal y como la define hoy el artículo 461 de la LOPJ, debe atender a la planificación, desarrollo y ejecución de las políticas públicas relativas a la Administración de

[83] Tratado multilateral adoptado por la Asamblea General de Naciones Unidas mediante la Resolución 2200A de 16 de diciembre de 1966. Entró en vigor el 23 de marzo de 1976.
[84] Adoptado por el Consejo de Europa en 1950, entro en vigor en 1953; tiene por objeto proteger los derechos humanos y las libertades fundamentales y permite un control judicial del respeto de dichos derechos individuales.

Justicia y, en particular, al ejercicio de la política legislativa del Estado en materia de Justicia; a la necesaria modernización de la organización judicial; a la adecuada planificación y gestión de los recursos humanos y medios materiales al servicio de la Administración de Justicia; y al ejercicio correcto de la función de inspección sobre los juzgados y tribunales.

16.5.-INSTRUMENTOS DEL PLAN DE TRANSPARENCIA JUDICIAL.

La consecución del objetivo general de transparencia, proclamado en el Carta de Derechos de los Ciudadanos[85], se articulará a través del Plan de Transparencia Judicial, comprometido firmemente con el propósito de desterrar para siempre la opacidad informativa que dificulta el seguimiento de la actividad jurisdiccional, pretendiéndose que las Cortes Generales, el Gobierno, las CCAA, el CGPJ, la Fiscalía General del Estado y los propios ciudadanos tengan una información continua, rigurosa y contrastada sobre la actividad y la carga real de trabajo de todos los órganos jurisdiccionales del Estado y sobre los medios materiales y el desempeño de todos los profesionales que intervienen en la Administración de Justicia.

El desarrollo de una nueva Estadística Judicial será obligatoriamente el instrumento básico para el despliegue operativo del propio Plan de Transparencia, proporcionando a las Administraciones Públicas, al CGPJ y a la Fiscalía General del Estado los elementos necesarios para la planificación, desarrollo y ejecución de las políticas públicas relativas a la Administración de Justicia.

La Estadística Judicial deberá asegurar la disponibilidad permanente de información actualizada, dotada de rigor y debidamente contrastada sobre la actividad y carga de trabajo de todos los órganos, servicios y oficinas judiciales del Estado, así como sobre las características estadísticas de los asuntos sometidos a su conocimiento, garantizando, en cualquier caso, que los ciudadanos tengan acceso a la misma, lo que se constituye en requisito imprescindible para conformar una opinión pública informada.

Lograr los objetivos propuestos, facilitando la obtención, tratamiento y transmisión de los datos estadísticos a través de tecnologías de la información

[85] La Carta de Derechos de los Ciudadanos ante la Justicia atiende a los principios de transparencia, información y atención adecuada y establece los derechos de los usuarios de la Justicia. Proposición no de Ley aprobada por el Pleno del Congreso de los Diputaos, por unanimidad de todos los grupos parlamentarios, el16 de abril del 2002.

avanzadas, exigirá aprobar planes estadísticos generales y especiales de la Administración de Justicia, estableciendo criterios uniformes y de obligado cumplimiento para todos sobre la obtención, tratamiento informático, transmisión y explotación de los datos estadísticos del sistema judicial español. Dicha misión ha sido encomendada a la Comisión Nacional de Estadística Judicial por el artículo 461 de la LOPJ.

Debe añadirse como un instrumento más que avale el propósito de transparencia judicial, la razonabilidad de que existiera una sola aplicación informática para todos los órganos judiciales y para todas las Fiscalías o, al menos que las aplicaciones informáticas fueran compatibles entre sí. Todos los sistemas informáticos de gestión procesal deberán seguir las normas establecidas en el Test de Compatibilidad de Aplicaciones de Gestión Procesal[86] para la Administración de Justicia aprobado por el CGPJ en 1999. Además de estas normas, deberán establecerse unos valores de dominio comunes para el intercambio de datos y unos esquemas comunes de tramitación, sobre todo en la definición de hitos que pudieran ser utilizados como referentes a la hora de obtener estadísticas sobre la vida procesal de los asuntos.

A la hora de plantearse un sistema de apoyo estadístico para la toma de decisiones, es claro ya que el entorno de la Administración de Justicia plantea al menos los siguientes inconvenientes: mucha dispersión geográfica; entornos tecnológicos heterogéneos; y una utilización no homogénea e incompleta de los sistemas por parte de los usuarios.

La información estadística de los asuntos sometidos a conocimiento de los Juzgados y Tribunales debería obtenerse de manera que el proceso estadístico esté integrado en el de gestión y no suponga para el funcionario del órgano correspondiente una tarea o esfuerzo adicionales. Se trata de incentivar la recogida correcta del dato ya desde la propia utilización de la aplicación de gestión procesal, lo que ayudaría además a que el personal de las oficinas judiciales comprobara que es útil para su propio trabajo, que facilita las tareas a llevar a cabo, sirve para la autoevaluación del desempeño, facilita la información demandada por los ciudadanos y sirve también para valorar la productividad.

[86]Se desarrolla con el fin de lograr la interconexión de los órganos judiciales entre sí; para que todas las aplicaciones de gestión procesal "se entiendan" y puedan comunicarse a efectos procesales. Se han realizado distintos protocolos de comunicación e intercambio de información para facilitar la interoperabilidad entre los órganos judiciales y las fiscalías así como con terceros a los que se les requiere información y documentación durante la tramitación de los procedimientos.

Desde el punto de vista técnico, la herramienta de gestión procesal ha de ser, en la medida de lo posible, la única fuente de registro y almacenamiento de la información cruda en lo que se refiere a los datos que deban obtenerse del propio proceso judicial. De esta manera se minimiza el coste necesario para alimentar los distintos registros o bases de datos ajenas a la aplicación procesal, y se minimiza el número potencial de errores ocasionados por los distintos sistemas de entrada de datos, lo que contribuye a garantizar la homogeneidad y fiabilidad de la información.

La información estadística una vez elaborada, se constituye en el único referente de apoyo a la toma de decisiones, el cual se fundamenta en tres pilares: la necesidad de construir un repositorio único de información; la necesidad de construir y asegurar los procesos de extracción, transporte y almacenamiento; y la explotación estadística de la información.

El repositorio único constituye un Directorio Nacional de Asuntos (DNA) basado en la aplicación Libra/Minerva[87], es decir, replica del modelo de datos de la aplicación procesal del Ministerio de Justicia, llevando un registro índice de todos los asuntos. Paralelamente, los modelos de datos de las aplicaciones procesales del resto de las CCAA, habrán de ser mapeados dentro del DNA, si se pretende llevar constancia de los mismos.

Para asegurar los procesos de extracción y transporte, es necesario previamente asegurar los canales de comunicación de datos entre los órganos generadores de la información y los servidores que actúan como repositorio del DNA, es decir, la red o redes físicas deben asegurar su visibilidad entre las mismas, los anchos de banda suficientes y la dedicación de caudal de transmisión asegurado para dicha tarea.

La explotación de dicha información habrá de generarse de manera gradual, para que los distintos colectivos de usuarios de la información agregada se incorporen al sistema no globalmente, sino en distintas fases con el fin de conseguir funcionalidades dependientes de cada grupo de usuarios.

En definitiva, el DNA debería recoger de manera sistemática todos aquellos datos que permitan responder a preguntas referentes a la misión del propio Plan de Transparencia Judicial (servicio público, ejecución del gasto, costes de la justicia, eficacia de la misma, calidad y costes de la no-calidad).

[87] Sistemas informáticos de tramitación y gestión procesal utilizados en las Oficinas Judiciales.

En cuanto a la transparencia del trabajo del Ministerio Fiscal en la Administración de Justicia, son dos los ámbitos principales en los que habrá de profundizarse.

En el primero de ellos, y en relación al desarrollo del Plan de Modernización Tecnológica de la Fiscalía General del Estado, se deberá establecer un marco uniforme de actuación del Ministerio Fiscal a través de medios informáticos y telemáticos para el más eficaz cumplimiento de sus funciones. Así, se configurará un Sistema de Información Único del Ministerio Fiscal que canalice el intercambio de información entre la Fiscalía General del Estado y las distintas Fiscalías. Dicho Sistema lo constituirá en esencia una base de datos centralizada que se alimentará de los datos existentes en los diferentes sistemas de gestión procesal puestos a disposición de las Fiscalías por las Administraciones competentes en la materia. A estos efectos, las distintas aplicaciones de gestión procesal implantadas en las Fiscalías deberán adecuarse a unos mismos estándares de codificación de valores (delitos, materias, tipos de procedimiento, tipos de intervención, órganos judiciales) y a unos mismos esquemas de tramitación aprobados por la Comisión Nacional de Informática y Comunicaciones Electrónicas del Ministerio Fiscal en el marco de los criterios uniformes que llegue a establecer la Comisión Nacional de Estadística Judicial.

Estos sistemas de gestión procesal deberán integrarse con el Sistema de Información del Ministerio Fiscal a través de una Red de Comunicaciones Electrónicas del Ministerio Fiscal. A través de esta Red, los miembros de la Carrera Fiscal podrán acceder a los Registros Públicos y aplicaciones de ámbito nacional gestionados por el Ministerio de Justicia y se asegurará eficazmente la unidad de actuación del Ministerio Fiscal, de conformidad con lo establecido en el artículo 124 de la Constitución, no solamente en los ámbitos penales, sino también en los procedimientos de carácter civil, contencioso-administrativo, laboral o de menores en los que interviene el Fiscal.

El segundo ámbito relacionado con el Ministerio Público en el que habrá de actuarse para lograr avances significativos en materia de estadística judicial es el del inmediato y continuado intercambio de información con los órganos judiciales. Normalmente en una Fiscalía sólo se tiene conocimiento de una causa a través del parte de incoación, pero todos los datos llegan a saberse cuando la causa entra físicamente en la Fiscalía, ya muy avanzado el procedimiento, por lo general cuando

se da traslado para formular escrito de acusación. Es entonces cuando el funcionario de la Fiscalía ha de insertar en su aplicación informática los datos relativos al procedimiento y a los intervinientes, produciéndose una situación de acceso duplicado, costoso, no uniforme y normalmente tardío de los datos en la Fiscalía, lo que lleva aparejado que, por conocer el Fiscal con tardanza la calificación, clave o código que se asigna al procedimiento, no pueda alertar al Juzgado acerca del modo en que ha sido registrado, por lo que durante toda la tramitación, y a efectos estadísticos, será computado como un asunto de una naturaleza, y no de otra. Se deben establecer las herramientas necesarias de comunicación entre las Fiscalías y los órganos judiciales, que permitan llegar a conocer fiablemente no sólo el número de asuntos tramitados sino su verdadera clasificación y naturaleza.

El buen funcionamiento del Servicio Común de Registro y Reparto de la Oficina Judicial es pieza o instrumento esencial del Plan de Transparencia.

Deberán establecerse normas estandarizadas sobre conceptos, definiciones, clasificaciones, nomenclaturas y códigos que permitan la obtención y clasificación homogénea de los datos, asegurando la compatibilidad de los distintos sistemas informáticos de las Administraciones implicadas en el Plan y también criterios uniformes, claros, precisos y de obligado cumplimiento para todos a la hora de registrar los asuntos que entren a trámite en los Juzgados y Tribunales españoles ya que el correcto registro de los asuntos es el punto de arranque ineludible para la posterior obtención, tratamiento informático, transmisión y explotación adecuada de los datos estadísticos del sistema judicial español. El correcto registro del asunto tiene aún una mayor trascendencia, en ocasiones, cuando puede llegar a afectar a los derechos fundamentales de los litigantes.

Instrumentos adecuados para la consecución del objetivo de transparencia judicial que avala este plan son también los portales de Justicia del Ministerio[88], del CGPJ, de las CCAA y de la Fiscalía General del Estado, debiendo recordar que el apartado 2 de la Carta de Derechos de los Ciudadanos ante la Justicia establece el derecho de los ciudadanos a conocer el contenido actualizado de las leyes españolas y de la UE mediante un sistema electrónico de datos fácilmente accesible, lo que evidencia la necesidad de mantener permanentemente actualizadas estas páginas de información, que posibilitarán también el acceso a las aplicaciones de información

[88] En octubre del 2006 se presenta www.mjusticia.es . Esta nueva Web mejora a la anterior en accesibilidad, organización y contenidos.

que se deseen, para cuyo acceso se utilizará la autentificación mediante certificados, mecanismos de usuario y clave o aquellos otros sistemas que se estimen convenientes en cada caso.

Este sistema exigirá la coordinación con las CCAA de manera que se pudiera acceder de modo distribuido a todos los sistemas de gestión procesal activos y se realizarán las normalizaciones adecuadas y el modelo de acceso a los datos, que podría ser descentralizado, en cuyo caso cada CCAA y el Ministerio de Justicia ofrecerían información a los interesados únicamente de los asuntos que se tramitasen en las oficinas judiciales del ámbito de sus competencias, o centralizado, para cuya hipótesis tanto el portal Justicia.es del Ministerio de Justicia como los de las CCAA informarían de todos los asuntos que afectaran al interesado en todo el territorio del Estado, lo que exigiría de las distintas Administraciones la elasticidad necesaria para compartir informaciones y contenidos.

En todo caso deberá contarse con un Documento de Seguridad que asegure al ciudadano y a la Administración que los procedimientos telemáticos reúnen las características necesarias para cumplir la normativa vigente en cada momento en lo relativo a la protección de datos de carácter personal.

Se establecerá igualmente el acceso de los interesados a los documentos, libros, archivos y registros judiciales que no tengan carácter reservado, buscando la implementación de sistemas que generen la documentación sin sobrecargar las comunicaciones y con formatos normalizados que se puedan presentar de modo coherente a través de Internet.

El acceso a la estadística judicial que pueda publicarse en el portal del Ministerio de Justicia será pleno para los ciudadanos, en cumplimiento de lo establecido en el artículo 461.2 de la LOPJ. Para la presentación de estos datos se estudiará el empleo de un Sistema de Información Geográfico [89](GIS) que sea alimentado automáticamente desde las propias aplicaciones de gestión procesal.

En otro orden de cosas, el Gobierno propondrá en el Plan de Transparencia la implantación generalizada de sistemas de interconexión e intercambio de documentos, tales como el sistema LexNet. Se trata de un sistema de correo "securizado", que permite el intercambio de documentos entre los operadores jurídicos y los órganos

[89] Es una integración organizada de hardware, software y datos geográficos diseñada para capturar, almacenar, manipular, analizar y desplegar en todas sus formas la información geográficamente referenciada con el fin de resolver problemas complejos de planificación y gestión.

judiciales, de modo que la presentación de escritos y el traslado de copias desde los procuradores y abogados hacia las oficinas judiciales y las notificaciones desde éstas hacia los operadores jurídicos se realiza de forma automática, a través de certificados de firma digital reconocida. Como consecuencia, el sistema se ve revestido de los principios de **autenticación** (el remitente es quien dice ser), **confidencialidad** (sólo el remitente y el destinatario pueden conocer el contenido de los documentos), **integridad** (el documento no puede ser alterado por nadie) **y no repudio** (el remitente no puede negar el hecho del envío ni el destinatario el hecho de su recepción). El sistema garantiza además el **sellado de tiempo**, de tanta importancia en el flujo de documentos entre operadores jurídicos para la consecución de los plazos vigentes en materia procesal.

Dentro del Plan de Transparencia Judicial, el Sistema Lexnet aportará grandes ventajas. Así, permitirá disponer de información estadística relativa al número de documentos que se intercambian entre los diferentes operadores jurídicos; permitirá disponer de información estadística relativa al tipo de procedimiento y orden jurisdiccional, así como el ámbito que genera mayor volumen de documentación; y constituirá una herramienta irrenunciable para la comunicación en tiempo real entre los Servicios Comunes Procesales y las Unidades Procesales de Apoyo Directo al Juez, evitando en lo posible el trasiego innecesario de papel.

Otro instrumento relevante en el Plan de Transparencia Judicial es el mejor desarrollo del derecho de los ciudadanos a formular quejas, reclamaciones y sugerencias relativas al incorrecto funcionamiento de la Administración de Justicia y a recibir respuesta a ellas con la mayor celeridad, y en todo caso en el plazo máximo de un mes, que fue recogido ya en la Carta de Derechos de los Ciudadanos ante la Justicia.

El Reglamento 1/1998, de 2 de diciembre, del CGPJ, de tramitación de quejas y denuncias relativas al funcionamiento de los juzgados y tribunales, y la Instrucción 1/1999, por la que se aprobó el protocolo de servicio y los formularios de tramitación de quejas, reclamaciones y previa información al ciudadano, vinieron a dar desarrollo reglamentario al artículo 110.2.m de la LOPJ en la redacción consagrada por la LO 16/1994[90], de 8 de noviembre, cubriendo así el vacío normativo existente en el ámbito

[90] Ley por la que se reforma la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

de la Administración de Justicia, sobre el derecho de los ciudadanos a recabar información, así como a formular quejas y reclamaciones en el citado ámbito.

Conforme al Reglamento e Instrucción citados, los interesados podrán presentar sus quejas o denuncias, así como en general iniciativas y sugerencias relativas al funcionamiento de los Juzgados y Tribunales, en el CGPJ, en los Servicios Comunes de Oficinas de Atención al Ciudadano y, allí donde no existan éstas, en los órganos judiciales o en los de gobierno. Igualmente podrán presentarse a través de los Registros contemplados en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre[91].

El Plan de Transparencia Judicial aboga igualmente por la definitiva mejora del Sistema de Registros Judiciales, que constituye un referente ineludible para el ejercicio eficaz de las funciones que, en materia penal, las leyes atribuyen a la Administración de Justicia. Su gestión se ha beneficiado de las innovaciones que las nuevas tecnologías han venido ofreciendo, lo que ha determinado unas posibilidades de información inimaginables en el momento en que su organización fue concebida, pero supone nuevas oportunidades y también riesgos en la utilización de la información en ellos contenida.

No parece necesario señalar detenidamente la singular sensibilidad de esta información. Es importante que los principios originales que motivaron su creación y sus fundamentales características se continúen manteniendo necesidades: atender eficazmente las necesidades de información de los órganos jurisdiccionales penales en relación con los antecedentes de las personas incursas en un determinado procedimiento.

No se trata de un Sistema de Registros de carácter público, de lo que se derivan importantes limitaciones en el uso de la información cuando ésta se dirige a fines distintos de los que originariamente justificaron su recogida. Ello no puede impedir, sin embargo, en el marco de la legislación sobre protección de datos de carácter personal, que la información contenida en los mismos pueda ser considerada útil para atender otros posibles fines que guarden conexión con la propia funcionalidad de los Registros.

El Sistema de Registros tiene que asegurar, por un lado, que las necesidades de los órganos judiciales estén atendidas sin más límites que los que las leyes establezcan, y, por otro, garantizar el derecho de los ciudadanos al acceso individual a

[91] Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

los datos contenidos en el Registro, solicitando su rectificación o cancelación, y expidiendo, en su caso, el correspondiente certificado, cuando así sea exigido por una norma para el ejercicio de un derecho. Por ultimo, los Registros se constituyen en un eficaz instrumento de gestión, de forma que las diferentes Administraciones Públicas, en el marco del Plan de Transparencia, puedan obtener información estadística de singular interés para la adopción de decisiones y la definición de prioridades en la agenda pública.

Los acuerdos o convenios suscritos con Estados en ámbitos de cooperación bilateral o multilateral obligan al Registro a una continua evaluación de sus procedimientos, innovándolos cuando sea necesario, con la ayuda de las nuevas tecnologías de la información, en un marco legal flexible, pero con respeto a los principios a que responde su creación.

Instrumento decisivo también de cualquier propósito de transparencia judicial es la existencia de un Sistema Central de Comunicaciones, seguro y restringido entre las distintas redes judiciales territoriales. En estos momentos el Punto Neutro Judicial[92], servicio de naturaleza técnica que presta el CGPJ, constituye el modo de comunicaciones a través del cual las CCAA con competencias asumidas en materia de Justicia acceden a las distintas aplicaciones centralizadas (acceso al Registro Central de Penados y Rebeldes, por ejemplo). El Punto Neutro Judicial constituirá el nexo de comunicaciones que permitirá a las CCAA acceder a dichas aplicaciones, pero es de prever que también a la información estadística derivada del plan de Transparencia Judicial y de los planes estadísticos, generales y especiales, de la Administración de Justicia. Será necesario optimizar sus prestaciones aumentando su margen de tolerancia a fallos así como su capacidad para dar respuesta al volumen de información que generará el Plan de Transparencia y los planes estadísticos de la Administración de Justicia. Y así mismo deberá convenirse con las CCAA las conexiones que sea preciso establecer para dar acceso a todos los datos estadísticos del sistema judicial español. La oferta de servicios que se viene prestando a través del Punto Neutro Judicial es variada y se extiende a la comunicación de los órganos jurisdiccionales en relación con la tramitación de los procedimientos judiciales, y ello en relación con la Agencia Tributaria, el Instituto Nacional de Estadística, la Tesorería

[92] Herramienta desarrollada por el CGPJ a través de la Comisión de Informática Judicial, que es uno de los instrumentos más útiles para los secretarios de los juzgados. Es una página Web que unifica las comunicaciones y peticiones de datos entre redes judiciales de las distintas CCAA, el Ministerio de Justicia y el CGPJ.

General de la Seguridad Social, el Instituto Social de la Marina o la Cuenta de Depósitos y Consignaciones.

Por fin, no olvida el Plan de Transparencia que la cooperación judicial internacional constituye en la actualidad un instrumento indispensable para la eficacia de la Justicia.

La existencia de información fiable y detallada acerca de la Administración de Justicia facilitará la respuesta a las demandas solicitadas para las evaluaciones internacionales que puedan realizar las instituciones de la UE, el Consejo de Europa u otras organizaciones internacionales; la progresiva eliminación de fronteras en el seno de la UE, la creación de un Espacio Judicial Europeo y la consolidación de una delincuencia organizada de carácter transnacional convierten al auxilio entre autoridades en herramienta indispensable para la lucha contra la delincuencia y para la protección de los derechos de los más necesitados. Para la correcta ejecución de estas solicitudes de auxilio judicial, y para poder informar correctamente al país solicitante del estado de ejecución de tal solicitud es preciso que los datos que suministren las aplicaciones de gestión procesal de las oficinas judiciales españolas respondan a la realidad.

Una correcta gestión de los datos suministrados por la Estadística Judicial permitirá a España contribuir de forma más eficaz cuando deba tomar parte en reuniones internacionales de coordinación en materias jurídicas específicas.

El Plan de Transparencia Judicial contendrá, por último, todos los datos de carácter general y relativo a cada órgano judicial cuya recogida y publicación se considera útil para cumplir con las finalidades y objetivos del Plan.

17.-BIBLIOGRAFÍA

- "FACTBOOK. COMERCIO ELECTRÓNICO". Davara&Davara Asesores Jurídicos.
- "MANUAL DE DERECHO INFORMÁTICO".2008. Miguel A. Davara Rodríguez.
- LA NUEVA REGULACIÓN DE LA OFICINA JUDIAL. Lourdes Menéndez González-Palenzuela.
- CLAVES PARA LA GESTIÓN DE LA NUEVA OFICINA JUDICIAL. José Manuel Balerdi Múgica. Rosa Bendala García. Manuela Carmena Castrillo.
- "LAS CUENTAS DE LA JUSTICIA Y EL ESTADO DE LAS AUTONOMÍAS". 2004. Rosa Bendala García.
- "REFORMA JUDICIAL Y ECONÓMICA DEL MERCADO".2001. Cabrillo Rodríguez, F. y Pastor Prieto, S.
- "GESTIÓN DE LA OFICINA JUDICIAL CON EFICACIA Y EFICIENCIA". 1999. CGPJ.
- "EL LIBRO BLANCO DE LA JUSTICIA".1997. CGPJ.

- "CALIDAD EN LA GESTIÓN DE LA OFICINA JUDICIAL". 2004. Rosa Gómez Álvarez.
- "LA PASIÓN DE MEJORAR".1996. Eugenio Ibarzabal.
- "LA GESTIÓN DEL PROCESO". 2001. Martín-Borregón y García de la Chica.
- "PROPUESTA SOBRE NUEVO DISEÑO DE LA OFICINA JUDICIAL".2004. Ministerio de Justicia.
- "LAS TIC EN LA JUSTICIA DEL FUTURO". 2009. Fundación Telefónica.
- "TEMARIO FACILITADO POR MAC-TIC". Davara&Davara Asesores Jurídicos.

18.-RELACIÓN DE NORMATIVA UTILIZADA.

- **Administración Electrónica**:
  - Orden JUS/485/2010 de 25 de febrero por la que se crea la Sede Electrónica del Ministerio de Justicia.
  - Ley 11/2007, de 22 de Junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
  - RD 1671/2009, de 6 de Noviembre, por el que se desarrolla parcialmente la Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos.
  - RD 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
  - RD 4/2010 de 8 de enero por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica
  - RD 951/2005 de 29 de Julio, por el que se establece el marco general para la mejora de la calidad en la Administración General del Estado.
  - Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
  - Orden JUS 3000/2009 de 29 de Octubre por la que se crea y regula el Registro Electrónico del Ministerio de Justicia.
  - Ley 59/2003 de 19 de Diciembre de Firma Electrónica.

- **Firma Electrónica:**
  - Ley 59/2003 de 19 de Diciembre de Firma Electrónica.
  - Ley 11/2007, de 22 de Junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
  - RD84/2007, de 26 de enero sobre implantación en la Administración de Justicia del sistema informático de telecomunicaciones Lexnet.
  - Ley Orgánica 6/1985 de 1 de Julio del Poder Judicial.

- **Protección de Datos de Carácter Personal**:
  - Constitución española 1978.
  - LO 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

- LOPD. Ley Orgánica 15/1999, de 13 de Diciembre de Protección de Datos de Carácter Personal
- RD 1720/2007 de 21 de diciembre por el que se aprueba el Reglamento de Desarrollo de la LOPD.
- Ley Orgánica 6/1985 de 1 de Julio del Poder Judicial.
- Orden JUS/1294/2003 de 30 de Abril por la que se regulan los ficheros automatizados con datos de carácter personal gestionados por el Ministerio de Justicia y sus Organismos Públicos
- Orden JUS 4166/2004 de 30 de Noviembre
- Orden JUS 283/2006 de 1 de Febrero.
- Orden JUS 837/2007 de 29 de Marzo
- Orden JUS 2474/2007 de 27 de Julio
- Orden JUS 2714/2009, de 25 de Septiembre
- RD 84/2007, de 26 de Enero, sobre implantación en la Administración de Justicia del sistema informático de telecomunicaciones Lexnet
- RD 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
- RD 1553/2005 por el que se regula la expedición del DNI electrónico y sus certificados
- Instrucción 1/2006 de la Agencia de Protección de datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras de firma electrónica,
- LO 4/1997 de 4 de agosto por la que se regula la utilización de las videocámaras por las Fuerzas y Cuerpos de Seguridad en Lugares Públicos.

- **Comercio Electrónico**:
  - RD 84/2007, de 26 de Enero, implanta en la Administración de Justicia el sistema informático de telecomunicaciones Lexnet.
  - Preámbulo de la Carta de los Derechos de los Ciudadanos ante la Justicia
  - Ley Orgánica 6/1985 de 1 de Julio del Poder Judicial.
  - Instrucción 2/2003 del Pleno del Consejo General del Poder Judicial por la que se aprueba el Código de conducta para usuarios de equipos y sistemas informáticos al servicio de la Administración de Justicia.
  - Ley de Enjuiciamiento Civil

- Ley 34/2002 de 11 de Julio de Servicios de la Sociedad de la información y de comercio electrónico.

- **Pago electrónico**:
  - Resolución de 10 de enero de 2008 de la Subsecretaria del Ministerio de Justicia por la que se establece la aplicación del procedimiento para el pago por vía telemática de las tasas administrativas del Ministerio de Justicia
  - Código Civil

- **Factura electrónica**:
  - Ley 56/2007 de 28 de Diciembre de Medidas de Impulso de la Sociedad de la Información.
  - Orden EHA 962/2007 de 10 de abril por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas contenidas en el RD 1496/2003
  - RD 1496/2003 de 28 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación y se modifica el Reglamento del IVA

- **Nombres de Dominio**:
  - RD84/2007 que implanta en la Administración de Justicia el sistema informático de telecomunicaciones Lexnet.
  - RD 1671/2009, de 6 de Noviembre, por el que se desarrolla parcialmente la Ley 11/2007 de acceso electrónico de los ciudadanos a los Servicios Públicos.
  - **Política Uniforme de Solución de Controversias** en materia de nombres de dominio 26 de agosto de 1999

- **Contratación Informática**:
  - Ley 30/2007 de 30 de octubre de Contratos del Sector Público
  - Reglamento General de la Ley de Contratos de las Administraciones Públicas aprobado por RD 1098/2001 de 12 de Octubre.
  - Plan de medidas, recomendaciones y buenas prácticas en la adquisición y uso de programas de ordenador por las Administraciones Públicas de la Comisión

Interministerial de Adquisición de Bienes y Servicios Informáticos del 12 de abril del 2000

- Directiva 2004/18/CE del Parlamento Europeo y del Consejo sobre coordinación de los procedimientos de adjudicación de los contratos públicos de obras, suministro y servicios.
- Orden JUS 764/2005 de 17 de marzo por la que se crea La Comisión Ministerial de Informática y Comunicaciones del Ministerio de Justicia
- Código Civil
- Código de Comercio

- **Propiedad intelectual**:
  - Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual (LPI).
  - Código Penal de 1995
  - Ley 11/1986 de 20 de marzo de Patentes.
  - Ley 5/1998, de 6 de marzo de Incorporación al Derecho Español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo sobre la Protección Jurídica de las Bases de Datos